שימוש בלוחמה קיברנטית למבצעי תודעה

דניאל כהן ואופיר בראל

אוקטובר 2017

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

TEL AVIV UNIVERSITY
אוניברסיטת תל אביב

Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

תוכן העניינים

הקדמה

בתחום הסייבר ישנו קושי ליצור שיתופי פעולה גם בתחומים בהם האינטרס המשותף ברור. על אחת כמה וכמה קשה לשתף פעולה בלחימה בטרור אידיאולוגי, במיוחד כשהוא מתבצע באמצעות מתקפות סייבר. הדבר מוביל לאי ודאות שממילא קיימת במידה מסוימת במתקפות סייבר.

בבחירות האחרונות ב־2016 בארה"ב, ומיד אחר כך בצרפת, נפתח עידן חדש בתחום לוחמת הסייבר. ראשי סוכנויות המודיעין העיקריות של ארה"ב חתמו יחד על מסמך גלוי שבו הם מודיעים לציבור כי יש להם ביטחון מלא בקביעה שגורמים ברוסיה התערבו בבחירות האחרונות. להערכתם, סביר מאוד שגורמים אלה הופעלו על ידי השלטון הרוסי. טכניקת ההתערבות הייתה פשוטה: תחילתה בפריצה למחשבי מטה המפלגה הדמוקרטית (ולמחשבה האישי של הילארי קלינטון) וסופה בפרסום אלפי מסמכים מתוך מאגרים אלה. חלק מהמסמכים רמזו על בעיות של קלינטון, במיוחד בכל הנוגע לבריאותה, ולחשדות הקשורים לשחיתות. כיום ברור כי המסמכים המפלילים, רובם ככולם, היו מזויפים. אולם בלהט הבחירות הם נפלו על קרקע פורייה והשפיעו על הבוחרים.

להיסטוריה של שתילת מידע מפוברק יש ברוסיה זקן ארוך. כך, למשל, מי שחיבר את "הפרוטוקולים של זקני ציון" (לפני יותר ממאה שנה) היתה ה"אוכרנה" – שירותי המודיעין של רוסיה לפני המהפכה – ששמם שונה מספר פעמים, כולל קג"ב מאוחר יותר, וכיום ה־פס"ב. ה"דיס־אינפורמציה" שימשה מאז ומתמיד תפקיד מפתח בדוקטרינה הרוסית, והסייבר רק נתן לה מכשיר נוח יותר לביצועה.

סדנת יובל נאמן למדע, טכנולוגיה וביטחון שמה לה למטרה לחקור את נושא הסייבר על כל היבטיו, כולל השפעת הנושא על ביטחון הפרט והחברה. מאמר זה בוחן את השפעת הסייבר במימד התודעתי ומביא לידי ביטוי את העולם החדש בו אנו חיים. עולה ממנו המסקנה כי ישראל צריכה להיערך לא רק לאיומי הסייבר המקובלים אלא גם להתערבות סייבר לא שגרתית שמטרתה להשפיע על תודעת האזרחים, כמו האפשרות להעצים את המחלוקות הקיימות בחברה הישראלית, לערער את אמון הציבור בשלטון ועוד.

פרופ' יצחק בן ישראל
ראש סדנת יובל נאמן למדע, טכנולוגיה וביטחון
ראש המרכז הרב־תחומי לחקר הסייבר ע"ש בלוונטניק

מבוא

המניפולציה במידע לצרכים פוליטיים או מדיניים קיימת לאורך ההיסטוריה האנושית. עם זאת, השיפורים הטכנולוגיים הקיימים מאז המצאת האינטרנט והשימוש של שחקנים מדינתיים ולא מדינתיים בלוחמת סייבר מעניקים יכולות חדשות ומאפשרים הוספת מרכיבים שלא היו קיימים בעבר. כיום, שחקנים מדינתיים ולא מדינתיים משתמשים במרחב הסייבר בכלל וברשתות החברתיות בפרט ככלי ליצירת שינויים חברתיים ופוליטיים ולעיצוב תודעה.[1] השוואה בין המדינות הפעילות במרחב התודעתי מצביעה על מיצוי שונה של כוח ועל שימוש בשיטות מגוונות ובכלי פעולה שונים. אלה כוללים, בין השאר, הפעלת מודיעין, לוחמה פסיכולוגית, דיפלומטיה ציבורית, ערוצים מדיניים ומשפטיים וכן שימוש בלוחמת סייבר.[2] בנקודת הזמן הנוכחית, בה לפעילות במרחב הסייבר ובפלטפורמות של רשתות חברתיות אין גבולות ברורים או הגבלים בידי מדינות, השימוש בטכנולוגיה בזירת התודעה ברשת בשילוב עם עולם המציאות, מהווה נשק עוצמתי כחלק מלוחמת מידע. השימוש בנשק זה ייקרא להלן "לוחמת תודעה קיברנטית".

ממד התודעה הוא האופן שבו נתפסת המציאות הסובייקטיבית (על פי השקפת עולם) בקרב קהלים שונים הבוחנים את המידע בנוגע לאירועים פיזיים. תפיסת המציאות מושפעת מהגורמים המדווחים ומזיקות בלתי נשלטות שקיימות בין קהלי יעד שונים.[3] בהמשך לכך, ההגדרה המוצעת ל"לוחמת תודעה קיברנטית" במאמר זה היא "פעולות בין שני שחקנים או יותר, בהן אחד הצדדים משבש את סביבת המידע הממוחשבת והאלקטרו־מגנטית שעליה מסתמך הצד היריב, ושמורכבת הן ממקורות אנושיים והן ממקורות טכנולוגיים. בפעולה זו, משבש הצד התוקף את יכולתו של הצד היריב לתווך

1 פעילות רציפה במרחב התודעתי מאפשרת צמצום ו/או שיבוש לגיטימיות הפעולה של היריב ויכולה אף להביא לסיכול ולשיבוש יוזמותיו ההתקפיות.

2 מחקר של אוניברסיטת אוקספורד מצא ש־28 מדינות פועלות במרחב התודעתי ברשתות החברתיות, תוך כדי השקעת סך של מאות מיליוני דולרים והפעלת מערכים הכוללים אלפי עובדים. ראו: Samantha Bradshaw and Philip Howard, Troops, "Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation," (working paper no. 2017.12, University of Oxford, 2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

3 שי שבתאי וליאור רשף, "מאמץ התודעה בצה"ל," **מערכות** 457 (אוקטובר 2014): 34–39.

לקהל היעד שלו תוכן אובייקטיבי, לתפוס את המציאות כהלכה ולגבש יכולת פעולה הגנתית אפקטיבית". בדרך זו, הצד התוקף יוצר לעצמו יתרון במערכה הכוללת ומנטרל אפשרות של תגובה קינטית של הצד הנתקף.

הצורך בהמשגת סוג כזה של פעילות בנפרד מפעילויות "מסורתיות" יותר (למשל לוחמה פסיכולוגית) טמון בכך שמאפיינים מרכזיים של פעילות במרחב הסייבר כוללים פגיעה במטרות בצורה אנונימית (ללא זיהוי היריב כעומד מאחורי המתקפה) ולעיתים אף אוטונומית (פיזור מידע באמצעות רשת בוטנטים, תקיפות מניעת שירות וכו'). כמו כן, מבצעי תודעה המתקיימים ברשת מאפשרים את ביזור המידע, והיכולת להפיץ אותו ברשת לקהל יעד ממוקד או רחב גבוהה מאוד. רשת האינטרנט שינתה את המודל המסורתי של ייצור המידע באמצעות תקשורת ובידי גורמי ממשלה לטובת השטחת הידע וביזורו בידי יחידים וקבוצות קטנות, שלעיתים אף פועלות ללא מודל היררכי ברור ולרוב גם ללא רגולציה, חוקים או אכיפה.

כאמור, מניפולציה במידע לצרכים פוליטיים או מדיניים איננה תופעה חדשה. עם זאת, השיפורים הטכנולוגיים הקיימים היום מאפשרים לשכלל את לוחמת המידע ולהוסיף לה אלמנטים שלא היו קיימים בה בעבר. לוחמת המידע הסובייטית, לדוגמה, נועדה לשבש את פעילות האויב באמצעות זריעת דיס־אינפורמציה במידע שהוא קיבל. לוחמת המידע הרוסית עושה היום שימוש באינטרנט על מנת להזין את יריביה במידע מוטעה. בד בבד, השיפורים הטכנולוגיים מוסיפים ללוחמת המידע הרוסית שני אלמנטים שלא היו קיימים בעבר. האלמנט הראשון הוא תיאום טוב יותר בין היחידות השונות העוסקות בלוחמת המידע, בהשוואה לעידן ברית המועצות. האלמנט השני הוא אפשרותה של הממשלה הרוסית לחבל בתשתיות המידע של יריביה על מנת לפגוע בתפקודן של תשתיות חיוניות במדינות היעד.[4]

ברחבי העולם קיימים גופים מסוגים שונים – צבאיים, ממשלתיים ופרטיים – העוסקים בתכנון וביישום של לחימה בזירה התודעתית. מאמר זה מבקש לטעון כי ניהול מערכה תודעתית אפקטיבית כמענה לאיומים ידרוש שיתוף פעולה גם עם יחידות מדיה חברתית ויחידות סייבר, שישמשו כמכפיל כוח למבצעי תודעה מדיניים וצבאיים ברמה הטקטית וברמה האסטרטגית. כיום, במערכות הביטחוניות והמדיניות במדינות המערב לא קיימת יכולת שילוביות מלאה של לוחמת סייבר בניהול מבצעים ברמות האסטרטגיות.

4 Maria Snegovaya, *Russia Report I: Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington: Institute for the Study of War, 2015), 10, 14.

כלומר, בניית יכולת השפעה על עיצוב התודעה, בכל המעגלים הנוגעים לקונפליקט מדינתי תדרוש הטמעת מרכיבים מתחום לוחמת הסייבר לביצוע מהלכים מערכתיים תודעתיים.

מאמר זה יסקור את הקמת גופי לוחמת התודעה בכמה מדינות מרכזיות ברחבי העולם, וכן ינתח שני מקרי בוחן בהם נעשה שימוש במערכה משולבת של לוחמת מידע, מבצעי השפעה ולוחמת סייבר. מקרה הבוחן הראשון הוא המערכה שניהלה ארצות הברית ברשת נגד ארגון "המדינה האסלאמית" עם שימוש מועט יחסית בלוחמת סייבר כחלק ממערכה תודעתית. מקרה בוחן נוסף כולל את המערכה המלחמתית של רוסיה נגד אוקראינה, בה נעשה שימוש נרחב יחסית בלוחמת סייבר ובלוחמת תודעה, וכן מערכה "רכה" של רוסיה נגד ארצות הברית. מטרת הצגת מקרי הבוחן היא להמחיש את הבדלי התפיסה בניהול מערכה כשהממסד הביטחוני נוקט בגישה בה דינמיקה צבאית טקטית־אופרטיבית בשטח ודינמיקה מדינית־דיפלומטית בפורומים בינלאומיים שונים הן חלקים אינטגרליים מן הרעיון המערכתי ושלובות בו. כנגזרת מתפיסה זו, לוחמת סייבר ומבצעים תודעתיים הם מאמצים משולבים. מקרה נוסף בו ארצות הברית ניהלה מערכה תודעתית ברשת כנגד ארגון המדינה האסלאמית מציג גישה לפיה מבצעי הסייבר ומבצעי התודעה מנוהלים כשתי מערכות נפרדות נגד אותו יריב. נוסף על כך, קיימת א־סימטריה בסיסית המאפיינת את כללי המשחק בניהול מערכה על התודעה, מעצם טיבן של דמוקרטיות ליברליות המחויבות לכללים של אחריות מדינתית ומתאפיינות בהיעדר הסכמה פנימית המונע גיבוש מסר אחיד ובסרבול ביורוקרטי ופוליטי. לעומת זאת, ישנם גורמים הרואים בכללים שקבעו הדמוקרטיות סדר עולמי קיים שיש לשבשו ולשנותו. אלה אינם מהססים לבצע מניפולציות תקשורתיות, ואחדותם היחסית מאפשרת הן הצגת מסר אחיד והן התאמה מהירה של הפעילות במערכה על התודעה לשם שינויים במציאות ובכלים.[5]

5 יוסי קופרווסר, "שדה הקרב על התודעה," **עדכן אסטרטגי**, כרך 12, גיליון 2 (אוגוסט 2009): 37–44.

ארגז הכלים לעיצוב תודעתי במרחב הקיברנטי

במרחב הקיברנטי, הפכו בשנים האחרונות האינטרנט בכלל והרשתות החברתיות בפרט לגורם המשפיע ביותר על התנהגות החברה האנושית. החיים ברשת ומחוצה לה נהיו חלק ממארג אחד והמודל ההיררכי "המסורתי" של ייצור מידע התחלף במודל מבוזר בו המידע חוצה במהירות גבולות פיסיים ומדינתיים, ללא חוקים המגבילים את זרימתו. מרחב הסייבר צמצם מאוד את הממדים הגיאופיזיים של סביבת חייו של האדם. כלומר, שינויים טכנולוגיים ותודעתיים הביאו להאצת מהירות התנועה והחישה האנושית במרחב באמצעות רשתות המחשבים של ימינו. בעת גלישה באינטרנט, התגובה העצבית המגיעה מגופו של הגולש והמידע המגיע מהרשת, מתקבלים בתודעתו באותו הזמן.[6] האינטרנט מאפשר למשתמש בו להיות בו־זמנית "בכל מקום ובשום מקום".[7] החיבור בין האינטרנט לטלפון החכם הפך את האדם לזמין כמעט בכל רגע לכל מידע ותקשורת, ללא קשר למרחב הפיזי שבו הוא נמצא. עיקרון זה מומחש היטב כשמסתכלים על חדירת האינטרנט לאפריקה, בהשוואה למקומות אחרים בעולם, ועל השפעותיו על האוכלוסייה המקומית. נכון להיום, שיעורם של תושבי אפריקה בקרב כלל משתמשי האינטרנט בעולם עומד על כ־9%, כששיעור החדירה לאוכלוסייה המקומית הוא הנמוך ביותר מבין כלל היבשות בעולם (28%). אף על פי כן, שיעור התפשטות האינטרנט באפריקה, החל משנת 2000, הוא הגבוה ביותר ביחס לכל יבשת אחרת באותה תקופה (שיעור של כ־7700% אחוזים לעומת ממוצע כלל עולמי של כ־940%).[8] על סמך מגמה זו, התחזית לשנת 2020 היא ששיעור השימוש באינטרנט באפריקה יזנק משמעותית ויגיע ל־60%.[9]

---

6 אבי רוזן, **דחיסת מרחב וזמן באמנות הסייברספייס** (תל אביב: אוניברסיטת תל אביב, 2009), 16.

7 Roy Ascott, "From Appearance to Apparition: Communications and Consciousness in the Cybersphere," *Leonardo Electronic Almanac* 1, no. 2 (1993): 3-9.

8 "World Internet Usage and Population Statistics", Internet World Stats, accessed October 1, 2017 http://www.internetworldstats.com/stats.htm

9 Mani James, "Business Impact in Africa: Mega Trends Driving Mega Opportunities in Sub Sahara Africa", *Team Finland Future Watch*, September 11, 2014, https://www.slideshare.net/futurewatch/mega-trends-driving-mega-opportunities-in-sub-saharan-africa, slide no. 19.

בד בבד, השימוש באינטרנט הסלולרי בקרב תושבי אפריקה נתפס כגורם משמעותי בשיפור איכות חייהם, יותר מאשר במדינות מסוימות במערב. תרומה זו היא רב־תחומית ונוגעת לתחומי החינוך, התעסוקה והבריאות.[10]

במגמתה הנוכחית, ארכיטקטורת הרשת מאפשרת יצירה ומסירה של מידע במודל עם מאפייני "פרסונליזציה". כלומר, המידע מונגש למשתמש יחיד או לקבוצה באמצעות "התערבות" (engagement) על פי פילוח של התנהגות, גיאוגרפיה, תחומי עניין, צרכים, רצונות ותשוקות. במציאות כזו, בה מוסרות המחיצות בין העולם הפיזי לעולם הקיברנטי, השילוב בין רגשות לתכנים ברשת עלול להשפיע על התודעה וליצור אצל קהלי יעד פחד, אי ודאות והטלת ספק. בהקשר זה ניתן לציין מושג הלקוח מהעולם העסקי: Fear, Uncertainty, Doubt (FUD). מדובר בטכניקת שיווק שנהוגה בידי חברות שונות ומטרתה לגרום ללקוחות להימנע מרכישת מוצרים של חברות מתחרות. חברה המשתמשת בטכניקת FUD מפרסמת מידע בנוגע למוצרי החברות המתחרות, שאמור לעורר אצל הלקוחות תחושות של ספק, אי ודאות ופחד ביחס למוצרים.[11] בכך היא מונעת מהם מלרכוש אותם. ניתן לזהות שימוש ב־FUD לא רק בעולם העסקי, אלא גם בעיצוב תודעתי לצרכים פוליטיים. במחלוקת פוליטית בין שתי מדינות או יותר, מטרתו של השימוש ב־FUD היא לערער על הלגיטימציה של הצד השני ועל אמינות טענותיו באמצעות יצירת רגשות שליליים כלפיו בקרב דעת הקהל.

הבסיס להשפעה של גורם אחד על גורם אחר הוא תקשורת מסוג כלשהו. במסגרתה תקשורת זו, כאשר צד אחד מעביר מידע מסוים לצד האחר, הצד שמקבל את המידע בוחר על פיו כיצד לפעול. לעיתים הצד שמעביר את המסרים ירצה להשפיע פעולותיו של הצד השני. הוא ירצה לגרום לו לבצע פעולות מסוימת הרצויות לו, או למנוע ממנו לבצע פעולות שאינן רצויות לו. מאחר שלמידע המתקבל יש השפעה על פעולות, לעיתים ירצה אחד הצדדים להשפיע על פעולותיו של הצד השני באמצעות בחינת המידע המועבר לו.

תקשורת אסטרטגית (Strategic Communication) היא תהליך המורכב מכמה שלבים. הראשון שבהם הוא המחקר המקדים. המחקר המקדים מאפשר ליוזם התהליך להגדיר את נושא התקשורת, לאפיין את קהל היעד של המסרים

10 "Impact of the Mobile Internet in Africa vs. UK", On Device Research. Updated October 22, 2014, https://www.slideshare.net/OnDevice/impact-of-the-mobile-internet-in-african-lives/2-Mobile.

11 ראו למשל: Fear, Uncertainty and Doubt", Changing Minds.org, accessed October 1, 2017, http://changingminds.org/disciplines/sales/articles/fud.htm.

ולקבוע יעדים שעל המהלך להשיג. על סמך ממצאי השלב המקדים מנוסחים המסרים שיש להעביר ונקבעות הדרכים להעברתם.[12] לאחר מכן מתקיים שלב של משוב, הכולל בחינה של תגובת קהל היעד למסרים. מכך מתקבל משוב על איכותה של התקשורת האסטרטגית.[13]

מושגים אשר דומים במהותם לתקשורת האסטרטגית הם "מאמץ השפעתי" ו"ניהול תפיסה".

מאמץ השפעתי (Influence Operation) הוא שם כולל לכל פעולה שנועדה להניע קהל יעד מסוים – יחיד, קבוצה בעלת השפעה או קהל רחב – לקבל גישות ולאמץ החלטות התואמות את האינטרסים של יוזמי הפעולה. מה שעומד בבסיס המאמץ ההשפעתי הוא פעולות, אשר משפיעות על התפיסות הקוגניטיביות והפסיכולוגיות של קהל היעד. הפעולות הללו יכולות לבוא לידי ביטוי באמצעים שונים: צבאיים, כלכליים, מדיניים ועוד.[14]

המאמץ ההשפעתי שם דגש מיוחד על ההיבט התכנוני. על מנת להוציא לפועל מאמץ השפעתי מוצלח, תהליך התכנון שלו צריך לתת מענה הולם לתשעה סוגים שונים של מאפייני פעולה: עיצוב מטרות (מהן המטרות של יוזם הפעולה? האם ניתן להשיגן? אם לא ניתן להשיגן במלואן, מהן התוצאות האפשריות שייחשבו להצלחה?), יצירת קהל היעד (מהו קהל היעד שאליו יש לכוון את הפעולה בכדי שתהיה יעילה?), התוויית הדרך (מהן האסטרטגיות בעלות ההשפעה הרבה ביותר על קהל היעד, שיוכלו להבטיח את התוצאה הרצויה?), יחסי היררכיה/שלטון בקהל היעד (מהי מידת ההשפעה של מנהיגי הקבוצה על חבריה?), מקורות המידע (מהם מקורות המידע מהם ניזון קהל היעד? אילו מקורות מידע נתפסים בעיניו כאמינים?) הבנת הגישות המחשבתיות של הצד השני (כיצד בנויות הגישות המרכיבות את תפיסת היריב ועד כמה הן חזקות ויציבות?), מאפייני המידע המצוי (אילו מסרים מקבל קהל היעד כבר היום ביחס לנושא המדובר?), קידום שינוי (אילו סוגי מסרים או מקורות

12 Carl Botan, "Ethics in Strategic Communication Campaigns: The Case for a New Approach to Public Relations," *The Journal of Business Communication* 34, no.2 (1997): 188.

13 Carsten Bockstette, *Jihadist Terrorist Use of Strategic Communication Management Techniques* (Garmisch-Partenkirchen: The Marshall European Studies for Security Studies, Center Occasional Paper Series, no. 20, 2008), 9.

14 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (California: RAND Cooperation, 2009), 2-4.

מידע יש לנצל בכדי לקדם את השינוי הרצוי?) וכמות המידע הנשלח (מהי כמות המידע שיש לשלוח אל היריב בכדי להשיג שינוי? אילו פעולות נוספות יש לבצע בכדי להשיג את המטרה הרצויה?).[15]

ניהול תפיסה (Perception Management) מתאר גם כן מסגרת המשמשת להעברת מידע מסוים לקהל יעד מובחן לשם שליטה בתגובותיו. הייחוד של ניהול התפיסה הוא שמקובל לראות בו דרך פעולה המכוונת יותר לזירה הפוליטית הבינלאומית ומיועדת למימוש בזמני שלום.[16] כך למשל, פעולות של ניהול תפיסה ניתנות ליישום באזורים המשתקמים ממלחמה שהתחוללה בהם. הן יכולות לייצר לגיטימציה לשלטון חדש הנמצא באזור או לסייע בשיקום התשתיות שנהרסו במהלך המלחמה.[17]

המידע, כאמור, עומד בליבו של תהליך ניהול התקשורת מול הצד שכנגד. כיוון שכך, חלק מרכזי ביישומו מכונה **לוחמת מידע** (Information Warfare) או **מבצעי מידע** (Information Operations). שני המושגים הללו מבטאים את כלל הדרכים שבהן נוקט הצד היוזם בכדי להשפיע סוג המידע שהצד השני נחשף לו ועל כמותו. כאשר הצד היוזם משבש את סביבת המידע שעליה מסתמך הצד היריב – המורכבת הן ממקורות אנושיים והן ממקורות טכנולוגיים – הוא משבש את יכולתו לתפוס את המציאות כהלכה ולגבש מולה צעדי פעולה אפקטיביים. בדרך זו, הצד היוזם יוצר לעצמו יתרון במערכה הכוללת והוא מסוגל להשתמש בלוחמת מידע בכדי להשיג הישגים משמעותיים או אף להכריע את המערכה. על מנת להימנע מתגובה דומה מצד היריב, כוללת לוחמת המידע גם היבט הגנתי – הצד שיוזם את מבצעי המידע מפעיל יכולות הגנתיות על מאגרי המידע שלו. [18] על פי רוב, מבצעי המידע מזוהים עם יכולות טכנולוגיות מעולם המחשבים, אך למעשה כל

15 Ibid., XV-XVI.

16 Khyber Zaman, *Perception Management: IO Capability* (California: Naval Postgraduate school, 2007), 18.

17 MAJ Noelle J Briand, *How to Win Friend and Influence People-Planning Perception Management at the Division and Corps Level,* (Kansas: school of advanced military studies, 2004), 19.

18 Blaise Cronin and Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts," *The Information Society* 15, no.4 (1999): 258.

פעולה שיש בה אלמנטים של תחבולה והונאה (כגון מסירת הצהרות כוזבות לתקשורת) תיחשב כצעד של לוחמת מידע.[19]

מידע מדויק ואיכותי הוא מרכיב חשוב בעיצוב דרך הפעולה של כל אדם או ארגון. עם זאת, זהו לא המרכיב היחיד: הנמען יבחר איך לפעול (או לא לפעול) לא רק על סמך העובדות שניצבות לפניו, אלא גם על סמך הדרך שבה הוא מפרש אותן. באופן ייחודי, הדרך שבה מקבל המידע מגיב לו מבחינה רגשית היא בעלת משקל רב בעיצוב תגובתו הסופית. לכן, מי שמשתמש במסגרת של תקשורת אסטרטגית עושה זאת גם על מנת לעורר בצד השני תגובות רגשיות ספציפיות, שיובילו לתגובות הרצויות לו. **לוחמה פסיכולוגית** (Psychological Warfare) היא שם כולל לניהול ההיבט הרגשי של התקשורת האסטרטגית. כאשר מידע ספציפי בעל מרכיבים פסיכולוגיים מועבר לקהל יעד מוגדר, משתנים רגשותיו של קהל היעד ותפיסת עולמו.[20] בעקבות זאת משתנות דרכי ההתנהגות של קהל היעד וכתוצאה מכך נפגעת יכולתו להשיג את המטרות שהציב לעצמו.[21] המסרים בהם נעשה שימוש במסגרת לוחמה פסיכולוגית יכולים להיות הבטחות, איומים, הגדרת תנאים לסיום הלחימה או לכניעה, עידוד עריקה וכן הלאה.[22]

לכל סוג מידע יש פוטנציאל לעורר תגובה רגשית כלשהי אצל מי שנחשף לו, בייחוד אם מדובר במידע המגיע מזירות מלחמה. אף על פי כן, לא כל פרסום של מידע כזה נחשב ללוחמה פסיכולוגית. פעולה יכולה להיחשב לפעולה של לוחמה פסיכולוגית רק אם היא נעשית בכוונה תחילה, בכדי להשפיע על הצד השני מבחינה פסיכולוגית. פעולות של לוחמה פסיכולוגית מכונות **מבצעים פסיכולוגיים** (Psychological Operations). פעולות כאלו ניתנות ליישום בזמני מלחמה ושלום כאחד, וניתן להבחין בין סוגים אחדים שלהן. כל סוג מופעל בעיתוי אחר, מכוון כלפי קהל יעד מובחן ומיועד

19 Robin Brown, "Information Operations, Public Diplomacy & Spin: The United States & the Politics of Perception Management," *Journal of Information Warfare* 1, no.3 (2002): 41.

20 Clay Wilson, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (Washington: Congressional Research Service, 2007), 3.

21 Alfred Vasilescu, "Evolution of Pathological Communication's Military Domains, from Propaganda to Information Operations," *Scientific Research and Education in the Air Force* Volume 2011, 282.

22 "OPNAV Instruction 3434.1: Psychological Operations," (Washington Naval Yard: Department of the Navy, Office of the Chief of Naval Operations, 1997), 1–2, http://www.iwar.org.uk/psyops/resources/us/3434_1.pdf

לעורר רגשות מסוימים בקרב קהל היעד. כך למשל, **לוחמה פסיכולוגית טקטית** (Tactical Psychological Operations), המופעלת מול לוחמי הצד היריב, שונה מ**לוחמה פסיכולוגית מייצבת** (Consolidation Psychological Operations), שמכוונת כלפי האזרחים של הצד היריב.[23]

דוגמה לפעולה בעלת השפעה פסיכולוגית היא **תקיפת רשתות מחשבים לצורכי השפעה** (Computer Network Influence). בניגוד לתקיפות רשתות מחשבים רגילות, התקיפות המיוחדות לצורכי השפעה מיועדות לייצר תחושה של פגיעה מהותית מבלי להוציא לפועל פגיעה שכזו. תקיפות לצורכי השפעה נועדו לטעת תחושות של חוסר ביטחון, חוסר שליטה, פגיעה בריבונות וחוסר יכולת להגן על אורח החיים הנורמטיבי. תקיפות כאלו ישיגו את האפקט הזה באמצעות שימוש בטקטיקות כגון פגיעה באתרים של גופי ממשל, שליחת הודעות פוגעות לאזרחים, השבתת אתרי תקשורת לפרקי זמן מוגבלים ועוד.[24]

תקיפות קיברנטיות משמשות לא רק לנטיעת תחושה של חוסר בטחון, אלא גם לניסיון לשבש את סביבת המידע של הצד היריב, באמצעות פגיעה בתשתיות המידע הקיברנטיות שלו. הפעולות הללו הן מאמצי השפעה המבוצעים במרחב הסייבר, כלומר מדובר בתקיפות של מערכות ממוחשבות, שמיועדות להשפיע על הגישות, על ההתנהגויות ועל תהליכי קבלת ההחלטות של אוכלוסיית המטרה באמצעות שליטה במידע המועבר במערכות הללו. תקיפות מסוג זה יכולות להופיע בכמה צורות: התקפות מניעת שירות מבוזרת (Distributed denial of service – השבתת אתר מסוים על ידי הצפתו בכמות מידע עצומה[25]), חשיפת פרטים מסווגים/אישיים על ארגון או על אישיות כלשהם באמצעות פרסום מסמכים חשאיים (Doxing/Doxxing), פריצה למערכות מידע ועוד.[26]

23 Ibid.

24 עופר אסף וגבי סיבוני, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, מזכר 149, תל אביב: המכון למחקרי בטחון לאומי, 2015, 18–19.

25 "Definition-distributed denial-of-service attack (DDoS)," *TechTarget,* accessed October 1, 2017, http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

26 Pascal Brangetto and Matthijs A. Veenedaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations* (Tallinn: NATO Cooperative Cyber Defence Centre for Excellence, 8th International Conference on Cyber Conflict, 2016): 117, 121–122, 124.

גופי פעולה בולטים בזירת התודעה

ברחבי העולם, כבר היום ניתן למצוא גופים מסוגים שונים – צבאיים, ממשלתיים ופרטיים – העוסקים בתכנון וביישום של היבטים שונים של עיצוב תודעה. פרק זה יסקור חלק מן הגופים הללו ויבצע הפרדה בין גופים צבאיים ומדיניים מתוך הבנה שגופים צבאיים מפעילים מאמצי תודעה לקידום פעילות מבצעית בזירות עימות. בישראל למשל, מאמץ התודעה הצבאי בזמני חירום או מלחמה מלווה את המערכה ואת המאמצים שלאחריה, כלומר הוא מכוון לליווי הפעולה הצבאית עד לסיומה בתנאים הרצויים ולשימור ההישגים האסטרטגיים של המערכה.[27] לעומת זאת, משרד החוץ משתמש בזירת התודעה ככלי התומך בניהול מדיניות החוץ של המדינה (ואולי אף תורם לעיצובה).[28] המדינות שנבחרו לפרק זה עומדות בשני קריטריונים המשמשים כהנחות יסוד. הראשון: במדינות אלו מופעל מאמץ נרחב בהיבטי התאמת העוצמה התודעתית והקיברנטית לאתגרים ברמה הטקטית וברמה האסטרטגית. השני: מדינות אלה מפעילות מאמצים ניכרים בתחום לוחמת התודעה לקידום פעילות מבצעית בזירות העימות בהן הן פועלות.

גופים צבאיים

בין הגופים הצבאיים בעולם הפועלים במרחב התודעתי ברשת ניתן למנות את:

נאט"ו

בנאט"ו ישנה הבחנה ברורה בין הדרג האחראי על עיצוב התקשורת האסטרטגית לבין הכוחות האחראים על יישומה בזמן אמת. הגוף שאחראי על הגדרת עקרונות התקשורת האסטרטגית של נאט"ו הוא The NATO Strategic Communications Centre of Excellence. מרכז זה ממוקם בלטביה וחברות בו עשר מדינות, החברות גם בברית נאט"ו. מטרתו של המרכז היא לשפר את תהליך הפיתוח, הלמידה והיישום של התקשורת האסטרטגית בפעילות של מדינות נאט"ו ומוסדותיה. לשם כך הוא מעניק סיוע מקצועי שוטף לגורמים

27 ראו למשל: "אסטרטגיית צה"ל", לשכת הרמטכ"ל, אוגוסט 2015, http://go.ynet.co.il/pic/news/16919.pdf

28 סוג זה מכונה "תקשורת אסטרטגית" או "דיפלומטיה ציבורית".

המעוניינים בכך, כאשר חלק מהפעילות היא תיאורטית וחלקה מנסה לתת מענה לסוגיות עכשוויות הנוגעות למדינות החברות בברית.[29]

יש לציין כי אין לנאט"ו גוף קבוע שייעודו הוא הפעלת לוחמת תודעה. גוף ביצועי ליישום לוחמה פסיכולוגית מורכב אד הוק ונקרא Combined Joint Psychological Operations Task Force (CJPOTF). היקף הכוח והרכבו משתנים בהתאם לאופי המשימה ולכוח האדם המצוי בארגון. עם זאת, המבנה של כל כוחות משימה כאלה הוא קבוע: כל אחד מורכב מכמה מחלקות, הנוגעות להיבטים השונים של יישום הלוחמה הפסיכולוגית: מרכז מחקר, מרכז פיתוח תוצרים, צוותים טקטיים ועוד. בכל כוח משימה שכזה תהיה למדינה מסוימת דומיננטיות בכוח האדם, והיא תיקרא המדינה המובילה (Lead Nation).[30]

ארצות הברית

בארצות הברית פועל ה־Joint Information Operations Warfare Center שהוקם בשנת 1999. המרכז כפוף למפקדת המטות המשולבים ומורכב ממומחים מרחבי צבא ארצות הברית, עובדי ממשל ועובדי חברות פרטיות.

פעילות המרכז מתבצעת בשני מישורים: טקטי ואסטרטגי. במישור האסטרטגי, המרכז משמש כמקור סמכות בנושא לוחמת מידע לכלל הסוכנויות המרכיבות את משרד ההגנה האמריקאי. המרכז אמון על הפצת ידע באמצעות כתבי עת וניירות עמדה, מגבש את דרכי היישום הטובות ביותר להשגת מטרות שונות של מבצעי מידע ומקדם תהליך למידה כלל־משרדי של יישום תוכניות אלו. במישור הטקטי, המרכז שולח צוותים מומחים בלוחמת מידע לכל מקום ברחבי העולם בו נמצאים כוחות משימה של ארצות הברית (joint task forces), בהתאם לדרישת מפקדת המטות המשולבים. הצוותים מספקים לכוחות הלוחמים בשטח ייעוץ בנוגע לדרכים ליישום תוכניות מבצעי המידע.[31]

29 "About Us," NATO Strategic Communications Centre of Excellence (StratCom), accessed October 1, 2017, http://www.stratcomcoe.org/about-us

30 "Allied Joint Doctrine for Psychological Operations," Ministry of Defense (UK), September 14,(3-1)–(3-6), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

31 "Information Operations," *The Information Warfare Site*, accessed October 1, 2017, http://www.iwar.org.uk/iwar/resources/jtf-cno/jioc.htm

לצורך פעילותו עושה המרכז שימוש בניתוחים חברתיים־תרבותיים של האוכלוסייה הנמצאת באזור העימות.[32]

בצבא היבשה של ארצות הברית יש שלוש חטיבות (שתיים סדירות ואחת במילואים), העוסקות בתכנון לוחמה פסיכולוגית וביישומה. כל חטיבה מורכבת מחמישה גדודים האחראים על תכנון, ייצור והפצה של תוצרי לוחמה פסיכולוגית בהתאם למאפייני הלחימה. במרבית המקרים הלוחמה הפסיכולוגית של צבא ארצות הברית מופנית כלפי האוכלוסייה האזרחית באזורי העימות ומיועדת להעביר את תמיכתה של זו מכוחות הגרילה אל הלוחמים של צבא ארצות הברית.[33]

אחד הגופים המרכזיים לעריכת מבצעי השפעה הוא הפיקוד המרכזי של צבא ארצות הברית, הפועל מבסיס חיל האוויר שבפלורידה (CENTCOM). מחלקת הלוחמה הפסיכולוגית ב־CENTCOM מכונה "Web Ops" וכוללת כ־120 איש. הלוחמה הפסיכולוגית מבוססת על שלוש אסטרטגיות מרכזיות: שיבוש מסרי התעמולה של האויב, הפצת מידע על מקרי צביעות ופשע של האויב במגעיו עם אוכלוסיות בסיכון והנעת מתנגדי האויב להילחם בו בצורה יעילה יותר באמצעות המדיה. בפיקוד מועסק גם צוות פעולה מיוחד, הנקרא Digital Engagement Team (DET). בצוות מועסקים 11 איש, השולטים בשפות שונות: ערבית, אורדו, פרסית, רוסית ועוד. אנשי היחידה מפעילים חשבונות טוויטר, פייסבוק ואינסטגרם שפונים לציבור הרחב המצוי בכ־20 מדינות במזרח התיכון ובמרכז אסיה.[34]

רוסיה

בשנים האחרונות אימץ הממסד הצבאי הרוסי גישה לפיה ההפעלה הצבאית הטקטית בשטח והאסטרטגיה המדינית הדיפלומטית בפורומים בינלאומיים שונים הן חלקים אינטגרליים ושלובים של הרעיון המערכתי.[35] כנגזרת מתפיסה זו, לוחמת סייבר ומבצעיים תודעתיים הם מאמצים משולבים, המכוונים לתמרן

32 "Joint Information Operations Proponent," Chairman of the Joint Chiefs of Staff Instruction, February 14, 2014, (A-1)–(A-4), https://archive.org/details/Joint-Information-Operations-Proponent-14-Feb-2014

33 טל טובי, "מלחמת שכנוע," **מערכות** 352 (דצמבר 2013): 44–51.

34 Karen Parrish, "Centcom Counters ISIL Propaganda," *U.S Department of Defense*, July 6, 2016, http://www.defense.gov/News-Article-View/Article/827761/centcom-counters-isil-propaganda

35 דימה אדמסקי, "ההתערבות הרוסית בסוריה: משמעויות אסטרטגיות ולקחים מערכתיים," **עשתונות** 13 (נובמבר 2016): 22, http://maarachot.idf.il/PDF/FILES/5/113925.pdf

את התנהגות הקורבן. אלה כוללים תקיפה של רשתות ממוחשבות, לוחמה פסיכולוגית, הונאה, הטעייה ודיס־אינפורמציה מערכתיות. אמצעים אלה מאפשרים להנחית על המערכת היריבה מהלומת מידע שמשלבת אלמנטים דיגיטליים, אלקטרוניים ותודעתיים.[36]

כאשר רוסיה מוציאה לפועל מתקפה צבאית, היא עושה זאת תחת מעטה כבד של חשאיות, הן ביחס לעצם קיומה של המתקפה והן ביחס למטרותיה. כל פעולה צבאית רוסית מוצגת כפעילות לשמירת שלום או כהתערבות במשבר הומניטרי.[37] טשטוש מטרותיה האמיתיות של רוסיה תורם לא רק להחלשת היריב, אלא גם להעצמת תדמיתה של רוסיה. אם רוסיה נכשלת בהשגת מטרה שחשובה לה, היא יכולה לבחור מטרה אחרת למימוש מבלי שהדבר ייחשב כלפי חוץ ככישלון. כך, הטשטוש מעניק לרוסיה תדמית של עליונות.[38]

לוחמת המידע ולוחמה פסיכולוגית, על סוגיהן השונים, תופסות חלק נכבד באסטרטגיה הצבאית הרוסית. דבריו של מפקד הצבא הרוסי משנת 2013 מחדדים נקודה זו: "התפקיד של צעדים לא־צבאיים בהשגת מטרות פוליטיות ואסטרטגיות נעשה חשוב יותר, ובמקרים רבים האפקטיביות של צעדים אלה גדולה יותר משל צעדים צבאיים".[39] ההסתמכות הגדולה על לוחמת מידע נובעת מהכרתה של רוסיה בחולשתה הצבאית והכלכלית, בייחוד למול ארצות הברית וסין. לפיכך, רוסיה רואה בלוחמת המידע אסטרטגיה צבאית בעלת יתרון כפול: מצד אחד, היא מסוגלת לבלבל את האויב בנוגע לכוונותיה האמיתיות, ומצד שני, מבחינת עלות־תועלת, היא מפחיתה משמעותית את ההשקעה הכלכלית הנדרשת במקרה של עימות צבאי בהשוואה לשימוש באמצעים קינטיים.[40]

דוקטרינת לוחמת המידע הרוסית אינה חדשה והיא מבוססת במידה רבה על הדוקטרינה הסובייטית בנושא. זו מוגדרת על בסיס המונח "שליטה

36 שם, 62.

37 Snegovaya, *Russia Report I*, 12.

38 Ibid., 15.

39 Mark Galeotti, "'Hybrid War' and 'Little Green Man': How it Works and How it doesn't, in *Ukraine and Russia: People, Politics, Propaganda and Perspectives, eds. Agnieszka Pikulicka-Wilczewska and Richard* Sakwa (Bristol: E-International Relations Publishing, 2016), http://www.e-ir.info/wp-content/uploads/2016/06/Ukraine-and-Russia-E-IR-2016.pdf 150

40 Snegovaya, *Russia Report I*, 11.

תגובתית" (reflexive control). משמעות מושג זה היא העברת מידע מסוים לגורם מסוים על מנת לגרום לו לבצע את הפעולות הרצויות לצד היוזם.[41]

בהתאם לכך, המסרים שרוסיה תשגר לצד היריב במסגרת לוחמת מידע וקמפיינים של דיס־אינפורמציה יהיו כאלו שיחזקו תחושות של ייאוש וכן גילויי עריקות.[42] רוסיה תנסה גם לפגוע בתשתיות חיוניות שונות (כגון תשתיות תקשורת) ולחתור תחת המבנים הפוליטיים, הכלכליים והחברתיים של הצד היריב.[43]

ישראל

בישראל ניתן למצוא שלושה גופים צבאיים העוסקים בתקשורת אסטרטגית ובמבצעי מידע מול קהלים שונים. המרכז למבצעי תודעה הוקם בשנת 2005 והוא כפוף לאגף המבצעים (מבחינה פיקודית) ולאגף המודיעין (מבחינה מקצועית).[44] במהלך מבצע עופרת יצוקה, הפעיל המרכז לוחמה פסיכולוגית הן מול האוכלוסייה האזרחית ברצועת עזה והן כלפי לוחמי חמאס. חלק מרכזי מהמסרים הועבר בצורה של מהדורות חדשות באמצעי התקשורת השונים.[45]

גדוד פסגות של חיל התקשוב אמון בעיקר על יישומה של לוחמת מידע מול האויב. הגדוד מסוגל להשתלט על אמצעים אלקטרומגנטיים של האויב, המונעים ממנו לבצע פעילות עוינת כלפי ישראל ופוגעים בתקשורת (פיקוד ושליטה) בין פעילי הטרור. פעילות הגדוד מתקיימת באוויר, בים וביבשה.[46]

בגוף הצבאי השלישי ניתן לראות יישום של ניהול תפיסה. ענף קשרי הציבור של דובר צה"ל אחראי על שורה של פעולות, המכוונות לקהלים מגוונים בחו"ל. הענף יוזם ומארגן ביקורים של דמויות מפתח בישראל (מפקדים זרים, אנשי ממשל, אקדמאים ועוד), מארגן משלחות הסברה לכנסים שונים בחו"ל ומסייע בכתיבת מחקרים בחו"ל העוסקים בצה"ל. כלל הפעולות

41 Ibid.,10.

42 Ibid.,11.

43 Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict", *Military Cyber Affairs,* 1, no.1 (2015): 2, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1001&context=mca

44 עמוס הראל, "צה"ל החליט להקים מחדש את היחידה ללוחמה פסיכולוגית בפלשתינאים," **הארץ**, 25 בינואר 2005, https://www.haaretz.co.il/1.1496075.

45 רון שלייפר, "הלוחמה הפסיכולוגית בעופרת יצוקה," **מערכות** 432 (אוגוסט 2010): 18-23.

46 מירב וייס, "יורים אלקטרונים: מערך הלוחמה האלקטרונית פעל בים, באוויר וביבשה במהלך מבצע 'צוק איתן'," **חדשות חיל הקשר והתקשוב**, 1 בספטמבר 2014, https://archive.is/MKk18

הללו נעשות מתוך הנחה שיצירת דעת קהל פרו־ישראלית בחו"ל תדחוף את מנהיגי המדינות הזרות לנקוט גישה ידידותית כלפי ישראל.[47]

בריטניה

בשנת 2015 הוקמה בבריטניה חטיבה 77, שמטרתה להוציא לפועל מבצעי לוחמה פסיכולוגית בערוצי תקשורת שונים (ובכללם הרשתות החברתיות) ברחבי העולם. החטיבה מתוכננת לפעול במקומות שונים ברחבי העולם, שבהם כוחות הצבא הבריטי מעורבים בפעילות צבאית ממושכת.[48] החטיבה כוללת שש יחידות, כאשר כל יחידה ממונה על היבט אחר של המבצעים הפסיכולוגיים. כך למשל, יחידה מספר 1 בחטיבה אחראית על ניתוח ההתנהגות של קהלי היעד הנבחרים.[49] דרך אחת שבה החטיבה פועלת היא פגיעה בגופים הנלחמים בבריטניה, באמצעות הפצת שמועות זדוניות עליהם בקרב תומכיהם ובקרב מי שעשוי לתמוך בהם.[50] החטיבה מעסיקה חיילים בשירות סדיר ובשירות מילואים מכל רחבי הצבא הבריטי וכן אזרחים. היא כוללת עובדים בעלי רקע בסייבר, פסיכולוגים ואנשי תקשורת. נוסף על כך, החטיבה מיועדת לעסוק בשיקום תשתיות אזרחיות ובהגשת סיוע הומניטרי באזורי לחימה, מתוך כוונה לצבור תמיכה של דעת הקהל באזורי הלחימה.[51] בזמן הקמת החטיבה, התכנון היה כי סדר הכוח שלה ינוע סביב 1500–20000 משרתים, מהם כ־40% אנשי מילואים (כאשר יעד הגיוס לשנת 2016 עמד על 448 איש). בפועל, נכון להיום, משרתים בחטיבה 276 איש בלבד, כאשר 125 חיילים גויסו אליה במהלך שנת 2016.[52] מאז הקמת החטיבה השתתפו מספר

47 ישראל טל־סרנגה, "דיפלומטיה ציבורית צבאית," **מערכות** 446 (דצמבר 2012): 11–19.

48 Military 'mask': British Army gets 'information warfare' focus, says top general," *RT*, February 18, 2015, https://www.rt.com/uk/233367-british-army-information-warfare

49 "77th Brigade," British Army, accessed October 1, 2017, http://www.army.mod.uk/structure/24047.aspx

50 Gareth Corfield, "Army Social Media Psyops Bods Struggling to Attract Fresh Blood, " *The Register*, January 3, 2017, https://www.theregister.co.uk/2017/01/03/77_brigade_struggling_recruit_40_pc_below_ establishment/

51 "New British Army Elite Unit to Hone Social Media and Psychological Warfare," *RT,* January 31, 2015, https://www.rt.com/uk/228227-british-army-psychological-warfare/

52 Gareth Corfield, "Army Social Media Psyops Bods Struggling to Attract Fresh Blood", The Register, January 3, 2017 https://www.theregister.co.uk/2017/01/03/77_brigade_struggling_recruit_40_pc_below_establishment/

קטן של אנשיה בכמה מבצעים בודדים. החטיבה צפויה להיכנס לכשירות מבצעית מלאה בסוף 2019.[53]

גוף נוסף במערכת הביטחון הבריטית שתומך במאמצי הצבא בתחום מבצעי התודעה במרחב הקיברנטי הוא ה־(JTRIG Joint Threat Research) Intelligence Group, יחידה הפועלת כחלק מסוכנות הביון והסיגינט GCHQ. היחידה כוללת מאות עובדים מתחומים שונים (סייבר, פסיכלוגיה, ומודיעין) וכן מומחי תוכן ושפות. הללו פועלים בשלוש מחלקות אופרטיביות (לוחמה בטרור, ביטחון פנים ומחלקה בינלאומית) ועוד כמה מחלקות לסיוע מבצעי כגון סייבר, משפט וכלכלה. היחידה תומכת במבצעי הצבא במשימותיו ברחבי עולם ומסייעת בפעילות גופי ביטחון פנים וביון בתוך בריטניה ומחוצה לה. היחידה מפעילה לוחמת סייבר התקפית כחלק מניהול המערכה נגד הטרור (תקיפות מניעת שירות, הפלת אתרים ועוד) וכן כלים טקטיים באזורי קונפליקט בהם פועלת בריטניה.[54]

גופים ממשלתיים־מדיניים

בריטניה

גוף ממשלתי העוסק בתקשורת אסטרטגית הוא המרכז למחקר, למידע ולתקשורת של ממשלת בריטניה: Research, Information and Communications Unit (RICU). המרכז, שהוקם בשנת 2007, נמצא תחת סמכותם של שלושה משרדי ממשלה. מטרת המרכז היא לתאם את מאמצי הממשלה הבריטית במלחמה נגד אידיאולוגיות המעודדות מעשי טרור. המרכז מייעץ לסוכנויות ביטחון ואכיפת החוק, ומייצר עבורם "ארגז כלים" להבנת המסרים הקיצוניים ולמלחמה בהם. RICU מאפשרת לסוכנויות אלה להבין את החולשות של האידיאולוגיות הקיצוניות, כמו גם לטפח אלטרנטיבות יישומיות. המרכז מורכב משלושה צוותים, האחראים על עיצוב ושידור המסרים הרצויים: צוות הניטור והתיאום (האחראי על ניתוח אמצעי התקשורת ואספקת תובנות מעשיות, כמו גם הבנת תגובות הציבור), צוות הקמפיינים הלאומי והבינלאומי (האמון על יישום טכניקות של תקשורת אסטרטגית הן במרחב הדיגיטלי והן מחוצה לו) וצוות התובנות והמחקר (המתמקד באופן ספציפי בהבנת קהלי היעד של

53 George Allison, "What does the secretive 77th Brigade do?," *UKDJ*, June 21, 2016, https://ukdefencejournal.org.uk/secretive-77th-brigade/

54 רוב המידע על היחידה נלקח ממסמך ייעוץ ארגוני של GCHQ שסיווגו "סודי ביותר" והודלף לרשת ב־2011. ראו: http://www.statewatch.org/news/2015/jun/behavioural-science-support-for-jtrigs-effects.pdf

המסרים). בשירות המרכז מועסקים מומחים מתחומים שונים: פסיכולוגיה חברתית, אנתרופולוגיה, שיווק ומלחמה בטרור.[55] חשוב לציין, שחלק גדול מפעילות המרכז מתבצעת באמצעות מיקור חוץ של חברות יחסי ציבור, כגון Breakthrough Media Network, חברת מדיה פרטית מלונדון שבונה אתרי אינטרנט ודפי פייסבוק, מכינה עלונים וקטעי וידאו, משדרת ברדיו ומצייצת בטוויטר. כל זאת בהתאם להנחיות של RICU.[56]

האיחוד האירופי

RICU הייתה המודל להקמתו שלThe Syria strategic communication advisory team.[57] מדובר בצוות של האיחוד האירופי, שאיגד בתוכו 25 מדינות החברות באיחוד. הצוות הוקם בתחילת שנת 2015 לאחר פיגועי טרור של האסלאם הקיצוני בצרפת.[58] הצוות התמקד בגיבוש דרכי הפעולה של המדינות החברות מול מסרים ברשתות החברתיות המעודדים אזרחים מוסלמים מאירופה להצטרף לארגוני טרור הנלחמים בסוריה. במהלך תקופת פעילות הפרויקט דיווחו חלק מן המדינות החברות על תוצאות חיוביות בהבנת המסרים ובמאבק בהם.[59] באוקטובר 2016 הוקם פרויקט המשך, ביוזמת בלגיה, ששמו The European Strategic Communications Network (ESCP). זהו פרויקט רב־לאומי שאמור להימשך שניים־עשר חודשים. כמו קודמו, גם ה־

55 "Case Study Report: Research, Information and Communication Unit," *The Institute for Strategic Dialogue*, https://www.counterextremism.org/resources/details/id/413/research-information-and-communications-unit-ricu

56 Ian Cobain Alice Ross, Rob Evans and Mona Mahmood, "Revealed: UK's covert propaganda bid to stop Muslims joining Isis," *The Guardian,* May 2, 2016, http://www.theguardian.com/uk-news/2016/may/02/uk-government-covert-propaganda-stop-muslims-joining-isis

57 Patryk Pawlak, *EU strategic communication with the Arab world (*Brussels: European Parliamentary Research Service, May 2016): 8, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581997/EPRS_BRI(2016)581997_EN.pdf

58 "Establishment of a European Anti-Propaganda Agency to Fight Radicalization", *European Parliament*, Parliamentary Questions, August 3, 2015 http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=P-2015-003103&language=EN

59 "The Syria Strategic Communication Advisory Team (SSCAT) and the Role of Counter-Narratives in Preventing Radicalization," *European Parliament*, Parliamentary Questions, May 17, 2016 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-000505&language=EN

ESCP מיועד לקדם תובנות ודרכי יישום של תקשורת אסטרטגית, על מנת להילחם בהקצנה, שעלולה להוביל למעשי טרור.[60]

בנובמבר 2015, ה־European External Action Service (EEAS) הקים כוח משימה מיוחד, שמיועד לתת מענה ללוחמת התודעה הרוסית – Disinformation Review".[61] כוח המשימה מתעד את מאמצי הדיס־אינפורמציה שהממשל הרוסי מפנה כלפי אזרחי מדינות אירופה וחושף בפני האזרחים והממשלות האירופיים את מהות הדיס־אינפורמציה ואת היקפה. תיעוד מקרי הדיס־אינפורמציה, במסגרת כוח המשימה המיוחד, נעשה באמצעות רשת הכוללת כ־400 עיתונאים, ארגונים של החברה האזרחית ומוסדות אקדמיה, הפרושים בכ־30 מדינות ברחבי אירופה. המידע שנאסף במסגרת ה־Disinformation Review מאפשר ל־EEAS להבחין לאורך זמן במגמות המאפיינות את לוחמת התודעה הרוסית.[62] נוסף על כך, באפריל 2017 הוקם בפינלנד המרכז האירופי למלחמה באיומים היברידיים: European Center of Excellence for Countering Hybrid Threats. הגוף הוקם בעקבות מסגרת עבודה שהוסכם עליה באיחוד האירופי שנה לפני כן. המרכז מיועד לקדם מדיניות כוללת, בינלאומית ומולטי־דיסציפלינרית, על מנת להילחם באיומים הנובעים מהמלחמה ההיברידית. הגוף אמור לקדם את המטרה הזו באמצעות שימוש במרכז כבסיס לשיתופי פעולה קבועים בין מדינות האיחוד האירופי ונאט"ו, פיתוח דוקטרינה וניהול הכשרות ואימונים שמטרתם לחזק את היכולות של כל מדינה לפעול בנפרד ובשיתוף פעולה עם מדינות אחרות בתחום.[63]

60 *Implementation of the Counter-Terrorism Agenda set by the European Council* (Brussels: Council of the European Union, 2016): 24 http://data.consilium.europa.eu/doc/document/ST-14260-2016-ADD-1-EXT-1/en/pdf

61 European Union in Ukraine. "Disinformation Review" - new EU information product." Facebook, November 4, 2015 https://www.facebook.com/EUDelegationUkraine/posts/1019727421405219

62 "Disinformation Review," *European Union External Action (EEAS*), September 2, 2016 https://eeas.europa.eu/headquarters/headquarters-homepage_en/9443/Disinformation%20 Review

63 "EU Welcomes Establishment of the Finnish Centre of Excellence for Countering Hybrid Threats," *European Union External Action*, updated April 11, 2017, https://eeas.europa.eu/headquarters/headquarters-homepage_en/24572/EU%20welcomes%20establishment%20of%20the%20Finnish%20Centre%20of%20Excellence%20for%20countering%20hybrid%20threats

התקציב השנתי של המרכז עמד ב2017 על מיליון וחצי אירו, כאשר מחציתו הגיע מפינלנד ומחציתו משאר המדינות החברות.[64]

ישראל

מבין משרדי הממשלה בישראל ניתן להצביע על משרד החוץ, על מחלקותיו השונות, כפועל בזירת התקשורת האסטרטגית. אגף התקשורת וההסברה של המשרד, למשל, ממפה את הארגונים המשתתפים בחרם על ישראל, מנחה את שגרירי ישראל בנוגע למסרים שיש להעביר ומפיץ מסרים פרו־ישראליים ברחבי הרשתות החברתיות. האגף אף יוצר מסגרת של שיתוף פעולה בין ממשלת ישראל לארגונים אזרחיים העוסקים בהסברת מדיניות החוץ של המדינה.[65]

נוסף על כך, המשרד למאבק בחרם ובדה־לגיטימציה נגד ישראל (השייך למשרד לנושאים אסטרטגיים), שהוקם בתחילת 2016 אמור לשמש כסמכות המרכזית של ממשלת ישראל להבנת תמונת מצב תנועת החרם על ישראל (ה־BDS), לגיבוש תוכניות הפעולה מולה ולייצוג הממשלה מול ארגונים אזרחיים נוספים הפועלים נגד החרם. פעילות המשרד מול תנועת החרם מתחלקת לשלוש: הוא אוסף מידע גלוי וסמוי על הגופים המרכיבים את תנועת החרם, הוא נוקט בצעדים משפטיים מול אותם גופים והוא מנחה את הארגונים האזרחיים בדבר המסרים שבהם יש להתמקד במלחמה נגד תנועת החרם.[66]

רוסיה

על הנעשה בתחום עיצוב התודעה ברוסיה ניתן ללמוד מהתבטאות של אחראי התעמולה בממשלת רוסיה, דימיטרי קיסליוב: "עידן העיתונות הניטרלית חלף כי ניטרליות במציאות הנוכחית היא בלתי אפשרית מאחר שמה שאדם בוחר מתוך ים המידע הינו כבר סובייקטיבי". רוסיה מפעילה סוכנות ידיעות לאומית בשם "רוסייה סגודנייה" (Rossiya Segodnya) המייצרת זרם קבוע של מידע סובייקטיבי. כמו כן מעסיק הקרמלין צבא של "טרולים" שמטרתו להילחם באזורי התגובות באתרי החדשות במערב וברשתות חברתיות כגון

64 Aleksi Teivainen, "EU's Hybrid Threat Centre to be set up in Helsinki," *Helsinki Times,* April 12, 2017. http://www.helsinkitimes.fi/finland/finland-news/domestic/14686-eu-s-hybrid-threat-centre-to-be-set-up-in-helsinki.html

65 "המאבק הדיפלומטי־תקשורתי בתנועת החרמות ובגילויי האנטישמיות בחו"ל", **דו"ח מבקר המדינה 66ג'**, מאי 2016, עמ' 866, 868, 871, 877, 881 /http://go.ynet.co.il pic/news/mevak-861-883.pdf

66 צביקה קליין, "המסרים הסודיים של ישראל: 'כך תגיבו לפעילי ה־BDS'", **NRG**, 22 בפברואר 2016, http://www.nrg.co.il/online/1/ART2/756/389.html

פייסבוק וטוויטר. הקרמלין מפעיל גם רשת של אלפי "בוטים" ברשתות חברתיות וסוגים אחרים של ספאם, על מנת לפגוע בתכני מידע מתחרים.

המערכה על התודעה הייתה מאז ומתמיד חלק מהעימותים בין מדינות וחברות, אך משקלה היחסי בעימותים הללו עלה מאוד בשנים האחרונות וניתן להבחין כי המדינות הדמוקרטיות החלו להשקיע משאבים בבניית יכולות במרחב התודעתי ובקידומן.

ניתוח מקרי בוחן

פרק זה יתמקד בניתוח מקרי בוחן בהם פועלות יחידות ללוחמת תודעה, לוחמה פסיכולוגית ולוחמת סייבר. מקרים אלו התרחשו במסגרות ניהול מערכות צבאיות שונות באופיין. לבד מן ההבדלים בין שני הצבאות הנבחנים קיימים הבדלים גם באופן הפעלת הכוח בשטח: מערכה אמריקאית גלויה במסגרת הקואליציה נגד ארגון המדינה האסלאמית בסוריה ובעירק לעומת מערכה רוסית שכוחותיה נלחמו באופן לא רשמי באוקראינה (לכאורה נלחמו רק כוחות אוקראיניים פרו־רוסיים כנגד הצבא האוקראיני). הבדל מרכזי נוסף הוא שבעוד ארצות הברית ניסתה להתמודד עם יוצרת ההשפעה במרחב הקיברנטי (ארגון המדינה האסלאמית ופעילותו לגיוס, השפעה ותעמולה), יצרה רוסיה בעצמה השפעה דרך מרחב הסייבר. המשותף לשני מקרי הבוחן הוא השימוש במערכה משולבת של לוחמת מידע, מבצעי השפעה ולוחמת סייבר, אך אלה באו לידי ביטוי ברמות שונות של הפעלת עוצמה וכוח. באמצעות ניתוח מקרי הבוחן אפשר יהיה להמחיש את ההבדלים הללו ולהצביע על הא־סימטריה הבסיסית בהפעלת כלי סייבר לטובת מבצעי תודעה בין מדינות המערב לבין רוסיה.

הפעילות התודעתית האמריקאית הרשתית מול ארגון המדינה האסלאמית

הצורך של ממשלת ארצות הברית להילחם, ברמה התודעתית והמודיעינית, בארגונים כמו המדינה האסלאמית ואל־קעידה, נובע מיכולותיהם המתפתחות של הארגונים הללו לפעול ברשתות החברתיות. ארגונים אלו הצליחו לרתום את הרשתות באופן יעיל ביותר למשימת איתור מצטרפים פוטנציאליים וגיוסם לשורותיהם. לשם כך הם הקימו כמות עצומה של אתרי אינטרנט ופרופילים ברשתות החברתיות, שפנו לצעירים בכל רחבי העולם. חלק מהאתרים הללו עשו שימוש בשרתים הממוקמים בארצות הברית. יכולותיהם של ארגונים אלו צפויות להשתכלל עוד יותר בעתיד, כאשר ירחיבו את פעילותם גם לרשת האפלה (Dark web).[67] המאבק במגמה הזו נשען על רשת של ארגונים – צבאיים, ממשלתיים ופרטיים – ועוסק בהיבטים שונים של תקשורת אסטרטגית בכלל ושל לוחמת מידע בפרט.

67 Dan Verton, "Pentagon Gets Authority to Fight Online ISIS Propaganda," *Meritalk,* November 30, 2015, https://www.meritalk.com/articles/pentagon-gets-authority-to-fight-online-isis-propaganda/

הפעלת לוחמת תודעה במערכה

אחד הגופים המרכזיים בצבא ארצות הברית הוא הפיקוד המרכזי, הפועל מבסיס חיל האוויר שבפלורידה (CENTCOM). בארגון מועסק צוות פעולה מיוחד: Digital Engagement Team (DET). הצוות מונה 11 איש, השולטים בשפות שונות: ערבית, אורדו, פרסית, רוסית ועוד. אנשי היחידה מפעילים חשבונות טוויטר, פייסבוק ואינסטגרם שפונים לציבור הרחב המצוי בכ־20 מדינות במזרח התיכון ובמרכז אסיה.[68] במקביל, אנשי היחידה מפגינים את נוכחותם גם בפורומים שונים המזוהים עם אנשי המדינה האסלאמית.[69] לטענת אנשי ה־CENTCOM, למסרים שלהם נחשפים בכל שבוע כמאה אלף איש.[70]

מחלקת הלוחמה הפסיכולוגית ב־CENTCOM מכונה "Web Ops" וכוללת כ־120 איש. הלוחמה הפסיכולוגית מבוססת על שלוש אסטרטגיות מרכזיות: שיבוש מסרי התעמולה של האויב, הפצת מקרים של צביעות ופשע של האויב במגעיו עם אוכלוסיות בסיכון והנעת מתנגדי היריב להילחם בו במדיה בצורה יעילה יותר. שיטה מרכזית להפצת המסרים נעזרת באנשים שלחמו לצד המדינה האסלאמית וערקו ממנה. העריקים הללו מספקים, מניסיונם, עדויות שיכולות לערער את המסרים שהמדינה האסלאמית מעוניינת להפיץ. לא פעם הם מספרים שהם הצטרפו לשורות המדינה האסלאמית כדי להילחם במשטר הסורי וב"כופרים". בפועל, הם מצאו את עצמם נלחמים לא פעם מול מוסלמים כמותם.[71] לצד מסרים שמנסים לערער את האמינות של היריב, פועלת היחידה גם ליצירת זיקה של קהלי היעד לערכים שמייצג המערב. כדי להשיג את התוצאה הרצויה, הפכו במרוצת הזמן מסרי היחידה ממסרים לעומתיים למסרים שמנסים ליצור דיאלוג וסקרנות. ההנחה היא שחשיפת עובדות על המערב יוצרת סקרנות בקרב קהל היעד ולבסוף משרישה בו השקפות מערביות.[72]

---

68 Karen Parrish, "Centcom Counters ISIL Propaganda."

69 Natalie Johnson, "Centcom's Anti-ISIS Propaganda Team Has Fewer Than a Dozen Members", *The Washington Free Beacon*, July 6, 2016, http://freebeacon.com/nationalsecurity/centcoms-anti-isis-propaganda-team-fewer-dozen-members/

70 Peter Cary, *The Pentagon and Independent Media–an Update*, (Washington: CIMA-Center for International Media Assistance, 2015), 10, http://www.cima.ned.org/wp-content/uploads/2015/11/CIMA-The-Pentagon-and-Independent-Media-Update.pdf

71 Parrish, "Centcom Counters ISIL Propaganda."

72 Cary, *The Pentagon and Independent Media–an Update*, 10.

הפעלת המתנגדים לארגון המדינה האסלאמית נעשית דרך האינטרנט, בשפתם. על מנת להבין מי תומך במדינה האסלאמית ומי מתנגד לה, מחפשים הצוותים מילות מפתח שונות, שיוצרות זיהוי של תומכי המדינה האסלאמית ומתנגדיה. בתוך הקבוצה יש יחידת הערכה שתפקידה הוא להעריך את היעילות של פעילות היחידה.[73]

נוסף על המאמצים הללו, ניתן לראות את השימוש שעושה צבא ארצות הברית בפרסומים של אנשי המדינה האסלאמית לטובתו. לדוגמה, פוסט שהעלה לוחם המדינה האסלאמית כלל צילומים של בניין פיקוד של הארגון. חיל האוויר הצליח לזהות את מיקום הבניין ולהרוס אותו בתוך פחות מ־24 שעות לאחר מכן.[74] כיוון נוסף של פעילות צבא ארצות הברית הוא הריסת תשתיות תקשורת בשטח, המשמשות את הארגון.[75]

במישור הממשלתי, ניתן להבחין במעורבות רבה של משרדי הממשלה וסוכנויותיה – מחלקת המדינה, הסוכנות לביטחון לאומי והמחלקה לביטחון המולדת. בשירות מחלקת המדינה פעל ה־(Centre of Strategic (CSCC Counterterrorism Communications בין השנים 2011–2016, והחל מ־2016 פועל ה־(Global Engagement Center (GEC. פעילותם של שני הגופים הללו ברחבי הרשת מאופיינת בהפצת מסרים (לתושבי ארצות הברית ומדינות זרות), שמנסה למנוע מראש את הצטרפותם של אזרחים אל המדינה האסלאמית. על מנת להשיג את האפקט הרצוי, מפיצים שני הגופים הללו שני סוגים עיקריים של מסרים: הסוג הראשון זהה לזה שמופעל בשירות ה־CENTCOM וכולל שורה של מסרים (בעיקר כאלו המגיעים מצד עריקים), שמנסים לערער את אמינותו ותהילתו של ארגון המדינה האסלאמית.[76] הסוג השני מתייחס באופן אישי יותר אל מי ששוקל להצטרף אליו. מסרים מסוג זה מאלצים את מי

73 Parrish, "Centcom Counters ISIL Propaganda."

74 Michael Hoffman, "US Air Force Targets and Destroys ISIS HQ Building Using Social Media," *Defensetech,* June 3, 2015, http://www.defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-building-using-social-media/

75 Lynne O'donnell, "U.S Airstrikes Have Destroyed an Islamic State-Operated Radio Station in a Remote Part OF Eastern Afghanistan," *U.S.News*, February 2, 2016, http://www.usnews.com/news/world/articles/2016-02-02/airstrikes-in-eastern-afghanistan-destroy-is-radio-station

76 Kristina Wong, "How the US is working to defeat ISIS online," *The Hill,* June 25, 2016, http://thehill.com/policy/defense/284826-how-the-us-is-seeking-to-defeat-isis-online

שמבקש להצטרף, לחשוב מה יהיו ההשלכות של צעד כזה על משפחתו, על קהילתו ועל חייו שלו.[77]

השוני הבולט בפעילותם של שני הארגונים נובע במקור ממנו מגיעים המסרים. במרבית תקופת פעילותו של ה־CSCC, הופצו המסרים בטוויטר, בפייסבוק וביוטיוב בשם ממשלת ארצות הברית.[78] החל משנת 2015, החליטה מחלקת המדינה (באמצעות הגופים הללו) שלא להפיץ את המסרים בשמה, אלא להעביר אותם דרך רשת של ארגונים ויחידים שונים שאינם מזוהים עם הממשל האמריקאי (כולל ממשלות זרות ומוסלמים מתונים), שמביעים ביקורת על המדינה האסלאמית.[79] זאת מאחר שלאותם ארגונים ויחידים יש יכולת טובה יותר להגיע אל קהלי היעד שעליהם מעוניינת ממשלת ארצות הברית להשפיע. כך, ה־GEC, בשונה מה־CSCC, משמש כמוקד של רשת בינלאומית שמתאמת את הפצת המסרים מבחינה רעיונית וטכנית.[80]

בפן האסטרטגי, מי שמוביל את הפעילות במחלקה לביטחון המולדת הוא המשרד לשותפות קהילתית (Office of Community Partnership), שהוקם בספטמבר 2015. מטרתו של המשרד היא לעודד את קשרי הממשל עם קהילות שונות ברחבי ארצות הברית, כדי למנוע את היווצרותן של השקפות קיצוניות בקרב אזרחי ארצות הברית.[81] מאחורי הקמת המשרד עומדת התפיסה שהדרך להחליש את המשיכה של בני אדם לרעיונות קיצוניים היא באמצעות חיזוקם של מסרים חלופיים שמעודדים סובלנות ושלום.[82] המשרד מעניק תמיכה ממשית לקהילות שמעוניינות להפעיל תוכניות למניעת רדיקליזציה בקרבן. בחודש מאי 2016 הודיע המשרד על הקדשת תקציב של 10 מיליון דולר

77 Patrick Tucker, "Meet the Navy SEAL Leading the Fight Against ISIS Messaging," *Defense One*, June 9, 2016, http://www.defenseone.com/technology/2016/06/navy-seal-isis-messaging/128938

78 Asawim Suebsaege, "The State Department Is Actively Trolling Terrorists on Twitter," *MotherJones*, March 5, 2014, http://www.motherjones.com/politics/2014/02/state-department-cscc-troll-terrorists-twitter-think-again-turn-away

79 Cary, *The Pentagon and Independent Media–an Update*, 9.

80 Patrick Tucker, "Meet the Navy SEAL Leading the Fight Against ISIS Messaging."

81 "Statement by Secretary Jeh C. Johnson on DHS's New Office for Community Partnerships," *U.S Department of Homeland Security*, September 28, 2015, https://www.dhs.gov/news/2015/09/28/statement-secretary-jeh-c-johnson-dhss-new-office-community-partnerships

82 Michael A. Brown and Christopher Paul, "Inciting Peace," *RAND Cooperation,* March 30, 2016, http://www.rand.org/blog/2016/03/inciting-peace.html

למענקים שיינתנו לקהילות שירצו לפתח תוכניות לקידום מסרים סובלניים נוגדי אלימות.[83]

צוות נוסף שאחראי על הפעילות מטעם המחלקה לביטחון המולדת הוא כוח המשימה למלחמה בקיצוניות (Countering Violent Extremism Task Force) שהוקם בתחילת שנת 2016. לצוות זה יש תפקיד מערכתי רחב יותר: הוא מפתח את התוכניות השונות הקשורות למלחמה בקיצוניות, מנהל את התיאום בין עשרה גופים ממשלתיים שונים (משרד המשפטים, ה־FBI ועוד) לשם יישום התוכניות, מנהל את העבודה מול הגורמים עימם נעשים שיתופי פעולה בנושא מחוץ לממשל, וכן מנהל מערך של מחקר וקבלת משוב על המאמצים שנעשים בתחום.[84]

במלחמה מול המדינה האסלאמית במרחב האינטרנטי, ניתן להצביע על יוזמות אחדות שהמחלקה מעורבת בהן. אחת מהן היא תחרות שמעודדת צוותים מוכשרים באוניברסיטאות ליצור קמפיינים מקוונים שמדגישים מסרים חיוביים וסובלניים ברחבי הרשת. אלפי סטודנטים מרחבי העולם משתתפים בתחרות הזו, כשפייסבוק מעניקה מימון חשוב לקיומה. בד בבד, כוח המשימה שואף גם להדק את קשרי העבודה עם חברות טכנולוגיה שונות. מטרתם של הקשרים הללו היא לסייע לכוח המשימה לגבש אסטרטגיה לעבודה במרחב הדיגיטלי, שתוכל לשמש סוכנויות ממשל נוספות. במטרה להגשים ייעוד זה נפגשו בכירים בממשל האמריקאי עם מנהלים בכירים בחברות הטכנולוגיות השונות בניו יורק (בנובמבר 2015) ובסן פרנסיסקו (בינואר 2016).[85]

הפעלת גופי סייבר במערכה

בחודש אפריל 2016, פתח פיקוד הסייבר האמריקאי במתקפה על רשת המחשבים של ארגון המדינה האסלאמית. מטרתה של המתקפה הייתה לפגוע

---

83 George Selim, "OCP and CVE Task Force Welcome President Obama's Top Homeland Security Advisor," *U.S Department of Homeland Security*, May 6, 2016, https://www.dhs.gov/blog/2016/05/06/ocp-and-cve-task-force-welcome-president-obamas-top-homeland-security-advisor

84 "Written Testimony of DHS Office for Community Partnerships Director George Selim for a Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations hearing titled 'ISIS Online: Countering Terrorist Radicalization & Recruitment On the Internet & Social Media'," *U.S Department of Homeland Security*, July 6, 2016, https://www.dhs.gov/news/2016/07/06/written-testimony-ocp-senate-homeland-security-and-governmental-affairs-permanent

85 Ibid.

ביכולות הפיקוד והשליטה של הארגון באמצעות שיבוש אפשרויותיו לבצע פעולות לוגיסטיות בתוך הארגון: גיוס פעילים חדשים, תשלום לפעילים הקיימים, הפצת פקודות ועוד.[86] ההתקפה הידועה והמתוחכמת ביותר של הכוחות האמריקאים הייתה שיבוש תעמולה של המדינה האסלאמית על ידי ה־NSA ופיקוד הסייבר הצבאי במסגרת מבצע "סימפוניה זוהרת" (Operation Glowing Symphony). במסגרת המבצע, שנערך במהלך שנת 2016, השיגו יחידות הסייבר האמריקאיות סיסמאות והרשאות של אנשי המדינה האסלאמית. לאחר מכן חסמו באמצעותן גישה לנכסים אינטרנטיים ומחקו מידע ששימש לתעמולה ולגיוס. המבצע הוכתר בהצלחה, אך זו הייתה זמנית בשל מעבר של המדינה האסלאמית לשרתים מאובטחים יותר. פיקוד הסייבר הפעיל מבצעים נוספים באינטגרציה עם הכוחות בשטח. מבצעים אלה כללו דחיקת פעילים שאותרו מחשבונות קיימים, במטרה לגרום להם להשתמש בכלים פחות מאובטחים שיחשפו את מיקומם ויאפשרו את סיכולם באמצעות מל"טים.[87] בסוף שנת 2016, פרץ הפיקוד לחשבונותיהם של מומחי תעמולה בארגון, שינה את הסיסמאות שלהם ומחק תוכן תעמולתי כמו קטעי וידאו שצולמו באזורי הקרבות.[88] מעבר לפגיעה בפן בטכני, למבצעים כאלו יש משמעות פסיכולוגית: כאשר מפקדי הארגון ופעיליהם יודעים כי פעולותיהם אינן מאובטחות, תחושת הביטחון שלהם מתערערת. חלק מן הפעילות כלל הנחת "שתלים" שונים ברשתות של הארגון, על מנת ללמוד את הרגליהם של הפעילים.[89] הפעילות מתבטאת הן בשיבוש הפיקוד והשליטה האופרטיבית והן בפעילות נגד רשת התקשורת של המדינה האסלאמית שייעודה גיוס פעילי טרור.

86 David E. Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat," *The New York Times*, April 24, 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=2

87 David E. Sanger and Eric Schmidt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," The New York Times, June 12, 2017, https://mobile-nytimes-com.cdn.ampproject.org/c/s/mobile.nytimes.com/2017/06/12/world/middleeast/isis-cyber.amp.html

88 Ellen Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies," *The Washington Post,* May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.30d3d00d99fb

89 Sanger, "U.S. Cyberattacks Target ISIS in a New Line of Combat."

פעולות כאלה מעוררות שני סוגי מחלוקת בתוך הממשל האמריקאי. המחלוקת הראשונה נוגעת ליעילותן של מתקפות סייבר כאלו, כלומר, נוגעת בשאלה אם פעילות הסייבר האמריקאית באמת הצליחה לשבש את פעילותו המקוונת של האויב. בעוד שפיקוד הסייבר ומשרד ההגנה הגדירו את המבצעים הללו כמוצלחים, בכירים יוצאי קהילת המודיעין (שלא הזדהו בשמם המלא) הטילו ספק בהצלחה של מבצעים כאלו. הסיבה למחלוקת נעוצה בהגדרת הצלחת מבצעי סייבר: בעוד שמשרד ההגנה ופיקוד הסייבר מגדירים הצלחה כשיבוש זמני של פעילות האויב, מומחי מודיעין מחפשים פגיעה ארוכת טווח שאותה, הם טוענים, קשה להשיג במבצעים מסוג זה. הם טוענים למשל, כי חלק מפעילות הארגון ניתנת לשחזור או להעברה לשרתים אחרים ובכך השפעת המבצע מתבטלת.[90]

מחלוקת נוספת נוגעת להשפעת מבצעי לוחמה מסוג זה על יחסי ארצות הברית עם בעלות בריתה. חלק מהשרתים בהם משתמשים אנשי המדינה האסלאמית נמצאים בשטחיהן של מדינות שהן בעלות בריתה של ארצות הברית. כך, פעולה נגד שרתים אלו היא למעשה פעולה התקפית נגד שטחן של מדינות אלו. מסיבה זו קיימת מחלוקת בממשל האמריקאי בשאלה אם ארצות הברית צריכה לתת התרעה מראש לבעלות בריתה לפני הפעלה של מבצעים כאלו. ה־FBI, ה־CIA ומחלקת המדינה טוענים שמבצעים מסוג זה ללא תיאום מראש עלולים לפגוע בשיתוף הפעולה בין המדינות בלוחמה בטרור ובתחומי המודיעין. מנגד, משרד ההגנה טוען שהודעה מוקדמת על מבצעי סייבר עלולה לגרום להדלפת פרטים רגישים הנוגעים למבצעים ולפגוע בהצלחתם.[91]

פעילות רוסיה בעימות עם אוקראינה ובמהלך הבחירות בארצות הברית

בשנים האחרונות, הממסד הצבאי הרוסי אימץ גישה לפיה דינמיקה צבאית טקטית אופרטיבית בשטח ודינמיקה מדינית דיפלומטית בפורומים בינלאומיים שונים הן חלקים אינטגרליים ושלובים של הרעיון המערכתי.[92] כנגזרת מתפיסה זו, לוחמת סייבר ומבצעים תודעתיים הם מאמצים משולבים, המכוונים לתמרן

90 Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies."

91 Ibid.

92 דימה אדמסקי, "ההתערבות הרוסית בסוריה: משמעויות אסטרטגיות ולקחים מערכתיים", 22.

את התנהגות הקורבן. אלה כוללים תקיפה של רשתות ממוחשבות, לוחמה פסיכולוגית, הונאה, הטעייה ודיס־אינפורמציה מערכתיות. אמצעים אלה מאפשרים להנחית על המערכת היריבה מהלומת מידע שמשלבת אלמנטים דיגיטליים, אלקטרוניים ותודעתיים.[93]

בפברואר 2014 פלשה רוסיה לחצי האי קרים והשתלטה עליו בתוך ימים ספורים. קודם להשתלטות היה חצי האי בשטח אוקראינה אך שימש את הצי הרוסי בים השחור. זמן רב לאחר שנכנסו הכוחות הרוסים לחצי האי קרים, הקפידה רוסיה להמשיך ולהכחיש את מעורבותה הצבאית באזור. עוד קודם לפלישה קיים צבא רוסיה תמרון צבאי נרחב בגבול אוקראינה, הרחק מחצי האי קרים. תמרון זה יצר הסחת דעת והקשה על גורמים אוקראיניים ומערביים לצפות נכונה את המהלך הרוסי לכיבוש חצי האי.[94] באפריל 2014 החלו בדלנים פרו־רוסים בהתקוממות אלימה במחוזות האוקראיניים דונייצק ולוחאסנק והכריזו על הקמת רפובליקות עצמאיות מתוך כוונה להצטרף לרוסיה בהמשך. ההכרזה של הבדלנים הובילה לתגובה צבאית מקיפה מצד השלטון בקייב. בינואר 2015, זמן רב לאחר הכניסה הצבאית לחצי האי קרים, התבטא בנושא שר החוץ הרוסי, סרגיי לבוב: "אני אומר זאת בכל פעם – אם אתם טוענים כך בביטחון גדול כל כך, הציגו את ההוכחות. למעשה, אף אחד לא יכול להציג את ההוכחות, או רוצה לעשות זאת. לכן, לפני שדורשים מאיתנו להפסיק לעשות משהו, תציגו הוכחה למה שעשינו". גם פוטין הכחיש בתוקף את מעורבות צבא רוסיה וטען שהכוחות שפועלים בחצי האי הם מליציות מקומיות (זאת על אף שחלק מן הכוחות שפעלו שם לבשו את מדי הצבא הרוסי). רק באפריל 2015 הודה פוטין כי כוחות צבאיים רוסיים מיוחדים היו מעורבים בפעילות צבאית בחצי האי.[95]

במהלך המלחמה עצמה מבצעי המודיעין של רוסיה לא מכוונים להכריע את מצב הלוחמה בשלב מוקדם אלא יכולים לתרום להתארכותה. בדרך זו, לרוסיה יש יכולת רבה יותר להשפיע על הנעשה בזירת המלחמה והיא יכולה לבחור לסיים את מעורבותה בנקודת הזמן הרצויה לה.[96]

---

93 שם, 62.

94 Ulrike Frank, *War by non-military Means-Understanding Russian Information Warfare*, (FOI: Swedish Defense Research Agency, 2015), 46 https://pdfs.semanticscholar.org/2869/71ba9762da1d039d0d40a27c94e0ec8d31ac.pdf

95 Snegovaya, *Russia Report I*, 17.

96 Ibid.,12.

כאשר רוסיה נהגה כך, היא השיגה יתרונות חשובים הן בזירה הצבאית והן בזירה הדיפלומטית/הסברתית: הכחשת הכניסה הצבאית קיצרה את זמני התגובה של הצד האוקראיני ופגעה ביכולתו להוציא לפועל תגובה צבאית ראויה. ההכחשה הרוסית נועדה להקשות על המעקב אחר הפעילות הרוסית ועל תכנון הצעדים של הצד שמנגד.

במהלך שנת 2015 הגדילה הממשלה הרוסית ב־50% את השקעתה בערוץ הטלוויזיה שלה – RT, שהגיעה לסכום של כ־300 מיליון דולר. סוכנות הידיעות Rossiya Segodnya (Russia Today), תוקצבה בשנה זו ב־89 מיליון דולר. חלק מהגידול אומנם משקף את הצורך לפצות על ירידת שער הרובל, אך חלקו משקף גידול בחשיבות שמייחסת הממשלה למסרים העוברים בערוצים אלו. בשנת 2015, שיעור ההוצאות על שידורים אלו היה 34% מכלל המימון הממשלתי לתקשורת, לעומת 25% בשנת 2014.[97]

ערוצי הטלוויזיה הממלכתיים הם מקור המידע העיקרי של כמעט כל תושבי רוסיה.[98] כלומר, הם נחשבים למייצגים את המיינסטרים הרוסי. כיוון שכך, דיווחיהם על המלחמה באוקראינה יהיו כלליים ומופשטים ככל האפשר, מבלי להעמיס על הצופה פרטים שאינם נחוצים. ערוצים אלו הצדיקו את הפלישה לחצי האי קרים כדי להגן על המיעוט הרוסי שחי שם.[99]

אף על פי כן, ניתן למצוא בערוצי הטלוויזיה הרוסיים נרטיב של מעשי זוועה ואלימות שמחוללים האוקראינים באזור.[100] הם גם כינו את הלוחמים האוקראינים "בנדריטים" (פרטיזנים ששיתפו פעולה עם הנאצים) או פשיסטים.[101] מטרה חשובה של הצגת האוקראינים באופן הזה היא להקשות על המערב להתערב לטובת אוקראינה.[102] על ידי הצגת האוקראינים כנאצים, יוצרים הרוסים ניכור של המערב כלפי אוקראינה. הצגה זו אמורה להרתיע במיוחד מדינות בעלות עבר נאצי, כמו גרמניה, מפני המשך תמיכה באוקראינה.[103]

97 Stephen Ennis, "Russia in 'Information War' with West to Win Hearts and Minds," *BBC* September 16, 2015, http://www.bbc.com/news/world-europe-34248178

98 Snegovaya, *Russia Report I*, 15.

99 Ilya Yashin and Olga Shorina, eds., *Putin. War-An Independent Expert Report* (Moscow: Free Russia Foundation, 2015), 10, http://4freerussia.org/putin.war/Putin.War-Eng.pdf

100 Unwala and Ghori, "Brandishing the Cybered Bear," 8.

101 Snegovaya, *Russia Report I*, 13–14.

102 Galeotti, "Hybrid War' and "Little Green Man'," 153.

103 Unwala and Ghori, "Brandishing the Cybered Bear," 7.

בפני הקהל הרוסי, תיארה התקשורת הרוסית את הממשלה האוקראינית באופן נוסף: בפברואר 2014, לאחר שנבחרה ממשלה חדשה באוקראינה, פרסמה התקשורת הרוסית בהרחבה "מיילים מקוריים" הממחישים את קרבתה הרבה של הממשלה החדשה למערב. "מיילים" אלה הוצגו ככאלו שהודלפו בידי "אוקראינים אנונימיים".[104]

לאורך זמן, המסרים הללו לא מצליחים לשכנע את דעת הקהל הבינלאומית בצדקת המאבק הרוסי.[105] פחות צופים נחשפים למסרים של RT לעומת הערוצים הבינלאומיים האחרים. דוגמה לכך מצויה ביחס לאל ג'זירה האנגלית: אם בשנת 2012 היה מספר הצופים בשני הערוצים פחות או יותר שווה, הרי שבשנת 2015, היה מספר הצופים ב־RT פחות ממחצית ממספר הצופים באל ג'זירה האנגלית.[106] תחת זאת, לשידורי הטלוויזיה יש השפעה גדולה על הקהל המצוי במדינות ברית המועצות לשעבר: רוסים רבים שהתנדבו להצטרף למלחמה מול אוקראינה עשו זאת בהשפעת שידורי טלוויזיה רוסיים.[107] בד בבד, אזרחים של מדינות רבות שהשתייכו לברית המועצות רואים את התקשורת הרוסית כאמינה יותר מזו המערבית. רבים מאלו שנחשפים לסיקור תקשורתי מערבי ורוסי על הנעשה באוקראינה מעדיפים את הסיקור הרוסי.[108]

הפעלת מבצעי השפעה ברשת

רוסיה עושה שימוש בשלושה סוגים עיקריים של אמצעים: בוטים (תוכנות המדמות פעילות אנושית), טרולים והאקרים. הבוטים הם תוכנות המפיצות מסרים קצרים, שלעיתים זהים למסרים של הטרולים. הטרולים הרוסים מנסים לשבש דיונים מסוגים שונים, להפיץ בהם תגובות שכוללות ספאם, לפרסם מידע מוטעה ולבטא מסרים פרו־רוסיים.[109] הם גם מפרסמים תגובות רבות

---

104 Frank, *War by non-military Means,* 45.

105 James Andrew Lewis, ''Compelling Opponents to our Will': The Role of Cyber Warfare in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO Cooperative Cyber Defense Center of Excellence, 2015), 45, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

106 Stephen Ennis, "Russia in 'Information War'."

107 Snegovaya*, Russia Report I*, 15.

108 Neli Esipova and Julie Ray, "Information Wars: Ukraine and the West vs. Russia and the Rest", *Harvard International Review,* May 6, 2016, http://hir.harvard.edu/information-wars-ukraine-west-vs-russia-rest/

109 Snegovaya, *Russia Report I*, 14.

למאמרים ביקורתיים על רוסיה, המתפרסמים באתרי חדשות מערביים.[110] הטרולים הרוסים יכולים להיות לא משכנעים במיוחד, אך בזכות פעילותם הם משיגים נוכחות רבה ברחבי הרשת. מטרת הפעילות אינה לנסות לשכנע להחזיק בהשקפת עולם מסוימת, אלא לשלוט באופן זרימת המידע כך שבקרב הצד השני – תושבי מדינות אירופה – ייווצרו תחושות של פחד ואי־ודאות.[111] מטרה נוספת היא לערער על אמינותם של אתרי אינטרנט יריבים כמקור מידע.[112]

לעיתים קרובות פעילות הטרולים ברשתות החברתיות נועדת לקדם סיפורים חדשותיים שפורסמו לראשונה בערוצי החדשות הרוסיים. הפרסום הנרחב של הסיפורים הפרו־רוסיים ברשתות החברתיות גורם לשרתים של אותן רשתות לזהות, על פי האלגוריתמים שלהן, את הסיפורים הללו כ"סיפורים טרנדיים", מה שיכול להגדיל את הסיכוי שהסיפורים הללו יסוקרו גם באמצעי התקשורת המסורתיים במדינות המערב.[113]

עד לסוף שנת 2016, פעל בסנט פטרסבורג "המרכז לחקר האינטרנט", ששימש כמרכז להעסקת טרולים, שפעלו בהנחייתה ובמימונה של ממשלת רוסיה.[114] לקראת סוף השנה שינה המרכז את שמו ואת מוקד פעילותו. שמו של המרכז הוסב ל־Federal news agency (FAN) על מנת להציג את עצמו

110 John B. Emerson, "Exposing Russian Disinformation*", Atlantic Council*, June 29, 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-russian-disinformation

111 Snegovaya, *Russia Report I*, 14.

112 Emerson, "Exposing Russian Disinformation."

113 Craig Timberg, "Russian Propaganda Effort Helped Spread 'Fake News' During Election, Experts Say", *The Washington Post,* November 24, 2016, https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html?utm_term=.ea80d3d009a3

114 Dmitry Volchek and Daisy Sindelar, "One Professional Russian Troll Tells All" *Radio Free Europe, Radio Liberty*, March 25, 2015, http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html

כסוכנות ידיעות לגיטימית. הסוכנות מפעילה 16 אתרי חדשות.[115] הללו מפיצים באופן קבוע תעמולה פרו־רוסית.[116]

ערוצי התקשורת הגדולים ברחבי העולם פועלים לא רק בטלוויזיה, אלא גם ברשתות החברתיות. כאן ישנו מצב מעניין: מצד אחד, בטוויטר ובפייסבוק, מספר הגולשים של הערוצים המערביים הגדולים (BBC, CNN וכו') גדול משמעותית ממספר הגולשים של RT. ביוטיוב, לעומת זאת, המצב שונה לחלוטין. בערוץ הרשמי של RT ביוטיוב נספרו בשנת 2015 מיליון וחצי מנויים ומיליארד וחצי צפיות.[117] לעיתים, אתרים שלא מצליחים להשפיע על דעת הקהל נסגרים. לדוגמה, אתרי חדשות של חברת ספוטניק (Sputnik), שפעלו בגרסאות שפנו לארצות סקנדינביה, נסגרו לאחר פחות משנת פעילות אחת מאחר שלא היו אטרקטיביים בארצות אלו.[118]

הפעלת לוחמת סייבר

שימוש אינטנסיבי יחסית בתקיפות סייבר נעשה בזמן הפלישה הרוסית לקרים, כאשר אתרי חדשות ורשתות טלפונים אוקראיניים הושבתו למשך שלושה ימים. נוסף על כך, בימים הראשונים לפלישה לאוקראינה דווח כי כמה אתרים אוקראינים הושבתו עקב מתקפות עליהם, בהם סוכנות המודיעין האוקראינית (UNIAN), המועצה להגנה ולביטחון לאומי ובית המשפט העליון של קרים.[119] התקיפות היו מסוג DDoS.

---

115 Sam Webb, "Vladimir Putin's Notorious 'Troll Factory' Attacked with Molotov Cocktails Amid Reports it Employs an Army of Teens to Flood Social Media with Praise for Russia", *The Sun,* October 28, 2016, https://www.thesun.co.uk/news/2068935/vladimir-putins-notorious-troll-factory-attacked-with-molotov-cocktails-amid-reports-it-employs-an-army-of-teens-to-flood-social-media-with-praise-for-russia/

116 Alexey Kovalev, "Russia's Infamous 'Troll Factory' Is Now Posing as a Media Empire", *The Moscow Times,* March 24, 2017, https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534?utm_source=push

117 Stephen Ennis, "Russia in 'Information War'."

118 Neil Macfarqhar, "A Powerful Russian Weapon: The Spread of False Stories", *Atlantic Council,* August 29, 2016, http://www.atlanticcouncil.org/blogs/natosource/a-powerful-russian-weapon-the-spread-of-false-stories

119 Andrew Foxall, Putin's Cyberwar: Russia's Statecraft in the Fifth Domain, Policy Paper No. 9 (London: Russia Studies Centre at the Henry Jackson Society, 2016), 4, https://relayto.com/the-henry-jackson-society/YDD2kgI1

במצב זה נגרמו כמה נזקים לצד האוקראיני. ראשית, גורמי ממשל אוקראינים לא יכלו ליצור קשר עם גורמים בחצי האי ולהעריך נכונה את היקף המתקפה הרוסית. שנית, הממשל האוקראיני התקשה לייצר תהליך של קבלת החלטות ביחס למשבר המתפתח. שלישית, האוקראינים לא יכלו ליצור קשר עם גורמים מערביים על מנת לקבל עזרה או לשדר תגובה לרוסיה.[120]

גם לאחר הכיבוש נמשכו מתקפות הסייבר מצד רוסיה, וכוונו גם כלפי המערב. כך למשל, במרץ 2014, נחסמה הגישה לאתרים אחדים של נאט"ו. המתקפה הזו הגיעה מצידם של אוקראינים פרו־רוסיים. באותו החודש חסם השירות הפדרלי הרוסי לפיקוח על התקשורת, הטכנולוגיה והמידע: The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) אתרי אינטרנט של קבוצות פרו־אוקראיניות ושל גורמי אופוזיציה רוסיים כגון אלכסיי נבלני וגרי קספרוב.[121]

לרוסיה יש יכולת לשבש את קבלת ההחלטות בצד השני באמצעות פגיעה בשידורי רדיו, מכ"מ ו־GPS. בצבא רוסיה יש יחידות גדולות בעלות יכולת לבצע מתקפות כאלו. הצבא האוקראיני נמצא בנחיתות מול הצבא הרוסי בתחום זה ולכן הוא מתקשה להגן על עצמו ממתקפות כאלו. כך, כאשר הצבא הרוסי תוקף את הצבא האוקראיני, מתקשה צבא אוקראינה לארגן תגובה הולמת. הקושי של הצבא האוקראיני נובע מכך שחייליו ומפקדיו פשוט לא מאומנים להילחם במצב של פגיעה בתקשורת שלהם. מה שיכול לסייע לצבא האוקראיני להתמודד עם המתקפות הללו הוא העבר הסובייטי המשותף, שמעניק לאוקראינה מושג מסוים לגבי מבנה הפעולה של רוסיה. עבור רוסיה, מדובר בטקטיקה רצויה לא רק בשל יעילותה, אלא גם בשל הקושי לאתר את מקורות המתקפות, מה שמקשה להאשים את רוסיה בתוקפנות.[122]

מעבר לכך, לרוסיה יש גם יכולת לפגוע ביריביה באמצעות פעילות סייבר התקפית אסטרטגית נגד תשתיות קריטיות. בשנתיים האחרונות ידוע על ביצוע שתי מתקפות רחבות היקף מסוג זה. במתקפה הראשונה, שבוצעה בדצמבר 2015, הצליחו האקרים לשבש את אספקת החשמל לכ־230 אלף אזרחים אוקראינים, באמצעות פגיעה בשלוש חברות חשמל מקומיות. באותה מתקפה נשארו האזרחים ללא חשמל לפרק זמן המוערך בין שלוש לשש

120 Unwala and Ghori, "Brandishing the Cybered Bear," 6–7.

121 Ulrike Frank, *War by non-military Means,* 46.

122 Joe Gould, "Electronic Warfare: What US Army can Learn from Ukraine," *Defense News,* August 2, 2015, https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine

שעות.[123] המתקפה השנייה נערכה שנה לאחר מכן, בדצמבר 2016, ופגעה באספקת החשמל באזור עיר הבירה, קייב. משך הזמן שבו היו הצרכנים מנותקים מחשמל היה קצר יותר ונמשך דקות ספורות. באותה מתקפה, הצליחו ההאקרים להשבית 200 מגה וואט, כלומר 20% מצריכת החשמל של העיר קייב בשעות הלילה (הזמן בו בוצעה המתקפה).[124]

הדפוס העומד בבסיס שתי המתקפות הוא זהה: חודשים לפני ביצוע המתקפה, השתמשו ההאקרים במתקפת דיוג שכוונה למוסדות ממשל שונים (ובניהם גם רשת החשמל האוקראינית). למיילים שהופצו צורפו תוכנות ריגול, אותן הורידו הנמענים. הורדת תוכנות הריגול בידי המשתמשים אפשרה להאקרים היכרות מקרוב עם מבנה מערכת החשמל, ובכך אפשרה לתקוף ביעילות גדולה יותר את אותה הרשת. מתקפת הדיוג בוצעה באופן כה מתוחכם, שההערכה היא שכמעט כל מי שקיבל את המייל פתח אותו והוריד את תוכנת הריגול שהותקנה בו.[125] באופן ספציפי, המתקפה שבוצעה בשנת 2015 עשתה שימוש בתוכנת BlackEnergy – תוכנה זדונית שמאפשרת למשתמשים בה להוציא לפועל מתקפות סייבר באמצעים שונים: התקפת מניעת רשת (DDoS), גניבת מידע ועוד.[126]

ההערכה היא שאותן מתקפות סייבר לא כוונו בהכרח לשתק את החיים האזרחיים באוקראינה, אלא שימשו את ההאקרים בעיקר כדי לבחון את יכולתם לבצע מתקפות מסוג זה במדינות אחרות בעולם.[127] הם מודעים לכך שאפילו שיבושים קצרים ברשת החשמל האוקראינית יכולים לייצר השפעה פסיכולוגית משמעותית על מדינות אירופה ועל ארצות הברית.[128]

123 Kim Zetter, "The Ukraine Power Grid was Hacked Again", *MotherBoard*, January 2, 2017, https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report

124 Jamie Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks", *MIT Technology Review*, December 22, 2016, https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks

125 Zetter, "The Ukraine Power Grid was Hacked Again."

126 "Frequently Asked Questions: BlackEnergy", *Trend Micro*, February 11, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

127 Zetter, "The Ukraine Power Grid was Hacked Again."

128 Sheera Frenkel, "The New Handbook for Cyberwar is being Written by Russia", *Buzzfeed News*, March 19, 2017, https://www.buzzfeed.com/sheerafrenkel/the-new-handbook-for-cyberwar-is-being-written-by-russia?utm_term=.iv8MjRNZa#.od7pRbqXd

רוסיה מפעילה את יכולותיה ההתקפיות במרחב הסייבר לא רק מול אוקראינה. היא עושה זאת מול מדינות רבות במערב ובראשן ארצות הברית. הדיווחים על תקיפות סייבר רוסיות על ארצות הברית הגיעו לשיאם בשנת 2016, במהלך הבחירות לנשיאות ארצות הברית, אך מתקפות אלו החלו זמן רב קודם לכן. כבר בשנת 2014, גייסה רוסיה ואימנה טרולים, על מנת שיפעלו באתרי החדשות האמריקאיים המובילים. ההנחה הרוסית מאחורי היוזמה הייתה שהתקשורת המערבית, שמושפעת במידה רבה מקהל הצרכנים שלה, לא תוכל לעמוד בפני מתקפה של מסרים פרו־רוסיים בכמות עצומה, מה שיאלץ אותה לשנות את אופן הסיקור כך שיהיה נוח יותר לרוסיה וירגיע את זעמם של הקוראים הפרו־רוסיים. בפועל, היוזמה לא זכתה להצלחה רבה: רוב הגולשים שנחשפו למסרים רוסיים שהופצו במסגרת זו הניחו כי מדובר במסרים שנכתבו מטעמים אידיאולוגיים טהורים או תמורת תשלום.[129]

במהלך שנת 2016 הגבירה רוסיה את מאמציה במרחב הסייבר באמצעות שתי שיטות עיקריות. השיטה הראשונה הייתה תודעתית: מקורות מדיה פרו־רוסיים הציפו את האינטרנט בדיווחים שקריים שונים שנועדו לזרוע דיס־אינפורמציה וספקות לגבי מערכת הבחירות והמשתתפים בה. בחקירת המודיעין האמריקאי עלתה השערה כי במהלך מערכת הבחירות פעלו כאלף אנשי צוות רוסיים להפצת חדשות בלתי מבוססות נגד המועמדת הדמוקרטית הילארי קלינטון.[130] דוגמה לכך התרחשה באוגוסט 2016, אז פוזרו דיווחים לא מבוססים שהעצימו את הספקות לגבי מצבה הבריאותי של קלינטון.[131]

במקביל, הוציאו האקרים לפועל מתקפות סייבר שונות על תשתיות הקשורות לניהול מערכת הבחירות בארצות הברית: בחודש יולי 2016, פרצו האקרים רוסיים למחשבי הוועידה הלאומית של המפלגה הדמוקרטית ופרסמו עשרות אלפי אימיילים שנפרצו. חודש לאחר מכן, פרצו האקרים שני מאגרי מידע –

---

129 Alexander Fokin, *Internet Trolling as a Hybrid Tool: the Case of Latvia,* (Riga: NATO Strategic Communications Centre of Excellence, 2015), 20, https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

130 "הסנאט יחקור: 1000 האקרים רוסיים הפיצו פייק ניוז נגד קלינטון", **Ynet**, 30 במרץ **2017**, http://www.ynet.co.il/articles/0,7340,L-4942627,00.html

131 Andrew Weisburd, Clint Watts and JM Berger, "Trolling for Trump: How Russia is Trying to Destroy our Democracy," *War on the Rocks*, November 6, 2016, https://warontherocks.com/2016/ 11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy

באריזונה ובאילינוי – והשיגו גישה לפרטיהם של כ־200 אלף מצביעים.[132] את המתקפות הללו ביצעו האקרים שאוגדו בשש קבוצות שונות.[133]

הממשל הרוסי כיוון את מאמציו לפעול לבחירתו של דונלד טראמפ לנשיאות. על פי קהילת המודיעין האמריקאית, העדפה זו נבעה מכמה מניעים: קלינטון נתפסה בעיני פוטין כמי שעומדת באופן אישי מאחורי הפגנות שאורגנו נגדו ברחבי רוסיה בסוף 2011 ובתחילת 2012. מנגד, טראמפ נתפס בעיני הרוסים, על סמך עמדותיו, כשותף פוטנציאלי ליצירת קואליציה בינלאומית שתילחם בעוצמה רבה יותר בארגון המדינה האסלאמית.[134]

אף על פי כן, אין לפרש את המעורבות הרוסית רק ככזו הנובעת מתמיכה בטראמפ. הפצת ה"פייק ניוז" נגד קלינטון, כמו גם שיבוש תשתיות שונות הקשורות למערכת הבחירות, היו חלק ממהלך רחב יותר, בעל חשיבות אסטרטגית לרוסיה: כאשר האזרחים האמריקאים נחשפים לתקלות במערכות ההצבעה והנשיא נבחר תחת עננה של חשדות, הם מתחילים לפתח תחושות של חוסר אמון לא רק גם כלפי מנהיגיו. בד בבד, כאשר האמינות של הדמוקרטיה האמריקאית נפגמת, יכולתה של ארצות הברית להקים ולחזק משטרים דמוקרטיים במזרח אירופה – מרחב רגיש עבור רוסיה – נפגעת גם היא.[135] פעולה זו תורמת גם לערעור אמינותם של מתווכים לגיטימיים ואובייקטיביים יחסית כגון התקשורת, האקדמיה ומומחי תוכן. יכולתם של גורמים אלה לבצע הנגדה לפעילות הרוסית נפגעת, ובכך מתקיים תהליך של שיבוש ידע והשפעה על מידת האמון של הציבור בתכנים אליהם הוא נחשף.

---

132 Clint Watts, "Why Russia Wants the U.S to Believe the Election was Hacked," *Public Broadcasting Service*, October 26, 2016, http://www.pbs.org/wgbh/nova/next/tech/election-cybersecurity/

133 Chris Strohm, "Russia Weaponized Social Media in the U.S Elections, FireEye Says", *Bloomberg,* December 1, 2016, https://www.bloomberg.com/news/articles/2016-12-01/russia-weaponized-social-media-in-u-s-election-fireeye-says

134 *Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, (Washington: Office of the Director of National Intelligence, 2017), 1, https://www.dni.gov/files/documents/ICA_2017_01.pdf

135 Dana Priest, Ellen Nakashima and Tom Hamburger, "U.S. Investigating Potential Covert Russian Plan to Disrupt November Elections", *The Washington Post,* September 5, 2016 https://www.washingtonpost.com/world/national-security/intelligence-community-investigating-covert-russian-influence-operations-in-the-united-states/2016/09/04/aec27fa0-7156-11e6-8533-6b0b0ded0253_story.html?postshare=8261473103304697&tid=ss_tw

ניתוח השוואתי של מקרי הבוחן

מקרי הבוחן משקפים את הא־סימטריה הבסיסית המאפיינת את כללי המשחק בניהול מערכה על התודעה. מעצם טיבן, דמוקרטיות ליברליות כארצות הברית מחויבות לכללים של אחריות מדינתית ומתאפיינות בהיעדר הסכמה פנימית המונע גיבוש מסר אחיד, ובסרבול ביורוקרטי ופוליטי. לעומת זאת, מדינות כרוסיה מתייחסות לכללים שקבעו הדמוקרטיות כאל סדר עולמי קיים שיש לשבשו ולשנותו. ככזו, רוסיה אינה מהססת לבצע מניפולציות תקשורתיות, תוך כדי הצגת מסר אחיד המאפשר התאמה מהירה של הפעילות במערכה על התודעה לשינויים בכללי התנהגות גמישים.

אומנם, מבצעי הצבא האמריקאי כנגד המדינה האסלאמית היו תקדימיים משום שהתבצעה בהם לראשונה הפעלה של פיקוד הסייבר במערכה צבאית, וכנגזרת מכך פיתוח הטכנולוגיות (או נשקי הסייבר) ושיטות הפעולה נוסו לראשונה בזמן אמת, אך עם זאת, ניתן לזהות מגבלות אחדות בהפעלה המשולבת של תודעה וסייבר:

No Logo Strategy

הוספת רובד של פעילות סייבר התקפית היא חשאית מטבעה, אך סינכרון עם פעילות תודעתית שמתבצעת בחתימה גלויה ולא חשאית הוא אתגר, משום שבהתאם לחומר הגלוי בנושא נראה כי המערכה האמריקאית התודעתית נעשתה ללא בניית נכסים אינטרנטיים מוסווים או מזויפים. לעומת זאת, הפעילות הרוסית הנעשית בשיתוף מודיעין צבאי, יחידות סיגינט ומיקור חוץ, משוחררת מהגבלות ומאפשרת פעילות חשאית ללא צורך בזיהוי העומדים מאחוריה. ההנחה הנגזרת מכך היא שהפעילות החשאית האמריקאית (וככל הנראה גם הבריטית) ברשת מתבצעת בידי גופי ביון כגון CIA או באמצעות מיקור חוץ. בהנחה שכך הדבר, הנגזרת היא שאפשרויות הפעולה של צבא ארצות הברית מוגבלות ומצומצמות מבחינת מרחב הפעולה והכלים האופרטיביים הנדרשים לביצוע מבצעי סייבר ותודעה באופן גלוי או סמוי (בניגוד לפעילות חשאית שמאפשרת גמישות בהפעלת כלי תקיפה בחתימה נמוכה).

שיתוף פעולה בינלאומי

הצורך האמריקאי בפעילות בזירת מדינות ידידותיות דורש שיתוף פעולה שיצר אפקטיביות נמוכה בכל הקשור לפגיעה בנכסי המדינה האסלאמית שהופעלו משרתי מדינות אחרות. הללו מנעו מן האמריקאים את היכולת לפעול באופן

חשאי, בשל הדרישה לעדכן גורמים אחרים ולבקש אישורים לפעילות סייבר התקפית (למשל לטובת הפלת שרתים הממוקמים במדינות אחרות). בהמשך לכך, בעוד ארצות הברית הגבילה את עצמה ונמנעה מפעילות במדינות אחרות בצורה חשאית, רוסיה לא מציבה קווים אדומים בכל הקשור לפעילות סייבר ותודעה כנגד מדינות אחרות או לפעילות נגד נכסים אינטרנטיים הממוקמים במדינות אחרות.

סנכרון הפעילות

לעומת הסינרגיה הרוסית בין הגופים השונים הפעילים בתחום, יש לשער שתיאום המאמץ האמריקאי בין יחידות הצבא השונות וכן מול מעגל רחב יותר של ארגוני ביטחון ודיפלומטיה, הקשה על מאמצי הצבא בהפעלת הכוח. בהקשר זה יש לציין, כי נראה שלאורך המערכה ברשת נגד המדינה האסלאמית, האחריות על תיאום המאמץ ותכלולו עברה בין כמה גופים (החל ממחלקת המדינה ועד למשרד ההגנה). בניגוד לכך, התפיסה הרוסית היא אינטגרטיבית ומשלבת מאמצים מדיניים וצבאיים בהפעלת יחידות סייבר, לוחמה פסיכולוגית ותודעה.

שגרה מול חירום

בעוד המאמץ האמריקאי הופעל בשעת חירום (וכחלק מהקואליציה הבינלאומית נגד המדינה האסלאמית), המאמץ הרוסי הופעל גם בשגרה לטובת השפעה ארוכת טווח מול קהל יעד מגוון (לא רק מול אוקראינה, אלא גם מול מדינות נוספות שלהן השפעה עקיפה על המערכה באוקראינה, כגון מדינות נאט"ו).

שימוש בלוחמת סייבר התקפית

ארצות הברית התמקדה במערכה נגד מטרות "רכות", כגון אתרים וחשבונות של רשתות חברתיות, לטובת שיבוש התקשורת בין פעילי המדינה האסלאמית, איסוף מודיעין מטרות ושיבוש התקשורת עם פעילים פוטנציאלים לגיוס. לעומת זאת, הפעילות הרוסית ההתקפית הופעלה גם כנגד מטרות פיזיות ופגעה במערכות המוגדרות כתשתיות קריטיות כגון רשתות חשמל.

סיכום

ניהול מערכה תודעתית אפקטיבית הכוללת שיתוף פעולה בין יחידות מדיה חברתית, מודיעין וסייבר תורם להכפלת כוחה של העוצמה הצבאית והמדינית ברמה הטקטית וברמה האסטרטגית. במציאות הנוכחית, האינטרנט בכלל והרשתות החברתיות בפרט הפכו לגורם משפיע ביותר על התנהגות החברה האנושית ולכלי מרכזי להשפעה על התודעה ולעיצובה. בעימות בין מדינות, כאשר אחד הצדדים משבש את סביבת המידע שעליה מסתמך הצד היריב, הוא משבש את יכולת היריב לתפוס את המציאות כהלכה ולגבש מולה צעדי פעולה אפקטיביים. בדרך זו, הצד היוזם יוצר לעצמו יתרון במערכה הכוללת. הוא מערער את הלגיטימציה של הצד השני ואת אמינות טענותיו, באמצעות יצירת רגשות שליליים, ספק, אי ודאות ופחד כלפיו בקרב דעת הקהל, או לחילופין באמצעות יצירת רגשות חיוביים כלפי הצד היוזם. פעולה כזו תורמת גם לערעור אמינותם של מתווכים לגיטימיים ואובייקטיביים יחסית כגון תקשורת, אקדמיה ומומחי תוכן.

במגמתה הנוכחית, ארכיטקטורת הרשת מאפשרת יצירת מידע ומסירתו במודל עם מאפייני "פרסונליזציה". כלומר, המידע מונגש למשתמש יחיד או לקבוצה באמצעות "התערבות" (engagement) על פי פילוח של התנהגות, גיאוגרפיה, תחומי עניין, צרכים, רצונות ותשוקות. במציאות כזו, פעילות תודעתית ברשתות החברתיות עלולה לנצל את האלגוריתמים במודל זה ולגרום להם לייצר חשיפה מוגברת לנרטיב שנועד לשבש מידע של הצד השני. כאשר פעילות כזו מתקיימת לצד פעילות סייבר התקפית שמתמקדת בשיבוש אמצעי התקשורת במדינה המותקפת, הסינרגיה בין סייבר לתודעה משמשת כמכפיל כוח לתוקף ופותחת בפניו סל חדש של יכולות כנגד מערכות המידע הממוחשבות של היריב, כגון הדלפת מידע, סחיטה ומחיקת מידע (שיבוש שרשרת האספקה).

בעידן הרשת, ארגון צבאי או מדיני שרוצה להשיג מטרות ויעדים, זקוק לפיתוח יכולות קיברנטיות "רכות" שיאפשרו לו להתגמש ולהשתנות במהירות, תוך כדי התאמת מסריו לקהל היעד הרלוונטי ופיתוח יכולות סייבר התקפיות להשפעה על היריב. על מנת לעמוד ביעדים מבצעיים במסגרת סוג לוחמה זה יש צורך בניהול מערכה שתכלול פעילות פרו־אקטיבית של לוחמת סייבר בשילוב לוחמת תודעה. הדרך לכך היא בניית סל יכולות ביצוע שיכלול פיתוח אמצעי לחימה קיברנטיים ייעודיים המותאמים לעולם הרשתי בכלל ולרשתות החברתיות בפרט.