

רשת האינטרנט והרשתות החברתיות הפכו לגורם המשפיע על התנהגות החברה האנושית ולכלי מרכזי להשפעה ולעיצוב תודעה, גם בעת מערכה צבאית. המבצע האמריקני נגד דאעש משקף את האסימטריה הבסיסית המאפיינת את כללי המשחק בניהול מערכה על התודעה

דניאל כהן, חוקר בכיר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל-אביב וראש תחום מחקר ואסטרטגיה במכון אבא אבן במרכז הבינתחומי הרצליה



גיל ברעם, מנהלת המחקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון, ועמיתת מחקר במרכז הרביתחומי לחקר הסייבר ע"ש בלווטניק, אוניברסיטת תל-אביב



בתחילת שנת 2018 פורסם בתקשורת כי נחנכה בצה"ל מחלקת תודעה באגף המבצעים במטכ"ל. על-פי הפרסום, זהו גלגול חדש של מחלקה אחרת, שעסקה בלגיטימציה בין-לאומית ובהיבטים משפטיים של פעילות צה"ל, והייתה כפופה לאגף התכנון.¹ במדינות רבות בעולם קיימים גופים צבאיים שונים העוסקים בתכנון וביישום של לחימה בזירה התודעתית. המודעות המדינית והציבורית למורכבותם ולתוצאותיהם של מבצעי ההשפעה הולכת וגדלה, בייחוד מאז שנחשפה המעורבות הרוסית בבחירות לנשיאות בארצות-הברית בשנת 2016.²

שימוש בלוחמת סייבר ←

סל הכלים העומד לרשותם של מדינות ושל צבאות הפועלים בזירת התודעה לצורך ביצוע מבצעי השפעה מאפשר מיצוי שונה של כוח, ושימוש בשיטות מגוונות ובכלי פעולה שונים.⁴ אלה כוללים הפעלת מודיעין, לוחמה פסיכולוגית, דיפלומטיה ציבורית, ערוצים מדיניים ומשפטיים וכן שימוש בלוחמת סייבר. בעוד שבמקרים רבים לוחמת סייבר ולוחמת תודעה נפרדות זו מזו, נראה שהשילוב ביניהן מהווה מכפיל כוח משמעותי עבור הצדדים הלוחמים בעת קונפליקט.⁵

ארכיטקטורת הרשת מאפשרת להנגיש את המידע למשתמש יחיד או לקבוצה ב"התערבות" על-פי פילוח התנהגותי, גיאוגרפי, תחומי העניין, צרכים, רצונות ותשוקות. במציאות שכזו, פעילות תודעתית ברשתות החברתיות עשויה ליצור חשיפה מוגברת לנרטיב ייעודי שנועד לשבש את המידע של הצד השני. כאשר פעילות כזו מתקיימת לצד פעילות סייבר התקפית, שמתמקדת בשיבוש אמצעי התקשורת במדינה המותקפת – הסינרגיה בין סייבר לתודעה פותחת בפני התוקף סל חדש של יכולות כמו הרלפת מידע, סחיטה ומחיקת מידע (שיבוש שרשרת האספקה) נגד מערכות המידע של היריב.⁶

מטרת המאמר היא לנתח את מקומה של לוחמת סייבר לצורך ביצוע מבצעי השפעה על-ידי הצבאות המודרניים. לשם כך אנו דנים במושגים הרלוונטיים לצורך אבחנה בין לוחמת מידע ובין לוחמת סייבר; מתארים את מקומם של מבצעי השפעה בשלושה מהצבאות המתקדמים בתחום התודעה בעולם – האמריקני, הרוסי והבריטי; מעמיקים במבצע שניהל הצבא האמריקני נגד דאעש ("המדינה האסלאמית") ברשת כחלק מהמערכה למיגור הארגון מסוריה ומעיראק, ומצביעים על היתרונות שבהפעלת אמצעים אלו בזירה ועל מגבלותיהם.

בין לוחמת מידע ללוחמת סייבר

המושגים לוחמת מידע או מבצעי מידע מבטאים את הדרכים שבהן נוקט הצד היוזם על-ימנת להשפיע על כמות המידע, ועל סוג המידע שהצד היריב נחשף לו. ההגדרה הצה"לית ללוחמת מידע מתייחסת לשיטות ולפעולות שנוקטות על-ימנת להשיג עליונות בממד המידע. כאשר הצד היוזם משבש את סביבת המידע שעליה מסתמך הצד היריב, הוא למעשה משבש את יכולתו לתפוס את המציאות כהלכה ולגבש את דרכי הפעולה שלו. כך יוצר הצד היוזם יתרון במערכה הכוללת. הוא מסוגל להשתמש בלוחמת מידע כדי להשיג הישגים, ואף להכריע את יריבו.

על-ימנת להימנע מתגובה דומה מהיריב, לוחמת המידע כוללת גם היבט הגנתני, כאשר הצד שיוזם את מבצעי המידע מפעיל יכולות הגנתיות על מאגרי המידע שלו.⁶ על-פי רוב, מבצעי המידע מזוהים עם יכולות טכנולוגיות מעולם המחשבים, אך למעשה כל פעולה



לוחם סייבר בצה"ל. ההגדרה הצה"לית ללוחמת מידע מתייחסת לשיטות ולפעולות שנוקטות על-ימנת להשיג עליונות בממד המידע. צילום: דו"ץ

למבצעי השפעה צבאיים



סמל של מפקדת הסייבר האמריקנית. בצבא היבשה האמריקני פועלות שלוש חטיבות העוסקות בתכנון וביישום מבצעי לוחמה פסיכולוגית

גופים צבאיים העוסקים בלוחמת תודעה משולבת בלוחמת סייבר

ברחבי העולם עוסקים גופים צבאיים שונים בתכנון לוחמת תודעה וביישומה. צבאות אלה מפעילים מאמצים ניכרים בתחום לוחמת התודעה לקידום פעילות מבצעית בזירות עימות בהן הם פועלים, ולכן קיים מידע רב על פעילותם. מידע זה מאפשר לבצע בחינה מעמיקה בנושא, במטרה להבין כיצד מתבצע השימוש בלוחמת סייבר לצורך ביצוע מבצעי השפעה במערכה.

ארצות-הברית

בארצות-הברית פועל ה"Joint Information Operations Warfare Center" שהוקם ב-1999, הכפוף למפקדת המטות המשולבים ומורכב ממומחים מצבא ארצות-הברית, עובדי ממשל ועובדי חברות פרטיות. במישור האסטרטגי, המרכז משמש מקור סמכות בנושא לוחמת מידע לכלל הסוכנויות במחלקת ההגנה. המרכז אמון על הפצת ידע, גיבוש דרכי היישום להשגת מטרת מבצעי מידע וקידום תהליך למידה כלל-מחלקתי ליישום תוכניות אלה. ברמה הטקטית, המרכז שולח צוותים שמומחים בלוחמת מידע לכל מקום ברחבי העולם שבו פועלים כוחות משימה של ארצות-הברית בהתאם לדרישת מפקדת המטות המשולבים. הצוותים מספקים ייעוץ לכוחות הלוחמים בשטח בדבר הדרכים ליישום תוכניות מבצעי המידע. לצורך פעילותו עושה המרכז שימוש בניתוחים חברתיים-תרבותיים של האוכלוסייה הנמצאת באזור העימות.¹⁴

בצבא היבשה האמריקני פועלות מספר חטיבות העוסקות בתכנון וביישום מבצעי לוחמה פסיכולוגית. כל חטיבה מורכבת מגדודים האחראיים על תכנון, על ייצור ועל הפצה של תוצרי לוחמה פסיכולוגית, בהתאם למאפייני הלחימה. במרבית המקרים, הלוחמה הפסיכולוגית של הצבא מופנית לאוכלוסייה האזרחית באזורי העימות, ומיועדת להעביר את תמיכתה מכוחות הגרילה אל הלוחמים האמריקניים.¹⁵ אחד הגופים המרכזיים שמבצע מבצעי השפעה הוא הפיקוד המרכזי של צבא ארצות-הברית (CENTCOM) הפועל מבסיס חיל-האוויר שבפלורידה. מחלקת הלוחמה הפסיכולוגית ב-CENTCOM מכונה "Web Ops" וכוללת כ-120 חיילים. הלוחמה הפסיכולוגית מבוססת על שלוש אסטרטגיות מרכזיות:

שיש בה אלמנטים של תחבולה והונאה, לדוגמה מסירת הצהרות כוזבות לתקשורת – עשויה להיחשב כצעדים של לוחמת מידע.⁷ לוחמה פסיכולוגית היא שם כולל לניהול ההיבט הרגשי של התקשורת האסטרטגית. כאשר מידע ספציפי בעל מרכיבים פסיכולוגיים מועבר לקהל יעד מוגדר, רגשותיו ותפיסות עולמו עשויים להשתנות.⁸ דרכי ההתנהגות של קהל היעד משתנות, וכתוצאה מכך יכולתה של הקבוצה להשיג את מטרתה עלולה להיפגע. המסרים שבהם נעשה שימוש במסגרת לוחמה פסיכולוגית יכולים להיות הבטחות, אימים, הגדרת תנאים לסיום הלחימה או לכניעה, עידוד עריקה וכדומה.⁹ פעולות של לוחמה פסיכולוגית מכונות מבצעים פסיכולוגיים. פעולות אלה ניתנות ליישום בזמני מלחמה ובזמני שלום. ניתן להבחין בין הסוגים השונים של פעולות לוחמה פסיכולוגית. כל סוג כזה מופעל בעיתוי אחר, מכוון כלפי קהל יעד מובחן ומיועד לעורר רגשות מסוימים בקרב קהל היעד. לדוגמה, לוחמה פסיכולוגית טקטית המופעלת מול לוחמי הצד היריב, שונה מלוחמה פסיכולוגית מייצבת שמכוונת כלפי האזרחים של הצד היריב.¹⁰

דוגמה לפעולות לוחמת סייבר בעלת השפעה פסיכולוגית היא תקיפת רשתות מחשבים לצורכי השפעה. מטרתן של תקיפות אלה היא לייצר תחושת פגיעה מהותית בלי להוציא לפעול פגיעה שכוו. תקיפות לצורכי השפעה נועדו לטעת תחושה של חוסר ביטחון, פגיעה בריבונות וחוסר יכולת להגן על אורח החיים הנורמטיבי. תקיפות כאלה ישיגו את התוצאה הרצויה על-ידי שימוש בטקטיקות כמו פגיעה באתרי ממשל; שליחת הודעות פוגעות לאזרחים; השבתת אתרי תקשורת לפרקי זמן מוגבלים ועוד.¹¹ תקיפות אלה כוונתן לשבש את סביבת המידע של היריב, באמצעות פגיעה בתשתיות המידע שלו. הפעולות הללו הן למעשה מאמצי השפעה המבוצעים במרחב הסייבר. מדובר בתקיפות של מערכות ממוחשבות שמיועדות להשפיע על הרגשות, על ההתנהגות ועל תהליכי קבלת ההחלטות של אוכלוסיית המטרה, באמצעות שליטה במידע המועבר במערכות אלה. ניתן להשיג זאת על-ידי סוגים שונים של מתקפות סייבר שיעודן מניעת גישה לשירות, הפרעה לשגרת החיים, העברת מסר פוליטי או אידיאולוגי, אך המהות אינה גרימת נזק אסטרטגי בלתי הפיך או מתמשך.

לדוגמה, שימוש בהתקפות מניעת שירות מבזורות (DDoS) שמהותן גרימת עומס פניות אל מחשב או שירות אינטרנטי מסוים, באופן שחורג מסף היכולת שלו לספק מענה עד כדי השבתה של השירות.¹² אחת השיטות המתמקדת בניסיון ליצור פגיעה תדמיתית היא באמצעות השחתת חשבונות של אנשים פרטיים או גורמים ציבוריים ברשתות חברתיות ובאתרי האינטרנט (Defacement). שיטה זו כוללת שתילת מסרים פוגעניים בעמוד הראשי או בחשבון ברשת חברתית; הכנסת תעמולה שהתוקפים מעוניינים להפיץ לקהל רחב ופגיעה תדמיתית בארגון. רמה גבוהה יותר של תחכום תושג על-ידי תקיפות של מערכות המידע והמחשוב של הארגון כדוגמת שרתים, מערכות מחשב, מאגרי נתונים, רשתות תקשורת ומכונות לעיבוד נתונים. הנזק הפוטנציאלי כולל פגיעה בשירותים חיוניים כמו בנקים, שירותי סולר ודואר אלקטרוני. תקיפות מסוג זה יתמקדו בדרדירכלל במחיקת מסמכים או בחשיפה של פרטים מסווגים, ביוש (shaming) ציבורי וסחיטה באמצעות הדלפת תמונות פרטיות, מידע, רשימות לקוחות וקוד, בחשיפת פרטים אישיים כמו מספרי תעודות זהות, סמאות, מיילים ואף כתובות פיזיות.¹³

1. שיבוש מסרי התעמולה של האויב.
 2. הפצת מקרי צביעות ופשיעה של האויב במגעיו עם אוכלוסיות בסיכון.
 3. הנעת מתנגדי היריב להילחם בו במדיה בצורה יעילה יותר.
- בפיקוד פועל צוות מיוחד הנקרא DET (צוות התערבות דיגיטלית – Digital Engagement Team), שכולל אנשי צוות השולטים בשפות שונות: ערבית, אורדו, פרסית, רוסית ועוד. אנשי היחידה מפעילים חשבונות טוויטר, פייסבוק ואינסטגרם, שפונים לציבור הרחב במדינות יעד ברחבי מזרח התיכון ובמרכז אסיה במטרה להעביר את המסרים הרצויים לקידום האינטרסים האמריקניים.¹⁶
- רוסיה**
- על פי תפיסתו של הצבא הרוסי ההפעלה הצבאית הטקטית בשטח והאסטרטגיה המדינית הבינלאומית מהווים חלקים אינטגרליים ושלובים של הרעיון המערכתי. כנגזרת מתפיסה זו, לוחמת סייבר ומבצעים תודעתיים הם מאמצים משולבים, המכוונים לתמרן את התנהגות הקורבן. אלה כוללים תקיפת רשתות ממוחשבות, לוחמה פסיכולוגית, הונאה, הטעייה וזריעת דיסאינפורמציה. מאמצים אלה מאפשרים להנחית על המערכת היריבה מהלומת מידע שמשלבת אלמנטים דיגיטליים, אלקטרוניים ותודעתיים.¹⁷
- כאשר רוסיה מוציאה לפועל מתקפה צבאית, היא עושה זאת תחת

במרבית המקרים, הלוחמה הפסיכולוגית של הצבא מופנית לאוכלוסייה האזרחית באזורי העימות, ומיועדת להעביר את תמיכתה מכוחות הגרילה אל הלוחמים האמריקניים



מעטה כבד של חשאיות ביחס לעצם קיומה של הפעילות וביחס למטרותיה. כמעט כל פעולה צבאית רוסית תוצג על-ידיה כפעילות לשמירת שלום או כהתערבות במשבר הומניטארי. שטוש מטרותיה האמיתיות של רוסיה תורם להחלשת היריב ולהעצמת תרמיתה של רוסיה. במידה ורוסיה נכשלה בהשגת מטרה שחשובה לה – היא יכולה לבחור מטרה אחרת בלי שהדבר ייתפס כלפי חוץ ככישלון, ובכך לשמר את תרמיתה.¹⁸

דוקטרינת לוחמת המידע הרוסית איננה חדשה, והיא מבוססת במידה רבה על הדוקטרינה הסובייטית בנושא. זו מוגדרת על בסיס המונח "שליטה תגובתית". משמעות מושג זה היא העברת מידע מסוים לגורם מסוים, במטרה לגרום לו לבצע את הפעולות הרצויות לצד היוזם. בהתאם לכך, המסרים שרוסיה תעביר לצד היריב במסגרת לוחמת מידע וקמפינים של דיסאינפורמציה יהיו כאלה שיחזקו תחושות של ייאוש ויחזקו גילויי עריקות.¹⁹ בנוסף, רוסיה מנסה לפגוע בתשתיות חיוניות, ולחזור תחת המכנים הפוליטיים, הכלכליים והחברתיים של הצד היריב.²⁰

לוחמת מידע ולוחמה פסיכולוגית על סוגיהן השונים, תופסות חלק נכבד באסטרטגיה הצבאית הרוסית. ההסתמכות הגדולה על לוחמת

מידע נובעת מהכרתה של רוסיה בחולשתה הצבאית והכלכלית בייחוד למול ארצות-הברית וסין. לפיכך, רואה רוסיה בלוחמת המידע אסטרטגיה צבאית בעלת יתרון כפול: מצד אחד, היא מסוגלת להטעות את האויב בנוגע לכוונותיה האמתיות, ומצד אחר היא מפחיתה באופן משמעותי את ההשקעה הכלכלית הנדרשת במקרה של עימות צבאי מבחינת עלות-תועלת בהשוואה לאמצעים קינטיים.²¹

בריטניה

בשנת 2015 הוקמה בבריטניה חטיבה 77 שמטרתה להוציא לפועל מבצעי לוחמה פסיכולוגית ברחבי העולם. פעילות החטיבה מתבצעת במקומות בהם הכוחות הבריטיים מעורבים בפעילות צבאית ממושכת.²² בחטיבה יש שש יחידות, כל אחת ממונה על היבט אחר של המבצעים הפסיכולוגיים. לדוגמה יחידה מס' 1 אחראית על ניתוח ההתנהגות של קהלי היעד.²³

אחת מדרכי הפעולה של החטיבה היא פגיעה בגורמים הנלחמים נגד בריטניה באמצעות הפצת שמועות ודוניות. החטיבה כוללת עובדים וחיילים בעלי רקע בסייבר, פסיכולוגים ואנשי תקשורת, בשירות סדיר ובשירות מילואים. בנוסף, החטיבה מיועדת לעסוק בשיקום תשתיות אזרחיות ובהגשת סיוע הומניטרי באזורי לחימה, במטרה לצבור תמיכה ברעת הקהל המקומית. בעת הקמתה תוכנן כי סדר הכוח של החטיבה ינוע בין 1500 ל-2000 משתתפים, מהם כ-40% אנשי מילואים.²⁴ החטיבה צפויה להגיע לכשירות מבצעית מלאה בסוף שנת 2019.²⁵

בספטמבר 2018 הודיעה בריטניה כי במטרה להתמודד עם איום הסייבר הגובר מצד רוסיה והצורך להמשיך לבצע פעילות סייבר התקפית נגד דאעש וארגוני טרור נוספים, בכוונתה לחזק את יכולות הסייבר ההתקפיות שלה. לשם כך תקים יחידה חדשה שתכלול כ-2,000 אנשי צוות ותקציבה יעמוד על 250 מיליון ליש"ט.²⁶

גוף נוסף במערכת הביטחון הבריטית שתומך את מאמצי הצבא בתחום מבצעי התודעה במרחב הסייבר הוא ה-Joint Threat Research Intelligence Group (JTRIG), הפועל כחלק מסוכנות הביון והסייגנט GCHQ. היחידה כוללת מאות עובדים מתחומים שונים (סייבר, פסיכולוגיה, מודיעין, מומחי תוכן ושפות) שפועלים בשלוש מחלקות אופרטיביות – לוחמה בטרור, ביטחון פנים ונושאים בין-לאומיים, ובמחלקות נוספות לסיוע מבצעי דוגמת סייבר, משפט, כלכלה וכדומה. היחידה תומכת את מבצעי הצבא במשימותיו ברחבי עולם, ומסייעת בפעילות גופי ביטחון פנים וביון בתוך המדינה ומחוצה לה. במסגרת פעילותה מפעילה היחידה כלי לוחמת סייבר התקפיים בהם תקיפות מניעת שירות, הפלת אתרים ועוד, וכן כלים טקטיים באזורי קונפליקט בהם פועלת בריטניה.²⁷

גוף נוסף הפועל תחת משרד ההגנה הוא מרכז המציאות שמופעל בקבלנות על-ידי תאגיד BAE Systems. מטרת המרכז היא לחקור תחומים כמו הבנת התנהגות אוואטרים ברשתות החברתיות, תפיסות קוגניטיביות בפעילויות סייבר וטכניקות ללוחמת סייבר להשפעה על דעת קהל. המרכז הוקם בשנת 2012 ומתוקצב על-ידי משרד ההגנה בסכום של כשבעה מיליון ליש"ט לשנה.²⁸

פעילות לוחמת תודעה וסייבר של ארצות-הברית מול "המדינה האסלאמית"

במרוצת השנים פיתח ארגון דאעש ("המדינה האסלאמית") יכולות מתקדמות מאוד ברשתות החברתיות. הארגון הצליח לרתום את



הפגזת מבנה של דאעש. פוסט שהעלה לוחם דאעש כלל צילומים של בניין פיקוד של הארגון. חיל האוויר האמריקני הצליח לזהות את מיקום הבניין ולהרוס אותו, פחות מ-24 שעות לאחר מכן

סמאות הכניסה אליהם ומחק תוכן תעמולתי של הארגון, כמו קטעי וידאו שצולמו באזורי הקרבות.³²

ההתקפה הידועה המתוכננת ביותר של הכוחות האמריקניים בוצעה על-ידי ה-NSA ופיקוד הסייבר הצבאי, במסגרת מבצע "סימפונייה זוהרת" שמטרתו הייתה לשבש את מנגנון התעמולה המוצלח של הארגון. במסגרת המבצע שיצא לפועל ב-2016 השיגו יחידות הסייבר האמריקניות סמאות והרשאות למחשבים של אנשי דאעש. לאחר מכן חסמו באמצעותן גישה לנכסים אינטרנטיים, ומחקו מידע ששימש לתעמולה ולגיוס. המבצע הוכתר בהצלחה, אך זו הייתה זמנית בשל מעבר הארגון לשרתים אחרים, מאובטחים יותר. מבצעים אחרים הופעלו על-ידי פיקוד הסייבר, ומטרתם הייתה איתור פעילים באמצעות דחיקתם מחשבונות קיימים, זאת במטרה לגרום להם להשתמש בכלים פחות מאובטחים שייחשפו את מיקומם ובכך יתאפשר סיכולם באמצעות מל"טים.³³

מעבר לפגיעה בפן הטכני, הייתה למבצעים משמעות פסיכולוגית: כאשר מפקדי הארגון ופעיליו הבינו כי פעולותיהם אינן מאובטחות, התערערה תחושת הביטחון שלהם. האתגר המרכזי הניצב בפני אנשי הסייבר האמריקנים היה ועודנו העובדה שפעילי דאעש השתמשו במחשבים לא בשביל לפתח מערכות נשק, אלא בשביל לגייס פעילים חדשים, לממן פעילות טרור ולתאם התקפות טרור עתידיות. מדובר בפעילות מתמשכת ורציפה, והטרוריסטים נהנים מיתרון יחסי בשל הנגישות לטכנולוגיות הצפנה וזלות.

האמריקנים ניסו להפעיל את פיקוד הסייבר נגד דאעש במדינות נוספות, אך פעולות מסוג זה עוררו מחלוקות בתוך הממשל ומחוצה לו. המחלוקת הראשונה נוגעת לייעילותן של מתקפות סייבר כאלו, כלומר האם פעילות הסייבר האמריקנית באמת הצליחה לשבש את פעילותן המקוונת של היריב. בעוד שפיקוד הסייבר ומחלקת ההגנה הגדירו את המבצעים מוצלחים, בכירים יוצאי קהילת המודיעין הטילו ספק בהצלחתם. הסיבה למחלוקת נעוצה בשוני שקיים בין שני הגופים בהגדרת הצלחת מבצעי סייבר: בעוד שמחלקת ההגנה ופיקוד הסייבר מגדירים הצלחה

הרשתות באופן יעיל ביותר, במטרה לאתר ולגייס מצטרפים פוטנציאליים לשורותיו. לשם כך הוקמו אתרי אינטרנט ופרופילים רבים ברשתות החברתיות, שפנו לצעירים בכל רחבי העולם. משום כך, הצורך של הממשל האמריקני להילחם בארגון ברמה התודעתית והמודיעינית היה מורכב, וחייב שילוב יכולות על-ימנת להטות את המערכה לטובתו.

הפעלת לוחמת תודעה במערכה

מחלקת הלוחמה הפסיכולוגית ב-CENTCOM מפעילה שיטה מרכזית להפצת מסרים באמצעות עריקים מדאעש. העריקים סיפקו עדויות שיכולות לערער את המסרים שדאעש מעוניין להפיץ. לדוגמה הם סיפרו לא פעם שהצטרפו לשורות הארגון על-ימנת להילחם במשטר הסורי וב"כופרים", אולם בפועל הם מצאו את עצמם נלחמים מול מוסלמים כמותם. הפעלת המתנגדים לדאעש נעשת בשפתם דרך האינטרנט. על-ימנת להבין מי תומך בדאעש ומי מתנגד לפעילות הארגון, הצוותים מבצעים חיפושים של מילות מפתח שונות, שיוצרות זיהוי של תומכי הארגון ומתנגדיו במטרה להפיץ את המסרים המותאמים.²⁹

לצד מסרים שמנסים לערער את אמינות היריב, היחידה פועלת על-ימנת ליצור זיקה לערכים אותם מייצג המערב, בקרב קהלי היעד. כדי להשיג את התוצאה הרצויה הפכו מסרי היחידה במרוצת הזמן ממסרים לעומתיים, למסרים שמנסים ליצור דיאלוג וסקרנות. ההנחה היא שחשיפת עובדות על המערב יוצרת סקרנות בקרב קהל היעד, במטרה לחשוף אותו להשקפות המערביות וליתרונות הדמוקרטיה. בנוסף, נעשה שימוש בפרסומים של אנשי דאעש לטובת איסוף מודיעין והקמת בנק מטרות לצורך תקיפה פיזית. לדוגמה, פוסט שהעלה לוחם דאעש כלל צילומים של בניין פיקוד של הארגון. חיל-האוויר האמריקני הצליח לזהות את מיקום הבניין ולהרוס אותו פחות מ-24 שעות לאחר מכן.³⁰

הפעלת גופי סייבר במערכה

בסוף 2015 הורה מזכיר ההגנה האמריקני אשטון קרטר להקים כוח משימה ייעודי נגד תשתיות דאעש ברשת, שהוכפף לפיקוד הסייבר האמריקני. בסתיו 2016 הוקם הכוח בשם ARES תחת פיקוד הסייבר של ארצות הברית השייך למשרד ההגנה והכוחות המזוינים (USCYBERCOM), ובו לקח חלק מרכזי פיקוד הסייבר של הצבא (ARCYBER), בשיתוף זרועות המודיעין האמריקניות. פעילות כוח המשימה התמקדה בשיבוש יכולתו האופרטיבית, ובפעילות נגד רשת התקשורת של דאעש שיעודה גיוס פעילי טרור. פעולותיו המרכזיות של ARES היו פריצה לחשבונות ברשתות החברתיות ולתיבות דואר אלקטרוני של חברי הארגון ושינוי סמאות; פגיעה במידע המאוחסן על שרתים הקשורים לארגון; ושיבוש או השמדה של רשתות תקשורת בהן השתמשו פעילי הארגון לצורך תקשורת פנימית.

באפריל 2016 פתח פיקוד הסייבר במתקפה על רשת המחשבים של הארגון. מטרת המתקפה הייתה לפגוע ביכולות הפיקוד והשליטה, באמצעות שיבוש האפשרויות של הארגון לבצע פעולות לוגיסטיות שונות כמו גיוס פעילים חדשים, העברת תשלום לפעילים הקיימים והפצת פקודות. חלק מן הפעילות כלל הטמנת כלי סייבר שונים לצורכי איסוף מידע ברשתות הארגון, על-ימנת ללמוד את הרגלי הפעילים.³¹ בד בבד, פגעה פעילות הסייבר האמריקנית ביכולת של הארגון להפיץ את מסרי התעמולה שלו: בסוף שנת 2016 פרץ הפיקוד לחשבונותיהם של מומחי תעמולה בדאעש, שינה את

כשיבוש זמני בפעילות האויב, מומחי המודיעין מחפשים פגיעה ארוכת טווח, שאותה לטענתם קשה להשיג במבצעים מסוג זה. הארגון יכול לשחזר חלק מפעילותו או להעבירה לשרתים אחרים, ובכך השפעת המבצע נחלשת.³⁴ עם זאת, ממחקר שפורסם באוגוסט 2018 המבוסס על חומר ארכיוני מסווג שנחשף על אודות מבצע "סימפוני זוהרת", עלה שבמקביל לביצוע המבצע חלה ירידה משמעותית בפעילותו של הארגון ברשת. מכך הסיקו החוקרים כי המבצע השיג את מטרותיו באופן מיטבי.³⁵ מחלוקת נוספת נוגעת להשפעת מבצעי לוחמה מסוג זה (אך גם השפעת מבצעי סייבר באופן כללי) על יחסי ארצות-הברית עם בעלות בריתה. חלק מן השרתים בהם משתמשים אנשי דאעש נמצאים בשטחי בעלות בריתה של ארצות-הברית, ולכן פעולה נגד שרתים אלה היא למעשה ביצוע פעולות התקפיות בשטחן הריבוני. לכן, יש מחלוקת בממשל האמריקני בדבר השאלה אם ארצות-הברית צריכה לתת התראה מראש לבעלות בריתה לפני הוצאה לפועל של מבצעים כאלה. גורמים ב-FBI, CIA ובמחלקת המדינה טוענים שהוצאה לפועל של פעולות מסוג זה ללא תיאום מראש עלולה לפגוע בשיתוף הפעולה בין המדינות בלוחמה בטרור ובתחומי המודיעין. בנוסף, מחלקת ההגנה טוענת כי הודעה מוקדמת על מבצעי סייבר עלולה לגרום לדליפת פרטים רגישים מהמבצעים ולפגוע בסיכויי הצלחתם.³⁶ מקרה זה משקף את האיסימטריה הבסיסית המאפיינת את כללי המשחק בניהול מערכה על התודעה. יש לקחת בחשבון כי מבצעי

השפעה ארוכת-טווח של שימוש בלוחמת סייבר התקפית. ארצות-הברית התמקדה במערכה נגד מטרות "דכות" כמו אתרים וחשבונות רשתות חברתיות, לטובת שיבוש תקשורת בין פעילי המדינה האסלאמית, איסוף "מודיעין מטרות" ושיבוש תקשורת המיועדת לגיוס פעילים חדשים. אמנם הצלחתם של מבצעים אלה ברורה, אולם הטענה נגד מבצעי סייבר התקפיים אלה היא שהשפעתם זמנית וכת חלוף.

שגרה מול חירום. בעוד שהמאמץ האמריקני הופעל בחירום, כלומר בעת קונפליקט צבאי וכחלק מהקואליציה הבינלאומית נגד דאעש, נשאלת השאלה האם ישנה בעיה אינהרנטית להפעיל את יחידות הצבא הייעודיות להשפעה גם בשגרה, לטובת יצירת השפעה ארוכת טווח מול קהל היעד. האם למשל אותו המודל שהופעל מול ארגון טרור יכול להיות מופעל כמב"ם (מערכה בין המלחמות) בצורה סמויה או חשאית?

סיכום

המבצע האמריקני נגד דאעש משקף את האיסימטריה הבסיסית המאפיינת את כללי המשחק בניהול מערכה על התודעה. מעצם טבעו, דמוקרטיית ליברליות כמו ארצות-הברית מחויבות לכללים של אחריות מדינית, מתאפיינות בהיעדר הסכמה פנימית המונעת גיבוש מסר אחיד, ובסרבול בירוקרטי ופוליטי. עם זאת, מבצעי הצבא האמריקני כנגד המדינה האסלאמית היוו תקדים, מכיוון שהייתה זו הפעם הראשונה שבה הופעלו יכולותיו ההתקפיות של פיקוד הסייבר במערכה צבאית ושיטות הפעולה נוסו לראשונה בזמן אמת.

כיום רשת האינטרנט והרשתות החברתיות הפכו לגורם המשפיע על התנהגות החברה האנושית ולכלי מרכזי להשפעה ולעיצוב תודעה, גם בעת מערכה צבאית. כאשר אחד הצדדים משבש את סביבת המידע שעליה מסתמך היריב, הוא משבש את יכולתו לתפוס את המציאות כהלכה ולגבש מולה צעדי פעולה אפקטיביים. בדרך זו, הצד היוזם יוצר לעצמו יתרון במערכה הכוללת באמצעות ערעור הלגיטימציה של הצד השני ופגיעה באמינות טענותיו. פעולה שכזו מובילה גם לערעור אמינותם של גורמים לגיטימיים כמו התקשורת, גורמי אקדמיה ומומחי תוכן.

בצה"ל יש כמה גופים שעוסקים בצורה ישירה ובצורה עקיפה בתודעה ובהשפעה, ביניהם מחלקת תודעה באגף המבצעים במטכ"ל;³⁷ יחידות הגנת סייבר באגף המודיעין;³⁸ גדודים באגף התקשוב;³⁹ דובר צה"ל⁴⁰ ועוד.

כיום, יכולתם של גופים אלה למקסם את שיתוף הפעולה בתוך המערכת ומחוצה לה מוגבלת. זאת למרות הכלים האופרטיביים שעומדים לרשות הצבא לצורך ביצוע מבצעי סייבר, ויצירת השפעה באופן ישיר (באמצעות דובר צה"ל), חשאי או סמוי. כדי לעמוד ביעדים במסגרת לוחמה כזו, יש צורך לנהל מערכה שתכלול פעילות פרו-אקטיבית ברבדים גלויים וברבדים סמויים.⁴¹ הדרך להשיג זאת היא בניית סל יכולות שיכלול פיתוח אמצעי השפעה ייעודיים, המותאמים לעולם הרשתי בכלל ולרשתות החברתיות בפרט, מתוך הבנה שגם הצבאות המתוחכמים והמתקדמים ביותר צריכים לפעול במקומות החשופים והגלויים ביותר כמו עולם הרשתות החברתיות.

העצרות למאמר הזה מתפרסמות בסוף הגיליון.

דוקטרינת לוחמת המידע הרוסית מוגדרת על בסיס המונח "שליטה תגובתית". משמעות מושג זה היא העברת מידע לגורם מסוים, במטרה לגרום לו לבצע את הפעולות הרצויות לצד היוזם



הצבא האמריקני נגד דאעש היוו תקדים מבחינת הפעלת פיקוד הסייבר במערכה צבאית, וכנגזרת מכך פיתוח הטכנולוגיות, כלי התקיפה ושיטות הפעולה נוסו לראשונה בזמן אמת. עם זאת, ניתן לזהות מספר מגבלות בהפעלה המשולבת של אמצעי תודעה ולוחמת סייבר:

שיתוף פעולה בינלאומי. הצורך לפעול בשטחן של מדינות יחידות דורש שיתוף פעולה מצדן, שעשוי לפגוע באפקטיביות של המבצעים נגד נכסי דאעש. במקרים מסוימים התקשו הכוחות האמריקנים לפעול באופן חשאי, בשל הדרישה לעדכן ולבקש אישורים לפעילות סייבר התקפית.

סנכרון הפעילות. תיאום המאמץ האמריקני בין יחידות הצבא השונות, וכן מול מעגל רחב יותר של ארגוני ביטחון ודיפלומטיה, הקשה על מאמצי הצבא בהפעלת הכוח. בנוסף נראה כי לאורך המערכה ברשת נגד דאעש, עברה האחריות על תיאום ותכלול המאמץ בין כמה גופי ביטחון, החל ממחלקת המדינה ועד מחלקת ההגנה, דבר שהקשה על ביצוע הפעילות באופן שוטף ומסונכרן.

