גיליון מס׳ 11 אוגוסט 2015

מרכז המחקר, המכללה לביטחון לאומי

שתונות

אומנות אופרטיבית קיברנטית:
מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית

דימה אדמסקי

מרכז המחקר
המכללה לביטחון לאומי

עשתונות

גיליון מס׳ 11

אומנות אופרטיבית קיברנטית:

מבט מזווית לימודי האסטרטגיה ומפרספקטיבה השוואתית

דימה אדמסקי

אוגוסט 2015, אב התשע״ה

עורכת: סגן-אלוף נאוה גרוסמן-אלוני

אודות המחבר: דר׳ **דימה אדמסקי**, מרצה בכיר בבית הספר לממשל, אסטרטגיה ודיפלומטיה במרכז הבינתחומי בהרצלייה ועמית מחקר במרכז המחקר של המכללה לביטחון לאומי. הוא שימש כעמית מחקר בתכנית ללימודי ביטחון באוניברסיטת הארוורד ובמכון לחקר מלחמה ושלום של אוניברסיטת קולומביה בניו יורק. תחומי התמחותו הם ביטחון בינלאומי, לימודי אסטרטגיה, תרבות אסטרטגית והיסטוריה צבאית מודרנית. מחקריו בנושאים אלו התפרסמו בארץ ובעולם בכתבי עת אקדמיים מובילים. ספריו: ׳מבצע קווקז׳ (מערכות, 2006) ו׳תרבות אסטרטגית וחדשנות צבאית׳ (מערכות, 2012) זכו בפרס צ׳צ׳יק לחקר ביטחון ישראל. במסגרת תפקידיו בצה״ל ובמשרד הביטחון, עסק במחקר מודיעיני ובתכנון אסטרטגי של מדיניות ביטחונית. בתפקידו האחרון שימש כעוזרו של מזכיר הוועדה לגיבוש תפיסת הביטחון (׳ועדת דן מרידור׳).

על העטיפה: ׳אודיסאוס והסירנות׳, ציור מאת ג׳ון ויליאם ווטרהאוס, 1891. המילה ׳סייבר׳ (cyber) נגזרת מהמילה היוונית ׳קיברנטיקה׳ (κυβερνήτης), המתייחסת לניווט ולתהליך קבלת החלטות במערכות מורכבות. ממקור זה אף נגזרה המילה ׳קִבֶּרְנֶטִי׳ (ביוונית kibernan) המתייחסת למנהיג הספינה, למנווט. בתמונה, מנווט אודיסאוס את ספינתו דרך אי הסירנות - אתגר רב ממדי, מהמסוכנים ומהמורכבים במסעו. באי, המוקף סלעים וצוקים, שרו הסירנות את שירתן הענוגה והיפה. מלחים שחלפו ליד מקום ושמעו את שירתן, נפלו בקסמן, איבדו את עשתונותיהם וקפצו מספינותיהם אל מותם. אתגר הסירנות, אם כן, מגלם סכנה פיזית, הנגזרת מסכנה תודעתית. אודיסאוס, שביקש לשמוע את שירתן, מבלי לסכן את יעדי מסעו, ציווה על מלחיו לאטום את אוזניהם בדונג ולקשור אותו לתורן הספינה, כך שלא יוכל להשתחרר ולקפוץ אל מותו, חרף השפעתן המניפולטיבית של הסירנות. כך זכה אודיסאוס לשמוע את שירתן ולהישאר בחיים, חרף המהלומה התודעתית. הדבר ממחיש את הניסיון לעצב התנהגות פיזית, באמצעות השפעה וירטואלית-תודעתית. מאמץ זה מונח בלבת הגישה הרוסית ההוליסטית לסייבר המובאת בגיליון זה.

הקדמה

תפיסתו של המרחב הקיברנטי במונחים של מרחב פעולה צבאי התפתחה מאד בעשור האחרון. תופעה חדשה זו הניעה התארגנות של מנגנוני מדינה וממסדים ביטחוניים ברחבי העולם. המהפכה הדיגיטלית לובשת שני פנים: האחד מתייחס למהלך הדיגיטליזציה כהשתנות הטומנת בחובה פוטנציאל חדש, מנקודת המבט של השגת יעדי הממסד; ואילו הפן השני מתייחס להופעת המרחב הקיברנטי כתווך חדש למימושן של אינטראקציות אסטרטגיות ואופרטיביות, כ'מגרש משחקים' חדש, המאפשר פעולה לשם השגת תכלית פוליטית. מדובר בשינוי סדרי עולם, המתבטא בטשטוש הגבולות בין מושגים מסורתיים, אשר באמצעותם נערכו הסדרות תבוניות בעניינים הצבאיים: טושטשו הגבולות בין 'מלחמה' ל'שלום', בין הממד הפיזי לווירטואלי, בין התחום הצבאי לאזרחי, בין הפרטי לציבורי ולבינלאומי, בין מאמץ מודיעיני איסופי לבין מאמץ מבצעי עיצובי, בין מהלך הגנתי למאמץ התקפי, בין תחרות למידה, מרוצי חימוש וזליגה של יכולות בין שחקנים מדינתיים ללא מדינתיים. בקרב המומחים, הן בארץ והן בעולם, מתקיים בירור אודות פוטנציאל ההשפעה של העוצמה הקיברנטית על קידום מטרות הביטחון הלאומי. ממד הסייבר נתפס כממד צבאי עצמאי או ככזה המשולב באחרים. בעוד שתובנות אלו נשענות על בקיאות במאפיינים הטכניים והטקטיים של העולם הקיברנטי, הרי שניכר, כי בשלב זה, הבנתנו את הפוטנציאל המערכתי של העידן הקיברנטי עודנה דלה יחסית. מסמך זה נועד להניח נדבך ולבסס תאוריה אסטרטגית אודות היכולת הקיברנטית בתחום המערכתי. דר' דימה אדמסקי, הנע במסעותיו האינטלקטואלים במרחב הקיברנטי, במרחבי המהפכות בעניינים צבאיים ובעקבות ה'אחרות' הרוסית, מציע בחיבור זה תובנות הנובעות מחקירתו. באמצעותן, ניתן לברר את המורכבות הקוגניטיבית של העידן הדיגיטלי החדש, למקם אותה בהקשר התאורטי של לימודי האסטרטגיה ולהשתית עולם מושגים, שיאפשר לקיים דיון ביקורתי, שיטתי ובונה

על אודות אומנות המערכה הקיברנטית. בחיבור זה יש ניסיון לקיים בירור עיוני אודות מקומו של ממד הסייבר ביחס למרחבי הפעולה הצבאיים המסורתיים, לאפיין את הייחודיות האסטרטגית ואת הטבע האופרטיבי של המרחב הקיברנטי כמרחב פעולה, להתבונן באופן שבו מדינות מגדירות מחדש את האסטרטגיות שלהן, בהקשרו של המרחב הקיברנטי, ולאתר אופנים חדשים של פעולה אסטרטגית, כפי שהם מומשגים לאחרונה וכפי שהם מתממשים.

היסטורית, בנוסף למרוצי חימוש, עודדה התהוותה של חדשנות צבאית תחרות למידה אגרסיבית בין קהילות אסטרטגיות שונות. החדשנות הקיברנטית ממחישה מגמה זו היטב, שכן במהלך העשור האחרון בוחנים פרקטיקנים ותאורטיקנים כיצד ניתן ליישב את העקרונות של המחשבה הצבאית הקלאסית בהקשר החדש, או מפתחים עולם מושגים ורעיונות חדש וייחודי להקשרה של החדשנות הנוכחית. גיליון זה של עשתונות מציע תובנות על אודות אומנות המערכה בתחום הקיברנטי, ומציג את המסע של המחשבה הצבאית הרוסית אל מרחב זה, כדרך ללמוד על עצמנו באמצעות העמדה של מחקר השוואתי.

הניתוח המרתק של התפתחויות הממד הקיברנטי ברוסיה, ערש 'אומנות המערכה', מאפשר לנו ללמוד פרק בהלכות תפיסה מערכתית אסטרטגית מושרשת וקוהרנטית, המביאה לידי ביטוי גם את ה'אחרות' הרוסית ושורשיה. בנייר מונחת מסגרת מושגית וידע בדבר ניסיונם של ממסדים ביטחוניים לאמץ לעולמם את המהפכה הדיגיטלית ועל אודות המרחב הקיברנטי כתווך חדש למימושן של אינטארקציות אסטרטגיות. בכירים בקהילת הסייבר בישראל והעוסקים בסוגיית העוצמה הקיברנטית בהקשר רחב יותר של האסטרטגיה הישראלית, בוודאי ימצאו עניין בדברים.

הקוראים מוזמנים להגיב.

בברכת למידה פורייה,

יוסי בידץ, אלוף
מפקד המכללות

תוכן העניינים

מבוא[1]

נייר זה מניח, בדומה למחקרים רבים בתחום, כי הופעתו של המרחב הקיברנטי והפיכתו לכלי מערכתי בקרב כל סוגי השחקנים, היא מן החדשנויות הצבאיות העיקריות בימינו (major military innovation) מדובר בתמורה דרמטית באומנות המערכה, אשר יש חוקרים המגדירים אותה כ׳מהפכה בעניינים צבאיים׳ (RMA - Revolution in Military Affairs). מדובר בחדשנות צבאית רדיקלית, שבמסגרתה מבנים ארגוניים חדשים, לצד תפיסות הפעלה חדשות - שבדרך כלל, אם כי לא תמיד, מתבססות על טכנולוגיות חדשות ואמצעי לחימה חדשים - משנים את אופייה של המלחמה.

למהפכה כזו ביטויים אסטרטגיים וטקטיים רבים, אולם בדרך כלל היא בולטת דווקא בהקשר של האומנות האופרטיבית הצבאית וברמה המערכתית של ניהול המלחמה. המונח ׳מהפכה׳ אינו מעיד בהכרח על שינוי מהיר, אולם הוא מרמז על כך שהשינוי הוא עמוק ומשמעותי ושהוא עתיד לגזור שיטות לחימה אפקטיביות יותר מהקודמות. לכן, ל׳מהפכה בעניינים צבאיים׳ חשיבות רבה בהקשרי הסייבר, משום שהיא מאבחנת את השינוי בסביבה ומחוללת את השינוי הפרדיגמטי, כלומר, הופכת את צורות הלחימה הקיימות למיושנות. על כן, העמדת החקירה של תופעת הסייבר בהקשר של מסגרת תאורטית של חדשנות צבאית ושל RMA, מתאימה ליצירת תובנות בתחום אומנות המערכה.

בין אם מדובר בחדשנות מהפכנית ובין אם באבולוציונית, מבחינת האקלים האינטלקטואלי והלכי הרוח במחשבה הצבאית, מזכירה ההתהוות הנוכחית תקופות היסטוריות אחרות, בהן התפתחו חדשנויות צבאיות משמעותיות. כך לדוגמה, מתכתבת התקופה הנוכחית עם שנות העשרים והשלושים של המאה הקודמת, כאשר

המחשבה הצבאית התמודדה עם מהפכת המיכון (הופעתם של הטנק והמטוס), או לחלופין עם שנות הארבעים והחמישים, כאשר המחשבה הצבאית ניסתה להפנים את משמעויות הגרעון והטילאות. בשני המקרים, כמו בחדשנויות צבאיות רבות אחרות, תחילה הכירו הקהילות האסטרטגיות את היכולות הטכנולוגיות והפעילו אמצעי לחימה חדישים, ורק לאחר מכן, תוך מאמץ מתמשך ופתלתל, המשיגו את משמעותם של כלי הלחימה החדשים לאומנות המערכה, ועמדו על ההשלכות לבניין הכוח, ארגונו והפעלתו.

הסייבר אינו יוצא מכלל זה. חדשנות צבאית בכלל, כמו בשתי הדוגמאות שהוזכרו לעיל, וחדשנות קיברנטית בפרט, מעלה שאלות תפיסתיות חדשות על אודות הדרך שבה על הקהילה האסטרטגית להתאים את עצמה ואת הכוחות המזוינים שלה לתופעה החדשה, במקרה הנדון - למהפכה הדיגיטלית. על כן, חקירה של עולם הסייבר, באמצעות העמדתו ביחס לחדשנויות צבאיות אחרות לאורך ההיסטוריה, עשויה להועיל אם נכיר במגבלותיה של גישה זו. האתגר האינטלקטואלי הוא בכך שסייבר, כחדשנות צבאית, אינו משנה כהוא זה את הנחות היסוד של החשיבה האסטרטגית. אולם, בשל ייחודיותו הטכנו-טקטית, כמו חדשנויות רבות צבאיות לפניו, הוא דורש פיתוח של אומנות אופרטיבית, שתאפשר לממש את ההיגיון האסטרטגי בהקשר ייחודי. יודגש, כי מהפכה זו ייחודית יחסית לקודמותיה, בין השאר, בכך ששחקנים לא מדינתיים או מדינתיים למחצה, כגון מעבדות קספרסקי, שחקנים פרטיים ותעשיית ההיי-טק, נמצאים באינטראקציה מתמדת עם ממסדים ביטחוניים, ולעתים אף מקדמים מטרות מנוגדות. הדיאלקטיקה המתמדת בין המגזר הביטחוני-מדיני לבין המגזר העסקי-טכנולוגי אפיינה פחות את המהפכות הקודמות בעניינים צבאיים. שם מדובר היה על פי רוב בדינמיקה טורית, כאשר פריצת דרך טכנולוגית אפשרה חדשנות צבאית רדיקלית.

מאחר שבדרך כלל ההתפתחות הטכנולוגית גדלה, משתכללת ומופעלת מהר יותר משמתגבשת תאוריה אסטרטגית בעניין אותה יכולת, מסתייעים פרקטיקנים בתאורטיקנים לשם ליבונן של שאלות יסוד, הנוגעות לחדשנות צבאית נתונה. בעת התהוותה של תופעה אסטרטגית חדשה, מקובל מאוד, במיוחד בקהילות אסטרטגיות מערביות, להעביר במיקור חוץ לתאורטיקנים באקדמיה ובמכוני המחקר את העיסוק בשאלות היסוד. מומחים ללימודי אסטרטגיה, העוסקים היום בתיאורה, הסברה והמשגתה של ההתנהגות האסטרטגית הקיברנטית, שואפים לצמצם את אי הוודאות בתחום מערכות הסייבר. כמו בשאר המקרים של חדשנות צבאית, מנסים המומחים ללימודי אסטרטגיה להשתמש בטרמינולוגיה צבאית קלאסית, להתאימה לתופעות חדשות ואף ליצור המשגה חדשה כדי לתאר תופעה חסרת תקדים. החקירה מתמקדת בתיאור המאפיינים של התופעה, בהבלטת השאלות האופרטיביות הנחוצות ובפיתוח של המשגה ורעיונות מערכתיים עבור פרקטיקנים. ככלל, ידע חדש מתגבש באמצעות חקירה אינטנסיבית, המתנהלת בחוגים תאורטיים ופרקטיים, תוך השראה, למידה הדדית והעתקה ממקום אחד למשנהו.

השיח האקדמי המחקרי של לימודי האסטרטגיה בסייבר כבר מציע מכלול של תובנות, טיפולוגיות, אנלוגיות וכן השערות מתחרות בשאלות היסוד של אומנות המערכה. במהלך העשור האחרון, באופן הדרגתי, יצרו גופים שונים בקהילה האקדמית המערבית, בראש ובראשונה בארצות הברית ובמדינות ברית נאט״ו, מַסָּד ידע משמעותי בנושא הסייבר. מסד ידע זה אינו מתיימר לספק תשובות נחרצות לשאלות היסוד, כי אם להציג פרספקטיבות ורעיונות שונים, שיאפשרו שיח, חשיבה ועשייה בקרב פרקטיקנים בתחום.

מסמך זה מתחקה אחר דיוני לבה אלו, ובהיעדר קונצנזוס מחקרי, מציע לקורא סינתזה תמציתית של עיקרי התובנות העולות מעשרות מחקרים, מאמרים מקצועיים וספרים על אודות ׳אומנות המערכה

הקיברנטית[1]. שימוש במונח זה כאן מבטא ניסיון לאמץ מושג צבאי קלאסי ולהתייחס באמצעותו לתאוריה ולפרקטיקה של עיצוב, תכנון וניהול של מערכות ברמה האופרטיבית בעידן הקיברנטי. על כל שאלת יסוד בשיח, יציג מחקר זה שתי דעות שונות או מתחרות, בבחינת ניגודיות משלימה, בהנחה כי הדבר עשוי לתרום לחשיבתם של פרקטיקנים ישראלים בעניינה.

מחקר זה סוקר את השיח האקדמי העוסק בהשפעת יכולות הסייבר על עיצוב וניהול המערכות הצבאיות ומציג חמש שאלות יסוד, המונחות בלבת השיח האקדמי על אודות אומנות המערכה קיברנטית:

השאלה הראשונה - האם הופעתן של יכולות הסייבר מהווה מהפכה בעניינים צבאיים?

השאלה השנייה - כיצד משפיעות יכולות הסייבר על היחס בין התקפה להגנה?

השאלה השלישית - מהו טבע ההרתעה במרחב הקיברנטי, והאם אסטרטגיה זו, לצד הרעיון של התרעה מוקדמת, ישימים במרחב זה?

השאלה הרביעית - האם יכולת הסייבר מעצימה שחקנים מדינתיים עתירי עוצמה טכנולוגית וכלכלית, או דווקא שחקנים שאינם ניחנים במאפייני העוצמה הקלאסיים, כגון מדינות חלשות או שחקנים לא מדינתיים?

השאלה החמישית - האם הופעתו של המרחב הקיברנטי תורמת או מערערת את היציבות האסטרטגית, כלומר, האם היא מעלה את את מספרם, עוצמתם, היקפם וממדיהם של החיכוכים האופרטיביים בין השחקנים במערכת הבינלאומית, מקרבת או מרחיקה עימות אסטרטגי?

חשוב לציין, כי תחרות הלמידה בשאלות היסוד של אומנות המערכה הקיברנטית מתנהלת אצל שחקנים אסטרטגיים שונים, מדינתיים ולא מדינתיים, צבאיים ואזרחיים, פרטים וציבוריים, ולא רק בקהילות הידע המערביות, ובכלל זה ישראל. פיתוח תאוריה אסטרטגית והפקת לקחים מהפרקטיקה הקיברנטית מתרחש גם אצל שחקנים מדינתיים ולא מדינתיים, כגון: איראן, צפון קוריאה, סין, רוסיה, סוריה, חזבאללה, חמאס ודאעש. בשל תרבות אסטרטגית שונה בקרב השחקנים, המשגה של שאלות היסוד ותהליכי פיתוח הידע משתנים משחקן אחד למשנהו. מדובר למעשה בתחרות חקירה קריטית, שכן שחקן אשר יגיע מהר יותר לתובנות מתקדמות ומתוחכמות יותר, ידו תהיה על העליונה.

מתוך הכרה זו, מוקדש פרק נפרד לסקירת החשיבה האסטרטגית הרוסית אודות אומנות המערכה הקיברנטית. חקירתו של מקרה הבוחן הרוסי משתלבת היטב בהקשר החקירה הישראלית בשל מספר טעמים: ראשית, מוסכם בקרב מומחים עולמיים, כי לרוסיה מסורת עשירה של המשגת חידושים טכנולוגיים, טרם הטמעתם בארגז הכלים הצבאי בכלל, והמשגה ייחודית של אומנות המערכה הקיברנטית בפרט. שנית, יחסית למדינות ולשחקנים אחרים, הצטבר ברוסיה ניסיון אופרטיבי עשיר ומגוון בתחום לחימת הסייבר, אשר משמש חומר להפקת לקחים ובבחינת ׳מעבדה תפיסתית׳, הן למומחים רוסים והן לאלו שבמערב. שלישית, מקרה הבוחן הרוסי משמש כזרז למידה בתחום הסייבר לשחקנים שונים בזירה האזורית והעולמית, ואף מהווה דרך ללמוד על עצמנו באמצעות העמדה של מחקר השוואתי. כלומר, דרך המקרה הרוסי ניתן להכיר את מכלול הסוגיות באומנות המערכתית ואת הגישות להתמודדות עמן. כמובן, אין להעתיק את הלקחים מהמקרה הרוסי כהווייתם, אלא לאמצם כפלטפורמה שתעודד חשיבה ביקורתית בהקשר ישראלי קונקרטי. חשיבה באמצעות אנלוגיות היסטוריות ואמפיריות ושימוש במקרה בוחן

כמסגרת התייחסות הם כלים שימושיים ללמידת ההקשר האופרטיבי הייחודי של ישראל.

מחקר זה מבדיל בין שתי קטגוריות עיקריות של התנהגות אסטרטגית במרחב הסייבר: בין חתרנות במרחב הדיגיטלי (digital abuse) לצרכים כגון פשע קיברנטי, ריגול קיברנטי ופורצים-מתנדבים המקדמים אינטרסים מדינתיים כלשהם (hacktivists), המפילים למשל אתרים מסוימים באמצעות התקפות DDoS או מנהלים מערכה על התודעה. המנעד יכול לכלול השבתה ושיבוש של מערכות מידע, פגיעה באיכות המידע, וגניבת מידע; לבין לחימה קיברנטית (cyber warfare) כגון תקיפה רשתית (Cyber Network Exploitation/Attack - CNE/CNA) של מערכות לאומיות חיוניות (לדוגמה, מערכות פיקוד ושליטה של תעשיות ותשתית אזרחית וצבאית, או יכולות קיברנטיות שהופעלו במקרה של הווירוס 'סטאקסנט'). מחקר זה סוקר את המאפיינים של שני סוגי לחימה אלו.

המחקר בנוי כדלקמן: הפרק הראשון מציג את התובנות העולות מחמש שאלות היסוד של אומנות המערכה הקיברנטית מתוך דיוני הלבה של לימודי האסטרטגיה. הפרק השני בוחן את הגישה הרוסית לאומנות המערכתית הקיברנטית ומבליט את ייחודיותה. הפרק השלישי מציע לקחים, תובנות וחומר למחשבה לטובת דיון ביקורתי ועיצוב של האומנות האופרטיבית הקיברנטית הישראלית.

פרק א׳ - דיון ביקורתי בשאלות היסוד של אומנות המערכה הקיברנטית

שאלת היסוד הראשונה[2] היא האם כניסתן של יכולות הסייבר לארגז הכלים הצבאי מהווה מהפכה בעניינים צבאיים? האם הסייבר הוא ממד חמישי של הלחימה או רק מרכיב המשתלב בארבעת הממדים המסורתיים של הלחימה, קרי - יבשה, ים, אוויר וחלל?

מהפכה בעניינים צבאיים היא חדשנות צבאית רדיקלית, וככל שיקדימו מומחים להכיר ולהבין את שבירת הרצף באופייה של המלחמה, כן ייטב. אמנם הכרה מוקדמת של התמורות בסביבה האסטרטגית ושל ה-RMA, במקרה הזה בתחום הסייבר, אינה מתכון קסמים לניצחון, אולם, קיימת סבירות גבוהה לכך שמי שיצפו מוקדם יותר את התרחשות ה-RMA ויערכו שינויים בהתאם, יחזקו מאוד את יעילותם הצבאית. מנגד, איחור יביא לתוצאה הפוכה. מחיר השגיאות עלול לנוע בין חוסר יעילות מערכתית, עם השלכות אופרטיביות כבדות משקל, עד לאסונות אסטרטגיים, שלהם תוצאות הרסניות בתחום הביטחון הלאומי.

על כן, תשובה לשאלת היסוד הראשונה בהקשר הקיברנטי תאפשר למוסד צבאי באשר הוא להתבונן בעצמו באופן ביקורתי, להחליט על היקף הרפורמה הדרושה, וזו בתורה תשליך על מגוון החלטות תקציביות, ארגוניות ופיקודיות בתחום בניין הכוח והפעלתו.

הסבורים כי הופעתה של העוצמה הקיברנטית אכן מהווה מהפכה בעניינים צבאיים טוענים, כי מאז הקמת רשת האינטרנט העולמית הגלובלית (www) הפך המרחב הווירטואלי לתחום עשייה אנושי לכל דבר ועניין, לרבות אינטראקציות אסטרטגיות מזוינות. על פי גישה זו מקנה טכנולוגיית המידע יכולות הרס ושיבוש בסדר גודל חסר תקדים,

במיוחד בהשוואה ליכולות הלוחמה האלקטרונית (ל״א) בעידן טרום תקופת הדיגיטציה הגלובלית. יתרה מזאת, לצד יכולת לייצר נזק קינטי אדיר ורחב ממדים, בכוחה של יכולת זו, להבדיל ממהפכות קודמות, להסב נזק מוגבל, מבוקר, מגוון, זמני והפיך, ועל כן היא מאפשרת שליטה חסרת תקדים במנעד הנזקים. לשיטתם, יכולת קיברנטית בעניינים צבאיים, אשר צמחה מתוך היגיון הלוחמה האלקטרונית, אינה ממשיכה אותה, כי אם מהווה שינוי מהותי (discontinuity).

יכולות לוחמה אלקטרונית שימשו כמכפיל כוח בלחימה הקונבנציונלית במרחבים מסורתיים, אך לא היו מסוגלות לייצר באופן עצמאי, אף לא בהקשרים גרעיניים, אפקטים אסטרטגיים מרחיקי לכת. לעומת זאת, טוענת אסכולה זו, מסוגלת העוצמה הקיברנטית, בדומה לעוצמה הגרעינית או האווירית, להשיג אפקטים אסטרטגיים תוך דילוג על שדה הקרב הקונבנציונלי. היא מאפשרת להטיל את הרצון האסטרטגי על כל יריב במרחבי הגלובוס מבלי לכבוש את שטחו, מבלי לייצר הרס מסיבי ומבלי שנורית ולו ירייה אחת. על פי גישה זו עשויה התקפה קיברנטית מוצלחת לשתק הן את הרצון והן את היכולת של היריב להמשיך להילחם. על כן, סייבר הוא תחליף מערכתי ולא תוספת אופרטיבית ללחימה קונבנציונלית.

כמכפיל וגם כמשתק את כל העוצמות המסורתיות, עשוי השימוש בסייבר, לדעת מומחים שונים, לחולל אפקטים מערכתיים ואסטרטגיים גם באופן עצמאי. על כן, על פי גישה זו, לוחמת סייבר (ל״ס) (CNA/E) היא כלי מערכתי עצמאי וחדשנות צבאית מהפכנית. זאת, מאחר שהיא מפחיתה את הצורך בלחימה במרחבים מסורתיים (domains) ואינה דורשת זמן ומרחב פיזי תחום; מסוגלת לייצר אפקטים מערכתיים ואסטרטגיים מדויקים, במהירות, תוך שליטה בהרס פיזי, באופן שעוצמה קונבנציונלית אינה מאפשרת; מרחיבה את מגוון האפשרויות האסטרטגיות, במיוחד במערכות בתקופה שבין

׳מלחמה׳ ל׳שלום׳ מסורתיים; מאפשרת להשיג אפקטים, שבעבר היו אפשריים רק באמצעות מערכות קינטיות, ועושה זאת מתחת לסף האלימות, אשר תודעתית נתפס כפעולה מלחמתית של ממש; ומאפשרת הקרנת עוצמה בזמן ובמרחב, אשר מבטלת את ההבדל המסורתי בין עימותים קרובים ומרוחקים.

ביטוי מובהק להנחת היסוד המקצועית, שתופסת את לוחמת הסייבר כמהפכה בעניינים צבאיים, הוא ריבוי גופים צבאיים חדשים, לרוב פיקודים עצמאיים, אשר זוכים לסמכויות רחבות לא רק בתחום בניין הכוח, אלא גם בתחום הפעלתו, וזאת לעתים במקום מבצעים במרחבים מסורתיים (ראו דוגמאות מהמקרים: האמריקאי, הסיני, הצפון קוריאני והאיראני). יודגש, כי ההנחה שלוחמת סייבר היא מהפכה בעניינים צבאיים וממד לחימה חמישי, היא נפוצה יותר בקרב פרקטיקנים, מאשר בקרב תאורטיקנים של לימודי האסטרטגיה באקדמיה.

מנגד, דעה ספקנית יותר, אשר אינה רואה בלוחמת הסייבר מהפכה בעניינים צבאיים, אלא חדשנות צבאית הדרגתית, גורסת כי היא המשך ישיר ואף חלק אינטגרלי מהמהפכה בעניינים צבאיים מבוססת המידע (RMA-IT), אשר פקדה את הממסדים הצבאיים מסוף שנות השבעים. על פי גישה זו, מדובר רק בשכלול יכולות הלוחמה האלקטרונית (ל״א) נגד מערכות שליטה ובקרה (שו״ב), תקשוב, מודיעין ורכישת מטרות (C4ISR).

בתוך כך, נתפסת לוחמת הסייבר כמרכיב וכהמשך של שתי דוקטרינות צבאיות המוכרות כבר קרוב לעשור - לחימה מבוססת רשת (NCW - Network Centric Warfare) ולחימה מבוססת אפקטים (EBO - Effect Based Operations). גישה זו אינה רואה בלוחמת הסייבר ממד עצמאי, שכן לשיטתה לא ניתן לחולל באמצעותו אפקטים

מערכתיים, מחוץ לארבעת ממדי הלחימה הקלאסיים. יתרה מזאת, על פי אסכולה זו, מתקפה קיברנטית רחבת היקף אינה אפשרית בהגדרה, בשל קישוריות הדדית בין המערכות, כך שתקיפה משמעותית על תשתיות לאומיות של היריב, לדוגמה, תשתית פיננסית ותשתית אנרגיה, עלולה לייצר נזק אגבי ואפקטים מסדר שני, אשר מהר מאוד ישליכו על הצד התוקף. על כן, יכולות לוחמת סייבר הן מוגבלות, פרט לתרחישים מסוימים המהווים המשך למבצעים המסורתיים. כמו כן, יכולת זו, במנותק ממבצעים בממדים אחרים, קרי, שלא במסגרת מערכה משולבת, היא חסרת כל משמעות אופרטיבית.

על כן, גורסת אסכולה זו, יש לתפוס את לוחמת הסייבר כהמשך משוכלל או כמכפיל כוח של הלחימה בממדים המסורתיים. מצדדי אסכולה זו אף טוענים, כי בשלב זה, מוקדם עדיין לקבוע קטגורית בעניין, משום שטרם הצטבר די ניסיון מערכתי אמפירי, שיאפשר להכריע בעניין. עובדתית, להוציא מספר מקרים של לוחמת סייבר, שגם עליהם אין לנו תמונה מלאה, טרם התרחש מפגש מערכתי בין שני שחקנים שהפעילו יכולות לוחמת סייבר, באופן שניתן יהיה לכנות את האירוע כ׳מלחמת הסייבר הראשונה׳. על כן, אסכולה זו רואה בסייבר רק חדשנות צבאית הדרגתית ומבקשת להתייחס אליה בעירבון מוגבל, מבחינת שיקולי תקציב, בניין הכוח וארגונו.

שאלת היסוד השנייה היא כיצד יכולת קיברנטית משפיעה בשדה המערכה על היחס בין ההגנה להתקפה? האם לוחמת סייבר מקנה יתרון לצד התוקף או לצד המגן? [3]

מבחינה היסטורית, כל חדשנות צבאית שינתה את היחס הדיאלקטי בין שתי צורות הלחימה הבסיסיות - הגנה והתקפה. כך, לדוגמה, המהפכה בניידות האסטרטגית (המבוססת על המצאת הקיטור, מסילות הברזל, הטלגרף ושיפורים בעוצמה, בקצב ובדיוק האש), אשר באה לידי ביטוי מלא במלחמת העולם הראשונה, הקנתה יתרון

מערכתי לצד המגן; המהפכה בניידות הטקטית (המבוססת על מנוע בערה פנימי ואלחוט, שאפשרו מיכון אווירי ויבשתי ושליטה ובקרה באמצעות רדיו) ואשר באה לידי ביטוי מובהק במלחמת העולם השנייה, הקנתה יתרון לצד התוקף. זאת ועוד, המהפכה הגרעינית-טילית, דחקה למעשה שאלה זו לשוליים, באמצעות דוקטרינת ההרתעה, בעוד שהמהפכה מבוססת מערכות המידע (RMA-IT), שביטויה העיקרי היה ׳תשלובת מודיעין-מהלומה׳ (חימוש מונחה מדויק, נשק מנגד, מערכות שו״ב ומודיעין, הפועלים כמכלול מערכתי אחוד) טשטשה למעשה את ההבדל בין שתי צורות הקרב. כעת, בעידן הדיגיטלי, בולטות בקרב תאורטיקנים של לימודי האסטרטגיה שתי אסכולות מתחרות בעניין דיאלקטיקת ההגנה-התקפה.

אסכולת ׳יתרון ההתקפה׳ טוענת, כי ראשית כל מבחינת המחיר, מרחב הסייבר מייקר את ההגנה לעומת ההתקפה. כדי להמחיש זאת, מאמצת אסכולה זו את אנלוגיית ׳אפקט המחט והבלון׳. על מנת לבצע דקירה אחת מוצלחת יש לרכז מאמץ בנקודה אחת ולהשיג אפקט מערכתי. ניתן לבחור את המקום ואת הזמן לצורך מיקוד המאמץ. לא כך הבלון, אשר יש להגן כל העת על כל שטח הפנים שלו, כשאין יודעים מתי והיכן תתרחש הדקירה. אנאלוגיה זו נועדה להמחיש את חוסר הפרופורציה במשאבים שעל הצד המגן להשקיע, לעומת הצד התוקף, ולרמוז על יתרונה של ההתקפה על ההגנה.

אסכולה זו טוענת, כי על ההגנה להצליח כל העת, בעוד שדי בהתקפה אפקטיבית אחת, שכן הצד התוקף הוא שבוחר את המקום והזמן. במקור, עוצבו המחשבים והרשת באופן שמאפשר חיבור וקישוריות בצורה מרבית וקלה, דבר שהפך את הניסיון לחסום את כל ההתקפות לבלתי אפשרי מבחינה טכנית. כמו במקרה של מכה גרעינית ראשונה, שאין נגדה הגנה אפקטיבית, אלא הרתעה בלבד, כך גם לא קיימת, על פי גישה זו, הגנה אפקטיבית בסייבר.

שנית, על פי אסכולה זו, קיים הבדל גם במהירות התגובה, קרי, בקצב המערכתי. מבחינה כרונולוגית, לעולם תקדים ההתקפה את המענה ההגנתי. לא ניתן להמציא מענה לווירוס או לקוד עוין, לפני שאלו נוצרו והופעלו במסגרת התקפה. האנטי וירוס בנוי על מאגרי מידע של וירוסים מוכרים. כמו כן, הצד התוקף יכול לשנות את חתימתם של כיווני ההתקפה, מהר יותר מאשר הצד המגן יכול לטפל בפריצות ובפגיעות, נוכח פרק הזמן הממושך הדרוש לשם פיתוח המענה.

שלישית, יכולות התקפיות מסוימות - לדוגמה, התקפה לשם שלילת השירות (DoSD) - יכולות לגייס תמיכה ברשת לסוג כזה של תקיפה (Offensive Botnet Armies). לעומת זאת, על פי גישה זו, הצד המגן אינו יכול לגייס תמיכה הגנתית ברשת והוא נמצא במצב של פיצול בין המגזר הציבורי לפרטי. הדבר מאפשר, בשל היעדר שיתוף פעולה הדוק בין השניים, כיווני חדירה מגוונים, וכתוצאה מכך, פגיעות מובנית. לבסוף, קוד התקפי עוין יכול לחדור לתוך מערכות קורבן ההתקפה ולהימצא בהן עד יום פקודה - מצב שמבחינה תאורטית מהווה חולשה מובנית של ההגנה נוכח ההתקפה.

מנגד, קיימת אסכולה, הרואה את היחס בין ההגנה להתקפה באופן מאוזן יותר. ראשית, גורסת גישה זו כי בניית יכולת סייבר התקפית (CNA), המאפשרת הרס משמעותי - כמו מקרה ה׳סטאקסנט׳ - היא פעולה מורכבת במיוחד, הדורשת משאבים רבים, תשתית טכנולוגית משוכללת ומאמץ מערכתי, ועל כן היא מכבידה מאוד על הצד התוקף ומקלה על הצד המגן. הגם שמרחב הסייבר נשלט בידי נטיות התקפיות בתחום הפשע הדיגיטלי, ריגול ואקטיביזם, אין כן בתחום הצבאי. מצב זה מתבטא, על פי הגישה זו, בכך שטרם היינו עדים למהלכים התקפיים רחבי היקף. שנית, על פי אסכולה זו, אף אם פעולה התקפית משמעותית אכן מתרחשת, אזי הנזק שהיא מסבה הוא הפיך, בצורה מהירה וזולה יחסית, מאחר שיש אפשרות להסתייע ברשת ובמקורות

גלויים (on line open source), כפי שהתרחש במקרה ה׳סטאקסנט׳. שלישית, הצד המגן מסוגל להקנות יתירות למערכות מחשוב וכן להפוך את הסביבה הדיגיטלית ללא מוכרת ולמורכבת לחדירת התוקף, לרבות שימוש בהונאה, בהטעיה ובמלכודות, שעלולות לסבך את הצד התוקף ולחשוף את זהותו.

כאשר החל השיח התאורטי, רווחה בו הטענה בדבר עליונות ההתקפה במרחב הסייבר. אולם, בשנים האחרונות, כנראה כביטוי ללמידה מהניסיון המצטבר, החלה ההגנה להיתפס כאפקטיבית יותר והיחס בין השתיים נעשה מאוזן יותר.

שאלת היסוד השלישית היא האם אפשרית הרתעה במרחב הדיגיטלי? ואם כן, אזי מהי מהותה ומהי זיקתה להתראה המוקדמת? [4]

הרתעה היא שימוש באיום, שנועד להשפיע על התחשיב האסטרטגי של היריב במטרה לשמר את הסטטוס קוו, קרי, את המציאות האסטרטגית שהתהוותה במצב נתון בין שני שחקנים (לעומת זאת, כפייה היא שימוש באיום, שנועד לשנות את המציאות האסטרטגית). הרתעה מונעת התנהגות אסטרטגית לא רצויה, על ידי שכנועו של היריב, כי היתרונות הצפוים לו מהמהלך שהוא שוקל לנקוט או מהמגמה המערכתית שהוא שוקל לחולל, מתגמדים מול העלויות האסטרטגיות הנלוות. על כן, ראוי כי תכנית ההרתעה תשכנע את הצד השני, כי הרווח הצפוי לו מאי תוקפנות הוא משמעותי ואכן צפוי להתממש.

החשיבה האסטרטגית מבדילה בין שתי צורות הרתעה: האחת באמצעות שלילה, והשנייה באמצעות ענישה. הסוג הראשון מתייחס לפעולות השוללות את ההישגים המצופים על ידי היריב ומותירות אותו עם מחיר התוקפנות. בקטגוריה זו נכללות יכולות הגנה אקטיבית ופסיבית לסוגיהן, המאותתות ליריב על הקושי להשיג את מבוקשו. סוג

ההרתעה השני מתייחס לפעולות, המענישות את היריב על ניסיונו לשנות את הסטטוס קוו. בקטגוריה זו נכללות יכולות התקפיות לסוגיהן, המאותתות ליריב על סוג העונש והיקפו, אשר עתידים להתלוות למהלך שהוא שוקל ליזום. כרונולוגית, שלילה מופעלת לפני הענישה, ולעתים אף במקביל אליה, ואילו ענישה יכולה להתרחש בזמן ובמקום שונים ואף בעוצמות גבוהות יותר. יודגש, כי בדיון אודות ההרתעה בהקשר הקיברנטי, לעתים אין מחדדים את ההבחנה בין שתי שאלות שונות: האם ניתן להרתיע תוקפנות באמצעות סייבר? לבין השאלה - האם ניתן להרתיע תוקפנות קיברנטית? הדיון כאן מתייחס בעיקר לשאלה השנייה.

הטענה הרווחת בשנים האחרונות היא כי להבדיל מתחומים אחרים של אינטראקציות אסטרטגיות, כגון הממד הגרעיני והקונבנציונלי, בהן התמסדה תאוריית ההרתעה במרחב הקיברנטי, לאור מאפייניו הייחודיים, ההרתעה, על שתי צורותיה, אינה מכשיר יעיל. אסכולה זו שוללת את ייתכנותה של 'הרתעה באמצעות ענישה' ממספר טעמים: ראשית, היא מדגישה את בעיית הייחוס (attribution). האנונימיות של המרחב הדיגיטלי אינה מאפשרת לקבוע במהירות את זהות התוקף (לעתים הוא אף לא יתגלה), ועל כן, אינה מותירה כתובת ברורה לפעולת תגמול. בעוד שהתקפה אנונימית יכולה לארוך שניות, הרי שאיסוף הראיות וגילוי העקבות (forensics) לשם זיהוי התוקף, יכולה לארוך חודשים. על כן, אין אפשרות לאיים על התוקף באופן אמין.

שנית, הרתעה באמצעות ענישה מדגישה את בעיית אמינות היכולות. גם אם נניח, כי מרחב הסייבר נתפס כממד שבו ההגנה נשלטת על ידי ההתקפה, מגלים שחקנים אסטרטגיים נטייה מובהקת להסתיר את יכולותיהם ההתקפיות תחת מעטה כבד של סודיות. להבדיל מהממד הגרעיני או הקונבנציונלי, מניחים שחקנים כי גילוין של היכולות ההתקפיות, המתקיים בעיקר באמצעות שימוש אופרטיבי בהן, מאפשר לצד השני להתחיל לשקוד על פיתוח המענה, והופך את היכולת

ההתקפית לבלתי רלבנטית ולכלי חד פעמי (Use it and loose it), אם כי במסגרת תחרות למידה מתמדת ורחבה הרבה יותר.

שלישית, מי שמטילים ספק בהרתעה מצביעים על בעיית הא-סימטריה הדיגיטלית - הצד התוקף עלול להתגלות כ׳לא מספיק דיגיטלי׳, על מנת ששחקן כלשהו יוכל להסב לו נזק קיברנטי משמעותי, דבר שעלול להפוך אותו לבלתי מורתע. כמו כן, הרתעה, על פי גישה זו, יכולה אולי להצליח מול ה-CNA, אבל תהיה אפקטיבית פחות מול סוגים אחרים של חתרנות ואיסוף קיברנטי. בנוסף, אותה אסכולה מטילה ספק גם באפקטיביות של ׳הרתעה באמצעות שלילה׳ שכן, תאורטית, עליה להיות מבוססת על הגנה אפקטיבית, בעוד שדעה רווחת מטילה ספק בעוצמתה של ההגנה מול תוקפנות קיברנטית. על כן, לא ניתן לשדר לצד השני כי תוקפנות פוטנציאלית מצדו נדונה לכישלון.

בנוסף, אותם ספקנים מדגישים את הקושי בהתראה מוקדמת בתחום הסייבר. מול אתגרים קונבנציונליים, על קונבנציונליים ותת קונבנציונליים, פיתחו מערכות המודיעין לאורך השנים תורה של חיפוש אחר סימנים מעידים, ועל בסיס ראיות אלו הן מספקות התראה מוקדמת אודות הכנות אופרטיביות של הצד השני להתקפה. לרוב, בפרקטיקה המודיעינית הקלאסית, דובר, לדוגמה, על איתור של תנועה וריכוז כוחות בגזרות ההתעניינות או בסמוך לגבול, הכנת מצבורי אמל״ח, העלאת כוננות במערכי התקיפה, וסימנים רבים נוספים. בתחום הסייבר, יישום הפרוצדורה המודיעינית הזו מאבד מהרלבנטיות שלו, מאחר שהכנות לקראת תקיפה קיברנטית, על בסיס הידע העומד לרשותנו, אינן מייצרות חתימה מודיעינית ברמה דומה.

זאת ועוד, עוצמה קיברנטית מאפשרת להחדיר יכולות עוינות למערכות דיגיטליות של היריב מבעוד מועד, תוך טשטוש העקבות, ולהפוך אותה ליכולת התקפית רדומה, שתתחיל לייצר אפקטים אופרטיביים קונקרטיים רק בעקבות הפעלתה ביום פקודה, יהיה אשר יהיה. מצב

מעין זה הופך את ההתרעה המודיעינית המסורתית לחסרת משמעות. אם כך, מאחר שהתראה מוקדמת אינה אפשרית, אין דרך אפקטיבית להעלות את הכוננות במערכים ההגנתיים ברגע האמת, ועל כן הרתעה באמצעות שלילה לוקה בחסר באופן משמעותי ואינה אפשרית.

מנגד, התגבשה בשנים האחרונות אסכולה המקדמת תפיסה אלטרנטיבית בדבר האפקטיביות והרלבנטיות של אסטרטגיית ההרתעה בתחום הסייבר. ראשית, לשיטתה, על ההרתעה בסייבר להתבסס על היכולת להפגין יתירות וחוסן קיברנטי (cyber resilience) - קרי, יכולת לאבחן את ההתקפה מיד עם התרחשותה, לספוג מכה קיברנטית, למזער תוך פרק זמן קצר את הנזק שנגרם ולחזור לתפקוד שגרתי של המערכות. יכולת זו של חוסן קיברנטי היא וריאציה של הרתעה באמצעות שלילה. (אם כי נשאלת השאלה האם כושר כזה המקנה חסינות, הוא מייצב או מערער יציבות אסטרטגית).

שנית, לדעת אסכולה זו, אף על פי שייחוס פעולה מסוימת ברשת לגורם מסוים (אטריבוציה קיברנטית) היא מורכבת, הרי שהיא בהחלט אפשרית. יכולות גילוי הראיות (forensic capabilities) משתפרות כל העת ומקבלות תשומות אינטלקטואליות, ארגוניות ופיננסיות משמעותיות. יתרה מזאת, לטענתם, ייחוס הפעולה נעשה לא רק באמצעות כלים דיגיטליים, אלא גם דרך דיסציפלינות איסוף ומחקר מודיעיניים מסורתיים. שהרי תקיפה קיברנטית היא פעולה מערכתית, שנועדה לקדם מטרה מסדר גבוה יותר, ועל כן, עליה להיות מלווה, כמו כל פעולת כפייה אחרת, במסר אסטרטגי, שאמור להשפיע על התנהגותו האסטרטגית של היריב. לכן, ניתן באמצעות ניתוח המגמות בהקשר האסטרטגי והאופרטיבי, תוך שילוב של מידע מודיעיני וראיות דיגיטליות, לאבחן את החשוד העיקרי בתקיפה.

ככל שמדובר בתקיפה קיברנטית משמעותית יותר, הדורשת יכולות רב מערכתיות, כך הולך ומצטמצם מעגל החשודים האפשריים. יתרה

מזאת, אסכולה זו גורסת כי הקושי של קורבן ההתקפה לייחסה לגורם מסוים יכול להתגמד מול המאמצים והמשאבים הרבים, שעל יזם התקיפה להשקיע בטשטוש עקבותיו - משימה קשה, המקיימת זיקה דיאלקטית לשיפור ולפיתוח בתחום הגילוי והזיהוי.

שלישית, אסכולה זו גורסת, כי גם איום והרתעה באמצעות ענישה אפשריים, הן בזכות יכולת ׳מכה שנייה׳ קיברנטית, והן בשל ׳א-סימטריה הפוכה׳ - יכולת לגבות מחיר באמצעים לא קיברנטיים, קונבנציונליים ואף בלתי קונבנציונליים, במיוחד אם וכאשר מדובר ביריב שלא ניחן בחתימה דיגיטלית משמעותית. גישה זו, המוכרת הן בקהילה האסטרטגית והן בקהילה האקדמית האמריקנית כהרתעה בין ממדית (cross domain deterrence), היא בגדר המדיניות הרשמית של ארצות הברית מול תוקפנות קיברנטית פוטנציאלית.

נראה, כי יחס דו ערכי להרתעה מאפיין את תהליך הלמידה שעוברת קהילת המומחים בשנים האחרונות. ניכר, כי כיום פחתה הספקנות כלפי ההרתעה במרחב הדיגיטלי, הן בתצורת הענישה והן בתצורת השלילה. המקרה של הזיהוי האמריקאי את התוקפנות הקיברנטית הצפון קוריאנית (2015) והענישה הקיברנטית שהוטלה על פיונגיאנג כתוצאה מכך, עשויה להוות אירוע מכונן, שבעקבותיה יחלו שחקנים אסטרטגיים בעולם להתייחס לממד ההרתעה בכובד ראש יותר מבעבר.

שאלת היסוד הרביעית היא האם יכולות הסייבר מעצימות שחקנים מדינתיים עתירי עוצמה צבאית, טכנולוגית וכלכלית, או דווקא שחקנים שאינם ניחנים במאפייני העוצמה הקלאסית, כגון מדינות חלשות או שחקנים לא מדינתיים?[5]

האסכולה הגורסת, כי יכולות הסייבר מעצימות את השחקנים החזקים, טוענת כי בראש ובראשונה הדבר קשור למאפייניה האובייקטיביים של יכולת לוחמת הסייבר (CNA). רק שחקנים

חזקים, קרי מדינות עתירות עוצמה טכנולוגית משמעותית ומשוכללת, יהיו מסוגלים לפתח יכולת התקפית קיברנטית. מדינות חלשות טכנולוגית ושחקנים לא מדינתיים ייוותרו מאחור ולכל היותר יהיו מסוגלים ליזום חתרנות קיברנטית בלבד (digital abuse), אשר לא תסב נזק ברמת הביטחון הלאומי. שנית, שחקנים א-סימטריים יהיו מסוגלים להפיק תועלת מערכתית ואסטרטגית מהסטטוס ומהיכולות שלהם רק עד רמה מסוימת, לא קריטית, קרי מתחת לרף של אינטרסי הלבה של הביטחון הלאומי. שלישית, עוצמה קיברנטית, על פי גישה זו, מקבלת משמעות רק כאשר היא נתמכת על ידי עוצמות לאומיות אחרות, והיא חסרת משמעות אסטרטגית כאשר היא מופעלת בפני עצמה.

על לוחמת סייבר להסתמך על עוצמה צבאית קונבנציונלית, פוליטית וכלכלית, אם היא מבקשת לייצר הישגים אסטרטגיים. כך, למשל, ניתן אולי לשתק ולשבש לזמן מה את התפקוד של התשתית הדיגיטלית הלאומית, כפי שעשתה רוסיה באסטוניה, בגרוזיה ובאוקראינה, אלא שההצלחה המערכתית בעקבות הפעולה הושגה באמצעות ממדים אחרים של עוצמה - פוליטית, כלכלית וצבאית. לוחמת סייבר, על פי גישה זו, אמנם מייצרת תנאים מערכתיים, בדומה לעליונות אווירית, ובכך מהווה מכפיל כוח ייחודי, אך היא אינה תנאי מספיק להשגת השפעה אסטרטגית. ככזו, העוצמה הקיברנטית אך מעצימה את פערי היכולות והעוצמות הקיימים בין השחקנים, אך אינה מגשרת ביניהם.

מנגד, על פי גישה אלטרנטיבית, יכולות לוחמת סייבר, באשר הן, מעצימות באופן משמעותי את השחקנים החלשים, קודם כל בכך, שהיא מגוונת את ארגז הכלים האסטרטגיים שלהם ואולי בפעם הראשונה בהיסטוריה מאפשרת להקרין עוצמה ולייצר אפקטים במרחקים גאוגרפיים, באופן שבעידן הקדם דיגיטלי, כאשר לרשותם עמדו רק יכולות קינטיות, לא היה כלל מתאפשר.

שנית, בניגוד לנטען לעיל, אסכולה זו מצביעה על מגמת ההוזלה של יכולות הסייבר ועל נגישות גוברת והולכת של שחקנים ׳חלשים׳ ליכולות, שעד לאחרונה היו נחלתם הבלעדית של שחקנים ׳חזקים׳. במקרים מסוימים, המחיר של מה שבשנה שעברה היה נחשב ליכולת קיברנטית מתקדמת ביותר, הולך ויורד, משום שקוד התקיפה הופך לנחלת הכלל (מקור גלוי) ונתון להנדסה מחדש (reverse engineering). בנסיבות אלו, לא נדרשת מומחיות פיתוח מתקדמת. במובנים רבים, מגמה זו מתכתבת עם תופעת הלחימה ההיברידית, כאשר שחקנים לא מדינתיים מצטיידים ביכולות צבאיות, שעד לאחרונה אפיינו רק שחקנים מדינתיים.

לבסוף, כמות יכולה בנסיבות מסוימות להפוך לאיכות. מספר רב של שחקנים א-סימטריים חלשים בעלי יכולות הקרנת עוצמה בממדים גלובליים, הפועלים בזירות שונות במקביל, מחוץ למרחב הדיגיטלי, אכן מסוגלים, בתיאום, להציג אפקטים אסטרטגיים משמעותיים ולהסב נזק מערכתי, שבעבר לא היו מסוגלים לחולל.

שאלת היסוד החמישית היא האם הופעתו של המרחב הקיברנטי תורמת ליציבות האסטרטגית או לחילופין מערערת אותה, לשון אחר, האם הוא מעלה את מספרם, עוצמתם, היקפם וממדים של החיכוכים האופרטיביים בין השחקנים במערכת הבינלאומית?[6]

זווית הסתכלות אחת רואה בהופעת הסייבר תרומה ליציבות האסטרטגית נוכח שורה של גורמים: ראשית, סייבר מאפשר תפקוד אסטרטגי מתחת לרף אלים, התנהגות אגרסיבית וקידום מטרות אסטרטגיות, מבלי לפנות לצורות לחימה מסורתיות, קינטיות. בכך, הוא מרדד ומייתר אלטרנטיבות הרסניות ואפוקליפטיות. שנית, יכולת קיברנטית, מעצם טבעה, אינה יכולה להיות מסווגת כמלחמה. שלישית, מלחמת סייבר, שבמסגרתה מטילים שני שחקנים זה על זה מהלומות דיגיטליות, שמייצרות אפקטים הרסניים, אינה סבירה, בשל

ההרתעה העצמית של השחקנים. כלומר, אף אם מעשית ניתן להטיל מהלומה כזו, יעדיף השחקן להימנע ממנה, בשל קישוריותן חסרת התקדים של מערכות המידע כיום; שכן כל תקיפה משמעותית מגלמת סיכון לפגיעה עצמית חוזרת. רביעית, תפוצה של טכנולוגיית מידע עשויה לאפשר מרחב שיתוף פעולה בין שחקנים מדינתיים ולא מדינתיים, סביב מטרות משותפות וכנגד אויבים משותפים, וכתוצר לוואי יכולה לתרום ליציבות בינלאומית.

לעומת זאת, תפיסה מנוגדת מציירת תמונה פסימית יותר. להלן טיעוניה המרכזיים של תפיסה זו: ראשית, על פי הגישה הרואה בסייבר מערער יציבות אסטרטגית, מכפיל הסייבר את מספר השחקנים, המדינתיים והלא מדינתיים כאחד, בעלי יכולת השפעה במערכת הבינלאומית, מייצר פיצול בקרב יחידות מדינתיות ומרחיק את העוצמה מידיה של המדינה. בכך, הוא מעלה את המורכבות של היחסים ה'בין (לא) לאומיים'. כל זאת, כאשר תודעתית איננו מורגלים לחשוב על קידום האינטרסים האסטרטגיים שלנו באופן אחר. שנית, תופעת ריבוי השחקנים (Large N) מייצרת אפקט מסדר שני של עלייה בסבירות לטעויות, לתאונות ולעיוותי תפיסה בקרב המדינות הגדולות. שלישית, לוחמת סייבר מעודדת מרוצי חימוש קיברנטיים, במיוחד על רקע היעדר רגולציה בינלאומית מוסכמת בתחום בקרת הנשק. בניגוד לתחום הגרעיני והקונבנציונלי - בהם הסכמי בקרת נשק ופירוק כוללות פרוצדורות אימות (verification procedures) - בתחום הסייבר, קשה להעלות על הדעת, לפחות בשלב זה, את היכולת לייצר העתק של פרוצדורה כזו, כאשר שחקן אחד מסוגל לאמת את הקודים והיכולות הדיגיטליות של שחקן אחר.

רביעית, בשל אמונה רווחת בדבר יתרונותיה של ההתקפה על ההגנה, ועל רקע האמונה כי קשיי ייחוס מאפשרים תקיפות אנונימיות חסרות תגמול, עלולים שחקנים לפתח נטייה חזקה לדוקטרינות התקפיות ולהשתמש במכות מנע. לבסוף, היעדר עומק אסטרטגי בתחום הסייבר

- קרי, היעדר זמן ומרחב בין תחילת המתקפה הקיברנטית ופגיעה ביכולות הלבה של הקורבן, לבין יכולתו להחליט היכן וכיצד להגיב, עלול לדרבן את מעצבי המערכות והמפקדים להאציל מראש סמכויות הפעלה (authority predelegation) לדרג המפעילים הטקטים, בדומה לסיטואציה של האצלת סמכויות להפעלתו של נשק גרעיני טקטי לדרגי השדה במהלך המלחמה הקרה. בדומה לדילמות ולהרהורים בתחום הגרעיני, כבר היום עולים רעיונות בדבר פיתוח מערכות תגובה אוטומטיות ואוטומטיות למחצה, מעין מכונת ״יום הדין״ (Cyber Dooms Day Machines) למתן תגובה קיברנטית מידית, ובכך לשפר, לכאורה, את יכולות ההרתעה. למעשה, מצב מעין זה עלול לא רק להעלות את הסיכוי להסלמה לא מכוונת, אלא גם לזליגה של העימות מחיכוך קיברנטי מינורי לממדים קונבנציונליים ואף בלתי קונבנציונליים ולמלחמה כוללת.

פרק ב' - הגישה הרוסית לאומנות המערכה הקיברנטית

ייחודיותה של הגישה הרוסית לאומנות המערכה הקיברנטית שואבת משלושה מקורות: משורשיה האינטלקטואליים הייחודיים לה; מישוג והמשגה שונים מהמקובל בקהילות הידע המערביות של המושג 'סייבר'; ותפיסה ייחודית של 'הרעיון המערכתי' בעת הפעלת עוצמה קיברנטית. ללא היכרות עם מקורות גנאלוגיים ייחודיים אלו, המהווים מעצבי על של הפרקטיקה הרוסית, לא ניתן להבין את התנהגותה הקיברנטית של רוסיה.

שורשיה האינטלקטואליים של הגישה הרוסית לסייבר[7]

השיח המקצועי אודות אומנות המערכה הקיברנטית המתנהל כיום בקהילה האסטרטגית הרוסית - בהיבטים: המודיעיני והמבצעי, ההגנתי וההתקפי - לא נוצר בחלל ריק, אלא הוא יונק היסטורית משלושה מקורות, המוסיפים לעצבו עד היום. מדובר למעשה בסינתזה של שלושה מקורות רעיוניים:

ראשית, בסיס הידע העשיר ביותר ממנו יונקת החשיבה הקיברנטית הרוסית הנוכחית בהקשר הצבאי, הוא אגד של ספרות, רעיונות ותפיסות של המהפכה בעניינים הצבאיים מבוססת המידע (IT RMA), שהחלה להתגבש במחשבה הצבאית הסובייטית במהלך שנות השמונים. טענתה המרכזית של אסכולת ה-RMA דאז, אשר פותחה בידי תאורטיקנים צבאיים סובייטים, כעשור לפני עמיתיהם בארצות הברית, גרסה כי מהפכת המידע תגרור מעבר מצבאות מסיביים של העידן התעשייתי למערכות המבוססות על כוחות קטנים, קלים יחסית ומשולבים, המסוגלים לייצר אפקטים מערכתיים בעלי השלכות אסטרטגיות. לשיטתם, טכנולוגיית המידע מאפשרת לשורה של

אמצעים ויכולות - כרכישת מטרות, מערכות שו״ב ומערכות חימוש (בתחום הדיוק, ההנחיה והטווח) - להפוך את צבאות העתיד למעין ׳תשלובת מודיעין-מהלומה׳.

בתוך כך, עולה באופן חסר תקדים חשיבותו של מה שמכונה בטרמינולוגיה הצבאית הסובייטית-רוסית ׳מאבק מידע׳ - informatsionnaia bor'ba, (המתורגם לרוב לאנגלית כ׳לוחמת מידע׳). זהו למעשה מאמץ כולל, שנועד לייצר שיבוש, שיתוק או השמדה (אם כי זו אינה נתפסת בהכרח כנחוצה) מערכתיים של ׳תשלובת מודיעין-מהלומה של היריב, באופן שיבטיח הכרעה במלחמה. מלכתחילה, ׳מאבק מידע׳, בהיותו מאמץ מערכתי, מתייחס הן להיבטים הטכנולוגיים והאלקטרוניים של הלחימה (ל״א) והן להשפעה הלא קינטית והתודעתית על תהליכי קבלת ההחלטות של היריב. מוסד הידע הדוקטרינרי שיצרו התאורטיקנים הסובייטיים, שימש בשנות התשעים מקור השראה להוגי הדעות האמריקאים, ובראש ובראשונה, לאנדרו (אנדי) מרשל, שמבית מדרשו במשרד ה-Net Assessment בפנטגון הופץ לקהילה האסטרטגית האמריקנית בשנות התשעים רעיון ה-RMA. רעיון זה הוליד בעשורים הבאים שלל תפיסות ודוקטרינות צבאיות כגון: Network Centric Warfare (NCW), Information Dominance, Information Warfare, Effect Based Operations (EBO). בשלב מאוחר יותר צמחה מתוך רעיונות אלו הגישה האמריקאית ללוחמת סייבר.

על פי האסכולה הסובייטית-רוסית, מאז ועד היום נתפס היריב כמערכת מורכבת, מעין תשלובת מודיעין-מהלומה, שניתן להכריעה באמצעות עליונות בתחום המידע ותהליכי קבלת ההחלטות. על כן, שיח בנושא האומנות המערכתית הקיברנטית מתנהל ברוסיה בהקשר רחב יותר, והוא נתפס כחלק אינטגרלי מתופעת ה-IT RMA ורעיונותיה. רעיונות אלו קיבלו משנה תוקף והולידו גל נוסף של ספרות

בנושא לוחמת המידע בעקבות הפקת לקחים ממלחמת המפרץ הראשונה. בתוך כך, אף החלו להבשיל מונחים כגון: 'מאבק מידע', 'לוחמת מידע' ו'מהלומת מידע', אשר יפורטו בהמשך.

בד בבד, מישור ההתייחסות בשיח המקצועי הרוסי ליכולות הסייבר היה מכלול הידע בתחום הלוחמה האלקטרונית נגד מערכות השו"ב והפו"ש של היריב. בשנות התשעים נתפסו ל"א ויכולות לוחמת מידע (בעיקר אלו המוכרים מהספרות המערבית העוסקת ב-RMA) כמכפיל כוח וכגורם המאזן נחיתות כמותית. חלקית, נעוצים שורשי התפיסה בדוקטרינת ההגנה האווירית (הגנ"א) הסובייטית, אשר שילבה את הלוחמה האלקטרונית במענה לעוצמה האווירית המערבית, אם כי יכולות ל"א נתפסו בתקופה הסובייטית בעיקר כאיום. ככל שהלכו והשתכללו תשתיות המידע והאלקטרוניקה של המערב והתלות המערבית בהם הפכה מוחלטת, כפי שבא הדבר לידי ביטוי בהפעלת יכולות אלו על ידי צבא ארצות הברית בעיראק וביוגוסלביה, החלו בהדרגה הרוסים לחשוב על יכולות ל"א כעל כלי מערכתי, שיש בכוחו לעצב במידה משמעותית את פתיחתה של מערכה, את מהלכה ואת תוצאותיה, במיוחד כאשר יכולות הל"א מופעלות בסנכרון עם המערכה על התודעה ועם פעולות קינטיות בשדה הקרב. הרוסים היו מודעים לפיגור האיכותי של האמל"ח הקונבנציונלי שלהם מאז תחילת שנות התשעים, והחלו לראות ביכולות הל"א שלהם (שם הם נהנו, לשיטתם, מיתרון מול המערב, בשל מומחים בעלי איכות טכנולוגית גבוהה), כמאזן לנחיתותם הקונבנציונלית האיכותית וכ'קלף מנצח'.

שנית, מאחר שעל פי הדוקטרינה הרוסית, מאמץ קיברנטי נועד בראש בראשונה להשפיע על תהליכי קבלת ההחלטות של המערכת היריבה, שואבת התפיסה הרוסית לסייבר השראה מ'מבצעי ההשפעה' והיא אף מהווה המשך ישיר שלהם (ברוסית - aktivnye meropriiatiia, באנגלית - measures active). פעילות זו היא אחד ממוקדי העשייה של

קהילת המודיעין הסובייטית (בעבר) והרוסית כיום. מאז היווסדם, בראשית התקופה הסובייטית, נועדו ׳מבצעי ההשפעה׳ לחולל בסביבה האסטרטגית (הבינלאומית ואצל היריב) אקלים תודעתי אופטימלי, לשם קידום יעדים לאומיים סובייטיים.

היסטורית, הורכבו ׳מבצעי ההשפעה׳ ממכלול מבצעים מיוחדים, כגון: הונאה, לוחמה פסיכולוגית, הפעלת סוכני השפעה, תעמולה, סחיטה, דה לגיטימציה והכפשה של מקבלי החלטות ואנשי מפתח, חתרנות וחבלה, יצירת חוסר יציבות פוליטית, חברתית, אתנית וכללית בתוך האוכלוסיות של מדינות היעד, תמיכה בקבוצות טרור וקבוצות קרימינליות והפעלתן ואף סיכול ממוקד. יודגש, כי הסובייטים קידמו בפועל היקף נרחב של ׳מבצעי השפעה׳, והם היו משוכנעים, כי הם נמצאים תחת מתקפה מתמדת וזהה של ׳מבצעי השפעה׳ מצד המערב.

זאת ועוד, הרוסים מייחסים אירועים מרכזיים בעשורים האחרונים (הכישלון באפגניסטן, התפרקות ברית המועצות, מהלכים מערכתיים שגויים במלחמות בצ׳צ׳ניה, ומנגד הצלחות של ארצות הברית במלחמות המפרץ ובמערכה הגלובלית נגד הטרור) לאפקטיביות של ארצות הברית ושל המערב, במה שהם מכנים ׳מבצעי השפעה׳, ומה שמוכר במערב כמערכה על התודעה, על המוחות, על הלבבות ועל הנרטיבים, Information Campaign; Strategic Communication.[8]

שלישית, ואולי החשוב מכל, למונח קיברנטיקה, שנעשה מוכר לרוב המומחים הצבאיים המערביים, בעיקר במהלך העשור האחרון, היסטוריה אינטלקטואלית ארוכה וייחודית ברוסיה, שממנה צמחה תפיסתו מיוחדת של המושג, שונה מזו המקובלת במערב. קיברנטיקה היה מונח שגור בחוגים המדעיים הסובייטיים שעסקו בדיסציפלינות בתפר שבין המדעים המדויקים למדעי החברה ולפילוסופיה. מושג זה גם היה נפוץ בצורה רחבה בשיח המדעי-פופולרי בברית המועצות החל משנות השישים. המושג התייחס לתורת הניהול ולטבע של תהליכי

קבלת החלטות במערכות גדולות. הכוונה הייתה ליצירה, העברה ושימוש בידע ובמידע לטובת הפעלת מערכות מורכבות למיניהן, בין אם גופים חיים, מכונות או חברות אנושיות. השיח המדעי הסובייטי דאז, והרוסי כיום, מעניק בכך פרשנות מילולית למושג היווני 'קיברנטיקה', קרי, אומנות הניווט והניהול (של מערכות מורכבות), ורואה בה תאוריה כללית לניהול מסדר גבוה, ויישומה בניהול תהליכי קבלת החלטות במדינות ובחברות (כמערכות מורכבות גדולות).

העיסוק בתחום הקיברנטיקה החל בחוגים המדעיים של ברית המועצות בשנות הארבעים. בשנת 1948, כשספרו של נורברט ווינר 'קיברנטיקה' יצא לאור (אך ללא קשר ישיר לכך), הורה סטאלין להקים מכון ל'מכניקה מדויקת ומערכות חישובים טכניים מדויקים' - המוסד ממנו עתיד לצמוח בהמשך תחום מדעי המחשב והתכנות הסובייטי. המדענים הסובייטיים דאז בהחלט הכירו את העיסוק המערבי בקיברנטיקה, אך הוא זכה בתקופת סטאלין לביקורת אידיאולוגית כתחום מדעי אימפריאליסטי, מיליטריסטי ואנטי פרולטרי, מאחר שבספרו הצביע וינר על יישומיה הצבאיים של הקיברנטיקה. למרות הביקורת, זכה התחום לתשומת לב בלתי פוסקת וקיבל הכשר אידיאולוגי לאחר מות סטאלין. מאמצע שנות החמישים, התנהל באקדמיות הסובייטיות העיסוק בקיברנטיקה תחת הכותרת של 'תאוריות של ניהול אוטומטי', והפך לאחד התחומים היוקרתיים ביותר במתמטיקה יישומית.

בין המדענים הראשונים שיישמו את עקרונות הקיברנטיקה בעניינים הצבאיים, היה בנו של ראש שירותי הביון הסובייטיים, לאברנטי ברייה, אשר פיתח בשנת 1955, תוך שימוש בעקרונות מדע זה, מערכת שו"ב ועיבוד נתוני מכ"מ (מגלה כיוון מרחק) עבור מערכת הגנה אלקטרונית סובייטית. בשנות השישים היה העיסוק בקיברנטיקה בתחומים מדעיים טכנולוגיים, כלכליים וצבאיים רחב. המושג החל לשמש כקורת גג לכל העיסוק במחשוב לטובת תהליכי שו"ב וניהול רב

מערכתי אוטומטי בברית המועצות. רוב עבודותיו של ווינר פורסמו במספר מהדורות חוזרות עד התפרקות ברית המועצות והיו בין התחומים הפופולריים ביותר של הספרות המדעית. [9]

המשגה שונה מבמערב[10]

עיסוקם של המומחים הצבאיים הרוסים בסוגיות הסייבר זינק בעשור האחרון, והוא מתנהל כאמור בתוך אקלים אינטלקטואלי, היונק משלושת המקורות שתוארו לעיל, אשר עיצבו תפיסה רחבה וכוללת של קיברנטיקה, כתחום ניהול ידע ותהליכי קבלת החלטות במערכות מורכבות. קיברנטיקה, לשיטתם של המדענים הרוסים, מגלמת בתוכה שני מרחבים: מרחב טכנולוגי-דיגיטלי ומרחב תודעתי-קוגניטיבי. על כן, מתחילת דרכה, תפסה הגישה הרוסית הפוסט סובייטית את המרחב הקיברנטי (Cyber space) כחלק אינטגרלי ממרחב גדול הרבה יותר - מרחב המידע (Information space).

על פי הדוקטרינה הרוסית בתחום ביטחון המידע (2011), ׳מרחב המידע׳ הוא סְפֵירה (sphere) הקשורה לעיצוב, ייצור, שינוי, שידור, שימוש ואגירה של מידע. ספירה זו מעצבת את התודעה האישית והחברתית, את תשתית המידע ואת המידע עצמו. על כן, מבחינה הטרמינולוגיה הרוסית בין שלושה מרחבי עשייה: ׳מרחב המידע׳ - מרחב של עשייה, המעצב תפיסת מציאות אישית וקבוצתית; ׳המידע׳ עצמו, כמכלול של תכנים, המאפשרים קבלת החלטות; ו׳תשתיות המידע׳ - מרחב טכנולוגי, המאפשר לשני המרחבים הראשונים, התודעתיים-קוגניטיביים ביסודם, לבוא לידי ביטוי דיגיטלי. המושג האחרון מתכתב למעשה עם מה שמכונה במערב ׳מרחב הסייבר׳, אשר לרוב, מוזכר כיום במסמכים דוקטריניריים רוסיים רשמיים כ׳תשתית המידע׳.

מכאן, שסוגיית הביטחון הקיברנטי נתפסת כחלק מביטחון המידע. אי לכך, יש כיום לרוסיה דוקטרינת ביטחון לאומי בתחום המידע, העוסקת בביטחון של תפיסת המציאות והתודעה של המדינה ואזרחיה במובנה הרחב, ולצדה, כנגזרת ממנה, אסטרטגיה לביטחון קיברנטי, המתמקדת בהיבטיו הטכנולוגיים של מרחב המידע. אמנם, מדובר בשני מסמכים דוקטריניריים נפרדים בתחום הביטחון הלאומי, אך הם מתכתבים ביניהם ומשלימים זה את זה. נראה בהמשך, כי ביטחון מידע דיגיטלי וקוגניטיבי שזורים זה בזה במידה, שמהלומה דיגיטלית ומהלומה קוגניטיבית-תודעתית הם פעולה משולבת באומנות המערכה הרוסית.

יודגש, כי הטרמינולוגיה הרוסית מצויה בשנים האחרונות בתהליך של למידה, בירור מושגי והשתנות. לדוגמה, במהלך העשור הקודם, מושג הלוחמה הקיברנטית או לוחמת סייבר (cyber warfare) התייחס בעיקר למהלכיהם של היריבים נגד רוסיה, במיוחד נגד 'תשתיות המידע' (תקיפות דיגיטליות נגד 'התשתיות הקיברנטיות' של רוסיה). לעומת זאת, כאשר מומחים צבאיים רוסים היו מתארים את העשייה שלהם, בהתאמה לערך במילון המונחים הצבאיים הרשמי שלהם, הם היו משתמשים במונח רחב יותר - 'מאבק מידע' או 'לוחמת מידע' - (informatsionnoe bor'ba; informatsionnoe protivoborstvo). למרות שהתרגום הנפוץ לאנגלית הוא 'לוחמת מידע' או 'מלחמת מידע', ברוסית המונח 'בורבה' או 'פרוטיוובורסטבו' נושא משמעות רחבה יותר של עימות או מאבק בהקשר אסטרטגי, אך לאו דווקא צבאי. כיום, המונח 'סייבר' נפוץ יותר בשיח הרוסי, בהתייחס לכוחותיהם הם. עם זאת, הוא מתייחס בעיקר למרכיב הדיגיטלי בלוחמת המידע.

אם כן, המערכה הקיברנטית הרוסית מגלמת בתוכה מאמץ רחב יותר, משולב ובינתחומי, יחסית למה שמכונה במערב cyber warfare. בדומה, שימוש במונח 'ביטחון' בתחום הסייבר ('kiber-bezopasnost)

נעשה בעיקר מתוך הצורך להשתלב בשיח הבינלאומי בתחום. מעשית, הכוונה היא לתחום מידע רחב יותר מהמרחב הדיגיטלי, באופן שכולל גם היבטים תודעתיים-קוגניטיביים.

התודעה כמרכז כובד מערכתי בלוחמת מידע (מערכה קיברנטית)[11]

על פי התאוריה הצבאית הרוסית, לוחמת מידע היא מרכיב במערכה מתואמת, שנועד להשיג את מטרותיה האסטרטגיות של מדינה כלשהי. לוחמת מידע, ככלי השפעה, הרתעה וכפייה, מאפשרת לחולל מספר אפקטים: כפיית רצונך על שחקן אסטרטגי אחר, ללא שימוש בכוח צבאי; שליטה בהתנהגות של הצד השני ובמשאביו, ללא פלישה פיזית מסיבית; הבשלת תנאים מערכתיים אופטימליים לשימוש בכוח וכן מכפיל כוח בעת לחימה. כלומר, מטרת לוחמת המידע היא לכפות את רצונך על היריב ולהשפיע על התנהגותו האסטרטגית והאופרטיבית, הן כמערכה עצמאית והן כחלק ממערכה קינטית בשדה הקרב, וכל זאת לטובת שליטה פוליטית, צבאית או כלכלית ביריבים. לאור מטרה זו, לוחמת מידע רואה בתודעת הצד השני ובתפיסת המציאות שלו את מרכז הכובד המערכתי, אליו יש לכוון את כלל המאמצים האופרטיביים ממגוון האמצעים. על כן, לוחמת מידע היא כלי אסטרטגי, שנועד להשיג הרתעה וכפייה.

על פי תפיסת ההפעלה במרחב המידע שפרסם משרד ההגנה הרוסי (2011), ׳לוחמת מידע׳ (informatsionnaia voina) היא מאבק במרחב המידע במטרה להסב נזק למערכות, תהליכים ותשתית המידע, ולמערכות תשתית קריטיות או אחרות, לערער (undermine) את המערכת המדינית, הכלכלית והחברתית של המדינה, לערער את יציבות החברה והמדינה באמצעות השפעה פסיכולוגית מסיבית, במטרה לכפות על השחקן היריב לקבל החלטות על פי האינטרסים

שלך. כלומר, בבסיס ההיגיון המערכתי של כל 'מבצע מידע' עומד ניסיון להתערב בתהליך קבלת ההחלטות ולחולל מניפולציה תודעתית של אדם, ארגון צבאי או אזרחי, חברה או מדינה.

יצירת תמונת מציאות כוזבת, מהרמה הטקטית עד לרמה האסטרטגית, באמצעות סילוף ומגה מניפולציה של מידע, במגוון הדרכים והאמצעים, נועדה לאפשר תמרון של התנהגותו האסטרטגית של שחקן כלשהו, מבלי שהוא מודע לכך, ובאופן צפוי ורצוי לשחקן המתמרן. בתרחישים מסוימים, ניתן להשיג כך, לשיטתם של מומחים רוסים, אפקטים אסטרטגיים, שבעבר ניתן היה לחולל רק באמצעות הפעלת כוחות צבא קינטיים מסיביים (לדוגמה, כיבוש חצי האי קרים). יש מקרים שבהם כדי להעביר מסר אסטרטגי ליריב יש להשמיד את צבאו, אולם לעתים די במסר עצמו, אם הוא עוצב ושוגר באופן מתוחכם. מנגנון ההבסה צריך לאפשר 'עליונות בתחום המידע' (Informatsionnoe Prevoskhodstvo) - קרי, לפגוע בקצב קבלת ההחלטות המערכתיות של היריב ובאיכותן ולהגביר יכולות אלו בצד שלנו.

תפיסת הפעלה זו, המוכרת בעגה הצבאית הרוסית כ'שליטה או ניהול רפלקסיבי' (Refleksivnoe Upravlenie), מבוססת על עקרונות ותובנות מתחום 'אומנות הניהול הקיברנטי' ו'הגישה המערכתית', שהיו, כפי שהוזכר לעיל, פופולריים מאוד בקרב אנשי מדע סובייטים ופוסט סובייטיים במגוון תחומים מדעיים. חשוב לציין, כי תאורטיקנים צבאיים רוסים מניחים, כי מדובר בכלי אפקטיבי לחתרנות אסטרטגית, שבאמצעותו אף ניתן להכריע במלחמה ולגרום לשינוי משטר, גם ללא הפעלת כוחות צבא סדירים בשדה הקרב הקינטי. יודגש, כי מבחינת הרוסים, מדובר ב'לוחמת מידע' גם בהיבט ההגנתי, קרי ממקום של קורבן התוקפנות של המערב, אשר לו הם מייחסים יכולות משוכללות ממה שמתקיים בפועל. (יצוין, כי המאמרים והמסמכים הדוקטרינריים הרוסיים כתובים מזווית

התבוננות הגנתית של קורבן התוקפנות הקיברנטית. השיטה מוכרת עוד מהתקופה הסובייטית כדי לאפשר שיח מקצועי בתחום, תוך שמירת ביטחון שדה סביב יכולותיהם ותפיסת ההפעלה שלהם עצמם).[12]

ההמשגה הרוסית של לוחמת המידע המודרנית, ובכלל זה לוחמת הסייבר, קשורה ישירות לתפיסת האיום ולאיום הייחוס של רוסיה. בפרשנותם כיום של מה שקרוי במערב לוחמת סייבר (cyber warfare), רואים הרוסים לנגד עיניהם מערכה משולבת ורב ממדית של מאמצים דיגיטליים ולא דיגיטליים, צבאיים ואזרחיים, המכוונים לשנות את תפיסת המציאות, את הערכים, את התרבות וההתנהגות של האליטות ושל האזרחים ברוסיה. זאת, בניסיון לתמרנם כנגד השלטון, ולגרום לשינוי המשטר, להפיכתה של רוסיה לווסאל, הכפוף לתכתיבים גאופוליטיים מערביים. הדוקטרינה הצבאית הרוסית (דצמבר 2014) מציינת את מאבק המידע והשפעתו (vozdeistvie), כאחד מהאיומים העיקריים, המופעל באופן הוליסטי לצד כלים צבאיים, כלכליים ומדיניים, תוך הפעלת פוטנציאל של מחאה חברתית וכוחות מיוחדים. כך, חתרנות קוגניטיבית-תודעתית נגד עולם הערכים והתרבות של האזרחים, ושיבוש של תשתיות מידע ותקשורת של רוסיה, מוזכרים בפרק של ׳סכנות פנימיות לביטחון הלאומי׳. כל תקיפה דיגיטלית, המיוחסת לגורמים צבאיים בארצות הברית אינה נתפסת כאירוע העומד בפני עצמו, אלא כפעולה, המשולבת במכלול מערכתי של יוזמות ברשתות חברתיות, דיפלומטיה ציבורית, הפעלת כוחות בפועל בשדה הקרב של מערכה ממושכת ורב ממדית, שבכוחה להשיג אפקט אסטרטגי - עיוות תפיסת המציאות ועולם הערכים של הקורבן.

ביטוי לכך ניתן למצוא בגישתם של הרוסים לאירועים מהפכניים בשנים האחרונות - ׳מהפכות הצבע׳ (colored revolutions) במרחב הפוסט סובייטי, אירועי הטלטלה האזורית במזרח התיכון, המחאות

נגד שלטון פוטין במהלך הבחירות האחרונות והמלחמה באוקראינה - כל אלו לשיטתם, הם מאמצי לוחמת מידע, אשר החלו בעיקר במרחב הווירטואלי, וחוללו בסופו של דבר מהלכים ממשיים (לא ווירטואליים) מסוכנים לביטחון הלאומי (כפי שיוצג בהמשך, זוהי בדיוק הגישה הרוסית באירועים באסטוניה, בגרוזיה ובעת כיבוש חצי האי קרים). על כן, מהלומות קיברנטיות הן חלק מ׳מאבק מידע׳ רחב יותר.

מתוך תפיסה רחבה ורב ממדית של לוחמת מידע, מנסה רוסיה בעקביות לקדם יוזמה בינלאומית לרגולציה של הביטחון והריבונות במרחב הסייבר. היא דורשת, כי רגולציה כזו לא תוגבל להיבטים של התערבות ׳דיגיטלית׳ במרחב הריבוני של השחקן, אלא תכלול גם ׳התערבות תוכנית׳ במרחב הקוגנטיבי-תודעתי של המדינה הריבונית. זאת, מאחר ששני סוגי התערבות אלו קשורים לשיטתה באופן אורגני ומהווים מאמץ מערכתי כנגד הביטחון הלאומי של מדינות ריבוניות. רוסיה, לשיטתה, נמצאת במהלך השנים האחרונות תחת מתקפת מידע משולבת (דיגיטלית-תודעתית) חסרת תקדים, המכוונת נגד המרחב התודעתי של אזרחיה.

מאפייניה הייחודיים של אומנות המערכה הקיברנטית הרוסית

תפיסת האיום המתוארת לעיל מכתיבה מדיניות מענה מסוימת, ובכלל זה אומנות מערכה קיברנטית בעלת מאפיינים ייחודיים. ההתנהגות האופרטיבית הרוסית בשנים האחרונות בזירות השונות (באסטוניה ב-2007, בגרוזיה ב-2008 ובאוקראינה ב-2014), שיח המומחים המתנהל בפרסומים מקצועיים של הכוחות המזוינים וגופי הביטחון של רוסיה, תפיסות ודוקטרינות רשמיות וכן רפורמה של קהילת הביטחון הקיברנטית ברוסיה כיום - כל אלו מבליטים שלושה מאפיינים של אומנות מערכה זו, הנבדלת מגישות של קהילות אסטרטגיות אחרות, בעיקר מערביות:

גישה מערכתית-הוליסטית להפעלת הכוח הקיברנטי

(Kompleksnyi Podhod)[13]

בראש ובראשונה, הגישה הרוסית שונה מהמערבית והיא מתכתבת עם הגישה הסינית, באופן שהיא תופסת את הקוד העוין ואת התוכן העוין כשלובים זה בזה, בלתי נפרדים ומסוכנים בה במידה. על פי התאוריה הרוסית, חבלה דיגיטלית (התקפות על רשתות מחשבים, שנועדו לשבש או להרוס את התשתית הניהולית של מוסדות השלטון והתשתיות החיוניות) וחתרנות פסיכולוגית (מאמץ להכפיש את ההנהגה, לזרוע בלבול אצל מפעילי המערכות, וליצור דה מורליזציה ואובדן כיוון של האזרחים) הן מאמצים קיברנטיים משולבים, המכוונים לתמרן את התודעה ואת התנהגות הקורבן.

בהתייחסותם כמעט לכל אירוע קיברנטי, בין שהם הצד היוזם או בין שהם הקורבן לשיבוש תהליך קבלת ההחלטות, דנים הרוסים בשני סוגים של ׳פצצות לוגיות׳: ׳מתקפת סינטקסיס׳, קרי, שיבוש של מערכות מחשב באמצעות קוד עוין; ו׳מתקפה סמנטית׳, קרי, שיבוש של תוכן. שתי צורות ההתקפה נועדו ליצור אצל היריב נחיתות מערכתית בתחום המידע, להוריד אצלו את איכות קבלת ההחלטות ואת קצבן, ולהבטיח דומיננטיות אינפורמטיבית בתחומים אלו אצל יוזם ההתקפה. מאחר שעל פי התאוריה הצבאית הרוסית, ניצחון והכרעה הם בראש ובראשונה מהלכים ואפקטים פסיכולוגיים-תודעתיים, עליונות אינפורמטיבית-קוגניטיבית היא תנאי מקדים, ולפעמים אף מספיק, לניצחון במערכה. גישה הוליסטית זו, המשלבת במהלומת המידע (Informatsionnyi Udar) מרכיבים דיגיטליים עם מרכיבים תודעתיים, עוברת כחוט השני בכל המסמכים הדוקטרינריים הרוסיים, החל מהפרסום הראשון של דוקטרינת ביטחון המידע של רוסיה בשנת 2000, ומשתקפת גם בפרסומים מקצועיים של אנשי צבא בעשור האחרון. פגיעה דיגיטלית במערכות מידע של תשתיות קריטיות

בתחומי התעשייה, הפיננסים, התחבורה והאנרגיה, יכולה אמנם לחולל אפקטים בפני עצמם, אולם אלו צריכים להיות מלווים בפגיעות תודעתיות-קוגניטיביות, שישבשו את תהליכי קבלת ההחלטות המדיניות והצבאיות, וייצרו דה מורליזציה ודה אוריינטציה של האוכלוסייה (פאניקה ותוהו ובוהו חברתי). לעומת זאת, פרשנים מערבים נוטים בדרך כלל להחמיץ את ההוליסטיות של המערכה הרוסית, להתמקד בפן הקיברנטי-דיגיטלי של התקיפה ולראותה במנותק מהמהלומה התודעתית-קוגניטיבית.

'אמצעי מאבק המידע' (sredstva informatsionnoi bor'by) אף הוא מונח רשמי במילון המושגים של המטכ"ל הרוסי, הממחיש נאמנה את הגישה ההוליסטית. על פי הטרמינולוגיה הרוסית, לוחמת מידע כוללת בתוכה שורה של כלים מערכתיים, כאשר הסייבר הוא מרכיב אינטגרלי בה, ועדיין אחד מיני רבים. מכלול 'אמצעי מאבק המידע' מקיף: מערכות תקיפה קיברנטית של רשתות ממוחשבות, מערכות לוחמה אלקטרונית, לוחמה פסיכולוגית, הונאה, הטעייה ודיסאינפורמציה מערכתיים (Operativnaia maskirovka) ואמצעי הגנה והתקפה של מערכות שו"ב ופו"ש. אמצעים אלו של 'לוחמת מידע' חותרים להנחית על המערכת היריבה הן מהלומה דיגיטלית והן מהלומה תודעתית-קוגניטיבית.[14] ככזו, לוחמת מידע, לשיטתם של אסטרטגים רוסים, היא אחד המרכיבים העיקריים של דור המלחמה הנוכחי, המכונה במערב 'לוחמה היברידית רוסית'. להבדיל מהלוחמה הקלאסית, בלוחמה זו מבצעים קינטיים הם לרוב בגדר מאמץ מסייע, ולא המהלך העיקרי, ולעתים הם אף אינם באים לידי ביטוי כלל, מאחר שאת רוב מטרות המערכה ניתן להשיג באמצעות כלי השפעה בתחום המידע (Sredstva informatsionnogo vozdeistviia). הרמטכ"ל הרוסי גרסימוב, שדן בטבע הלוחמה ובאופי העימותים הנוכחיים, קבע כי מאחר שמאבק המידע מנוהל באופן בלתי פוסק (ראו בעניין זה בהמשך), הפעלה נקודתית של כוח צבאי היא רק מאמץ מינורי, המסייע

לשלל האמצעים הלא צבאיים, אשר תופסים מקום דומיננטי יותר בעימות.[15] למעשה, במה שקרוי במערב ׳לוחמה היברידית׳, כורכת לוחמת המידע את כל המאמצים הצבאיים והלא צבאיים יחדיו, במיוחד מהלכים ומסרים הרתעתיים, הן בתחום הקונבנציונלי והן בתחום הלא קונבנציונלי, כפי שבא הדבר לידי ביטוי בכיבוש חצי האי קרים.

איחוד המאמצים הקיברנטיים והיברידיות השחקנים

(Edinstvo Usilii)[16]

בהתאם לגישה ההוליסטית המתוארת לעיל, עוסקים המקורות הרוסיים בסנכרון ובסינרגיה של המאמצים הדיגיטליים והפסיכולוגיים (מערכה על התודעה), הן בינם לבין עצמם והן מול מהלכים קינטיים בשטח ובשלל יוזמות מדיניות-דיפלומטיות בזירה הבינלאומית. על אירועים, נרטיבים ומהלכים ב׳רשת הווירטואלית׳ להניע מגמות מערכתיות ׳מחוץ לרשת הווירטואלית׳, לרבות שדה הקרב, ולהפך. יודגש, כי סינרגיה של המאמצים מתאפשרת, בין השאר, באמצעות ההיברידיות של שחקנים צבאיים ולא צבאיים, מדינתיים ולא מדינתיים כאחד. תפקודה של רוסיה בעשור האחרון ממחיש נאמנה מאפיין זה של איחוד והיברידיות של מאמצים.

מהלומות מידע מערכתיות באסטוניה, בגרוזיה ובאוקראינה התאפיינו אף בהיברידיות השחקנים המופעלים. בכל אחד מהמקרים מספר רב של התקפות דיגיטליות על מוסדות שלטון מיוחס לקבוצות האקרים (האקטיביסטים) ולקבוצות פשע קיברנטי, המגויסים הן בחירום והן בשגרה לטובת גופי הביטחון הרוסיים. מבלי שהם מזוהים איתם רשמית, מחזיקים שירותי הביטחון הרוסיים ׳צבא צללים קיברנטי׳, במסווה של חברות וגופי תקשורת פרטיים, המסוגל לייצר אפקטים דיגיטליים ופסיכולוגיים, תוך סנכרון עם מאמצים דומים המנוהלים

מתוך גופי הממסד. לתופעה ממדים עצומים, והיא הפכה בשנים האחרונות למקור פרנסה עבור אלפי בני אדם ברוסיה.

תופעה זו מצויה במקומות רבים במדיה החברתית ובתקשורת, הן הרוסית והן הבינלאומית, מרשת חברים רוסית עד ה-facebook, ממקומונים בעיתונות הרוסית והאירופאית ועד ה- New York Times לרבות ערוצי טלוויזיה פרו-רוסיים בינלאומיים. רשת זו מייצרת מאמרים, תגובות למאמרים, תמונות, סרטוני וידאו וכדומה. סביר להניח, כי קיימת מערכת מקבילה, אם כי הרבה יותר מסווגת וחשאית, לחתרנות דיגיטלית. 'צבאות הטרולים' אינם משנים בהכרח את דעת הקהל בהתאם למסרים פרו-מוסקבאיים שהם מפיצים, אך הם מסוגלים לייצר שיבוש ושיתוק תודעתי, שלאחריו קל יהיה לתמרן את השומעים למקומות הרצויים.

סימנים רבים מעידים על מערכת מאורגנת ומשומנת היטב של הפעלת מיקור חוץ קיברנטי, הן דיגיטלי והן פסיכולוגי. במציאות מושחתת ועבריינית למחצה, המתנהלת על בסיס קוד פעולה של פשע מאורגן ושל שירותים חשאיים, צורת התנהלות כזו היא אורגנית וטבעית והיא אינה מחייבת מאמצי הבנייה ארגוניים או פרוצדורליים משמעותיים. כפי שהכוחות הפרו-רוסיים הנלחמים כיום במזרח אוקראינה הם ערב רב אמורפי והיברידי של אנשים וקבוצות, המנוהלים ברמה משתנה של ריכוזיות על ידי מוסקבה (באמצעות היחידות המודיעיניות שלה), כך מנוהלים גם מאמצי הסייבר ההיברידיים שלה. כאמור, הדבר נתפס כטבעי והוא מתכתב היטב עם מסורת ארוכה של 'מבצעי השפעה', כששירותי המודיעין מפעילים התערבות היברידית של סוכנים, טרוריסטים, גורמים עבריינים ומתנגדי משטר.

מערכה קיברנטית מתמדת (Bezpriryvnost')[17]

מומחים רוסים תופסים את לוחמת המידע, הדיגיטלית והתודעתית-קוגניטיבית, כפעולה מערכתית בלתי פוסק ומתמשך בין המלחמות, לקראת המלחמה, במהלכה ולאחריה. החלוקה לעתות שלום ולעתות מלחמה, המקובלת במערב, אינה מתקיימת במקרה הרוסי. כאן, המדובר ברצף של מערכות, הקשורות ברעיון מכונן, הכורך יחדיו את כל הפעולות: ברמה האסטרטגית, האופרטיבית והטקטית. אין לרצף מערכות זה התחלה ברורה ומצב סיום ברור, אלא רק רעיון מערכתי מכונן. הגורמים המשתנים היחידים הם: היקף המהלומה ועוצמתה, דיגיטליות ותודעתיות, בהתאם לנסיבות ולרמת החיכוך עם שחקן אסטרטגי אחר, וכן סנכרון בין לוחמת המידע לבין הפעלת הכוחות הקינטיים בשדה הקרב או מבצעים מיוחדים אחרים.

המקרים המפורסמים יותר כמו: אסטוניה, גרוזיה ואוקראינה, מסמלים אירועים מערכתיים מבודדות במערכה רחבה, המהווה חלק מהמאבק האסטרטגי של מוסקבה בארצות הברית ובעלי בריתה על השליטה באזור ההשפעה של רוסיה. למרות השוני בין האירועים - באסטוניה, לוחמת מידע ללא התערבות צבאית, אך תוך עידוד הפגנות מתנדבים; בגרוזיה, לוחמת מידע רב זירתית, המסונכרנת עם הפעלה גלויה ומאסיבית ביותר של כוחות הצבא הרוסי; ובחצי האי קרים, לוחמת מידע התומכת בהפעלה סמויה של כוחות מיוחדים - אין לראות בכל אחד מהם אירוע יחיד העומד בפני עצמו. מבחינת מוסקבה, כולם מהווים מרכיבים מערכתיים בעימות שהחל זמן רב קודם לכן, וממשיך עד היום. גישה זו עומדת בניגוד לתפיסה המערבית המסורתית של המלחמה, שהתאפיינה בחלוקה לשני מצבי יסוד ׳מלחמה׳ או ׳שלום׳.

על פי הגישה הרוסית, בעת של מה שקרוי במערב ׳שלום׳, נועדה לוחמת המידע ליצור אפקטים של השפעה, הרתעה וכפייה, ובעת הפעלת הכוח, קרי, בעת ׳מלחמה׳, היא נועדה לאפשר עליונות בתחום קבלת

ההחלטות. בכך, נבדלת הגישה הרוסית מהגישות של רוב הקהילות האסטרטגיות המערביות, ומתכתבת למעשה עם המאפיינים של הגישה הסינית. זוהי מערכת הוליסטית יותר, המגלמת בתוכה סינתזה בין תקיפות קוד לתקיפות תוכן, קרי מהלומות דיגיטליות ומהלומות תודעתיות-קוגניטיביות. היא אינה מבדילה בין עת שלום לעת מלחמה ומנהלת מערכה רב ממדית בלתי פוסקת. יודגש, כי תפיסת הזמן המערכתי במקרה הרוסי (והסיני) היא ארוכה יותר ואינה מוגבלת לאירוע מסוים, כשכל אירוע בה נתפס בהקשר רחב יותר. מומחים מערבים, ובתוכם מומחים ישראלים, בהתמקדם באירועים בודדים במנותק מההקשר המערכתי, עלולים להחמיץ את 'היער הקיברנטי הרוסי' שמאחורי 'העצים'.

אחרות מערכתית בפעולה

מאפייניה הייחודיים של הגישה הרוסית לאומנות המערכה הקיברנטית, אשר פורטו לעיל - הוליסטיות בהפעלת הכוח, איחוד המאמצים, היבירדיות השחקנים ומערכה מתמדת - משתקפים היטב בשלושה אירועים אסטרטגיים בעשור האחרון.

מהלומת המידע המערכתית באסטוניה גילמה בתוכה סינתזה של מרכיבים דיגיטליים ותודעתיים. הפגיעה הדיגיטלית במוסדות השלטון המדיניים, הכלכליים והתשתיתיים (הפלתם, באמצעות מתקפת DDoS של אתרי אינטרנט חדשותיים ואתרי השידור המרכזיים הפרו-ממשלתיים, של אתרי משרדי הממשלה, של בנקים ואף של מחשבים אישיים של דמויות קונקרטיות) סונכרנה עם תעמולה אנטי-ממשלתית, שנועדה להכפיש את ממשלת אסטוניה בעיני אזרחיה, לפלג בין קבוצות אתניות שונות ולחולל מהומות והפגנות. ייזום מצב כאוטי זה נוהל באמצעות רשתות חברתיות והפעלה של קבוצות אופוזיציה מהפזורה הרוסית המקומית וסוכני השפעה אסטוניים, כאשר ברקע מושקעים מאמץ הסברתי רשמי ומאמצי דיפלומטיה ציבורית רוסית. באשר

להיברידיות השחקנים, למרות היעדר מידע קונקרטי, רמת התיאום, התחכום והסנכרון של ההתקפות עם ההפגנות ברחובות ועם המתקפה ההסברתית-דיפלומטית של רוסיה ועם מהלומות דיגיטליות, אפשרה למומחים להניח כי מוסקבה עמדה מאחורי חתרנותם של האקרים ושחקנים מעורבים אחרים מחוץ לאסטוניה ובתוכה. במקרה זה, מערכת המידע החלה קודם לפריצתן של ההפגנות, והיא נמשכת עד היום, הגם שהמאמצים ההוליסטיים והשחקנים ההיברידים הופעלו ללא המרכיב הקינטי.

מהלומת מידע מערכתית בגרוזיה, לעומת זאת, הביאה לידי ביטוי מלא את כול המאפיינים הייחודיים של הגישה הרוסית. פגיעה דיגיטלית במוסדות השלטון, במיוחד בגופים המנהלים תקשורת בין הממשלה לציבור, נועדה להכניס את האזרחים לוואקום תקשורתי, למלאו בתוכן תעמולתי וליצור פאניקה באמצעות פגיעה, אמנם זמנית, במערכת הבנקאית. המאמצים הדיגיטליים כללו גם חסימה והפלה של מספר אתרי תקשורת בגרוזיה, אוסטיה, רוסיה ואזרבייג׳ן. האקרים רוסים הפילו אתר חדשות אזרי מרכזי, שסיפק כיסוי פרו-גרוזיני של המלחמה. אתרו של נשיא גרוזיה הופל לפני תחילת הקרבות למשך עשרים וארבע שעות ושב והותקף מספר פעמים במהלך המלחמה. קיימת סברה, כי הפיצוץ בצינור הנפט באקו-טביליסי-צ׳יחאן ועצירת הזרימה בו, מקורם בתקיפה קיברנטית על מערכת השליטה של הצינור. עם תחילת המלחמה, מרבית התעבורה של האינטרנט הגרוזיני תומרנה לשרתים בשליטה רוסית ונחסמה שם. מרבית אתרי האינטרנט של הממשלה הגרוזינית הותקפו במתקפת DDoS ובאתר של נשיא גרוזיה ובאתרים של בנקים הופיעו תמונות של היטלר ושל רודנים אחרים. כל זאת, במקביל למתקפות דיגיטליות ואלקטרוניות על מכ״מים ומערכות שו״ב של צבא גרוזיה, בניסיון (אם כי לא מוצלח במיוחד) ליצור ׳סנוור׳ מערכתי בחזית, כאשר ברקע מתנהלת לחימה קונבנציונלית, הכוללת הפעלת כוחות כבדים. במקביל, ניהלה מוסקבה

מאמץ דיפלומטי הסברתי שנועד לבודד את המערכה ולמנוע מגרוזיה תמיכה צבאית ומדינית של המערב.

עקרונות אלו של אומנות המערכה הרוסית יושמו גם בעת כיבוש חצי האי קרים, אם כי בהיקף גדול יותר, בהשוואה למקרים קודמים. בקרים, החלה מהלומת המידע המערכתית חודשים לפני הפלישה לחצי האי. טרם נפילתו של הממשל הפרו-מוסקבאי של הנשיא ינוקוביץ', החלו מתקפות DDoS רוסיות על אתרי האופוזיציונרים בתוך אוקראינה; התקיפות התמקדו בעיקר בהחלפת תוכן האתרים או בהפלתם. ההכנות והחדרתם של כוחות מיוחדים בהיקף עצום (כחמשת אלפים לוחמים) הוסתרו באמצעות מכלול של מבצעי הונאה מערכתית ומבצעי השפעה, אשר מיקדו את תשומת הלב של המערב בריכוז הכוחות ובתרגילים שדימו פלישה בגבולות אוקראינה, אלפי קילומטרים מחצי האי. עם תחילת הכיבוש, כחלק מאותה מגמה, תפסו כוחות רוסיים סיבים אופטיים של תקשורת וניתקו את חצי האי מתעבורת הטלפוניה עם אוקראינה. במקביל להחדרת הכוחות המיוחדים, התרחשו התקפות דיגיטליות ואלקטרוניות על מערכות שו"ב ותקשורת של כוחות היבשה, הים והאוויר האוקראיניים הפרוסים בחצי האי, אשר ניתקו אותם לאורך זמן מהמטה וממוסדות השלטון בקייב, עד כדי שיבוש ואובדן של תמונת המציאות ודה מורליזציה של הכוחות.

ברקע, הופלו מספר אתרי ממשלה ושודרה תעמולה אגרסיבית וטוטלית, שכללה הדלפת דואר אלקטרוני אישי של מנהיגים אוקראינים; בוצעו פריצות לטלפונים סלולריים של חברי פרלמנט אוקראיני; הודלפו שיחות טלפון של דיפלומטים מערבים (שהושגו באמצעי פריצות מודיעיניות); בוצעו תקיפות וגניבת מידע רגיש ממחשביו של ראש הממשלה החדש של אוקראינה ושל נציגויות בחוץ לארץ, באמצעות קוד עוין בשם Snake. מאמצים אלו כוונו כלפי האוכלוסייה המקומית, במטרה ליצור דמוניזציה והכפשה של

הממשלה בקייב. כן, נרשמו תקיפה של מרכז הגנת הסייבר של נאט״ו באסטוניה, בידי אקטיביסטים אוקראינים פרו-רוסים (cyber berkut), וכן ניסיון לשבש את מערכת חישוב הקולות בבחירות הדמוקרטיות באוקראינה. כמו כן, התקיימה צנזורה על רשתות חברתיות ואתרים, שמקדמים תוכן פרו-אוקראיני ואנטי-רוסי, הן ברוסיה והן באוקראינה, לרבות אתרים של מנהיגי האופוזיציה ברוסיה. במקביל לשלל פעולות אלו, התבצע בשטח כיתור בזק של היחידות האוקראיניות, במעין איגוף אנכי סימולטני, באמצעות כוחות מיוחדים רוסיים, במסוקים ובכלי רכב קלים. כוחות אלו אמנם היו קטנים בגודלם, אך הם התפרסו לאורך כל העומק המערכתי של חצי האי קרים. לבסוף, מבלי שהתרחשו קרבות קינטיים כלל, הצליחה רוסיה להכניע מספר רב של יחידות צבאיות ברמת כשירות גבוהה יחסית, ולכבוש שטח עצום, תוך זמן יחסית קצר. תמרונים דיגיטליים, פסיכולוגיים וקינטיים יצרו סילוף של תמונת המציאות, עיוות התודעה של הצד השני, מהרמה הטקטית עד הרמה האסטרטגית, ותמרון של התנהגותו לכיוון רצוי. היכולת לסנכרן מאמצים אלו במספר זירות ולשלב מאמצים הוליסטיים בזמן אמת היא זו שהרשימה ובעיקר הפתיעה אסטרטגית את המומחים במערב.

תהליך הלמידה ובניין הכוח הקיברנטי ברוסיה

׳לוחמת מידע׳ אינה ארגון, גוף או זרוע, כי אם מושג, המתאר היגיון מערכתי ייחודי. המסמכים הדוקטרינריים בתחום, שיצאו לאור במהלך שני העשורים האחרונים אינם כוללים הסדרה מוסדית, אלא מפרטים את עקרונות האומנות המערכתית בתחום מאבק המידע ברוסיה. בימים אלו, מנוהלים מאמציה של רוסיה בתחום מאבק המידע בידי קהילה קיברנטית משוסעת ומסובכת, הלוקה בהיעדר פיקוד אחוד, הסדרת תפקידים ומנגנון ברור לחלוקת עבודה. זאת, בשל הגדרה רחבה וכוללת של לוחמת מידע בכתריסר גופים, זרועות וארגונים בקהילה האסטרטגית הרוסית ובגופי הממשלה הנמנים עם

הקהילה הקיברנטית. בין הגופים העיקריים ניתן למנות את שירות הביטחון הפדרלי (FSB), שירות מודיעין החוץ (SVR), זרועות ומפקדות שונות של צבא רוסיה, ובעיקר המודיעין הצבאי (GRU) ומנהל הלוחמה האלקטרונית (REB), שירות האבטחה הפדראלי האחראי על תשתיות התקשורת המיוחדת (FSO), הצנזורה בתחום התקשורת וה-IT (Roskomnadzor), משרד החוץ ומשרד הביטחון. לכאורה, גוף התיאום הכללי של מדיניות הביטחון הלאומי, שהוקם בהסכמת המטה הכללי ומשרד ההגנה וכפוף לשר ההגנה, נוטל על עצמו את רוב פונקציות התיאום, אולם בפועל מדובר באלתור, יותר מאשר בהסדרה לטווח ארוך.

חיפוש אחר הסדרה, לרבות דיונים על הקמת פיקוד או זרוע סייבר בכוחות המזוינים, אף הוא משקף תהליך למידה ובירור מושגי ותפיסתי, אשר נמשך כיום בחוגים המקצועיים ברוסיה. בנוסף, פרסום עדכני מסוף שנת 2014, בכתב העת של המטכ"ל הרוסי, קורא למסד טרמינולוגיה אחידה בתחום לוחמת המידע, להבהיר את מטרותיה ועקרונותיה של האומנות המערכתית בתחום ולכונן בו הסדרה ארגונית וניהול משאבים.[18] חלקים מסוימים בשיח המקצועי משקפים מאמצים של מומחים מתחום הל"א לנכס לעצמם את העיסוק בתחום לוחמת המידע והסייבר ולהפוך אותו להמשך קונצפטואלי ישיר של אומנות המערכה בתחום. חלקים אחרים בשיח זה עוקבים מקרוב אחר פיתוח הידע והשיח הדוקטרינרי המנוהל במערב, מקיימים עליו דיון ביקורתי ומאמצים חלק מרעיונותיו. כך או כך, הקהילה האסטרטגית הרוסית, שנמצאת כרגע בשלב של ניסוח מחדש של עקרונות אומנות המלחמה שלה בכלל, ובתחום הסייבר בפרט, תמשיך להשקיע בנושא זה אנרגיה מקצועית רבה. בשלב זה, תחום לוחמת המידע הוא הציר המרכזי בגישה החדשה של רוסיה למלחמה, המכונה במערב 'לוחמה היברידית'.

פרק ג׳ - תובנות לעיצוב אומנות אופרטיבית קיברנטית ישראלית

הרפורמה הקיברנטית בצה״ל ובמערכת הביטחון צוברת תאוצה. על כן, עוצמת הסייבר תהווה, ככל הנראה בעתיד הנראה לעין, את אחד הכוחות המשפיעים המשמעותיים ביותר בבניין הכוח של ישראל והפעלתו. נייר זה, ניסה להעמיד לטובת המעצבים והממשים של הרפורמה, מסד ידע רלבנטי, שהצטבר בעולם האקדמי, במיוחד בדיסציפלינה של לימודי הביטחון, ואת הגישה הרוסית, המהווה במובנים רבים את האנטיתזה לגישה המערבית בתחום הסייבר. מסד ידע זה, על הרעיונות התאורטיים וניתוחי האירוע האמפיריים שבו, אשר נפרשו בגיליון זה, נועדו לספק חומר למחשבה ולזקק את מגוון עבודות המטה ותהליכי העבודה בצה״ל בתחום הסייבר. מתוך שלל הרעיונות ראוי להדגיש שלוש מסקנות מרכזיות:

תפיסת הפעלה מערכתית - לבת החדשנות הצבאית

רוב המהפכות בעניינים צבאיים, בדומה למקרה החדשנות הקיברנטית, אירעו בעקבות התקדמות טכנולוגית. עם זאת, מפנים טכנולוגיים כשלעצמם אינם מבטיחים חדשנות מוצלחת. הטכנולוגיה אך מתווה את המסגרת ויוצרת פוטנציאל למהפכה צבאית. מה שמחולל את החדשנות הוא המידה שבה ארגונים צבאיים מכירים בהזדמנויות הטבועות באמצעי המלחמה החדשים ומנצלים אותן, באמצעות הקמת מבנים חדשים וגיבושן של תפיסות הפעלה חדשות. אנדרו מרשל, מהאישים המובילים בעולם החשיבה האסטרטגית המודרנית, טען כי האתגר המרכזי בכל מהפכה בעניינים צבאיים הוא דווקא אינטלקטואלי, הקשור בפיתוחן של תפיסות הפעלה מערכתיות, ולא טכנולוגי, הקשור לפיתוחן של מערכות הנשק. בהיעדר ראייה עתידנית ברורה באשר לאופייה של המערכה הבאה וטבע העימותים, או בהיעדר

דוקטרינה קוהרנטית ותפיסת הפעלה מגובשת, גוברת מאוד הסבירות לכך שהכוחות ייבנו ויצוידו, שלא בהתאם לדרישותיהן של הסביבות האסטרטגית והאופרטיבית. בוודאי שחקירה מערכתית של שדה הקרב הקיברנטי העתידי אינה מבטיחה זיהוי נכון של העתיד וקיום דוקטרינה קוהרנטית, אינו מבטיח שזו אינה שגויה, אך היעדר בחינתן של דוקטרינה ותפיסת הפעלה, לאור מסקנות של חקירה מערכתית מתמדת, אכן מגביר את הסבירות לכך. ללא מחויבות מוסדית-אינטלקטואלית לעצב חזון בדבר המלחמה העתידית, וללא מחויבות מקבילה לבקר דרך קבע את הפרדיגמה החדשה, עלול הצבא לאבד את הרלבנטיות שלו נוכח הסביבה המשתנה, האתגרים וההזדמנויות. לטענה זו נודעת רלבנטיות מידית לתחום הסייבר.

מכורח הנסיבות האסטרטגיות ועל רקע השינויים הארגוניים האחרונים בצה״ל, נדרשת מערכת הביטחון להשקיע, ללא דיחוי, אנרגיה אינטלקטואלית בפיתוחה של הגרסה הישראלית לאומנות המערכה הקיברנטית. עד כה, וכמו במקרים של כמעט כל חדשנות צבאית ישראלית הצבאיות קודמת, בניין הכוח ואף הפעלתו המבצעית הנרחבת יחסית, קדמו לפיתוחה של תפיסה הפעלה, ולא להפך. תפיסות וחשיבה מעמיקה בדרך כלל מדביקות את הפער מול היכולות בקצב אטי מאוד, וכך הדבר גם במקרה שבנדון. יש לפעול לגשר על פער זה מידית. גיבוש הגרסה הישראלית לאומנות המערכה הקיברנטית ייצר מערכת מושגים מקצועיים, יאפשר דיון ביקורתי עליה, יתרום לשיח בין-מדרגי ובין-גופי וייצר לדרג הצבאי הבכיר אקלים רעיוני מועיל לטובת תכנון אסטרטגי ואופרטיבי בצה״ל. מאחר שמהפכות בעניינים צבאיים הן קודם כל פריצות דרך תפיסתיות, אזי אנו נמצאים מול יריבנו, לא רק במרוץ חימוש טכנולוגי, אלא בעיקר בתחרות למידה תפיסתית על שימוש יצירתי ביכולות טכנולוגיות. שחקנים אחרים עלולים להגיע להישגים מולנו, פחות בשל עליונותם הדיגיטלית, אלא דווקא בזכות פיתוח גרסה מתוחכמת יותר של אומנות המערכה הקיברנטית.

בהקשר זה, העשייה של מטה הסייבר הלאומי, מהווה, על רקע הפרקטיקה המקובלת בישראל, דוגמה טובה הראויה לחיקוי בהקשר הצבאי. חזון אסטרטגי ותכנית פעולה לטווח ארוך, המעוגנים במסמכי יסוד דוקטרינריים, ככלל, אינם קיימים ברמת הביטחון הלאומי בישראל, ועל כן אינם מכוונים את העשייה בקהילה האסטרטגית בה. לעומת זאת, ההיסטוריה של הקמת המיזם הקיברנטי ברמה הלאומית, גיבוש התפיסה הלאומית והרגולציה של הקהילה הקיברנטית הישראלית בהתאם לחזון של מטה הסייבר, הם דוגמה לתפיסה שקדמה לפרקטיקה ומובילה אותה. על כן, יש לקיים חקירה מערכתית של שדה הקרב ואופי העימותים בעידן הסייבר, ולאפיין את המגמות המרכזיות בקרב השחקנים המעורבים בתחרות הלמידה בעניין זה באזורנו ובעולם.

תפיסה הוליסטית של המערכה הקיברנטית

העמדה של הידע האקדמי שהצטבר במערב, מול התאוריה והפרקטיקה של האומנות המערכתית הקיברנטית הרוסית, מבליטה מספר תובנות אשר עשויות לתרום לארגון הכוח של צה״ל, בניינו והפעלתו בתחום הסייבר. תובנות אלו רלבנטיות, הן בהקשר של איום הייחוס והן בהיבט מתן המענה לו והשימוש היזום בסייבר לקידום מטרות הביטחון הלאומי. הגישה ההוליסטית הרוסית מראה, כיצד מאמצים וגופים בתחום הסייבר נוטלים אחריות מערכתית על מרחב המידע, המידע ואמצעי המידע ומפעילים אותם באופן מסונכרן. למעשה, תפיסת הסייבר שלהם כלל אינה מבדילה בין שלושת התחומים הללו ותופסת אותם כשלם מערכתי שאינו ניתן לפירוק. גישה כזו מאפשרת, כפי שממחיש הניסיון הרוסי, את מיצוי אופטימלי בין שילוב וסנכרון של מבצעים קיברנטיים (דיגיטליים ותודעתיים), מבצעים קינטיים ומאמצי דיפלומטיה מדינית, כלכלית וציבורית. התחכום המערכתי של הגישה הרוסית ההוליסטית בולט על רקע הגישה האמריקאית המתאפיינת כחד ממדית באופן יחסי, ומותנית טכנולוגיה. בכוחה של

מערכה קיברנטית, הקושרת יחדיו אפקטים אופרטיביים, דיגיטליים ותודעתיים, להשיג באופן עצמאי את התכלית האסטרטגית של המערכה. הניסיון של רוסיה בעימות שלה עם המערב בשנים האחרונות ממחיש את המאמצים לכפות את הרצון האסטרטגי על הצד השני, תוך מזעור החיכוך הקינטי ותוך היסמכות על יכולות קיברנטיות תודעתיות בעיקר, כאשר המאמץ הדיגיטלי משרת את זה התודעתי ומשלים אותו.

בנוסף, גישה מותנית טכנולוגיה בולטת לא רק בתפיסת המענה, אלא גם בתפיסת האיום, הן במערב והן בישראל. הנטייה האינסטינקטיבית של ישראל היא לגמד את האיומים התודעתיים מול האיומים הדיגיטליים, להם היא מייחסת את פוטנציאל הנזק המשמעותי ביותר, ועל כן אותם היא מציבה במוקד תפיסת האיום. ראשית, תפיסה כזו, אינה מבטאת בהכרח את ההתנהלות, ההעדפות והשקעת המשאבים של הצד השני, אלא מהווה תמונת ראי של המענה הישראלי; הן בתחום הקיברנטי והן בתחום הקינטי יצר צה״ל בעשורים האחרונים, ידע וניסיון מצומצמים בתחום מבצעי תודעה והשפעה. מסורתית, זכו מבצעי תודעה ללחימה (עוצמה) רכה ושלל ההשפעות הלא קינטיות על הצד השני בתכנון המבצעי בצה״ל, לתשומת לב ולמאמצים דלים יחסית. מאמצים כאלו, אם נכללו בתכניות המבצעיות, נתפסו כמשניים, והציפיה לאפקטיביות שלהם הייתה נמוכה יחסית.

שנית, אם יריביה של ישראל יאמצו לעצמם צורות התנהלות, שמתכתבות עם הגישה הרוסית, אזי תעמוד ישראל מול מהלומת סייבר, שבה אפקטים דיגיטליים יתקשרו במסגרת אותה תכנית מערכתית לאפקטים תודעתיים. יצירה וניהול מתוחכמים של אפקטים קיברנטיים תודעתיים בתחום המדיני, הפיננסי, הכלכלי והחברתי, בהיקף רחב, עלולים לשבש את שגרת החיים ואת הרציפות התפקודית בצורה משמעותית ואף להשפיע על תהליכי קבלת ההחלטות המדיניות. נוכח אתגר כזה, יש לתת מענה משולב, או לפחות להפנים, כי חיכוכים

מערכתיים בזירות שונות הם פנים שונות המבטאות את ההיגיון המערכתי של הצד השני.

הגישה הקיברנטית ההוליסטית מקבלת משנה תוקף כאשר הפעלת כוח קינטי, הן מנגד והן כתמרון קרקעי, הופכת מורכבת, בשל הרגישות לאבדות ולנזק אגבי, על רקע המערכה על הלגיטימציה הבינלאומית ודעת הקהל בארץ ובחוץ לארץ. על כן, גישה הוליסטית לעוצמה הקיברנטית עשויה לאפשר לצה״ל להרחיב את מרחב התמרון האופרטיבי שלו, הפעם בשדה הקרב הקיברנטי. מהלומת סייבר הוליסטית עשויה לפרק ולשתק את המערכת היריבה מבלי להשמידה, תוך מזעור הנזק הקינטי הישיר והעקיף. על כן, מומלץ לבחון את האיזון המסורתי בין היכולת והתפיסות בתחום הקיברנטי-דיגיטלי והקיברנטי-תודעתי ולעצב תפיסת הפעלה אחודה, שתגלם בתוכה את שני המרכיבים הללו בעוצמת הסייבר. כיום, צה״ל עודנו שרוי ב׳עידן התמימות׳ בתחום ההשפעה האסטרטגית בסייבר, הן בהיבט הבנת האיום והן בהיבט הכנת המענה.

העוצמה הקיברנטית כחלק אינטגרלי מארגז הכלים של צה״ל ושל מדינת ישראל

מממצאי המחקר עולה הצורך המידי בשילובם המלא של מאמצי הסייבר, הדיגיטלי והתודעתי, ככלי בארגז הכלים של צה״ל, וכן בעיצוב המערכתי ובתכנון המבצעי של צה״ל. יש לפתח מודעות מקצועית לפוטנציאל העוצמה הקיברנטית, במובן ההוליסטי של המושג, דבר שיאפשר את שילובה בתהליכי התכנון האסטרטגי והאופרטיבי. יתר על כן, יש לשלב את המרכיב הקיברנטי, לא רק בתכנון המבצעים הקינטיים בתוך הצבא, אלא אף לסנכרן את המערכה הקיברנטית, בהובלת צה״ל, עם שלל המאמצים ברמה הלאומית ובזירות האחרות. הדוגמה הרוסית, בהשתלטות על חצי האי קרים, ממחישה כי עיצוב מערכתי מתוחכם, המסנכרן באופן אופטימלי את שלל העוצמות ברמה

הלאומית במסגרת מערכה אחת יכול להשיג תכלית אסטרטגית, אף ללא הפעלה מסיבית של כוח קינטי. יודגש, בהקשר זה, כי דווקא היכולת לעצב מערכה בסגנון כזה, ולהוציא אותה לפועל בצורה אפקטיבית, היא זו שהפתיעה בצורה הכי משמעותית את קהילות הביון המערביות.

משחקי מלחמה וסימולציות ביטחוניות מהשנים האחרונות, בפורומים אקדמיים בארץ ובחוץ לארץ, ממחישים את האפקטיביות הרבה של המבצעים הרוסיים, לא רק במישור הביטחוני-צבאי המסורתי, אלא נגד גופי האנרגיה, יעדים פיננסים מערביים ותשתיות תחבורה, כגון נמלים ושדות התעופה - דבר המאפשר להם, תוך שילוב של סוגי עוצמה שונים, לכפות את רצונם האסטרטגי על שחקנים מערביים. באותו אופן, אימוץ של גישת הרתעה וכפייה רב ממדית תאפשר לישראל להפעיל מבצעים קיברנטיים תודעתיים, הן כמבצעים העומדים בפני עצמם והן כחלק ממאמץ המשולב עם מבצעים קינטיים. עוצמת הסייבר ממצה באופן מרבי את הפוטנציאל שלה, כאשר אפקטים דיגיטליים ואפקטים תודעתיים שהיא מייצרת משלימים ומעצימים זה את זה לטובת התכלית האסטרטגית של המערכה, וכאשר הם משתרעים על זירות המאבק השונות, צבאיות ולא צבאיות.

יודגש, כי סינרגיה בין מכלול המאמצים, הנצפית במקרה הרוסי, מתאפשרת בין השאר בשל הגדרה ברורה יחסית של מטרות ויעדים מעבר לרמה הטקטית-אופרטיבית. בהיעדר דירקטיבה מדינית-אסטרטגית ברורה, יש קושי מהותי לעצב מבצעי השפעה מראש, ואף לכוננם תוך כדי המערכה. בנסיבות כאלו, מורכב מאוד, ולעתים בלתי אפשרי, לסנכרן את הכלים הדרושים להצלחה, קל וחומר להכינם מראש לשם השגה אופטימלית של מטרה לאומית-אסטרטגית (במיוחד כאשר נדרשת הכנה מוקדמת משמעותית ורב ממדית). בשל התרבות הפוליטית והאסטרטגית הייחודיות של ישראל, מאמץ כזה הוא קשה ומורכב שבעתיים.

לקחים מנייר זה, ובמיוחד מהמקרה הרוסי, קוראים למצות את פוטנציאל שיתוף הפעולה בין שחקנים ממשלתיים ללא ממשלתיים. הניסיון הרוסי ממחיש כיצד ניתן להפיק תועלת אסטרטגית משמעותית מהפעלה יצירתית של מתנדבים בהיקפים גדולים, וממיקור חוץ של פונקציות דיגיטליות ותודעתיות,לטובת המערכה הקיברנטית שמנהל הממסד הביטחוני. סנכרון ממשלתי של יכולת אזרחית, בבחינת ׳משמר אזרחי בסייבר׳, יכול לשמש את מדינת ישראל הן בשגרה והן בחירום. כיוון חשיבה כזה מזמין גם לבחון את ההשלכות לעולם המילואים לטובת המערכה הקיברנטית ולטובת הדיפלומטיה הציבורית בעידן המדיה החדשה.

לבסוף, המחקר מלמד כי על המערכה הקיברנטית להיות בלתי פוסקת ומונעת היגיון אחוד, אשר יחבר את כלל המאמצים בשגרה ובחירום. על הפעולות ההתקפיות, ההגנתיות, הדיגיטליות, התודעתיות, המודיעיניות-איסופיות להיות מסונכרנות ומשלימות הדדית במסגרת מערכה הוליסטית.

סיכום

אין ספק, כי הופעתו של המרחב הקיברנטי והפיכתו לכלי מערכתי היא מהחדשנויות הצבאיות העיקריות בנות זמננו, וכי לעוצמה הקיברנטית השפעה דרמטית על קידום מטרות הביטחון הלאומי. אולם, הבנתנו את הפוטנציאל המערכתי של העידן הקיברנטי עודנה דלה יחסית. מסמך זה ביקש להניח נדבך תאורטי אודות היכולת הקיברנטית בתחום המערכתי, בניסיון לברר את מקומו של ממד הסייבר ביחס למרחבי הפעולה הצבאיים המסורתיים ולאפיין את הייחודיות של הטבע האופרטיבי של ממד זה.

חדשנות קיברנטית בעניינים צבאיים מעלה שאלות תפיסתיות חדשות על אודות הדרך שבה על הקהילה האסטרטגית להתאים את עצמה ואת הכוחות המזוינים שלה לתופעה החדשה. בתוך כך, עודדה חדשנות זו תחרות למידה בין קהילות אסטרטגיות שונות. כל קהילה לומדת מנסה ליישב את העקרונות של המחשבה הצבאית הקלאסית בהקשר החדש, או לפתח עולם מושגים ורעיונות ייחודי להקשרה של החדשנות הנוכחית. כתוצאה ממאמצים אינטלקטואליים אלו, נוצר מכלול של תובנות אודות אופי המערכה בתחום הקיברנטי, בעיקר סביב חמש שאלות היסוד הבאות:

האם הופעתן של יכולות הסייבר מהווה מהפכה בעניינים צבאיים? כיצד משפיעות יכולות הסייבר על היחס בין ההתקפה להגנה? מהו טבע ההרתעה וההתרעה המוקדמת במרחב הקיברנטי, והאם מאמצים אלו ישימים במרחב זה? האם יכולת הסייבר מעצימה שחקנים מדינתיים עתירי עוצמה טכנולוגית וכלכלית, או דווקא שחקנים שאינם ניחנים במאפייני העוצמה הקלאסיים, כגון מדינות חלשות או שחקנים לא מדינתיים? האם הופעתו של המרחב הקיברנטי תורמת ליציבות האסטרטגית או מערערת אותה, כלומר, האם היא מעלה את

מספר החיכוכים האופרטיביים בין השחקנים במערכת הבינלאומית, מקרבת או מרחיקה עימות אסטרטגי?

על כל שאלת יסוד בשיח הוצגו במחקר זה שתי דעות שונות או מתחרות, בבחינת ניגודיות משלימה, בהנחה כי הדבר עשוי לתרום לחשיבתם של פרקטיקנים ישראלים בעניין. יודגש, כי בשנים האחרונות, כביטוי ללמידה ולניסיון מצטבר, איזון הדעות אודות שאלות יסוד אלו משתנה, וככל הנראה יוסיף להיות דינמי.

יצוין, כי תחרות הלמידה בשאלות היסוד של אומנות המערכה מתנהלת בקרב שחקנים שונים, הן ידידותיים והן יריבים לישראל. בשל תרבות אסטרטגית, המשגה של שאלות היסוד ותהליכי פיתוח ידע המשתנים משחקן אחד למשנהו. מדובר למעשה בתחרות חקירה קריטית, שכן שחקן, אשר יגיע מהר יותר לתובנות מתקדמות ומתוחכמות יותר, ידו תהיה על העליונה. המחשבה הצבאית הרוסית בהקשר זה נועדה ללמוד על עצמנו באמצעות העמדה של מחקר השוואתי. הגישה הרוסית מפגינה אחרות מערכתית בתפיסת הפעלת הכוח, בארגונו ובהפעלתו. מאפייניה הבולטים של הגישה, הנובעים משורשים אינטלקטואליים ייחודיים, הם: תפיסת התודעה כמרכז הכובד של מערכת הסייבר, גישה הוליסטית להפעלת הכוח, המשלבת בין מאמץ טכנולוגי-דיגיטלי לבין מאמץ קוגניטיבי-תודעתי, איחוד וסנכרון המאמצים הקיברנטיים עם שלל המאמצים של העוצמה הלאומית ורציפות של המערכה הקיברנטית בכל הרמות, הן בשגרה והן בחירום. ביטוי מובהק לאחרות מערכתית זו ניתן לראות בהפעלת העוצמה הקיברנטית הרוסית באסטוניה, בגרוזיה ולאחרונה גם בעת כיבוש חצי האי קרים.

הרפורמה הקיברנטית בצה״ל ובמערכת הביטחון צוברת תאוצה. הרעיונות התאורטיים אשר נפרשו בגיליון זה, נועדו לספק חומר למחשבה ולזקק את מגוון עבודות המטה ותהליכי העבודה בצה״ל בתחום הסייבר.

ראוי להדגיש שלוש מסקנות מרכזיות: ראשית, על רקע השינויים הארגוניים האחרונים בצה"ל, נדרשת מערכת הביטחון להשקיע, ללא דיחוי, אנרגיה אינטלקטואלית בפיתוחה של הגרסה הישראלית לאומנות המערכה הקיברנטית. עד כה, וכמו ברוב רובן של החדשנויות הצבאיות הישראליות הקודמות, בניין הכוח ואף הפעלתו המבצעית הנרחבת יחסית, קדמו לפיתוחה של תפיסה הפעלה, ולא להפך. מאחר שמהפכות בעניינים צבאיים הן קודם כל פריצות דרך תפיסתיות, אזי אנו נמצאים מול יריבינו, לא רק במרוץ חימוש טכנולוגי, אלא בעיקר בתחרות למידה תפיסתית על שימוש יצירתי ביכולות טכנולוגיות. שחקנים יריבים יכולים להגיע להישגים מולנו, לא משום עליונות דיגיטלית, אלא דווקא בזכות פיתוח גרסה מתוחכמת יותר של אומנות המערכה הקיברנטית. יש לקיים חקירה מערכתית של שדה הקרב ואופי העימותים בעידן הסייבר ולאפיין את המגמות המרכזיות בקרב השחקנים המעורבים בתחרות הלמידה בעניין זה, באזורנו ובעולם.

שנית, מומלץ לשקול לאמץ תפיסה הוליסטית למערכה הקיברנטית. גישה מעין זו מאפשרת, כפי שממחיש הניסיון הרוסי, מיצוי אופטימלי בין שילוב וסנכרון של מבצעים קיברנטיים (דיגיטליים ותודעתיים), מבצעים קינטיים ומאמצי דיפלומטיה מדינית, כלכלית וציבורית. המערכה הקיברנטית, הקושרת יחדיו אפקטים אופרטיביים דיגיטליים ותודעתיים, יכולה להשיג באופן עצמאי את התכלית האסטרטגית של המערכה. הניסיון של רוסיה בעימות שלה עם המערב בשנים האחרונות ממחיש את המאמצים לכפות את הרצון האסטרטגי על הצד השני, תוך מזעור החיכוך הקינטי ותוך היסמכות על יכולות קיברנטיות תודעתיות, בעיקר כאשר המאמץ הדיגיטלי משרת את זה התודעתי ומשלים אותו. ישראל נוטה לגמד את האיומים התודעתיים מול האיומים הדיגיטליים - להם היא מייחסת פוטנציאל נזק משמעותי יותר, ועל כן אותם היא מציבה במוקד תפיסת האיום ובמוקד תפיסת המענה. מסורתית, הקדיש צה"ל בתכנון המבצעי שלו תשומת לב ומאמצים מועטים יחסית למבצעי תודעה, ללחימה (עוצמה) רכה

ולשלל ההשפעות הלא קינטיות על היריב. ישראל עלולה לעמוד מול מהלומת סייבר, שבה אפקטים דיגיטליים יתקשרו במסגרת אותה תכנית מערכתית לאפקטים תודעתיים. הגישה הקיברנטית ההוליסטית מקבלת משנה תוקף כאשר הפעלת כוח קינטי, הן מנגד והן כתמרון קרקעי, הופכת מורכבת, בשל הרגישות לאבדות ולנזק אגבי, על רקע המערכה על הלגיטימציה הבינלאומית ודעת הקהל בארץ ובחוץ לארץ. גישה הוליסטית לעוצמה הקיברנטית עשויה לאפשר לצה״ל להרחיב את מרחב התמרון האופרטיבי שלו, הפעם בשדה הקרב הקיברנטי. על כן, מומלץ לבחון את האיזון המסורתי בין היכולת לתפיסות בתחום הקיברנטי-דיגיטלי והקיברנטי-תודעתי ולעצב תפיסת הפעלה אחודה, שתגלם בתוכה את שני המרכיבים הללו בעוצמת הסייבר. כיום, צה״ל עודנו שרוי ב׳עידן התמימות׳ בתחום ההשפעה האסטרטגית בסייבר, הן בהיבט הבנת האיום והן בהיבט הכנת המענה.

שלישית, ממצאי המחקר עולה הצורך המידי בשילוב מלא של מאמצי הסייבר, הדיגיטלי והתודעתי, ככלי בארגז הכלים של צה״ל, בעיצוב המערכתי ובתכנון המבצעי של צה״ל. יש לפתח מודעות מקצועית לפוטנציאל של העוצמה הקיברנטית, במובן ההוליסטי של המושג, דבר שיאפשר את שילובה בתהליכי התכנון האסטרטגי והאופרטיבי. יתר על כן, יש לשלב את המרכיב הקיברנטי לא רק בתכנון המבצעים הקינטיים בתוך הצבא, אלא אף לסנכרן את המערכה הקיברנטית, בהובלת צה״ל, עם שלל המאמצים ברמה הלאומית. בתוך כך, לקחים מנייר זה, ובמיוחד מהמקרה הרוסי, קוראים למצות את פוטנציאל שיתוף הפעולה בין שחקנים ממשלתיים ללא ממשלתיים. סנכרון ממשלתי של יכולת אזרחית, בבחינת ׳משמר אזרחי בסייבר׳, יכול לשמש את מדינת ישראל, הן בשגרה והן בחירום. חשיבה כזו אך מזמינה לבחון את ההשלכות לעולם המילואים לטובת המערכה הקיברנטית ולטובת הדיפלומטיה הציבורית בעידן המדיה החדשה.

לבסוף, המחקר מלמד כי על המערכה הקיברנטית להיות בלתי פוסקת ומונעת היגיון אחוד, אשר יחבר את כלל המאמצים בשגרה ובחירום. על הפעולות ההתקפיות, ההגנתיות, הדיגיטליות, התודעתיות, המודיעיניות-איסופיות להיות מסונכרנות ומשלימות הדדית במסגרת מערכה הוליסטית.

מקורות

Adamsky Dima, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolutions in Military Affairs in Russia, the US and Israel* (Pale Alto: Stanford UP, 2010).

Andrew Christopher, *The Sword and the Shield: Mitrokhin Archive* (New York: Basic Books, 1999).

Andrew Christopher and Oleg Gordievsky, *KGB: The Inside Story of Foreign Operations from Lenin to Gorbachev* (New York: Harper Collins, 1999).

Betz David and Tim Stevens, *Cyberspace and the State*, (London: IISS Adelphi Papers, 2011).

Clark David D. and Susan Landau, "Untangling Attribution", *Proceedings of a Workshop on Deterring Cyberattacks*, ed. National Research Council (Washington, DC: National Academies Press, 2010), pp. 25-40.

Clarke Richard A. and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harpercollins, 2010).

Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: US Army War College, 2013).

Collins Sean and Stephen McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications", *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1 (2012), pp. 80-91.

Even Shmuel and David Siman-Tov, *Cyber Warfare:*

Concpets and Strategic Trends (Tel Aviv: INSS, Memo No.117, May 2012).

Farwell James P. and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1 (February-March 2011), pp. 23-40.

Goldman Emily and John Arquilla (eds.), *Cyber Analogies* (Monterey, CA.: Naval Post-Graduate School, 2014).

Gartzke Erik, "The Myth of Cyberwar: Brining War in Cyberspace Back Down to Earth", *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41-73.

Gartzke Erik and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies* (forthcoming).

Geer Keneth, *Strategic Cyber Security* (Brussels: NATO CCDCOE, 2011).

Granit Amos, *Cyberspace as a War-fighting Domain - In What Sense? Offerings from a Systemic Theory of Cybernetic Mediums* (Gliliot IS: Malam, March 2010).

Hanska Jan, "The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories of War", in: *The Fog of Cyber Defense*, (National Defense University, Helsinki, 2013), pp. 169-190.

Kello Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2, (2013), pp. 7-40.

Kiravuo Timo and Mikko Sarela, "The Care and Maintanace of Cyberweapons", in: *The Fog of Cyber Defense*, (National Defense University, Helsinki, (2013), pp. 218-231.

Kramer Franklin D., Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, (Washington, DC: NDU Press, 2009).

Krepinevich Andrew F., *Cyber Warfare: A "Nuclear Option?"*, (Washington, DC: CSBA, 2012).

Liber Kier, "The Offense-Defense Balance and Cyber Warfare", in: *Cyber Analogies* (Monterey, CA.: Naval Post-Graduate School, 2014), pp. 96-108.

Libicki Martin C., *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

Libicki Martin C., *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, UK: Cambridge UP, 2007).

Lindsay Jon R., "Correspondence on the Cyber Revolution", *International Security*, (forthcoming).

Lindsay Jon R., "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365-404.

Lindsay Jon R. and Lucas Kello, "Cyber Disagreements: A Correspondence", *International Security*, Vol. 39, No. 2, (Fall 2014), pp. 181-192.

Limnell Jarno, "Offensive Cyber Capabilities are Needed Because of Deterrence", in: *The Fog of Cyber Defense*, (National Defense University, Helsinki, 2013), pp. 200-208.

Lupovich Amir, "Cyber Deterrence: Trends and Challenges in Research", *Military and Strategic Affairs*, Vol. 3, No.3, (December, 2011), pp. 49-62.

Lupovici Amir, "The 'Attribution Problem' and the Social

Construction of 'Violence'", *International Studies perspectives* (2014), pp. 1-21.

Liff Adam P., "Cyberwar: A New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401-428.

Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace", *Joint Forces Quarterly*, Vol. 63, No. 4 (4th Qtr. 2011), pp. 64-69.

Lynn William J. III, "Defending a New Domain", *Foreign Affairs*, Vol. 89, No. 5 (September 2010), pp. 97-108.

Mallery John C., *"Models of Escalation in Cyber Conoict"*, presentation at the Workshop on Cyber Security and Global Affairs, Budapest (May 31-June 2, 2011).

Morgan Patrick M., "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", in: *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), pp. 55-76.

Nye Joseph S., "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), pp. 18-38.

Paget François, *Cybercrime and Hacktivism* (Santa Clara, Calif.: McAfee, 2010).

Palokangas Tero, "Cyberwar: Another Revolution in: Military Affairs?", in: *The Fog of Cyber Defense*, (National Defense University, Helsinki, 2013), pp. 146-154.

Rantapelkonen Jari and Mirva Salminen, *The Fog of Cyber*

Defense, (National Defense University, Helsinki, 2013).

Rattray Gregory J., *Strategic Warfare in Cyberspace*, (Cambridge, MA: Massachusetts Institute of Technology (MIT) Press, 2001).

Rid Thomas and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, Vol. 38, No. 1, (2015), pp. 3-36.

Rid Thomas, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5-32.

Shakarian Paulo, "Stuxnet: Cyber Revolution in Military Affairs", *Small Wars Journal* (15 April, 2011), pp.1-10.

Singer P.W. and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford UP Press, 2014).

Sheldon John B., "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, Vol. 5, No. 2 (Summer 2011), pp. 95-112.

U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (Washington, D.C.: U.S. Department of Defense, July 2011).

Wirtz James, "Cyber Pearl Harbor", in: *Cyber Analogies* (Monterey, CA.: Naval Post-Graduate School, 2014), pp. 7-15.

מסמכי יסוד רוסיים

Voennaia Doktrina Rossiskoi Federatsii (2014).

Kontseptsiia Obshchestvennoi Bezopasnosti Rossiiskoi Federatsii (2013).

Kontseptual'nue Vzgliady na Deiatel'nost' Rossiskikh VS v Informatsionnom Prostranstve (2011).

Strategiia Natsionalnoi Bezopasnosti Rossiiskoi Federatsii do 2020 goda (2009).

"Informatsionnoe protivobostvo", in: *Voenno Entsiklopedicheskii Slovar'* (Moscow: (Moscow: Voenizdat, 2007).

"Sredstva Informatsionnoi bor'by (informatsionnoe oruzhie)" in: *Voenno-Entsiklopedicheskii Slovar'* (Moscow: Voenizdat, 2007).

Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii (2000).

מקורות ברוסית

Antonovich P.I., "O sushchnosti i soderzhanii kibervoiny", *Voennaia mysl*', No. 7, (2011), pp. 39-46.

Balybin V.A., Y.Y. Donskov, and A.A.Boiko, "O terminologii v oblasti radioelektronnoi borby v usloviiakh sovremennogo informatsionnogo protivoborstvo", *Voennaia mysl*', No. 9, (2013), pp. 28-32.

Bazylev S.I., I.N.Dylevskii, S.A. Komov, and A.N. Petrunin, "Deiatelnost Vooruzhennykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve: printsipy, pravila, mery doveriia", *Voennaia mysl*', No. 6. (2012), pp. 25-28.

Chausov Fedor, "Osnovy Refleksivnogo Upravleniia", *Morskoi Sbornik*, No. 9, 1999.

Chekinov S.G. and S.A. Bogdanov, "Vliianie nepriamykh deistvii na kharakter sovremennoi voiny", *Voennaia mysl*', No. 6 (2011), pp. 3-13.

Chekinov S.G. and S.A. Bogdanov, "Priroda I Soderzhanie voin novogo pokoleniia", *Voennaya Mysl'*, (2013).

Chibisov I.N., and V.A. Vodkin, "Informatsionno-udarnaia operatsiia", *Armeiskii sbornik*, No. 3 (2011), pp. 46-49.

Gerasimov V., "Tsennost' Nauki V Predvidyenii", *Voenno-Promyshlennyi Kur'er*, 8 (476) (2013).

Goncharov S.V. and N.F. Artamonov, "Dostizhenie informatsionno-psikhologicheskogo prevoskhodstva v sovremennykh boevykh deistviiakh (po vzgliadam rukovodstva armii SShA)", *Voennaia mysl*', No. 6, (2014), pp. 61-69.

Ionov M.D., "O Refliksivnom Upravlenii Protivnikom v Boiu", *Voennaia Mysl'*, No. 1, 1995.

Kuznetsov V.I., Y.Y. Donskov, and A.S. Korobeinikov, "O sootnoshenii kategorii 'radioelektronnaia borba' i 'informatsionnaia borba'" *Voennaia mysl*', No. 3, (2013), pp. 14-20.

Kuznetsov V.I., Y.Y. Donskov, and O.G. Nikitin, "K voprosu o roli i meste kiberprostranstva v sovremennykh boevykh deistviiakh", *Voennaia mysl*', No. 3, (2014), pp. 13-17.

Kuznetsov V.I., Y.Y. Donskov, and A.S. Korobeinikov, "O sootnoshenii kategorii 'radioelektronnaia borba' i 'informatsionnaia borba', *Voennaia mysl*, No. 3, (2013), pp. 14-20.

Leonenko S., "Refleksivnoe Upravlenie Protivnikom," Armeiskii Sbornik, No. 8, 1995.

Pospelov D.A. and Ui.I. Fet (eds.), *Otcherki Istorii Informatiki v Rossii*, (Novosibirsk: RAN, 1998).

Saifetdinov K.I., "Informatsionnoe protivoborstvo v voennoi sfere", *Voennaia mysl*', No. 7, (2014), pp. 38-41.

Slipchenko Vladimir, *Voiny Shestogo Pokoleniia* (Moscow: Olma Press, 2002)

Slipchenko Vladimir, *Voiny Pokoleniia Novogo* (Moscow: Olma Press, 2004).

Starodubtsev, Y.I., V.V. Bukharin and S.S. Semenov, "Tekhnosfernaia voina", *Voennaia mysl*', No. 7, (2012), pp. 22-31.

Strel'tsov A.A., "Osnovnye zadachi gosudarstvennoi politiki v oblasti informatsionnogo protivoborstva", *Voennaia mysl'*, No. 5, (2011), pp. 18-25.

Turko N.I. and S.A.Modestvov, "Refleksivnoe Upravelenie Razvitiem Strategicheskikh Sil Gosudarstva", in: *Sistemnyi Analiz na Poroge 21 Veka* (Conference Proceedings, Moscow, 1996).

Varfolomeev A. A., "Kiberdiversiia i kiberterrorizm: predely vozmozhnostei negosudarstvennykh subiektov na sovremennom etape", *Voennaia mysl*', No. 12, (2012), pp. 3-11.

Viner Norbert, *Kibirnetika, ili upravlenie I sviaz' v zhivotnom I mashine* (Moscow: Nauka, 1968); *Ia Matematik* (Moscow: Nauka, 1967).

Vorob'ev I.N., "Informatsionno-udarnaia operatsiia", *Voennaia mysl*', No. 6, (2007), pp. 14-21.

הערות

[1] פרק המבוא מתבסס על המקורות הבאים:

P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford UP Press, 2014); David Betz and Tim Stevens, *Cyberspace and the State*, (London: IISS Adelphi Papers, 2011); Emily Goldman and John Arquilla (eds.), *Cyber Analogies* (Monterey, CA.: Naval Post-Graduate School, 2014); Colin Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: US Army War College, 2013); Amos Granit, *Cyberspace as a War-fighting Domain - In What Sense? Offerings from a Systemic Theory of Cybernetic Mediums*, (Gliliot IS: Malam, March 2010); Shmuel Even and David Siman-Tov, Cyber Warfare: Concepts and Strategic Trends (Tel Aviv: INSS, Memo no.117, May 2012); Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, (Cambridge, UK: Cambridge UP, 2007); Jari Rantapelkonen and Mirva Salminen, *The Fog of Cyber Defense* (National Defense University, Helsinki, 2013); Jan Hanska, "The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories of War", in: *The Fog of Cyber Defense*, pp. 169-190; Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, (Washington, DC: NDU Press, 2009); François Paget, *Cybercrime and Hacktivism* (Santa Clara, Calif.: McAfee, 2010).

[2] לדיון מעמיק בסוגיה ראו במקורות הנבחרים הבאים:

Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No.2,

2013; Tero Palokangas, "Cyberwar: Another Revolution in: Military Affairs?", in: *The Fog of Cyber Defense*, pp. 146-154; Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option?"* (Washington, DC: CSBA, 2012); Gartzke Eric, "The Myth of Cyberwar"; Paulo Shakarian, "Stuxnet: Cyber Revolution in Military Affairs", *Small Wars Journal*, 15 April, 2011; Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011); Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do about It (New York: Harpercollins, 2010); James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival* 53, No. 1 (February-March 2011), pp. 23-40; Sean Collins and Stephen McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications", *Journal of Policing, Intelligence and Counter Terrorism* 7, No. 1 (2012), pp. 80-91; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); Lindsay Jon R., "Stuxnet and the Limits of Cyber Warfare"; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: Massachusetts Institute of Technology (MIT) Press, 2001); Lindsay Jon R., "Stuxnet and the Limits of Cyber Warfare".

[3] לדיון מעמיק בסוגיה ראו במקורות הנבחרים הבאים:

Kier Liber, "The Offense-Defense Balance and Cyber Warfare", in: *Cyber Analogies*, pp. 96-108; Gartzke Eric, "The Myth of Cyberwar"; Kello Lucas, 'The Meaning of the Cyber Revolution"; William J. Lynn III, "Defending a New Domain", *Foreign Affairs*, Vol. 89, No. 5 (September 2010), pp. 97-108; U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (Washington,

D.C.: U.S. Department of Defense, July 2011); Keneth Geers, *Strategic Cyber Security* (Brussels: NATO CCDCOE, 2011); Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies* (forthcoming); Jon Lindsay and Lucas Kello, "Cyber Disagreements: A Correspondence",. *International Security*, Fall 2014, Vol. 39, No. 2, Pages 181-192; Amir Lupovich, "Cyber Deterrence: Trends and Challenges in Research", Military and Strategic Affairs, Vol. 3, No. 3, December, 2011. Jon R. Lindsay, "Correspondence on the Cyber Revolution", *International Security* (forthcoming).

[4] לדיון מעמיק בסוגיה ראו במקורות הנבחרים הבאים:

Jarno Limnell, "Offensive Cyber Capabilities are Needed Because of Deterrence", in: The Fog of Cyber Defense, pp. 200-208; James Wirtz, "Cyber Pearl Harbor", in: *Cyber Analogies*, pp. 7-15; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", *Journal of Strategic Studies*, Vol. 38, No. 1, 2015, pp. 3-36; Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence'", *International Studies Perspectives* 2014, pp. 1-21; Gartzke, "The Myth of Cyberwar"; Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", in: *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), pp. 55-76; Lindsay Jon R., "Stuxnet and the Limits of Cyber Warfare"; David D. Clark and Susan Landau, "Untangling Attribution", *Proceedings of a Workshop on Deterring Cyberattacks*, ed. National Research Council (Washington, DC: National Academies Press, 2010), 25-40; Geers, *Strategic Cyber Security*.

[5] לדיון מעמיק בסוגיה ראו במקורות הנבחרים הבאים:

Timo Kiravuo and Mikko Sarela, "The Care and Maintanace of Cyberweapons", in: *The Fog of Cyber Defense*, pp. 218-231; Gartzke Eric, "The Myth of Cyberwar"; Kello, "The Meaning of the Cyber Revolution"; Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5-32; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), John C. Mallery, "Models of Escalation in Cyber Conoict", presentation at the Workshop on Cyber Security and Global Affairs, Budapest, May 31-June 2, 2011; Lindsay Jon R., "Stuxnet and the Limits of Cyber Warfare"; Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace", *Joint Forces Quarterly* 63, No. 4 (4th Qtr. 2011), pp. 64-69.

[6] לדיון מעמיק בסוגיה ראו במקורות הנבחרים הבאים:

Erik Gartzke, "The Myth of Cyberwar: Brining War in Cyberspace Back Down to Earth", *International Security*, Vol. 38, No.2 (Fall 2013), pp. 41-73; Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365-404; Peter Feaver and Keneths Geers, "When the Urgency of Time and Circumstances Clearly Does Not Permit...": Re-delegation in Nuclear and Cyber Scenarios", in: *Cyber Analogies*, pp. 33-46; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, Vol. 5, No. 2 (Summer 2011), pp. 95-112; Kello Lucas, "The Meaning of the Cyber Revolution"; Thomas G. Mahnken, "Cyber War and Cyber

Warfare", in: Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, D.C.: Center for a New American Security, 2011); Rid Thomas, "Cyber War Will Not Take Place"; Liff, "Cyberwar".

[7] ראו בעניין זה:

Vladimir Slipchenko, *Voiny Shestogo Pokoleniia* (Moscow: Olma Press, 2002); *Voiny Novogo Pokoleniia* (Moscow: olma Press, 2004); I.N. Chibisov, and V.A. Vodkin, "Informatsionno-udarnaia operatsiia", *Armeiskii sbornik*, No. 3 (2011), pp. 46-49; Vorob'ev (2007); Safetdinov (2014); V.I.Kuznetsov, Y.Y. Donskov, and A.S. Korobeinikov, "O sootnoshenii kategorii 'radioelektronnaia borba' i 'informatsionnaia borba'" *Voennaia mysl*', No.3, (2013), pp.14-20; V.A. Balybin, Y.Y. Donskov, and A.A.Boiko, "O terminologii v oblasti radioelektronnoi borby v usloviiakh sovremennogo informatsionnogo protivoborstvo", *Voennaia mysl'*, No.9, (2013), pp. 28-32; Antonovich (2012); Y.I. Starodubtsev, V.V. Bukharin and S.S. Semenov, "Tekhnosfernaia voina", *Voennaia mysl*', No. 7, (2012), pp. 22-31; Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolutions in Military Affairs in Russia, the US and Israel* (Pale Alto: Stanford UP, 2010).

[8] ראו בעניין זה:

Christopher Andrew and Oleg Gordievsky, KGB: The Inside Story of Foreign Operations from Lenin to Gorbachev (New York: Harper Collins, 1999); Christopher Andrew, *The Sword and the Shield*: *Mitrokhin Archive* (New York: Basic Books, 1999).

[9] ראו בעניין זה:

D.A. Pospelov and Ui.I. Fet (eds.), *Otcherki Istorii Informatiki v Rossii*, (Novosibirsk: RAN, 1998); Norbert Viner, *Kibirnetika, ili upravlenie I sviaz' v zhivotnom I mashine* (Moscow: Nauka, 1968); *Ia Matematik* (Moscow: Nauka, 1967).

[10] "Informatsionnoe protivobostvo", in: *Voenno Entsiklopedicheskii Slovar'* (Moscow: (Moscow: Voenizdat, 2007); For doctrinal publications see: *Doktrina Informatsionnoi Bezopasnosti Rossiiskoi Federatsii* (2000); *Kontseptual'nue Vzgliady na Deiatel'nost' Rossiskikh VS v Informatsionnom Prostranstve* (2011); *Strategiia Natsionalnoi Bezopasnosti Rossiiskoi Federatsii do 2020 goda* (2009); *Kontseptsiia Obshchestvennoi Bezopasnosti Rossiiskoi Federatsii* (2013); *Voennaia Doktrina Rossiskoi Federatsii* (2014). A.A. Strel'tsov, "Osnovnye zadachi gosudarstvennoi politiki v oblasti informatsionnogo protivoborstva",. *Voennaia mysl'*, No. 5, (2011), pp. 18-25; V.I.Kuznetsov, Y.Y. Donskov, and A.S. Korobeinikov, "O sootnoshenii kategorii 'radioelektronnaia borba' i 'informatsionnaia borba'" *Voennaia mysl'*, No. 3, (2013), pp. 14-20; V.A. Balybin, Y.Y. Donskov, and A.A. Boiko, "O terminologii v oblasti radioelektronnoi borby v usloviiakh sovremennogo informatsionnogo protivoborstvo", *Voennaia mysl*', No. 9, (2013), pp. 28-32; P.I. Antonovich, "O sushchnosti i soderzhanii kibervoiny",. *Voennaia mysl*', No. 7, (2011), pp. 39-46; V.I. Kuznetsov, Y.Y. Donskov, and O.G. Nikitin, "K voprosu o roli i meste kiberprostranstva v sovremennykh boevykh deistviiakh", *Voennaia mysl*', No. 3, (2014), pp. 13-17.

[11] למקורות נבחרים בעניין זה ראו:

Safetdinov (2014); *Doktrina Informatsionnoi Bezopasnosti*; *Kontseptual'nue Vzgliady*; *Strategiia Natsionalnoi Bezopasnosti*; *Kontseptsiia Obshchestvennoi Bezopasnosti*; *Voennaia Doktrina*; Strel'tsov (2012); Antonovich (2012); V.I. Kuznetsov, Y.Y. Donskov, and O.G. Nikitin, "K voprosu o roli i meste kiberprostranstva v sovremennykh boevykh deistviiakh", *Voennaia mysl'*, No. 3, (2014), pp. 13-17; S.G. Chekinov and S.A. Bogdanov, "Vliianie nepriamykh deistvii na kharakter sovremennoi voiny", *Voennaia mysl*', No. 6 (2011), pp. 3-13.

[12] בעניין השליטה הרפלקסיבית ראו:

M.D. Ionov, "O Refliksivnom Upravlenii Protivnikom v Boiu", *Voennaia Mysl*', No. 1, 1995; Fedor Chausov, "Osnovy Refleksivnogo Upravleniia", *Morskoi Sbornik*, No. 9, 1999; N.I. Turko and S.A.Modestvov, "Refleksivnoe Upravelenie Razvitiem Strategicheskikh Sil Gosudarstva", in: *Sistemnyi Analiz na Poroge 21 Veka* (Conference Proceedings, Moscow, 1996). S. Leonenko, "Refleksivnoe Upravlenie Protivnikom", Armeiskii Sbornik, No. 8, 1995.

[13] למקורות נבחרים בעניין זה ראו:

K.I. Saifetdinov, "Informatsionnoe protivoborstvo v voennoi sfere", *Voennaia mysl'*, No. 7, (2014), pp. 38-41; Chibisov and Vodkin (2011); Vorob'ev (2007); Strel'tsov (2012); "Sredstva Informatsionnoi bor'by (informatsionnoe oruzhie)" in: *Voenno-Entsiklopedicheskii Slovar'* (Moscow: Voenizdat, 2007); I.N. Vorob'ev, "Informatsionno-udarnaia operatsiia", *Voennaia mysl*', No. 6, (2007), pp. 14-21; S.I. Bazylev, I.N.

Dylevskii, S.A. Komov, and A.N. Petrunin, "Deiatelnost Vooruzhennykh Sil Rossiiskoi Federatsii v informatsionnom prostranstve: printsipy, pravila, mery doveriia", *Voennaia mysl*', No. 6. (2012), pp. 25-28; V.I. Kuznetsov, Y.Y. Donskov, and A.S. Korobeinikov, "O sootnoshenii kategorii 'radioelektronnaia borba' i 'informatsionnaia borba', *Voennaia mysl*', No. 3, (2013), pp. 14-20; Antonovich (2012).

[14] השינוי העיקרי שעוברת הגישה ההוליסטית בימים אלו, כפי שמשתקף בפרסומים מקצועיים רוסיים, קשור ליכולות דיגיטליות, המופעלות נגד מערכות מידע ותשתית של היריב, לצד מהלומה תודעתית-קוגניטיבית נגד האוכלוסייה ומקבלי ההחלטות, המאפשרות כיום למלחמת המידע להשיג מטרות אסטרטגיות, ללא צורך בעימות צבאי קינטי ישיר.

[15] V. Gerasimov, "Tsennost' Nauki V Predvidyenii", *Voenno-Promyshlennyi Kur'er* 8 (476) (2013).

[16] למקורות נבחרים בעניין זה ראו:

Gerasimov (2013); Safetdinov (2014); Strel'tsvo (2012); V.I. Kuznetsov, Y.Y. Donskov, and O.G. Nikitin, "K voprosu o roli i meste kiberprostranstva v sovremennykh boevykh deistviiakh", *Voennaia mysl*', No. 3, (2014), pp. 13-17; S.G. Chekinov and S.A. Bogdanov, "Vliianie nepriamykh deistvii na kharakter sovremennoi voiny", *Voennaia mysl*', No. 6 (2011), pp. 3-13; "Priroda I Soderzhanie voin novogo pokoleniia", *Voennaya Mysl'*, (2013).

[17] למקורות נבחרים בעניין זה ראו:

Gerasimov (2013); Safetdinov (2014); A.A.Varfolomeev, "Kiberdiversiia i kiberterrorizm: predely vozmozhnostei negosudarstvennykh subiektov na sovremennom etape", *Voennaia mysl'*, No. 12, (2012), pp. 3-11; Chekinov and Bogdanov (2011 and 2013).

[18] לדוגמה ראו:

Safetdinov (2014); V.A.Balybin, Y.Y. Donskov, and A.A. Boiko, "O terminologii v oblasti radioelektronnoi borby v usloviiakh sovremennogo informatsionnogo protivoborstvo", *Voennaia mysl'*, No. 9, (2013), pp. 28-33; Antonovich (2011); S.V. Goncharov and N.F. Artamonov, "Dostizhenie informatsionno- psikhologicheskogo prevoskhodstva v sovremennykh boevykh deistviiakh (po vzgliadam rukovodstva armii SShA)", *Voennaia mysl'*, No. 6, (2014), pp. 61-69.

עשתונות - במה למחשבות ורעיונות

עורכת הסדרה: סגן-אלוף נאוה גרוסמן-אלוני

מרכז המחקר של המכללה לביטחון לאומי

מרכז המחקר של המכללה לביטחון לאומי שואף לעסוק בחקר תופעות מתהוות בהקשרי הביטחון הלאומי, מפתח ידע אקטואלי להוראה במכללה ומשתתף בניסיון לנסח תפיסת ביטחון רשמית ועדכנית למדינת ישראל, בהובלת המטה לביטחון לאומי. חצר המכללות מבקשת לשמש אכסניא ובית מדרש, אשר בו יתפתח ידע חדש ורלבנטי עבור גופי הביטחון הלאומי, מכללות צה"ל וגופי מחקר עמיתים, בארץ ובחוץ לארץ, ובהשתתפותם. המרכז שם לו למטרה לממש את הייעוד המחקרי של המכללה לביטחון לאומי, תוך ניצול יתרונו היחסי בתחום הביטחון הלאומי כמקום מפגש בין-ארגוני ולאור ניסיונם המעשי של התלמידים, הבא לידי ביטוי במחקר.

מרכז המחקר של המכללה לביטחון לאומי

מחנה דיין, גלילות, ד"צ 02624, צה"ל

טל': 03-7607335, דוא"ל: navag@mail.gov.il

הוודפס בבית הדפוס של המכללות הצבאיות

קבצי PDF של גיליונות '**עשתונות**' באתר כתב העת 'מערכות'

maarachot.idf.il/

ראו אור בסדרה:

ליש גור (2015), **עיקרי תפיסת הביטחון של המטה לביטחון לאומי - לשגרה ולחירום** (גיליון 10)

שלום דרור (2014), **מי ישתה את 'כוס התרעלה'? - 'גמישות הרואית' בחשיבה על המענה לאתגר האיראני** (גיליון 9) (מסווג, פנימי, לא להפצה)

בידץ יוסי, דימה אדמסקי (2014), **התפתחות הגישה הישראלית להרתעה - דיון ביקורתי בהיבטיה התאורטיים והפרקטיים** (גיליון 8)

ר"ז (2014), **המחאה בקרב ערביי ישראל - מאפיינים, סיבות ומגמות** (גיליון 7)

אל"ם ש' (2014), **מרכיבי חוסן ארגוני כמפתח לרציפות תפקודית בצה"ל** (גיליון 6)

אפק שרון (2013), **ההתקפה הקיברנטית - קווים משפטיים לדמותה, יישום כללי המשפט הבינלאומי על לוחמה במרחב הקיברנטי** (גיליון 5)

צפרי-אודיז מירב (2013), **השלכות התגרענותה של איראן על 'הסדר הגרעיני העולמי'** (גיליון 4)

אורטל ערן (2013), **על העברת מלחמות האש לשטח האויב ועל הכרעה פרדיגמטית** (גיליון 3) (מסווג, פנימי, לא להפצה)

אורטל ערן (2013), **חדשנות פרדיגמטית בצה"ל? על למידה בהקשרי בניין הכוח, הפעלתו ומה שביניהם** (גיליון 2)

אורטל ערן, תמיר ידעי (2013), **'פרדיגמת סבבי ההרתעה' - דפוס אסטרטגי ודוקטרינה במבוי סתום** (גיליון 1)

עשתונות* - במה למחשבות ורעיונות היא סדרה עתית הרואה אור במסגרת מרכז המחקר של המכללה לביטחון לאומי. הדברים המובאים בה נועדו להביא לקהילת הביטחון הלאומי מחשבות, תפיסות ורעיונות רעננים וחדשניים בנושאים הרלבנטיים לה. הקוראים מוזמנים להרהר ולערער אחר הדברים. אנו חותרים לשיח מאתגר, פתוח וביקורתי, מתוך אמונה ששיח כזה יחדד את עשתונותינו - לבל נאבדם.

***במקרה של אובדן, נא לפנות לגורמים המוסמכים.**

עֶשְׁתּוֹן ז' (מן עשת; מצוי בספרות בעיקר בריבוי) עֶשְׁתּוֹנוֹת, עֶשְׁתּוֹנִים - מחשבות, רעיונות. "כי רבים עשתוני בני אדם" (בן-סירא ג כב); "ורחקו מאד מחשבות איש מעזוז עשתונותיו" (אברהם אבן-עזרא, א 192); "עיניו מפליגות בחלומות וברעיונות עשתונות שונים" (הזז, צל, 120); "אבדו עשתונותיו" (שאול מתהילים קמו ד): נבוך, התבלבל.

(מילון אבן-שושן)

מרכז המחקר, המכללה לביטחון לאומי