לוחמת מידע בין המעצמות במאה ה־21

גיל ברעם ואופיר בראל[1]

במשך שנים נהגה ארצות הברית להניח שיש לה עליונות במרחב הסייבר. תפיסה זו הקשתה עליה לראות כיצד רוסיה וסין הצליחו לשלב בין "לוחמת מידע" ל־"לוחמת סייבר" באופן מוצלח ובכך לחזק את יכולותיהן האסטרטגיות מולה. במאמר נבחנים יחסי הכוחות בין שלוש המעצמות - רוסיה, סין וארצות הברית - בתחום לוחמת המידע בעת הנוכחית. הניתוח מתבצע באמצעות בחינת הדרכים השונות בהן כל מדינה תופסת את מרכיבי לוחמת המידע ומרכיבים קשורים כמו לוחמת סייבר, לוחמה אלקטרונית ועוד, וכן באמצעות סקירת תהליכי בניין הכוח שלהן שמבטאים, הלכה למעשה, את המימוש בפועל של תפיסות אלו.

מבוא

בדצמבר 2018 אמר סגן יושב ראש ועדת המודיעין של הסנאט האמריקני: "בשנת 2016, המוסדות הפדרליים שלנו נתפסו לא מוכנים, והרשתות החברתיות שלנו לא העריכו שגורמים רוסיים יוכלו לבצע בהן מניפולציות. בכנות, היינו צריכים לראות את זה מגיע".[2] במשך שנים נהגה ארצות הברית להניח שיש לה עליונות במרחב הסייבר. תפיסה זו הקשתה עליה לראות את האופן שבו רוסיה וסין הצליחו לשלב בין "לוחמת מידע" ל"לוחמת סייבר" באופן מוצלח ובכך לחזק את יכולותיהן האסטרטגיות מולה.

---

1 גיל ברעם היא מנהלת המחקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון. אופיר בראל הוא חוקר בסדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל אביב. המחברים מבקשים להודות לד"ר הראל מנשרי, ראש תחום סייבר במכון הטכנולוגי בחולון, לסא"ל רווה גלילי ולסרן אור גליק על הערותיהם המועילות וסיועם בכתיבת מאמר זה.

2 Sen. Mark Warner, "A New Doctrine for Cyberwarfare & Information Operations", *Gizmodo,* December 7, 2018, 1-3, https://gizmodo.com/senators-cyber-doctrine-calls-for-u-s-to-redraw-the-bl-1830943004 (accessed: January 9, 2019).

מטרת מאמר זה היא לבחון ולנתח את יחסי הכוחות בין שלוש המעצמות - רוסיה, סין וארצות הברית - בתחום לוחמת המידע בעת הנוכחית. הניתוח מתבצע באמצעות בחינת הדרכים השונות שבהן כל מדינה תופסת את מרכיבי לוחמת המידע השונים, ובאמצעות סקירת תהליכי בניין הכוח שלהן המבטאים, הלכה למעשה, את המימוש בפועל של תפיסות אלו.

המאמר בנוי באופן הבא: בחלק הראשון מוצגות ההגדרות הקיימות למונח המנחה של המאמר - לוחמת מידע - והקשר בינו לבין המונח "אבטחת סייבר" הבא לידי ביטוי בצורה שונה אצל כל מעצמה. כן נדונים מונחים קשורים נוספים כגון לוחמת סייבר, לוחמה אלקטרונית ועוד. בחלק השני אנו מדגימים את המשמעות השונה שמעניקה כל מדינה למושגים הללו, דנים בה ובוחנים את תהליכי בניין הכוח הצבאי שמקיימת כל אחת בתחומים אלה. בחלק השלישי מבוצע ניתוח השוואתי בין המדינות במטרה לבחון את האופן שבו כל מדינה תופסת את תחום לוחמת המידע, ואת האופן שבו תפיסה זו באה לידי ביטוי בפעולותיה בזירה הבינלאומית. בחלק האחרון אנו מצביעים על מגמות עתידיות בנושא ועל הדרכים שבהן יכולה ארצות הברית לפעול כדי לשמור על עליונותה בתחום.

לוחמת מידע ותפיסתה במעצמות

לצורך הגדרת המונח לוחמת מידע העומד בבסיס מאמר זה ובמטרה להציג את המובן הרחב ביותר של לוחמת המידע אנו מתבססים על הגדרות אקדמיות בשילוב ההגדרות הקיימות בצה"ל. לוחמת מידע היא מסגרת שבה התוקף מפעיל יכולות (בדרך כלל טכנולוגיות) כדי להשפיע על תהליך קבלת ההחלטות של היריב או לשבשו תוך הגנה על יכולות אלו בצד שלו. מדובר בצעדים שמכוונים להשפיע על מאגרי המידע של היריב על מנת להשיג הישג משמעותי או הכרעה.[3] באמצעות שיבוש סביבת המידע שהיריב מסתמך עליה, יכולותיו לתפוס את המציאות ולגבש צעדי פעולה נפגעות.[4] צה"ל מגדיר לוחמת מידע כך: "כלל השיטות והפעולות שנוקטים כוחותינו על מנת להשיג עליונות במרחב המידע, באמצעות פעולות המכוונות לשלושה תחומים שונים: השפעה על המידע המצוי בידי האויב, על תהליכי קבלת החלטותיו ועל מערכות המידע והתקשוב שלו; השפעה על קהלי יעד ניטרליים ועל אזרחי מדינת ישראל; והגנה על המידע, על תהליכי קבלת ההחלטות ועל מערכות המידע של כוחותינו".[5]

רוסיה, סין וארצות הברית פיתחו הבנות שונות למונחים לוחמת מידע ואבטחת סייבר (cyber security) שנבעו בין היתר מהבדלים מהותיים בהגדרות ובמשמעות

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

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

5 אמ"ץ-תוה"ד, המילון למונחי תורה צבאית (טיוטה פנימית), מטכ"ל 10-1, התשע"ט-2018.

של כל מונח. ניתן לזהות שתי גישות שונות לאבטחת סייבר שהמעצמות פיתחו. הראשונה, המאופיינת כגישה הגנתית, היא הגישה המערבית בהובלת ארצות הברית ומדינות ברית נאט"ו. גישה זאת מגדירה אבטחת סייבר כהגנה על מערכות המחשוב מפני נזקים של מתקפות הרסניות ואיסוף מידע. הגישה השנייה, המאופיינת כהתקפית יותר והיא הגישה שרוסיה וסין מובילות אותה, מגדירה אבטחת סייבר כאבטחת מידע וכשליטה על מידע כפוטנציאל לערעור היציבות הפנימית. בהתאם לכך ניתן להבין שפעולות התקפיות בתחום הסייבר מיועדות להעמיק את השליטה באינטרנט ובמרחב הסייבר כמרחב של מידע.[6]

המונחים 'לוחמת מידע' ו'אבטחת סייבר' כוללים בין היתר ביצוע פעולות התקפיות והגנתיות מגוונות בתחומי המידע והטכנולוגיה. הפעולות כוללות מספר מונחים נוספים וביניהם 'לוחמת סייבר', 'לוחמה אלקטרונית' ו'לוחמה פסיכולוגית'. "לוחמת סייבר" (Cyber Warfare) מוגדרת בצה"ל 'לוחמת סב"ר' (סביבת בינה רשתית) ומשמעותה היא לוחמת מידע המנצלת את מרחב הסייבר או הפועלת כלפי המשתמשים בו. בלוחמה זאת כלולים שלושה תחומים: איסוף מידע על משתמשים, על מערכות אלקטרוניות והתקניהן; התקפת גורמים עוינים, אמצעיהם ומערכותיהם; והגנת מערכות צה"ל מפני חדירות של גורמים עוינים.[7]

חלוקה נוספת המוצעת בספרות היא ההבדלה בין 'לוחמת סייבר אסטרטגית' (Strategic Cyberwar) לבין 'לוחמת סייבר אופרטיבית' (Operational Cyberwar). לוחמת סייבר אסטרטגית היא כלל תקיפות הסייבר שצד אחד מפעיל נגד צד אחר. לוחמת סייבר אופרטיבית היא שימוש במתקפות סייבר בהקשר של מלחמה פיזית נגד הצד השני, כלומר לוחמת סייבר אופרטיבית מתבצעת בנוסף ללוחמה קינטית.[8]

'לוחמה אלקטרונית' (Electronic Warfare) היא היכולת למנוע מהאויב להשתמש ביתרונות הספקטרום האלקטרומגנטי תוך כדי שימור היכולת לכוחות ידידותיים. היא מיושמת לגבי כל הספקטרום, והיא יכולה להתבצע מהאוויר, מהים, מהיבשה ומהחלל. לוחמה אלקטרונית כוללת שלושה ענפי משנה: 'תמיכה אלקטרונית' (Electronic Support) שמטרתה היא לזהות את האותות שהאויב משדר על מנת ללמוד את מאפייניו האלקטרוניים; 'התקפה אלקטרונית' (Electronic Attack) הכוללת את כלל האמצעים הננקטים על מנת להפריע לאויב להשתמש בספקטרום האלקטרומגנטי; ו'הגנה אלקטרונית' (Electronic Protection) המיועדת להגן על תשתיות אלקטרומגנטיות מפני פעולות התקפיות של האויב.[9] יש לציין כי במרוצת

6 Valentine Weber, "States and their Proxies in Cyber Operations", *Lawfare*, May 15, 2018 https://www.lawfareblog.com/states-proxies-cyber-operations (accessed: April 2, 2019).

7 אמ"ץ-תוה"ד, המילון למונחי תורה צבאית.

8 Martin Libicki, "Cyberdeterrence and Cyberwar", *RAND*, 2009, . 8. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed: April 2, 2019).

9 G.W. Stimson. et. al., *Stimson's Introduction to Airborne Radar, Electronic Warfare 3rd Edition* (Institution of Engineering and Technology, 2014): 509, 510, 514, 517.

השנים יחידות לוחמה אלקטרונית שונות, כמו הצי העשירי האמריקני (U.S. Tenth Fleet), הפכו ליחידות לוחמת סייבר המשלבות בתוכן עיסוק בלוחמה אלקטרונית.

'לוחמה פסיכולוגית' (Psychological Warfare) היא מונח שקיבל במרוצת הזמן הגדרות שונות מחוקרים רבים,[10] והמשותף להן הוא שהלוחמה הפסיכולוגית היא שימוש באמצעים שאינם אלימים, ושמכוונים כלפי האויב ומיועדים לפגוע ברצונו להמשיך להילחם.[11] לשם כך ניתן להעביר לאויב מסרים מסוגים שונים, כמו הבטחות, איומים, הגדרת תנאים לסיום הלחימה, עידוד עריקה ומסרים נוספים.[12] כיום נראה שהלוחמה הפסיכולוגית וניסיונות להשפיע על התודעה הם חלק בלתי נפרד מלוחמת המידע בין מדינות.

באמצעות הצגת ההגדרה הרחבה למונח 'לוחמת מידע' ומרכיביו במדינות השונות אנו מניחים את התשתית לניתוח אופן השימוש שעושות שלוש המעצמות בכלים אלה, כפי שיוצג בפרק הבא. כבר כאן חשוב להצביע על ההבדלים בהגדרות השונות המובילים לכך שלכל אחת משלוש המעצמות יש תפיסה שונה, שתוצאתה בניין כוח שונה בתחום הרחב של לוחמת המידע. השוני בין המעצמות בא לידי ביטוי גם בפער הקיים בין ההגדרות ללוחמת מידע לבין המשמעות המבצעית השונה שכל מעצמה מעניקה לכל פן של לוחמת המידע, והדרכים שבהן מונחים אלה ממומשים בפועל.

מאפייני המעצמות בתחומי לוחמת המידע - כדי לעמוד על מאפייני השימוש של כל מעצמה בלוחמת מידע נבחן את האופן שבו כל אחת משלוש המעצמות מגדירה את המונחים 'לוחמת מידע', 'לוחמת סייבר', 'לוחמה אלקטרונית' ו'לוחמה פסיכולוגית'; את התחומים שבהם לכל מדינה יש עליונות טכנולוגית; את השינויים האסטרטגיים שכל מדינה נקטה בתחומים הללו; את מערך הכוחות של כל מדינה בתחומים הללו; באיזה תחום משקיעה כל מעצמה; וכיצד התפיסות התיאורטיות בנושא לוחמת מידע באות לידי ביטוי בפועל. כך נוכל להבין טוב יותר את חלוקת העוצמה הנוכחית בזירת לוחמת המידע העולמית.

---

10 מבין ההגדרות השונות, ניתן לציין את P. M. Taylor. שהגדיר את הלוחמה הפסיכולוגית כתהליך שכנוע המיושם בתיאום עם מבצעים צבאיים, ושמטרתו היא לשכנע את קהל היעד של האויב לפעול בהתאם לרצונות של יוזם הל"פ, (בדרך כלל כדי לעודד עריקה או כניעה).
P.M Taylor, *War and the media: propaganda and persuasion in the Gulf War* (Manchester University Press, United Kingdom. 1992): 22, 155.
כמו כן ניתן לציין גם את A. H. Paddock. המציין שלצד דיכוי רצון האויב להילחם, הלוחמה הפסיכולוגית מיועדת גם להעלות את המורל של קבוצות שאינן עוינות.
A. H. Paddock., "U.S Military Psychological Operations: Past, Present, and Future", in *Psychological Operations and Political Warfare in Long-Term Strategic Planning*, ed. J. Radvanyi, (New York: Praeger Publishers, 1990): 19.

11 Ahmadhasan Sauffiyan and Anitawati Mohd Lokman, "Prelude to Psychological Warfare in Malaysia - A Conceptual Understanding, Experience and Future Advancement", *IEEE Symposium on Humanities, Science and Engineering Research* (2012): 1326.

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

לוחמת מידע

רוסיה

רוסיה מנסה לפצות על חולשתה הכלכלית והצבאית באמצעות שימוש באסטרטגיות לוחמת מידע המאפשרות להשיג תוצאות משמעותיות, ושעלותן פחותה בהשוואה לפעולות קינטיות.[13] ללוחמת המידע הרוסית יש שתי מטרות מרכזיות: הראשונה, שימוש במידע כדי ללבות מחלוקות פוליטיות וחברתיות שמטרתן להחליש את מדינות המערב.[14] לשם כך הממשל הרוסי מקדיש מאמצים להפיץ מסרים שנועדו לפגוע בדומיננטיות הפוליטית והערכית של המערב ולקדם מסד ערכים חלופי.[15] המטרה השנייה היא הטעיית האויב בנוגע לכוונות האמיתיות של הממשל הרוסי. הטעיית האויב היא יסוד מפתח באסטרטגיית לוחמת המידע הרוסית, בייחוד בזמני מלחמה.[16] כך שומרת רוסיה על אי־הבהירות לגבי פעולותיה המלחמתיות, והדבר מפחית את הסיכוי שהמערב יפעל נגדה.[17] רוסיה אינה מכריזה על מלחמה באופן רשמי, אלא היא מוציאה אותה לפועל בחשאיות. כך היא יוצרת חוסר ודאות בצד הנתקף ומקשה עליו לגבש תגובה מהירה בהתאם. שימוש בלוחמת מידע תומך במבצעים הצבאיים של רוסיה, מסייע להארכת המלחמה ומגדיל את היכולת של רוסיה להשפיע על מהלך העניינים ולכוון להארכת משך המלחמה באופן הנוח לה.[18] למעשה ניתן לומר כי ברוסיה תחום הסייבר מוכפף במידה רבה מאוד ללוחמת המידע.

תפיסת לוחמת המידע הרוסית כוללת מאמצים מקדימים שנועדו להשיג רווח פוליטי ולשלוט במרחב המידע תוך שימוש בכלל האמצעים בחברה, כולל קבוצות האקרים ("פצחנים") ואזרחים פרטיים.[19] לפי תפיסתה לוחמת המידע היא ארגון עולם המידע והתפיסות הפסיכולוגיות לפי האינטרסים של הצד המשתמש בלוחמת המידע, והיא אמצעי מרכזי להשגת עוצמה כלכלית ופוליטית במאה ה־21.[20] רוסיה משתמשת בלוחמת המידע לצורך פגיעה במערכות תקשורת, מחשוב, מערכות

13 Maria Snegovaya, *Putin's Information Warfare in Ukraine - Soviet Origins of Russia's Hybrid Warfare*, (Institution for the Study of War, September 2015), 11.

14 Brian Klaas, "Stop Calling it 'Meddling', It's Actually Information Warfare", *The Washington Post*, July 17, 2018 https://www.washingtonpost.com/news/democracy-post/wp/2018/07/17/stop-calling-it-meddling-its-actually-information-warfare/?utm_term=.873026b227e9 (accessed: January 15, 2019).

15 Defense Intelligence Agency, *Russia Military Power- Building a Military to Support Great Power Aspirations* (Washington, 2017), 39.

16 Snegovaya, *Putin's Information Warfare in Ukraine*, 11.

17 Rod Thornton, "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *RUSI Journal*, 160, no. 4 (July 2015): 44.

18 Snegovaya, *Putin's Information Warfare in Ukraine*, 11-12.

19 Catherine A. Theohary, "Information Warfare: Issues for Congress", *Congressional Research Service* (Washington, March 5, 2018), 1-2.

20 Ieva Berzina, "The Narrative of 'Information Warfare against Russia' in Russian Academic Discourse" *Journal of Political Marketing*, 17 no.2 (2018): 164.

אלקטרו־מגנטיות ועוד. במקביל היא מתמקדת בתפיסות הפסיכולוגיות של מקבלי ההחלטות, של הציבור ושל האליטות בצד שנגדו מפעילים לוחמת מידע.[21]

פעילות לוחמת המידע הרוסית החלה עוד לפני המלחמה הקרה, והיא המשך למדיניות "האידיוטים השימושיים" שנוסדה בימי המהפכה הקומוניסטית ונהגתה על ידי וילי מיינצברג, ידידו הגרמני של לנין. העקרונות העומדים בבסיס אסטרטגיית לוחמת המידע הרוסית מתבססים על עקרונות שפיתחו תיאורטיקנים סובייטים במהלך המלחמה הקרה. במהלך שנות השישים פותח המונח "שליטה תגובתית" (Reflexive Control) הכולל צעדים שנועדו לעצב את תפיסת היריב ובכך לגרום לו לבצע צעדים לטובת היוזם. על מנת להשתמש בשליטה התגובתית באופן מוצלח צריך להכיר היטב את טבע האויב, את תפיסת עולמו ואת דרכי החשיבה שלו. הכרת האויב מאפשרת ליצור עבורו מסרים שמעצימים את פחדיו, וכך לשלוט בצורה טובה יותר במהלכיו.[22]

שורת אירועים שהתרחשו במהלך העשור הראשון של המאה ה־21, הובילה לעלייה בחשיבותה של לוחמת המידע באסטרטגיה הרוסית. בשנים הללו התרחשו מהפכות אזרחיות שהובילו לחילופי שלטון וביניהן "המהפכה הכתומה" בשנת 2004 באוקראינה ו"מהפכת הצבעונים" שנה לאחר מכן בקירגיזסטן וכן המלחמה מול גיאורגיה בשנת 2008.[23] לאחר המלחמה, שבה התגלתה הנחיתות של לוחמת המידע הרוסית מול המערב, החליט הממשל הרוסי לגבש אסטרטגיה שתנצל אמונות וערכים פוליטיים של המערב על מנת לקדם את האינטרסים של הממשל הרוסי.[24]

רוסיה משקיעה סכומים גבוהים יותר מארצות הברית בתחום לוחמת המידע. נכון לשנת 2015 השקיעה רוסיה 1.4 מיליארדי דולרים במבצעי מידע בתוך המדינה ומחוצה לה. לעומתה, ארצות הברית השקיעה באותה התקופה כ־730 מיליוני דולרים לאותה מטרה.[25] מתוך הסכום שהשקיעה ממשלת רוסיה, הופנו מדי שנה 400-500 מיליוני דולרים למבצעי מידע שכוונו לקהילה הבינלאומית, לעומת 20

21 Ibid, 164.

22 Alexander Averin, "Russia and it's Many Truths", in *Fake news - a Road Map* (Riga: NATO Strategic Communications Centre of Excellence, 2018), 62.

23 Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea", *Parameters*, 47 no. 2 (summer 2017): 59.

24 Bradley Jardine, "Russia's New 'Useful Idiots'?", *Coda Story*, October 5, 2017 https://codastory.com/disinformation-crisis/foreign-proxies/russia-s-new-useful-idiots (accessed: January 9, 2019).

25 Maj. Luke Karl, Maj. Joseph Lane & Cmdr. David Sanchez, "How to Stop Losing the Information Warfare", *Defense One*, July 26, 2018, https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/ (accessed: April 2, 2019).

מיליוני דולרים שממשלת ארצות הברית השקיעה במבצעי מידע המכוונים לקהלים דוברי רוסית.[26]

הוצאה לפועל של מבצעי לוחמת מידע. בעשור האחרון השקיע צבא רוסיה בפיתוח יכולותיו בתחום לוחמת המידע.[27] אחד מסוגי הפעולות העיקריים המזוהים עם לוחמת המידע והסייבר הרוסית הוא מעורבות במערכות בחירות זרות. רוסיה התערבה במערכות בחירות בשני גלים. הגל הראשון התרחש בשנים 1991–2014. לאחר התמוטטות הגוש הסובייטי החלה רוסיה להתערב במערכות בחירות במדינות שהיו בעבר חלק מברית המועצות. היא חיזקה את המועמדים הפרו־רוסיים וניסתה להחליש מועמדים אנטי־רוסיים. הגל השני החל בשנת 2014 ונמשך עד היום. החל משנה זו המעורבות הרוסית התרחבה למקומות נוספים ובהם הבלקן, מערב אירופה וארצות הברית. המעורבות הייתה הן במערכות בחירות והן בתהליכים ובאירועים שבהם היה הציבור מפולג, והפעילות של רוסיה ליבתה את הפילוג והקיטוב החברתי.[28] מאחורי מתקפות הסייבר הרוסיות על דמוקרטיות עומד מניע אידיאולוגי, כלומר רצון להראות שבחירות דמוקרטיות הן פגומות מיסודן, מאחר שהן למעשה מעשה הונאה.[29] בינואר 2017 אמר ראש המודיעין הלאומי האמריקני, כי מטרת ההתערבות הרוסית בבחירות לנשיאות ארצות הברית בשנת 2016 הייתה לערער את אמון הציבור האמריקני במשטר הדמוקרטי ולפגוע בתקינות התהליך הדמוקרטי.[30]

מבין הגופים האזרחיים השותפים למאמץ הרוסי ניתן למנות את Roskomnadzor האחראי על הצנזורה על כלי תקשורת ואתרי אינטרנט במדינה. באמצעות גוף זה הממשל הרוסי בוחן מניפולציות תקשורתיות שונות, והן מיושמות בהמשך ברשתות החברתיות כלפי קהלי יעד זרים.[31] מאחורי השימוש ברשתות החברתיות לצורך זה עומדת הסוכנות לחקר האינטרנט (Internet Research Agency) המעסיקה מאות

26 Warren Strobel, "U.S Losing 'Information War' to Russia, Other Rivals: Study" *Reuters*, March 25, 2015 https://www.reuters.com/article/us-usa-broadcasting-idUSKBN0ML1MN20150325 (accessed: April 2, 2019).

27 Defense Intelligence Agency, *Russia Military Power,* 38.

28 Lucan Ahmad Way and Adam Casey, "Russia has been meddling in Foreign Elections for Decades. Has it Made a Difference?", *The Washington Post*, January 8, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/?utm_term=.3497a14027cd (accessed: January 13, 2019).

29 Weber, "States and their Proxies in Cyber Operations".

30 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (Washington: January 6, 2017): 1.

31 Clint Watts, "Russia's Active Measures Architecture: Task and Purpose", *Alliance for Securing Democracy*, May 22, 2018 https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/ (accessed: April 4, 2019).

עובדים המוציאים לפועל מבצעי השפעה ברשתות החברתיות.[32] לדוגמה, במהלך הבחירות בארצות הברית בשנת 2016 התחזו עובדי הסוכנות לאזרחים אמריקניים והפיצו מסרים שנועדו להשפיע על מהלך הבחירות.[33]

גוף חשוב נוסף הוא שירות המודיעין הרוסי (Foreign Intelligence Service - SVR). תפקידיו, בין היתר, הם לאתר גופים שונים מחוץ לרוסיה האוהדים את הגישה הרוסית, לגייסם ולתמוך בהם.[34]

מעורבות רוסיה בבחירות בארה"ב כחלק מלוחמת מידע (אילוסטרציה, מרכז דדו)

סין

החל משנת התשעים של המאה העשרים החלו השלטונות הסיניים לגלות התעניינות במלחמות של ארצות הברית, שהתבססו על טכנולוגיה רשתית ושאופיינו בא־סימטריות, במערכות בקוסובו, באפגניסטן ובעיראק.[35] סין התמקדה בשימוש בלוחמת מידע על מנת לשבש את מערכות הפיקוד והשליטה של היריב מתוך הבנה כי פגיעה במערכות אלו תוביל לפגיעה בכלל יכולות הלחימה שלו.[36]

המטרה הראשונה במעלה של המשטר הסיני היא להגן על עצמו, ולפיכך חלק ניכר מפעילות לוחמת המידע מיועד לצורכי פנים במשולב עם הפעילות החיצונית. התיאוריה הסינית ללוחמת מידע משויכת לקונספט "המלחמה העממית" (the people's war) שפותחה עוד בימי מאו זדונג, והיא כוללת שימוש בטכנולוגיות מידע באמצעות מאות מיליוני אזרחים במטרה להשפיע על מקבלי החלטות של הצד השני ולהשיג רווח בלוחמה א־סימטרית.[37] בהגות הצבאית הסינית נעשה שימוש

32 Adrian Chen, "The Agency", *The New York Times*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html (accessed: January 13, 2019).

33 Dan Mangan & Mike Calia, "Special Counsel Mueller: Russians Conducted 'Information Warfare' Against US During Elections to Help Donald Trump Win", *CNBC*, February 16, 2018. https://www.cnbc.com/2018/02/16/russians-indicted-in-special-counsel-robert-muellers-probe.html (accessed: January 13, 2019).

34 Watts, "Russia's Active Measures Architecture".

35 Jason Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness", *Culture Mandala*, 8 no. 1 (October 2008): 28.

36 John Costello and Peter Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations", in *China's Evolving Military Strategy*, ed. Joe McReynolds (Washington, DC: Jamestown Foundation, 2016), 179-180.

37 Theohary, "Information Warfare: Issues for Congress", 2.

במונח Assassin's Mace (shashoujian בסינית) שמשמעותו "נשק" או "טקטיקה" היכולים, באמצעות מהלכים מפתיעים ומחושבים היטב, להפתיע ולשנות את מאזן הכוחות.[38] בימינו לוחמת המידע נתפסת אצל הסינים כאמצעי להפעלת מתקפה בלתי צפויה על היריב על מנת להשיג רווח אסטרטגי בעימות.[39] התפיסה הסינית רואה בחבלה במערכות המידע ובמניפולציות על המידע עיקרון אחד, ולא שני עקרונות נפרדים, כפי שתופסת זאת ארצות הברית. הסינים רואים את תחום הסייבר כמבטא תהליך מעבר מחברה מבוססת תעשייה לחברה מבוססת מידע - תהליך שנקרא informatisation. עבור סין מרחב הסייבר הוא משני למרחב המידע הכולל את התקשורת בין בני האדם ואת הצד הקוגניטיבי של עיבוד המידע.[40]

ללוחמת המידע הסינית יש שתי מטרות מרכזיות: לשמור על הדומיננטיות של המפלגה הקומוניסטית בפוליטיקה הפנימית (באמצעות צנזורה והפצת דיסאינפורמציה) ולהוציא לפועל לוחמת מידע לטובת האינטרסים הסיניים הבינלאומיים. החל מתחילת שנות האלפיים לוחמת המידע הסינית מכוונת ליישם את אסטרטגיית "שלוש המלחמות" בתחום המידע - מלחמה על דעת הקהל, לוחמה פסיכולוגית ולוחמה משפטית. מטרת האסטרטגיה היא לשלוט בשיח הדומיננטי ולכוונו לטובת סין[41] ולצמצם את יכולת יריביה לפעול באמצעות שלוש דרכים: לגרום לאויב לפקפק במניעים שלו עצמו, לייצר מחלוקות בתוכו ולהצר את פעולותיו. בזמן מלחמה פעילות זו יכולה גם לפגוע ברצון של האויב להילחם. במסגרת אסטרטגיית שלוש המלחמות נעשה שימוש בסוגי מידע שונים על מנת להשיג מטרות צבאיות אסטרטגיות, לזכות בניצחון בלוחמה פסיכולוגית ולרשום הישגים פוליטיים.[42]

האסטרטגיה הסינית ללוחמת מידע ולוחמת סייבר מבוססת על ביקורתיות כלפי הדומיננטיות המערבית בזירה הבינלאומית. סין מודאגת מכך שארצות הברית מנצלת את מעמדה - הן כמובילה עולמית בסייבר והן כמעצמה - על מנת לעצב סביבה בינלאומית הנוחה לה.[43] לפי התפיסה של סין המערב מנסה לפגוע בשלום האומה הסינית ובאחדותה ובשלטון המפלגה הקומוניסטית באמצעות עידוד תהליכי דמוקרטיזציה וליברליזציה במדינה.[44] הביקורת הסינית כלפי הפעילות האמריקנית

38 Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness", 67-68.

39 Costello and Mattis, "Electronic Warfare and the Renaissance of Chinese Information Operations", 179-180.

40 Mikk Raud, *China and Cyber: Attitudes, Strategies, Organizations* (Riga: NATO Cooperative Cyber Defence Centre of Excellence, 2016), 10.

41 Jean-Baptiste Jeangène Vilmer et al., *Information Manipulation - A Challenge for our Democracies* (Paris: The Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces, 2018): 58-60.

42 Dean Cheng, "China and Cyber: The Growing Role of Information in Chinese Thinking", in *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, ed. F. Rugge (Milano: Italian Institute for International Politics Studies, 2018), 85-87.

43 Ibid, 7.

44 Cheng, "China and Cyber", 84.

מתבצעת מתוך תפיסה של שוויון כוחות ולא מעמדת נחיתות. בהתאם לכך נוצר מתח בנוגע לשאלה מי צריכה להיות המעצמה הדומיננטית במרחב האינטרנט - ארצות הברית או סין.[45] יש בכך שינוי מהתפיסה הסינית מתחילת שנות התשעים שלפיה סין הייתה נחותה מול ארצות הברית, ובהתאם לכך היא ראתה בלוחמת המידע אמצעי של לוחמה א־סימטרית.[46]

הסינים מייעדים תפקיד מיוחד ללוחמת המידע וללוחמת הסייבר גם בזמני עימות. הצבא הסיני רואה חשיבות גדולה בהרס מערכות האויב, והעדיפות היא לפגיעה בפעילות המערכת או בשיתוקה ולאו דווקא הרס מוחלט שלה.[47] לכן הרצון של סין להשיג עליונות במרחב המידע קשור להנחה שפגיעה במערכים הרגישים של האויב תוביל לניצחון מהיר.[48] בסיס העדפה זו טמון בגישה הסינית של ניצחון ללא מאבק. מונח זה קיים עוד מימי מאו זדונג, ומשמעותו כיום היא השפעה על קבלת ההחלטות של היריב באמצעים שהם מתחת לסף המלחמה. כך ניתן להשיג מטרות אסטרטגיות בלי להיגרר למלחמה. בעיני הסינים אם שיטה זו נכשלת, הצבא צריך להתכונן לאפשרות של הכרעה מהירה. בהכרעה כזו המידע משמש מרכיב חשוב, מאחר שהוא מספק את האפשרות לקבל החלטות במהירות במישור הפוליטי ובמישור המעשי.[49]

לוחמת המידע הסינית, כמו הרוסית, מנוהלת באמצעות מערך נרחב הכולל גופים צבאיים וגופים אזרחיים. במישור הצבאי ניתן למנות את ה־Political Work Department, שהיא חלק ממשרד ההגנה הסיני, ואת הפיקוד המרכזי של הצבא המנהלים קשרי עבודה צמודים בתחום לוחמת המידע. בתחום האזרחי אחראית ה־General Political Department, אחת מארבע המחלקות הכלליות שמרכיבות את המפלגה הקומוניסטית הסינית, על השימוש בלוחמת מידע באמצעות הוצאה לפועל של אסטרטגיית "שלוש המלחמות". המיניסטריון לביטחון המדינה והמיניסטריון לביטחון הפנים, יחד עם כמות גדולה של אמצעי תקשורת הנמצאים בבעלות המדינה, אחראים על הפצת המסרים בתוך המדינה ומחוצה לה בהתאם לאסטרטגית הממשל.[50]

כוח הסיוע האסטרטגי, ה־SSF (Strategic Support Force), הוא הגוף המרכזי ביישום אסטרטגיית לוחמת המידע הסינית. ה־SSF הוקם בסוף שנת 2015 כחלק מרפורמה נרחבת בבניין הכוח הצבאי של סין, והוא משמש כיחידה המרכזית ללוחמת מידע, לוחמה פסיכולוגית, לוחמה אלקטרומגנטית ותחום החלל של

45 Raud, *China and Cyber: Attitudes, Strategies, Organizations*, 8.

46 John Costello & Joe McReynolds, *China's Strategic Support Force: a Force for a New Era* (Washington: National Defense University Press, 2018), 4.

47 Costello & McReynolds, *China's Strategic Support Force,* 45.

48 Raud, *China and Cyber: Attitudes, Strategies, Organizations,* 20.

49 Costello & McReynolds, *China's Strategic Support Force,* 45.

50 Vilmer et al., *Information Manipulation - A Challenge for our Democracies,* 58-60.

הצבא.[51] בין היתר אחראי ה־SSF על הפעלה משולבת של מערכות לוחמת מידע, לוחמה אלקטרונית ולוחמת סייבר במטרה לשתק את מערכות האויב, בייחוד את מערכות הפיקוד שלו, בשלבים מוקדמים של המלחמה.[52] הקמת ה־SSF מייצגת שלושה עקרונות מרכזיים באסטרטגיית לוחמת המידע הסינית, ואלה הם: (1) מעבר מתפיסה של מדינה חלשה הנעזרת ביכולות של לוחמה א־סימטרית לשם יצירת איזון, למדינה שוות כוח למערב; (2) תפיסת לוחמת המידע כמאבק הנמצא בכל מקום ובכל עת, והמאבק הצבאי הוא אלמנט אחד שלו;[53] (3) איחוד הפן ההתקפי והפן ההגנתי בסייבר.[54]

הוצאה לפועל של מבצעי לוחמת מידע. סין מנהלת מבצעי לוחמת מידע בשלוש חזיתות שונות. החזית הראשונה היא הזירה הבינלאומית שבה הממשלה מנהלת מערך ענף של פעולות לוחמת מידע. בין פעולות אלו ניתן למנות ניסיונות השפעה על מנהיגים לשעבר של מדינות אירופה, השתלטות על אמצעי התקשורת בשפה הסינית באירופה והשפעה על קהילות סינים המתגוררות ברחבי העולם.[55] פעולות אלה שמטרתן לשפר את התדמית של סין ברחבי העולם, זוכות לתקצוב שנתי הנע בין שבעה לעשרה מיליארדי דולרים.[56]

החזית השנייה היא החזית הפנימית. על פי ההערכות ממשלת סין מעסיקה בין חצי מיליון לשני מיליוני איש בהפצת תכנים ברשתות החברתיות. ההערכה היא שבכל שנה ממשלת סין מייצרת באמצעותם 448 מיליון תכנים (רשומות ["פוסטים"], חדשות, תגובות ועוד). מספר זה מתייחס גם לפרסום רשומות מזויפות מטעם הממשל – המציגות דעות אותנטיות של אנשים מהשורה. התכנים הללו מתעמתים עם כל אדם המבקר את מדיניות הממשל או את מנהיגיו, בתוך המדינה ומחוצה לה.[57] פעילות זו משקפת את ההנחה שהאיום הגדול ביותר על יציבות הממשל אינו נובע מאיומים צבאיים חיצוניים, אלא מהתערערות השלטון מבפנים באמצעות מחאות. בהתאם לכך הרשומות הללו מקדמות בעיקר השקפות חיוביות על הממשל ועל ההיסטוריה של המפלגה הקומוניסטית ונמנעות מעימות ישיר עם הטענות השליליות.[58]

החזית השלישית היא טאיוואן. קיימת סבירות מסוימת שסין תעשה שימוש

51 Claude Arpi, "Be Prepared for China's Electronic Warfare", *Rediff News*, June 27, 2017. https://www.rediff.com/news/special/be-prepared-for-chinas-electronic-warfare/20170627.htm (accessed: January 13, 2019).

52 Costello & McReynolds, *China's Strategic Support Force: a Force for a New Era*, 2.

53 Ibid, 45.

54 Secretary of Defense, *Annual Report to Congress - Military and Security Developments Involving the People's Republic of China 2018* (Washington, 2018), 41.

55 Vilmer et al., *Information Manipulation - A Challenge for our Democracies,* 58-61.

56 David L. Shambaugh, *China Goes Global - The Partial Power* (Oxford: Oxford University Press, 2013), 207.

57 Gary King, Jennifer Pan & Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument", *American Political Science Review*, 11 no.3 (2017): 484-488.

58 Ibid, 496-497.

באינטרנט כדי להשפיע על תודעת האזרחים בטאיוואן, כדי להתכונן למתקפה או לערער את עצמאות סין באופן הנמנע מקונפליקט.[59] כבר היום סין משתמשת בטאיוואן בתור שדה ניסויים שבו היא בודקת כלי פריצה שונים, לפני שהיא מנסה אותם במקומות אחרים.[60] זאת בדומה לרוסיה המבצעת תקיפות סייבר באוקראינה גם לשם בחינת יכולתה לבצע תקיפות סייבר נרחבות יותר במקומות אחרים בעולם.[61] בנוסף פועלת סין גם באזורים נוספים המשמשים מוקד עניין עבורה בדרום מזרח אסיה ואפילו במחוזות שהוחזרו לסין דוגמת מקאו והונג קונג.

ארצות הברית

לפי תפיסת מפקדת המטות המשולבים "לוחמת מידע" מופעלת על מנת להשיג שלוש מטרות: (1) לשנות או לשמר תפיסות המעצבות את התנהגות השחקנים; (2) לשמור ולהגן על התפיסות שמנחות את פעולת המטות המשולבים ובעלות הברית; (3) לעשות שימוש במידע כמרכיב המחזק את היתרון הצבאי האמריקני.[62] בצבא ארצות הברית רווח השימוש במונח "מבצעי מידע" (Information Operations), ומחלקת ההגנה האמריקני מגדירה אותם כיישום במהלך מבצע צבאי של אמצעים שונים שנועדו להשפיע, להפריע או לפגוע במעגלי קבלת ההחלטות של היריב ושל יריבים פוטנציאליים תוך כדי הגנה על מעגלי קבלת ההחלטות של הצד האמריקני.[63] מונח נוסף שצבא ארצות הברית פיתח הוא "מבצעי תמיכת מידע צבאיים" (Military Information Support Operations) המוגדרים כמבצעים שנועדו להעביר מידע לקהלי יעד זרים (ממשלות, ארגונים, קבוצות אנשים ויחידים) על מנת להשפיע על רגשותיהם, מניעיהם והבנתם את המציאות. המטרה היא להשפיע על התנהגותם באופן המיטיב עם מטרות ארצות הברית.[64]

---

59 Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness", 69.

60 Rene Millman, "Taiwan to Share Chinese Jacking Attempts with Private Firms to Train AI Defences", *ITPRO*, October 23, 2018, https://www.itpro.co.uk/hacking/32183/taiwan-share-chinese-hacking-attempts-with-private-firms (accessed: January 13, 2019).

61 Kim Zetter, "The Ukrainian Power Grid was Hacked Again", *Motherboard*, January 10, 2017, https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report (accessed: January 13, 2019).

62 Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment* (JCOIE) (Washington: July 25, 2018): viii, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830 (accessed: March 24, 2019).

63 Department of Defense Directive no. 3600.01 (May 2, 2013), 12.

64 Joint Chiefs of Staff, *Military Information Support Operations* (Washington, January 7, 2010), GL-4, https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf (accessed: April 4, 2019).

תיעוד איש לוחמה פסיכולוגית בזמן הדגמת יכולת
(Photo by: Senior Airman Cynthia Innocenti)[65]

במהלך שנת 2018 עבר צבא ארצות הברית תהליך שבמסגרתו הוא פעל למזג בצורה הדוקה יותר בין לוחמת המידע ובין לוחמת הסייבר. תהליך זה בא לידי ביטוי באיחוד ההכשרות לחיילים בתחומי לוחמת הסייבר[66] והלוחמה האלקטרונית ופיתוח צוותים ללוחמת סייבר אלקטרו־מגנטית. הצוותים יוטמעו באוגדות ויבצעו משימות ספציפיות.[67] השילוב בין שני התחומים מתבצע היום בפועל, ופיקוד הסייבר אינו עוסק רק בתקיפות סייבר אלא גם בלוחמת מידע ובלוחמה אלקטרונית.[68] העמקת השילוב הכרחית, אפוא, על מנת להפיק את המיטב מכל תחום.[69] השילוב בין היכולות נדרש גם לאור העובדה שאצל היריבות של ארצות הברית כבר מתקיים השילוב בין התחומים. המלחמה באוקראינה (שבה שילב הצבא הרוסי בין לוחמת

65 https://www.centcom.mil/MEDIA/IMAGERY/igphoto/2001729587/

66 Jared Serbu, "Army Vows to Reinvigorate Electronic Warfare by Combining it with Cyber, Intelligence Functions", *Federal News Network*, December 14, 2017 https://federalnewsnetwork.com/defense-main/2017/12/army-vows-to-reinvigorate-electronic-warfare-by-combining-it-with-cyber-intelligence-functions/ (accessed: January 13, 2019).

67 Todd South, "The Army is Putting Cyber, Electronic Warfare Teams in its BCTs", *Army Times*, February 20, 2018, https://www.armytimes.com/news/your-army/2018/02/20/the-army-is-putting-cyber-electronic-warfare-teams-in-its-bcts/ (accessed: January 13, 2019).

68 Sarah LeBlanc, "Army's Top Cyber Chief Discusses Threats", *The Augusta Chronicle*, August 21, 2018, https://www.augustachronicle.com/news/20180821/armys-top-cyber-chief-discusses-threats (accessed: January 13, 2019).

69 Serbu, "Army Vows to Reinvigorate Electronic Warfare by Combining it with Cyber, Intelligence Functions".

מידע, לוחמת סייבר ולוחמה אלקטרונית) נחשבת לזירה שממנה הצבא האמריקני יכול ללמוד רבות.[70]

ביולי 2018 פרסמה מפקדת המטות המשולבים אסטרטגיה לשינוי מקיף בלוחמת המידע האמריקנית. לפי האסטרטגיה על מנת להשיג את השינוי הנדרש בתחום לוחמת המידע על הצבא לפעול בשלושה תחומים: חיזוק ההבנה של מושג המידע והיבטיו בלוחמה הקינטית; יצירת תהליך ממוסד להטמעת לוחמת מידע בלוחמה קינטית; להביא לידי ביטוי את השילוב בין לוחמת מידע ללוחמה קינטית בשדה הקרב.[71] לשם כך על המטות המשולבים לפעול במספר דרכים, ואלה הן: (1) להבין את התפיסות של הגורמים הרלוונטיים בזירה; (2) להבין איך אותם גורמים מצליחים להשתמש בלוחמת המידע כדי לקדם את מטרותיהם; (3) לשנות את התפיסה של אנשי המטות כלפי לוחמת המידע כמרכיב בלוחמה הקינטית; (4) לתכנן טוב יותר מבצעים צבאיים המשלבים לוחמה קינטית ולוחמת מידע וליישמם בהצלחה רבה יותר.[72]

צבא ארצות הברית הצליח להטמיע יכולות של לוחמת מידע ולוחמת סייבר בפעולותיו השונות. עם זאת בכירים העריכו כי יש צורך להפוך את שרשרת הפיקוד סביב לוחמת הסייבר לפשוטה יותר ולהעניק סמכויות נרחבות יותר באופן שהמערכת הצבאית תוכל להוציא לפועל במהירות וביעילות מתקפות סייבר, ובכך היא תפיק מהן רווח רב יותר.[73] לוטננט גנרל סטפן פוגרטי (Stephen Fogarty), מפקד פיקוד הסייבר של צבא היבשה (ARCYBER), הגדיר את שילוב לוחמת הסייבר, לוחמת המידע והלוחמה האלקטרונית כמהלך ארוך טווח שיגיע לסיומו בשנת 2028 עם הפיכת פיקוד הסייבר לפיקוד שיתמקד בלוחמת מידע. לדבריו השינוי יסייע להתמודד עם הדומיננטיות העולה של המידע בשדה הקרב המודרני ולהבין טוב יותר את דרכי הפעולה של היריב.[74]

הוצאה לפועל של מבצעי לוחמת מידע. הפיקוד המרכזי של צבא ארצות הברית

---

70 Mark Pomerleau, "'Your Wife is Cheating on you', and Other Military Strategies for Controlling the Information Space", *Defense News*, October 4, 2018, https://www.defensenews.com/digital-show-dailies/ausa/2018/10/04/your-wife-is-cheating-on-you-and-other-military-strategies-for-controlling-the-information-space/ (accessed: January 13, 2019).

71 Ibid.

72 Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment (JCOIE)* (Washington: July 25, 2018), xi https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830 (accessed: September 12, 2019).

73 Gen. Joseph L. Votel, Maj. Gen. David J. Julazadeh & Maj. Weilum Lin, "Operationalizing the Information Environment: Lessons Learned for Cyber Integration in the USECNTCOM AOR", *The Cyber Defense Review* (Fall 2018): 3-5.

74 Kimberly Underwood, "Army Cyber to Become Information Warfare Command", *SIGNAL*, March 14, 2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command (accessed: March 27, 2019).

(CENTCOM) משמש היום הגורם המוביל בביצוע מבצעי השפעה ולוחמת מידע.[75] דוגמה למבצעי השפעה שהוא מנהל ברשת, הם המבצעים המכוונים נגד דאע"ש.[76] למרות מבצעים אלו נראה כי ארצות הברית התקשתה במהלך השנים להבין את מלוא הפוטנציאל הגלום בלוחמת המידע ולנהלו. כך למשל הייתה ארצות הברית איטית יחסית בהבנתה את חשיבות המידע והקרב על הנרטיב בהשגת מטרות כוללות, והיא לא השתמשה בהם להשגת מטרותיה.[77] קושי זה נבע גם מקשיים מנהלתיים, כמו מחסור בכוח אדם ובהכשרה ייעודית לניהול מבצעי השפעה.[78] סין ורוסיה, לעומתה, השכילו לנצל ביעילות רבה יותר את מבצעי לוחמת המידע לצרכיהן.[79]

לוחמת סייבר

רוסיה

רוסיה משתמשת במונח 'מידע' גם בהקשר של לוחמת סייבר. בעשותה כן היא מקשרת את תקיפות הסייבר למונח רחב יותר של לוחמת מידע הכולל מבצעים של רשתות מחשבים (Computer network operations), לוחמה אלקטרונית, לוחמה פסיכולוגית ומבצעי מידע. שיוך זה מדגיש את העובדה שמטרת התקיפות היא לשלוט במרחב המידע הכולל גם את מרחב הסייבר, באופן שיסייע להשגת מטרותיה האסטרטגיות.[80] שירות הביטחון הפדרלי של רוסיה Federal Security Service (FSB), , הוא הגוף האחראי על גיוס האקרים למבצעים שונים בתוך רוסיה ומחוצה לה. בנוסף פועל בתחום גם המודיעין הצבאי (ה־GRU) העומד מאחורי תקיפות סייבר רבות בשנים האחרונות - מתקפות סייבר נגד ארגונים פוליטיים, עסקים וגופי תקשורת בבריטניה,[81] מתקפות נגד תשתיות חיוניות בארצות הברית[82] וביצוע

75 Linda Robinson et al., *Modern Political Warfare - Current Practices and Possible Responses* (California: RAND Cooperation, 2018), xxi.

76 Karen Parrish, "Centcom Counter ISIL Propaganda", *US Department of Defense*, July 6, 2016, https://dod.defense.gov/News/Article/Article/827761/centcom-counters-isil-propaganda/ (accessed: January 13, 2019); Peter Cary, *The Pentagon and Independent Media - an Update* (Washington: Center for International Media Assistance, 2015), 10.

77 Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment*, 7-8.

78 Robinson et al., *Modern Political Warfare,* xxi.

79 Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment*, 7-8.

80 Michael Connell and Sarah Vogler*, Russia's Approach to Cyber Warfare*, (CNA - Analysis and Solutions, March 2017), 3.

81 "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed", *National Cyber Security Centre (NCSC)*, October 3, 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed: March 24, 2019).

82 "GRIZZLY STEPPE - Russian Malicious Cyber Activity", *Department of Homeland Security*, December 29, 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (accessed: March 24, 2019).

מתקפות סייבר בגרמניה לשם איסוף מידע פוליטי.[83] הקבוצה המכונה APT28 ו־Fancy Bear המקושרת ל־GRU עמדה מאחורי הפריצה למטה ועידת המפלגה הדמוקרטית בבחירות 2016.[84]

סין

כמו רוסיה, גם סין אינה משתמשת במונח 'סייבר' אלא במונח 'מידע' גם בהקשר של לוחמת סייבר. הסינים משתמשים במונח 'לוחמת סייבר' רק אם הם מתארים את פעולות המערב בתחום מבצעי הסייבר.[85]

600 מוקדים של התקפות סייבר על חברות אמריקאיות שבוצעו על ידי האקרים סיניים (NSA, USA)

צבא סין יוצר הבחנה בין פעולות סייבר בזמני שלום לבין פעולות סייבר בזמן מלחמה. בזמני שלום משימת צבא סין היא הגנה על המרחב האלקטרומגנטי במטרה

83 Andrea Shalal, "Germany Challenges Russia Over Alleged Cyberattacks", *Reuters*, May 4, 2017, https://www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA (accessed: March 24, 2019).

84 David E. Sanger & Nick Corasaniti, "D.N.C. Says Russians Hackers Penetrated Its Files, Including Dossier on Donald Trump", *The New York Times*, June 14, 2016, https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html (accessed: January 13, 2019); Connell & Vogler, *Russia's Approach to Cyber Warfare,* 10-12.
יש להזכיר כי בבחירות בארה"ב פעלו בו בזמן יחידות ממספר ארגונים ברוסיה, כמו ה־SVR, הסוכנות לחקר האינטרנט ועוד. לא ידוע אם הללו תואמו ביניהן, אך ברור כי הוכוונו על ידי הקרמלין. הפעילות החלה ככל הנראה בשנת 2013, לפני שהיה ידוע מה זהות המועמדים הסופיים.

85 Connell & Vogler, "Russia's Approach to Cyber Warfare", 3.

להשיג אבטחה ושליטה על המידע שבמרחב הסייבר. בתקופות שלום סביר להניח שסין גם תסמוך על יכולות מעקב (reconnaissance) לצורכי איסוף מידע וקטלוג חולשות בצבא ארצות הברית ובתשתיותיו.[86] בזמן מלחמה אמצעי הסייבר משמשים את סין להבין את כיווני הפעולה את היריב, לתכנן את המבצעים הצבאיים ולהבטיח ניצחון בשדה הקרב.[87]

חוקרים בצבא הסיני מעריכים שבניית יכולות סייבר חזקות היא דבר הכרחי שיאפשר הגנה על הרשתות הסיניות, וכך גם תושג עליונות בתחום הסייבר באמצעות מבצעים התקפיים כדי להרתיע את היריב מביצוע מבצעים צבאיים נגד סין.[88] סין רואה ביכולות הסייבר אמצעי לאסוף מודיעין ואמצעי לשתק את המערכות החיוניות של היריב ובכך להשיג ניצחון.[89]

נכון לשנת 2018 סין היא המדינה המובילה בתדירות תקיפות הסייבר שנעשות בחסות מדינתית.[90] עם זאת מוערך כי מבחינה טכנולוגית מצוי צבא סין בין דור למספר דורות מאחורי המערב.[91] לכן אחת מהמטרות המרכזיות של תקיפות הסייבר הסיניות היא גניבת מידע טכנולוגי ומסחרי[92] שיעניק יתרון מסחרי לחברות הסיניות ברחבי העולם, יתרום לפיתוח היכולות הצבאיות־טכנולוגיות של סין[93] ויאפשר לה לדלג על שנים של מחקר ולהתקדם בקצב מהיר במיוחד.[94]

על פי ההערכות הסינים יגבירו את פעילות הריגול התעשייתי שלהם בזירת הסייבר בשל הצורך לעמוד ביעדי התוכנית הכלכלית של סין Made in China 2025.[95] המועצה הלאומית של סין אישרה את התוכנית במאי 2015, ובסופה, עד שנת 2049, תהפוך סין למעצמה עולמית בתחום הייצור.[96] על פי התוכנית סין תהיה מובילה עולמית בייצור בעשר תעשיות מובחנות ובהן תעשיית המידע וציוד החלל.[97]

---

86 Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness",68-69.

87 Secretary of Defense, *Annual Report to Congress*, 40-41.

88 Ibid, 61.

89 Ibid, 74.

90 " China Overtakes Russia as World's Biggest State Hacker", *The Week*, October 10, 2018, https://www.theweek.co.uk/96999/china-overtakes-russia-as-world-s-biggest-state-hacker (accessed: January 9, 2019).

91 Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness",38-39

92 Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage", *The Diplomat,* May 23, 2014, https://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/ (accessed: January 9, 2019).

93 Raud, *China and Cyber: Attitudes, Strategies, Organizations,* 23.

94 Fritz, "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness", 68-69.

95 סיכום המחצית הראשונה של 2018 במרחב הסייבר (ClearSky, יולי 2018), 3, http://www.hadashot.com/Downloads/News_345862_2.pdf (גישה אחרונה: 4 באפריל 2019).

96 "'Made in China 2025 Plan' Unveiled to Boost Manufacturing", *GB Times*, May 20, 2015, https://gbtimes.com/made-china-2025-plan-unveiled-boost-manufacturing (accessed: April 2, 2019).

97 Dan Harris, "China's Ten Favorite Industries", *China Law Blog*, August 25, 2015, https://www.chinalawblog.com/2015/08/chinas-ten-favorite-industries.html (accessed: April 2, 2019).

ארצות הברית

הצבא האמריקני משתמש במונחים 'מבצעי סייבר הגנתיים' ו'מבצעי סייבר התקפיים'.[98] מבצעי סייבר הגנתיים הם מבצעים שמבטאים יכולות שונות: שימור יכולות להגן על מידע, על רשתות ועל יכולות נוספות והתמודדות עם תקיפות סייבר זדוניות. מבצעי סייבר התקפיים מוגדרים כמשימות שנועדו להפגין עוצמה במרחב הסייבר.[99] האמריקנים רואים בלוחמת הסייבר אמצעי בלתי נפרד מתקיפות קינטיות בכל מבצע ואמצעי להרס מערכות מידע.[100]

במהלך שנת 2018 התפרסמו בארצות הברית שלוש אסטרטגיות חדשות לתחום הסייבר: (1) אסטרטגיית הסייבר הנשיאותית; (2) אסטרטגיית הסייבר של מחלקת ההגנה; (3) אסטרטגיית הסייבר של פיקוד הסייבר. בשלושתן באו לידי ביטוי שני עקרונות חשובים - אינטגרציה בין מרחבים ומעבר ממדיניות הגנתית למדיניות בעלת מאפיינים התקפיים יותר, המכונה "defending forward".

אינטגרציה בין מרחבים. שלא כמו בעבר, מרחב הסייבר אינו נחשב עוד למרחב נפרד משאר המרחבים המבצעיים שבהם פועלת ארצות הברית, ופעולותיה במרחב הסייבר משתלבות בפעולות אחרות שהיא מבצעת במסגרת מימוש עוצמתה הלאומית.[101]

מעבר ממדיניות הגנתית למדיניות התקפית יותר כפי שבא לידי ביטוי במונח defending forward המצוין באסטרטגיית מחלקת ההגנה. הפרשנות שניתנה למונח זה כוללת שילוב בין צעדים התקפיים להגנתיים, והוא נועד לשמור על עליונות ארצות הברית במרחב הסייבר.[102] לדברי ג'ון בולטון, היועץ לביטחון לאומי, השינוי במדיניות הסייבר היה נדרש משום שארצות הברית מעוניינת ליצור הרתעה שתמחיש לאויביה שמחיר ביצוע מבצעי סייבר נגדה יהיה גבוה מאוד.[103]

לוחמה אלקטרונית

רוסיה

עבור רוסיה לוחמה אלקטרונית היא מערך של פעולות מתואמות היוצרות התקפה רדיו־אלקטרונית (Radioelektronnaia borba) על תשתיות מידע ותשתיות רדיו־אלקטרוניות של היריב; הגנה על תשתיות מידע ותשתיות רדיו־אלקטרוניות; ומניעת

98 Theohary, "Information Warfare: Issues for Congress", 6.

99 Joint Chiefs of Staff, *Cyberspace Operation* (Washington, June 8, 2018): GL-4 GL5.

100 Costello & McReynolds, *China's Strategic Support Force,* 47-48.

101 The White House, *National Cyber Strategy of the United States of America* (Washington, September 2018): 20.

102 Max Smeets & Herb Lin, "An Outcome-Based Analysis of U.S Cyber Strategy of Persistence & Defend Forward", *Lawfare,* November 28, 2018 https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward (accessed: January 13, 2019).

103 Christopher Bing, "White House Pledges to Step Up Cyber Offense of Hackers", *Reuters*, September 20, 2018 https://www.reuters.com/article/us-usa-cyber/white-house-pledges-to-step-up-cyber-offense-on-hackers-idUSKCN1M031I (accessed: January 13, 2019).

ריגול מצד גורמים זרים בתשתיות הרדיו־אלקטרוניות. הלוחמה האלקטרונית בתפיסה הרוסית מחולקת לארבעה תתי סוגים: התקפה אלקטרונית; הגנה אלקטרונית; הגנה מפני ריגול מצד גורמים זרים נגד התשתיות הרוסיות; קיום צעדים תומכים שנועדו לזהות את התפקוד של כלל האמצעים הרדיו־אלקטרוניים; וניהול כלל המידע הנאסף מאמצעים אלה על מנת לנהל מתקפה אלקטרומגנטית.[104]

תחום הלוחמה האלקטרונית ברוסיה עובר בשנים האחרונות שינויים בארגון, בדוקטרינה, במבנה הפיקוד והאימונים וברמה הטקטית. בשנים 2008–2015 חלו שינויים מבניים, ובמהלכן הוקמו חמש חטיבות לוחמה אלקטרונית (החטיבה ה־15 עד החטיבה ה־19) המוטמעות כחלק אינטגרלי בכוחות הלוחמים.[105] החל משנת 2010 כוחות הלוחמה האלקטרונית עוברים תהליך מודרניזציה מקיף הצפוי להימשך עד שנת 2025 לכל הפחות, ומטרתו היא ליצור בסיס למערכת לוחמה אלקטרונית אוויר־יבשה יעילה שתוכל לנטרל את היתרון הטכנולוגי של האויב במרחבי החלל והאוויר ובמרחב התקשורת שלו. כחלק מתהליך זה יצטיידו הכוחות במערכות המסוגלות לשבש מערכי פיקוד, מוצבי שליטה, תקשורת ומודיעין אויב. שינויים אלה מובילים לכך שבכוחות היבשה הרוסיים, לא כמו בכוחות המערב, הלוחמה האלקטרונית היא חלק בלתי נפרד ואינטגרלי ממבנה הכוחות, ולמעשה הכוחות בשטח אינם פועלים בלי שיכולות הלוחמה האלקטרונית יעמדו לרשותם. הדבר נכון במיוחד לכוחות היבשה הנחשבים לתומכים הגדולים ביותר של הלוחמה האלקטרונית בצבא הרוסי.[106] באפריל 2017 הצהיר מפקד המערך שמערכות הלוחמה האלקטרונית צריכות לתרום לעליונות הצבא בתחומי השליטה והפיקוד ובהפעלת כלי נשק שונים, וכי כוחות הלוחמה האלקטרונית ימלאו תפקיד חשוב בתוכנית ההגנה הרוסית.[107]

עדות לשינוי זה באה לידי ביטוי במלחמה באוקראינה שכללה שימוש בכלי טיס בלתי מאוישים ובמערכות קרקעיות, שמטרתן הייתה לחסום לוויינים ורשתות רדיו ותקשורת סלולרית. זאת יחד עם שיבוש GPS ותקיפה אלקטרונית של כלי טיס בלתי מאוישים של הצבא האוקראיני.[108]

הרוסים השתמשו בלוחמת סייבר ובלוחמה אלקטרונית על מנת לנהל מבצעי מודיעין. באוקראינה קיבלו חיילים אוקראיניים הודעות טקסט שנועדו לפגוע בלכידות הכוחות ובמורל שלהם, למשל בהודעה אחת הם קיבלו מסר: "אתם

---

104 Jonas Kjellen, *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*, (Swedish Defence Research Agency, September 2018), 21-22.

105 Roger McDerMott, *Report - Russia's Electronic Warfare Capabilities to 2025 - Challenging NATO in the Electromagnetic Spectrum* (Tallinn: International Centre for Defence and Security, 2017), IV, 5-6, 17.

106 Ibid, 5, 11, 13.

107 Ibid, IV, 5-6, 17.

108 Col. Liam Collins, "Russia Gives Lessons in Electronic Warfare", *The Magazine of the Association of the United States Army,* 68 no.8 (August 2018): 18-19.

מכותרים ומבודדים". דקות לאחר מכן בני המשפחה של החיילים קיבלו הודעה "בנכם נהרג". פעולה כזו גרמה להורים להתקשר לבניהם, וכך הצליחו הכוחות הרוסיים לאתר את מיקום החיילים ולשגר לעברם ארטילריה כבדה.[109]

סין

סין רואה בלוחמה האלקטרונית אמצעי המאפשר פגיעה בתשתיות האלקטרומגנטיות של היריב,[110] והיא מוגדרת "צעדי נגד אלקטרוניים" (electronic countermeasure). הדוקטרינה מחולקת לשלושה חלקים: צעדי מנע נגד פעילות האויב ברשתות הסיניות; הגנה אלקטרונית; והתקפה אלקטרונית.[111] בתפיסה הצבאית הסינית תחומי הסייבר והחלל אינם נפרדים אלא משמשים המשך האחד של השני, והשידור האלקטרומגנטי מחבר ביניהם. זאת מתוך הבנה שתרחיש המלחמה העיקרי שסין מתכוננת אליו במלחמה כוללת ורחבה יותר הוא שימוש באלמנטים מתחומי החלל, הסייבר והלוחמה האלקטרומגנטית. השילוב בין סייבר, חלל ואלקטרומגנטיות הוא טבעי ויעיל, והוא אף חלק מהדרישה למלחמה יעילה בכללותה.[112] לדוגמה, מערכת הניווט הסינית ביידו (Beidou) המיועדת להתחרות במערכת ה־GPS האמריקנית תוכל לתרום משמעותית לכוחות ה־SSF, בתנאי שהם ישלטו בכישורי הלחימה המודרניים הנדרשים כיום, שבהם נמצאים אבטחת סייבר ותקשורת אלקטרונית.[113]

בשנים האחרונות השקיעה סין בפיתוח אמצעי לחימה מבוססי לוחמה אלקטרונית בכל מרחבי הלחימה. במרחב היבשה היא מפתחת ארטילריה מבוססת לוחמה אלקטרונית המסוגלת להגיע לטווח של כ־200 קילומטרים ושעלויותיה נמוכות יותר בהשוואה לארטילריה קונבנציונלית.[114] בזרוע הים מפותח תותח אלקטרומגנטי המסוגל להגיע לטווח של כ־125 מיילים.[115] בנוסף מטוסים רבים בחיל־האוויר

---

109 Ibid.

110 Secretary of Defense, *Annual Report to Congress,* 74.

111 Zi Yang, "Blinding the Enemy: How the PRC Prepares for Radar Countermeasures", *China Brief*, 18, no. 6 (April 2018), https://jamestown.org/program/blinding-the-enemy-how-the-prc-prepares-for-radar-countermeasures/ (accessed: January 9, 2019).

112 Costello & McReynolds, *China's Strategic Support Force,* 47.

113 Minnie Chan, "Welcome to the Modern Military: China's News Combat Units Prepare for Electronic Warfare", *South China Morning Post*, July 11, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2154550/welcome-modern-military-chinas-new-combat-units-prepare (accessed: April 28, 2019).

114 Liu Xuanzun, "China's New Electromagnetic Rocket More Powerful than Most Conventional Artillery on Qinghai-Tibet Plateau: Expert", Global Times, August 2, 2018, http://www.globaltimes.cn/content/1113596.shtml (accessed: April 28, 2019).

115 "Chinese Tank-leading Ship with Electromagnetic Railgun Passes Sea Trials", Defence Blog, April 1, 2019, https://defence-blog.com/news/chinese-tank-landing-ship-with-electromagnetic-railgun-passes-sea-trials.html (accessed: April 28, 2019).

כוללים יכולות לוחמה אלקטרונית מתקדמות, כגון מערכות jamming אלקטרוניות ואמצעי לוחמת נגד הניתנים להתאמה.[116]

ארצות הברית

מחלקת ההגנה האמריקנית מגדירה לוחמה אלקטרונית כפעולה צבאית הכוללת שימוש באנרגיה אלקטרומגנטית או אנרגיה מכוונת (directed energy), כגון לייזר, על מנת לשלוט בספקטרום האלקטרומגנטי של היריב או כדי לתקוף את האויב. בלוחמה אלקטרונית נעשה שימוש באנרגיה אלקטרומגנטית, בנשק אנרגיה מכוונת או בנשק נגד קרינה (antiradiation weapons) על מנת לפגוע באנשים, במקומות ובציוד באופן המשבש או הורס את יכולות לחימת האויב.[117] קיימת חלוקה לשלושה תחומי משנה: סיוע בלוחמה אלקטרונית (electronic warfare support), הגנה אלקטרונית (electronic protection) והתקפה אלקטרונית (electronic attack).[118]

בשנת 2014 התייחס צבא ארצות הברית לראשונה לשילוב בין לוחמת סייבר ללוחמה אלקטרונית. הוא יצר מונח המשלב בין השניים והנקרא "פעילויות סייבר אלקטרומגנטיות" (Cyber Electro־magnetic Activities). המונח מוגדר כך: "פעולות שנועדו להשיג, לשמר, ולמצות יתרון על פני יריבים ואויבים במרחב הסייבר ובמרחב האלקטרומגנטי כאחד, כשבאותו זמן ישנה מניעה מצד האויב להשיג יתרונות אלו".[119]

ניתוח: יחסי הכוחות בין שלוש המעצמות בתחום לוחמת המידע

שלוש המעצמות רואות בלוחמת מידע אמצעי להשגת יתרון בשדה הקרב באמצעות השפעה על התנהגות היריב. מרחב הסייבר, לעומת זאת, נתפס בצורה שונה אצל כל אחת מהן. התפיסה האמריקנית רואה את אבטחת הסייבר כהגנה על תשתיות שונות מפני פריצה, ואילו רוסיה וסין רואות בו בעיקר מרחב של שליטה על מידע. מתוך ההבדלים בהגדרות הבסיסיות של המונח לוחמת מידע נובעים הבדלים מהותיים בהבנות של שלוש המדינות את תפיסת ההפעלה והיישום של לוחמה זו. בעוד שניתן למצוא מאפיינים דומים בתפיסות של רוסיה וסין הרואות בלוחמת הסייבר חלק בלתי נפרד משליטתן במרחב המידע, עד לאחרונה התייחסה ארצות הברית לשני מונחים אלה כמונחים נפרדים, וכיום היא מצויה בעיצומו של תהליך שילוב ביניהן ושינוי תפיסות הפעולה שלה. יש לציין כי לאורך השנים שלוש המעצמות עושות שימוש ברמה זו או אחרת בחברות פרטיות ובתאגידים למימוש מדיניותן בתחום.

116 Defense Intelligence Agency, *China Military Power - Modernizing a Force to Fight and Win* (Washington, 2019), 86.

117 Collins, "Russia Gives Lessons in Electronic Warfare": 18.

118 Department of Defense, *DOD Dictionary of Military and Associated Terms* (Washington: November 2018): 77-78.

119 United States Department of the Army, *FM 3-38 Cyber Electromagnetic Activities* (Washington, February 2014), 1.

למידה מניסיון העבר

האירועים שהתרחשו במהלך שנות התשעים ותחילת שנות האלפיים - סיום המלחמה הקרה, מלחמת המפרץ ומלחמות ארצות הברית בקוסובו ובאפגניסטן - חיזקו אצל כל מעצמה את תפיסותיה המוקדמות לגבי לוחמת מידע ולוחמת סייבר. עבור רוסיה וסין אירועים אלה היו הוכחה לחשיבות של לוחמת המידע, והם שימשו זרז לחיזוק אלמנט לוחמת המידע בדוקטרינה הצבאית שלהן. למרות הקרבה הרעיונית ביניהן רוסיה וסין מייעדות תפקידים שונים ללוחמת המידע. ברוסיה השימוש בלוחמת מידע על גווניה נעשה מתוך צורך לפצות על חולשתה הצבאית והכלכלית מול ארצות הברית וסין. למרות חולשה זו התפיסה הרוסית מייעדת ללוחמת המידע תפקיד ייחודי שהוא הארכת משך המלחמה לנקודת זמן הנוחה לרוסיה. זאת בשונה מסין וארצות הברית השואפות לקצר את המלחמה ככל הניתן באמצעות לוחמת המידע.

בסין ניתן להבחין בשינוי בתפיסת העוצמה ובשימוש בלוחמת המידע משימוש בלוחמת מידע כלוחמה א־סימטרית מול יריב עדיף לתפיסת סין את עצמה כמדינה שווה לארצות הברית, שמולה מתקיים מאבק על קביעת הנורמות הבינלאומיות.

עבור ארצות הברית היו אירועים אלה הוכחה לעליונותה הטכנולוגית, ולכן היא ממשיכה לראות בעליונות זו רכיב מהותי באסטרטגיית הסייבר שלה. בשנים שלאחר המלחמה הקרה ארצות הברית נלחמה בעיקר מול צבאות הנחותים ממנה מבחינה טכנולוגית או מול ארגוני טרור. כל עוד ארצות הברית לא התמודדה מול אויב השווה לה או המתקרב אליה ברמה הטכנולוגית, לא התקיים חיבור הדוק בין סייבר, חלל ולוחמה אלקטרומגנטית. מסיבה זו האמריקנים לא תפסו את מרחב הסייבר כאמצעי למניפולציות פסיכולוגיות, עד שהם הבינו את היקפם של מבצעי ההשפעה הרוסיים במערכת הבחירות ב־2016.[120]

הבנות אלה גיבשו אצל כל מדינה את **הדרך להשגת ניצחון במלחמה העתידית**. ארצות הברית תשתמש בעליונות הטכנולוגית במהלך מלחמה על מנת להסב ליריביה הפסדים שלאורך זמן יגרמו להם להשקיע יותר מאמצים בהגנה על חשבון מאמצי ההתקפה. רוסיה וסין, לעומתה, סבורות שניצחון על היריב יושג באמצעות פגיעה במערך השיקולים שלו באמצעות יצירת בלבול וספק במניעים שלו ובאמצעות חבלה במערכות הלוחמה הקריטיות האחראיות על הפיקוד והשליטה.

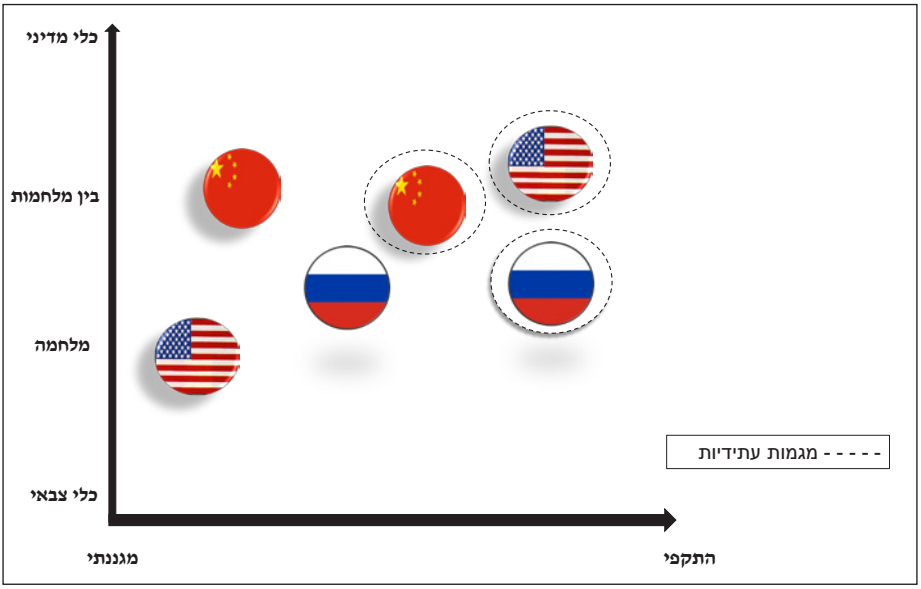
למרות עליונותה הטכנולוגית ארצות הברית ניצבת בפני אתגר ייחודי בהתמודדותה מול יריבים בעלי יכולות גבוהות בתחומי לוחמת הסייבר והמידע. מתוך כך ניתן לזהות בארצות הברית שני שינויים חשובים. השינוי הראשון מתבטא במעבר אסטרטגי ממדיניות הגנה למדיניות השמה הדגש רב יותר על האלמנט ההתקפי (defending forward). השינוי השני מתבטא בביצוע מיזוג משמעותי יותר בין לוחמת הסייבר, לוחמת המידע והלוחמה האלקטרונית. מיזוג זה מופיע בשלושה מישורים:

[120] Costello & McReynolds, *China's Strategic Support Force*, 47-48.

הגדרת הסייבר כחלק אינטגרלי מהעוצמה הלאומית; איחוד יכולות לוחמת הסייבר והלוחמה האלקטרונית בצבא; ופיתוח יכולות מתקדמות יותר של לוחמת מידע בתמיכה לכל אורך שלבי הלחימה. כל אלו מייצגים גם שינוי בתפיסת הכוח הצבאי ומעבר מתפיסתו ככוח הרסני או משבש לתפיסה הרואה בו כוח היברידי המשלב גם את יתרונות לוחמת המידע.[121]

תפקידי לוחמת המידע בזמנים שבין המלחמות

הבדל מהותי נוסף בין המעצמות נעוץ לא רק בתפקידי לוחמת המידע במלחמה אלא גם בתפקידה בזמנים שבין המלחמות. שלוש המעצמות מייחסות ללוחמת המידע תפקיד משמעותי בשינוי תפיסות היריב לשם השגת רווחים פוליטיים. אולם רוסיה וסין משקיעות מאמצים כבירים ביישום לוחמת מידע בזמני שגרה. הבדל זה נובע מכך שרוסיה וסין רואות את הסדר הבינלאומי הקיים בשלושת העשורים האחרונים כסדר הפוגע בהן והמשקף ערכים הזרים להן. מתוך כך הן משתמשות באמצעי לוחמת מידע גם בזמני שגרה לשם יצירת סדר בינלאומי מאוזן יותר שישקף גם את ערכיהן. בסין הדבר מתבטא בהפצת תכנים ביקורתיים כלפי המערב. ברוסיה מדובר בשימוש במסרים היוצרים קיטוב במדינות המערב ובביצוע מתקפות סייבר על מערכות בחירות ברחבי העולם כדי להראות לעיני כל את פגמי השיטה הדמוקרטית. פעולות אלו משמשות אמצעים משלימים ללוחמת הסייבר שנוקטות שתי מדינות אלו (ראו תרשים 1).



תרשים 1: המצב הקיים בלוחמת המידע בין המעצמות ותיאור המגמות

[121] Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment,* viii-ix.

ניתן לומר שההבדל המהותי בין רוסיה וסין לבין ארצות הברית בתחום לוחמת המידע חורג מהשדה הצבאי, משום שרוסיה וסין רואות בלוחמת המידע (גם) אמצעי מדיני המיושם בעיתות מלחמה ובעיתות שלום, ובהתאם לכך הוא מקודם גם באמצעים דיפלומטיים. לעומתן התפיסה האמריקנית רואה בלוחמת המידע כלי נשק שעיקר ייעודו מתבטא בזמן מלחמה. הבנה זו עלולה להכניס את ארצות הברית לעמדת נחיתות מול רוסיה וסין, שכן ערכים בינלאומיים הם דבר המשתנה תדיר, והעובדה שארצות הברית איננה משקיעה מאמצים באותה הרמה כמו רוסיה וסין ביישום לוחמת המידע גם בזמנים שבין המלחמות, עלולה לפגוע במעמדה העולמי לאורך זמן.

שינויים בבניין הכוח הצבאי

ברוסיה ובסין התרחשו בשנים האחרונות שינויים חשובים בבניין הכוח הצבאי עם הקמת ה־SSF בסין וחיזוק יכולות הלוחמה האלקטרונית של רוסיה והפיכתה לחלק אינטגרלי ממהלכים קינטיים (כפי שהתרחש במלחמה באוקראינה). שינויים אלה מעידים שרוסיה וסין מצליחות להשיג רמת שילוביות גבוהה יותר בין לוחמת מידע, לוחמת סייבר ולוחמה אלקטרונית והטמעה גבוהה יותר של יכולות אלו בלוחמה הקינטית של כל מדינה. ארצות הברית, אף על פי שהיא מכירה בצורך במיזוג נרחב יותר, ולמרות צעדים שהיא מבצעת בתחום, עדיין נמצאת בפיגור מסוים לעומת רוסיה וסין.

לוחמת מידע בין המעצמות - מבט לעתיד

על סמך מערך הכוחות הנוכחי בין ארצות הברית לסין ניתן להעריך שבמקרה של עימות סייבר סביר להניח כי ארצות הברית תימצא בעמדת עליונות מול סין, הן במישור ההגנתי והן במישור ההתקפי, ולכן תצא ממנו וידה על העליונה.[122] עם זאת היכולת של ארצות הברית להשיג דומיננטיות בלוחמת המידע העתידית, שלוחמת הסייבר היא רק מרכיב אחד שלה, תהיה תלויה באופן שבו תתמודד עם שתי סוגיות עתידיות חשובות.

הסוגיה הראשונה היא עד כמה תצליח ארצות הברית לאחד את לוחמת המידע שלה עם יכולות לוחמת הסייבר והלוחמה האלקטרונית. יוזמת הפיכת פיקוד הסייבר של צבא היבשה לפיקוד לוחמת המידע, כפי שהגדיר אותה לוטננט גנרל פוגרטי, מפקד פיקוד הסייבר של צבא היבשה, עשויה לשמש מבחן משמעותי. על פניו אם מהלך זה ייצא לפועל בפרק הזמן המתוכנן, וכפי שפוגרטי תיאר אותו, הפיקוד המחודש יציג מודל חדשני ביחס לארצות הברית, שיאפשר שילוב מוצלח בין סוגי

[122] "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities", in *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017*, Eric Heginbotham (Santa Barbara: RAND Cooperation, 2015), 269, 283.

לוחמת המידע, והוא ידמה ביכולותיו ובכוונותיו ל־SSF הסיני.

אולם היכולת להפיק מהמהלך את מלוא התועלת האסטרטגית המבוקשת נפגמת בשל שני חסמים. חסם ראשון הוא העדפה אסטרטגית של ארצות הברית, כפי שמתבטאת באסטרטגיית פיקוד הסייבר, המדגישה את שמירת עליונותה במרחב הסייבר. בניית עליונות בלוחמת המידע מורכבת יותר מבנייה כזו במרחב הסייבר, מאחר שהיא איננה מבוססת רק על פיתוח הכלים הטכניים הנחוצים ללחימה אלא גם על הבנה מעמיקה של העקרונות העומדים בבסיס לוחמת המידע. נראה כי מפקדת המטות המשולבים מודעת לכך שעד היום היא לא מימשה את מלוא הפוטנציאל הגלום בהם, למרות המאמצים הגדולים שהצבא משקיע בשנים האחרונות. לכן ניתן להטיל ספק ביכולת של ארצות הברית להשלים בפרק זמן של פחות מעשור את הפערים בתחום זה מול שתי מדינות שהשימוש בלוחמת המידע מוטמע בהן בצורה עמוקה במשך תקופה ארוכה.

החסם השני נובע מהיקף המהלך הצפוי. בעוד שה־SSF הוקם כחלק מרפורמה נרחבת בצבא הסיני ובהתאם לכך הוא רב־זרועי, המהלך המדובר של פוגרטי מתמקד רק בפיקוד הסייבר של צבא היבשה, כך שעדיין נותרה השאלה האם וכיצד גופים נוספים בארצות הברית, בצבא או מחוצה לו, יבצעו מהלכים דומים.

הסוגיה השנייה היא עד כמה תנצל ארצות הברית את ההתפתחויות העולמיות בתחום הבינה המלאכותית הצפויות לתרום לשדרוג יכולות לוחמת המידע באופן ניכר. על פי הגדרת האקדמיה הלאומית למדעים בארצות הברית בינה מלאכותית היא: "כל שיטה לתכנות מחשבים המאפשרת להם להוציא לפועל מטלות או דרכי התנהגות שהיו מחייבות אינטליגנציה אילו היו מבוצעות על ידי בני־אדם".[123] בשנים הקרובות הכלים להשפעה על דעת הקהל יהפכו למתוחכמים יותר ולקשים יותר למעקב. השימוש בבינה מלאכותית יאפשר לשחקנים בעלי כוונות זדוניות לפגוע בדמוקרטיות באופן אפקטיבי יותר, וכלי הפצת התעמולה יהיו מורכבים וקשים יותר לאיתור, מאחר שהחשבונות האוטומטיים יחקו בצורה אותנטית יותר התנהגות אנושית. מערכות בינה מלאכותית תהיינה מסוגלות להציע תכנים רלוונטיים לגולשים, והן תוכלנה לחזות ברמת דיוק גבוהה יותר תגובות אנושיות לתכנים. הכלים הללו יוכלו גם לנתח את המידע שאנשים משתפים ולהשתמש בפילוחים מדויקים יותר כדי לפנות לקבוצות אנשים רלוונטיות יותר.[124]

ישנן הערכות המדברות על כך שבעתיד תעקוף סין את ארצות הברית בתחום הבינה המלאכותית, והיא תהיה המדינה הדומיננטית בעולם בתחום. בנובמבר 2017 העריך אריק שמידט, יושב ראש חברת גוגל, שבשנת 2020 סין צפויה להשתוות

---

[123] דפנה גץ ואחרים, בינה מלאכותית, מדעי הנתונים ורובוטיקה חכמה – דו"ח ראשון, שלב ב' (חיפה: מוסד שמואל נאמן, 2018), 24.

[124] Alina Polyakova & Spencer P. Boyer, *The Future of Political Warfare: Russia, the West and the Coming Age of Global Digital Competition* (Brookings - Robert Bosch Foundation Transatlantic Initiative, March 2018), 6-15.

לארצות הברית ביכולות הבינה המלאכותית שלה, ובשנת 2025 היא צפויה לעקוף אותה בתחום זה.[125] הערכות עדכניות תומכות בכך, ונראה כי בשנת 2020 מספר המחקרים האקדמיים בנושא בינה מלאכותית שמפרסמים חוקרים סיניים, ישתווה למספר שמפרסמים חוקרים אמריקניים.[126]

ההתפתחויות וההזדמנויות הגלומות בתחום הבינה המלאכותית מציבות אתגר לא פשוט בפני מדינות המערב: שכלול מניפולציות לוחמת המידע שהבינה המלאכותית מספקת, מזיזה את מטוטלת לוחמת המידע מהתמקדות בלוחמת סייבר להתמקדות בלוחמת תודעה ולוחמה פסיכולוגית - תחום שבו לרוסיה ולסין יש יתרון על פני המערב. בהסתמך על הכוונות והיכולות של המעצמות ניתן להעריך כי כל אחד מן הצדדים יחזיק ביתרון אסטרטגי מסוים בתחום זה. ארצות הברית תהיה, ככל הנראה, המובילה בתחום חיזוי המגמות בבינה המלאכותית ובהתגוננות מול שימוש בבינה מלאכותית נגדה בשל יתרונה הטכנולוגי. לעומת זאת בתחום השימוש ההתקפי בבינה מלאכותית ארצות הברית עלולה למצוא עצמה בעמדת נחיתות מול כוחות שמוכנים להשקיע יותר ממנה בנושא (כמו סין) ושמנוסים בתחום לוחמת המידע הרבה יותר ממנה (כמו רוסיה). ייתכן כי אימוץ גישת ה־defending forward גם בתחום זה יוכל לסייע לארצות הברית להתמודד עם האתגרים הללו.

---

125 Sam Shead, "Eric Schmidt on AI: 'Trust me, these Chinese People are Good'", *Business Insider*, November 1, 2017, https://www.businessinsider.com/eric-schmidt-on-artificial-intelligence-china-2017-11 (accessed: January 15, 2019).

126 Tom Simontie, China is Catching up to the US in AI Research - FAST, *Wired*, March 13, 2019,;https://www.wired.com/story/china-catching-up-us-in-ai-research/ (accessed: August 8, 2019).

רשימת מקורות

- אמ"ץ-תוה"ד. **המילון למונחי תורה צבאית (טיוטה פנימית).** מטכ"ל 10-1, התשע"ט-2018.
- גץ, דפנה; כץ שחם, אושרת; קליין, רינת; צזנה, רועי; רוזנברג, שלמה; שהם, אבידע; ברזני, אלה; לק, ערן וציפרפל, סימה; **בינה מלאכותית, מדעי הנתונים ורובוטיקה חכמה - דו"ח ראשון, שלב ב'**, חיפה: מוסד שמואל נאמן, 2018.
- **סיכום המחצית הראשונה של 2018 במרחב הסייבר**, ClearSky, יולי 2018. http://www.hadashot.com/Downloads/News_345862_2.pdf (גישה אחרונה: 4 באפריל 2019)

- Arpi, Claude. "Be Prepared for China's Electronic Warfare", *Rediff News*, June 27, 2017, https://www.rediff.com/news/special/be-prepared-for-chinas-electronic-warfare/20170627.htm (accessed: January 13, 2019).
- Averin, Alexander. "Russia and its Many Truths. In *Fake News - a Road Map,* Riga: NATO Strategic Communications Centre of Excellence, 2018.
- Berzina, Ieva. "The Narrative of 'Information Warfare against Russia' in Russian Academic Discourse". *Journal of Political Marketing*, 17 no.2 (2018): 161-175.
- Bing, Christopher. "White House Pledges to Step Up Cyber Offense of Hackers", *Reuters*, September 20, 2018, https://www.reuters.com/article/us-usa-cyber/white-house-pledges-to-step-up-cyber-offense-on-hackers-idUSKCN1M031I (accessed: January 13, 2019).
- Brown, Robin. "Information Operations, Public Diplomacy & Spin: The United States & the Politics of Perception Management". *Journal of Information Warfare* 1, no.3 (2002): 40-50.
- Cary, Peter. *The Pentagon and Independent Media - an Update.* Washington: Center for International Media Assistance, 2015.
- Chan, Minnie. "Welcome to the Modern Military: China's News Combat Units Prepare for Electronic Warfare", *South China Morning Post*, July 11, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2154550/welcome-modern-military-chinas-new-combat-units-prepare (accessed: April 28, 2019).
- Chen, Adrian. "The Agency", *The New York Times*, June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html (accessed: January 13, 2019).
- Cheng, Dean. "China and Cyber: The Growing Role of Information in Chinese Thinking", in *Confronting an "Axis of Cyber? China, Iran North Korea, Russia in Cyberspace",* edited by Fabio Rugge, 59-88. Milano: Italian Institute for International Politics Studies, 2018.
- "China Overtakes Russia as World's Biggest State Hacker", *The Week*, October 10, 2018, https://www.theweek.co.uk/96999/china-overtakes-russia-as-world-s-biggest-state-hacker (accessed: January 9, 2019).
- "Chinese Tank-leading Ship with Electromagnetic Railgun Passes Sea Trials", *Defence Blog*, April 1, 2019, https://defence-blog.com/news/chinese-tank-landing-ship-with-electromagnetic-railgun-passes-sea-trials.html (accessed: April 28, 2019).

- Collins, Liam (Col). "Russia Gives Lessons in Electronic Warfare", *The Magazine of the Association of the United States Army*, 68, no.8 (August 2018):18-19.
- Connell, Michael and Vogler, Sarah. *Russia's Approach to Cyber Warfare*, CNA - Analysis and Solutions, March 2017.
- Costello, John and McReynolds, Joe. *China's Strategic Support Force: a Force for a New Era.* Washington: National Defense University Press, 2018.
- Costello, John and Mattis, Peter. "Electronic Warfare and the Renaissance of Chinese Information Operations", in *China's Evolving Military Strategy*, edited by Joe McReynolds, 174-213. Washington, DC: Jamestown Foundation, 2016.
- Cronin, Blaise and Crawford, Holly. "Information Warfare: Its Application in Military and Civilian Contexts", *The Information Society*, 15 no.4 (1999): 257-263.
- Defense Intelligence Agency, *China Military Power - Modernizing a Force to Fight and Win*, Washington, 2019.
- Defense Intelligence Agency, *Russia Military Power - Building a Military to Support Great Power Aspirations*, Washington, 2017.
- Department of Defense, *DOD Dictionary of Military and Associated Terms*, Washington: November 2018.
- Department of Homeland Security, *GRIZZLY STEPPE - Russian Malicious Cyber Activity*, December 29, 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (accessed: March 24, 2019).
- Fritz, Jason. "How China will Use Cyber Warfare to Leapfrog in Military Competitiveness", *Culture Mandala*, 8 no. 1 (October 2008): 28-80.
- Harris, Dan. "China's Ten Favorite Industries", *China Law Blog*, August 25, 2015, https://www.chinalawblog.com/2015/08/chinas-ten-favorite-industries.html (accessed: April 2, 2019).
- Heginbotham, Eric. *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power*, *1996-2017*, Santa Barbara: RAND Cooperation, 2015.
- Iasiello, Emilio J. "Russia's Improved Information Operations: From Georgia to Crimea", *Parameters*, 47 no. 2 (summer 2017): 51-63.
- Jardine, Bradley. "Russia's New 'Useful Idiots'?", *Coda Story*, October 5, 2017, https://codastory.com/disinformation-crisis/foreign-proxies/russia-s-new-useful-idiots (accessed: January 9, 2019).
- Jeangène Vilmer, Jean-Baptiste, Escorcia. A., Guillaume. M. and Herrera. J, *Information Manipulation - A Challenge for our Democracies*, The Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.
- Joint Chiefs of Staff, *Joint Concept for Operation in the Information Environment* (JCOIE), Washington: July 25, 2018,
- https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_

jcoie.pdf?ver=2018-08-01-142119-830 (accessed: March 24, 2019).
- Joint Chiefs of Staff, *Cyberspace Operation*, Washington, June 8, 2018.
- Joint Chiefs of Staff, *Military Information Support Operations*, Washington, January 7, 2010, https://www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf (accessed: April 4, 2019).
- Karl, Luke, (Maj), Lane, Joseph (Maj) and Sanchez, David, (Cmdr). "How to Stop Losing the Information Warfare", *Defense One*, July 26, 2018,
- https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/ (accessed: April 2, 2019).
- Keck, Zachary. "Robert Gates: Most Countries Conduct Economic Espionage", *The Diplomat*, May 23, 2014, https://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/ (accessed: January 9, 2019)
- King, Gary Pan, Jennifer and Roberts, Margaret E. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument", *American Political Science Review*, 11 no.3 (2017): 484-501.
- Kjellen, Jonas. *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*. Swedish Defence Research Agency, September 2018.
- Klaas, Brian. "Stop Calling it 'Meddling', It's Actually Information Warfare", *The Washington Post*, July 17, 2018, https://www.washingtonpost.com/news/democracy-post/wp/2018/07/17/stop-calling-it-meddling-its-actually-information-warfare/?utm_term=.873026b227e9 (accessed: January 15, 2019).
- LeBlanc, Sarah. "Army's Top Cyber Chief Discusses Threats", *The Augusta Chronicle*, August 21, 2018, https://www.augustachronicle.com/news/20180821/armys-top-cyber-chief-discusses-threats (accessed: January 13, 2019).
- Libicki, Martin. "Cyberdeterrence and Cyberwar", *RAND*, 2009, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed: April 2, 2019).
- "'Made in China 2025 Plan Unveiled to Boost Manufacturing", *GBTimes*, May 20, 2015, https://gbtimes.com/made-china-2025-plan-unveiled-boost-manufacturing (accessed: April 2, 2019).
- Mangan, Dan and Calia, Mike. "Special Counsel Mueller: Russians Conducted 'Information Warfare' Against US During Elections to Help Donald Trump Win", *CNBC*, February 16, 2018, https://www.cnbc.com/2018/02/16/russians-indicted-in-special-counsel-robert-muellers-probe.html (accessed: January 13, 2019).
- McDerMott, Roger. *Report - Russia's Electronic Warfare Capabilities to 2025 - Challenging NATO in the Electromagnetic Spectrum.* Tallinn: International Centre for Defence and Security, 2017.
- Millman, Rene. "Taiwan to Share Chinese Jacking Attempts with Private Firms to Train AI Defences", *ITPRO*, October 23, 2018, https://www.itpro.co.uk/hacking/32183/taiwan-share-chinese-hacking-attempts-with-private-firms (accessed: January 13, 2019).
- National Cyber Security Centre (NCSC), "Reckless Campaign of Cyber Attacks by

Russian Military Intelligence Service Exposed", October 3, 2018,
- https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed: March 24, 2019).
- Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections,* Washington: January 6, 2017.
- Department of the Navy, Office of the Chief of Naval Operations*, OPNAV Instruction 3434.1: Psychological Operations*, Washington Naval Yard: 1997, http://www.iwar.org.uk/psyops/resources/us/3434_1.pdf
- Parrish, Karen. "Centcom Counter ISIL Propaganda", *US Department of Defense*, July 6, 2016, https://dod.defense.gov/News/Article/Article/827761/centcom-counters-isil-propaganda/ (accessed: January 13, 2019).
- Polyakova, Alina and Boyer, Spencer P. *The Future of Political Warfare: Russia, the West and the Coming Age of Global Digital Competition*. Brookings - Robert Bosch Foundation Transatlantic Initiative, March 2018.
- Pomerleau, Mark. "'Your Wife is Cheating on you', and Other Military Strategies for Controlling the Information Space", *Defense News*, October 4, 2018,
- https://www.defensenews.com/digital-show-dailies/ausa/2018/10/04/your-wife-is-cheating-on-you-and-other-military-strategies-for-controlling-the-information-space/ (accessed: January 13, 2019).
- Raud, Mikk. China and Cyber: Attitudes, Strategies, Organizations. Riga: NATO Cooperative Cyber Defence Centre of Excellence, 2016.
- Robinson, Linda, Helmus, Todd C., Cohen, Raphael S., Nader, Alireza, Radin, Andrew Magnuson, Madeline and Migacheva, Katya. *Modern Political Warfare - Current Practices and Possible Responses*, California: RAND Cooperation, 2018.
- Sanger, David E. and Corasaniti, Nick. "D.N.C. Says Russians Hackers Penetrated Its Files, Including Dossier on Donald Trump", *The New York Times*, June 14, 2016,
- https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html (accessed: January 13, 2019).
- Sauffiyan, Ahmadhasan and Lokman, Anitawati Mohd."Prelude to Psychological Warfare in Malaysia - A Conceptual Understanding, Experience and Future Advancement*". IEEE Symposium on Humanities, Science and Engineering Research* (2012): 1325-1330.
- Secretary of Defense, *Annual Report to Congress - Military and Security Developments Involving the People's Republic of China 2018*, Washington, 2018.
- Serbu, Jared. "Army Vows to Reinvigorate Electronic Warfare by Combining it with Cyber, Intelligence Functions", *Federal News Network*, December 14, 2017, https://federalnewsnetwork.com/defense-main/2017/12/army-vows-to-reinvigorate-electronic-warfare-by-combining-it-with-cyber-intelligence-functions/ (accessed: January 13, 2019).
- Shalal, Andrea. "Germany Challenges Russia Over Alleged Cyberattacks", *Reuters*, May 4, 2017, https://www.reuters.com/article/us-germany-security-cyber-russia/germany-challenges-russia-over-alleged-cyberattacks-idUSKBN1801CA

(accessed: March 24, 2019).
- Shambaugh, David L. *China Goes Global - The Partial Power,* Oxford: Oxford University Press, 2013.
- Shead, Sam. "Eric Schmidt on AI: 'Trust me, these Chinese People are Good'", *Business Insider*, November 1, 2017, https://www.businessinsider.com/eric-schmidt-on-artificial-intelligence-china-2017-11 (accessed: January 15, 2019).
- Simontie, Tom. China is Catching up to the US in AI Research - FAST, *Wired*, March 13, 2019, https://www.wired.com/story/china-catching-up-us-in-ai-research/ (accessed: August 8, 2019).
- Smeets, Max and Lin,Herb. "An Outcome-Based Analysis of U.S Cyber Strategy of Persistence & Defend Forward", *Lawfare,* Novermber 28, 2018, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward (accessed: January 13, 2019).
- Snegovaya, Maria. Putin's *Information Warfare in Ukraine - Soviet Origins of Russia's Hybrid Warfare*, Institution for the Study of War, September 2015.
- South, Todd. "The Army is Putting Cyber, Electronic Warfare Teams in its BCTs", *Army Times*, February 20, 2018, https://www.armytimes.com/news/your-army/2018/02/20/the-army-is-putting-cyber-electronic-warfare-teams-in-its-bcts/ (accessed: January 13, 2019).
- Stimson, George W; Griffiths, Hugh D; Baker, Chris J and Adamy, Dave. *Stimson's Introduction to Airborne Radar, Electronic Warfare 3rd Edition*, Institution of Engineering and Technology, 2014.
- Strobel, Warren. "U.S Losing 'Information War' to Russia, Other Rivals: Study" *Reuters*, March 25, 2015, https://www.reuters.com/article/us-usa-broadcasting-idUSKBN0ML1MN20150325 (accessed: April 2, 2019).
- The White House, *National Cyber Strategy of the United States of America,* Washington, September 2018.
- Theohary, Catherine A. "Information Warfare: Issues for Congress"*, Congressional Research Service,* Washington, March 5, 2018.
- Thornton, Rod. "The Changing Nature of Modern Warfare: Responding to Russian Information Warfare", *RUSI Journal*, 160, no. 4 (July 2015): 40-48.
- Underwood, Kimberly. "Army Cyber to Become Information Warfare Command", *SIGNAL*, March 14, 2019, https://www.afcea.org/content/army-cyber-become-information-warfare-command (accessed: March 27, 2019).
- United States Department of the Army, *FM 3-38 Cyber Electromagnetic Activities,* Washington, February 2014.
- Votel, Joseph L. (Gen), Julazadeh, David J. (Maj. Gen.) and Lin, Weilum (Maj.). "Operationalizing the Information Environment: Lessons Learned for Cyber Integration in the USECNTCOM AOR", *The Cyber Defense Review* (Fall 2018): 3-13.
- Warner, Mark. "A New Doctrine for Cyberwarfare & Information Operations", *Gizmodo,* December 7, 2018 https://gizmodo.com/senators-cyber-doctrine-calls-

for-u-s-to-redraw-the-bl-1830943004 pp. 1-3, (accessed: January 9, 2019).

- Watts, Clint. "Russia's Active Measures Architecture: Task and Purpose", *Alliance for Securing Democracy*, May 22, 2018, https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/ (accessed: April 4, 2019).
- Way, Lucan Ahmad and Casey, Adam. "Russia has been meddling in Foreign Elections for Decades. Has it Made a Difference?", *The Washington Post*, January 8, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference/?utm_term=.3497a14027cd (accessed: January 13, 2019).
- Weber, Valentine. "States and their Proxies in Cyber Operations", *Lawfare*, May 15, 2018, https://www.lawfareblog.com/states-proxies-cyber-operations (accessed: April 2, 2019).
- Xuanzun, Liu. "China's New Electromagnetic Rocket More Powerful than Most Conventional Artillery on Qinghai-Tibet Plateau: Expert", *Global Times*, August 2, 2018, http://www.globaltimes.cn/content/1113596.shtml (accessed: April 28, 2019).
- Yang, Zi. "Blinding the Enemy: How the PRC Prepares for Radar Countermeasures", *China Brief*, 18, no. 6 (April 2018), https://jamestown.org/program/blinding-the-enemy-how-the-prc-prepares-for-radar-countermeasures/ (accessed: January 9, 2019).
- Zetter, Kim. "The Ukrainian Power Grid was Hacked Again", *Motherboard*, January 10, 2017, https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report (accessed: January 13, 2019).