

שילוב לוחמה קיברנטית בסוגי לוחמה אחרים : חקר מקרה : ארצות הברית / הראל מנשרי

תקציר

עולם מערכות המידע והביטחון השתנה מן הקצה אל הקצה במהלך העשורים האחרונים. כבר במלחמת המפרץ בשנת 1991 הפעילה ארצות הברית יכולות לוחמה קיברנטית, אך ידוע שעוד שנים קודם לכן עסקו גורמי המודיעין האמריקאים בפעילות קיברנטית חשאית. לנוכח הדברים, הוחלט לבדוק כיצד נערכת ארצות הברית לפעילות במרחב הקיברנטי.

מטרת המחקר הנוכחי הייתה לבחון את מקומה של הפעילות הקיברנטית בארצות הברית, את השינויים בכוחות הלוחמים בהיבטי יכולות התקיפה וההגנה במרחב הקיברנטי, ואת שילוב הלוחמה הקיברנטית בסוגי לוחמה אחרים. הבחינה הקיפה את שהתרחש במהלך השנים האחרונות ובעיקר בתקופת ממשל אובמה, תוך התמקדות בנושאים אלו:

1. אפיון בניית היכולות ופיתוח המתודולוגיות שכוונו להשגת עליונות קיברנטית של ארצות הברית;
 2. מיפוי הגופים הממוסדים העוסקים בלוחמה קיברנטית, בחינת כפיפותם למסגרות צבאיות ואזרחיות והערכת תקציביהם;
 3. בחינת החקיקה הקיימת בתחום זה;
 4. אפיון התלות בין תשתיות אסטרטגיות ובחינת השפעתה של תלות זו על ההחלטה לפגוע פגיעה קיברנטית בתשתיות;
 5. זיהוי החברות המסחריות המעורבות בפעילות הלוחמה הקיברנטית של ארצות הברית;
 6. זיהוי וניתוח הגורמים המשפיעים על ריסון גורמי הכוח האמריקאים בבואם להחליט על הפעלת אמצעי לחימה (אמל"ח) קיברנטיים.
- באמצעות בחינה זו אפשר יהיה להסיק מסקנות על אודות מוכנות ארצות הברית לתקוף במרחב הקיברנטי, כחלק מפעילות לוחמנית של הכוחות המזוינים בארצות הברית.

שיטת המחקר שנבחרה מתבססת על מחקר איכותני והשוואתי: ניתוח תוכן כתוב (Content Analysis) של מידע שנאסף ממקורות גלויים העוסקים בגורמי תקיפה והגנה וממקורות העוסקים בהגנה על התשתיות הלאומיות החיוניות בארצות הברית, ניתוח מחקרים שפורסמו, מידע שהתפרסם על תרגילים ומשחקי מלחמה ועל אירועי לוחמה קיברנטית. בין השאר נכללו כמקורות ראשוניים מסמכי מדיניות, מסמכי חקיקה, החלטות ופרסומים מטעם מוסד הנשיאות והמשרדים הרלוונטיים, גופי המחקר של הקונגרס וגורמי הלוחמה הקיברנטית, שימועים בקונגרס וספרי תקציב של גופים פדרליים. בין המקורות המשניים נכללו מחקרים וספרות מקצועית בנושאי לוחמת מידע והעולם הקיברנטי, מאמרים בעיתונות חוקרת, מידע מתוך אתרי אינטרנט שעיקר עיסוקם לוחמה קיברנטית ופרסומי כנסים.

מניתוח מקורות המחקר עולים ממצאים אלו :

פיתוח מתודולוגיות ללוחמה קיברנטית

המלחמה במרחב הקיברנטי מתנהלת כבר היום במלוא עוזו. בעשור האחרון, ובעיקר מאז נכנס הנשיא אובמה לתפקידו בבית הלבן, עוסק הממשל האמריקאי בהכנת תשתית חוקית ומנהלתית לגיבוש אסטרטגיה מקיפה להגנה ולהתקפה במרחב הקיברנטי. כך הותוו אסטרטגיות לאומיות לפעולה במרחב הקיברנטי, עד לגיבוש של אסטרטגיה עדכנית על ידי ממשל אובמה בשנים 2011-2012.

הקמת גופי לוחמה קיברנטית

במקביל לעשייה המתודולוגית הוקמו יחידות לחימה קיברנטית במסגרת הכוחות המזויינים ובגופי המודיעין האמריקאים. לצדם הוקמו יחידות הגנה ואבטחה בממשל ובמסגרות מקומיות. הוקם מרכז לוחמה קיברנטי – פיקוד הסייבר – בצמוד לסוכנות לביטחון לאומי (National Security Agency) NSA, וראש ה-NSA משמש במקביל גם כמפקד פיקוד הסייבר. הזרועות הלוחמות של ארצות הברית הקימו בשנים האחרונות מערכים קיברנטיים. הגדרות המשימה של יחידות אלו כוללות, בצד אבטחת המרחב הקיברנטי הצבאי ותמיכה טכנולוגית ביחידות הקינטיות, גם הגדרה מפורשת הנוגעת להכרעת כל יריב פוטנציאלי, ושמירה על העליונות האמריקאית במרחב הקיברנטי תוך תקיפת מערכי היריב במרחב זה. ריבוי הארגונים ותת-הארגונים הפעילים במרחב הקיברנטי בארצות הברית יצר בעיות הנוגעות לשליטה, למידור ולאחריות פיקודית בין הגופים השונים.

חקיקה במרחב הקיברנטי

הפעילות האמריקאית הנרחבת לחקיקה בין-לאומית עוסקת גם בבחינת האפשרויות להגבלת הפצת אמל"ח קיברנטי והפעלתו, בדומה לאמנות להגבלת תפוצת הנשק הלא קונבנציונלי. פעילות זו נתקלת בפעילות "לעומתית" ומתנגדת מצדן של רוסיה וסין, בצירוף מדינות נוספות.

תלות בין תשתיות

התלות הקיימת בין התשתיות מחייבת את גורמי התקיפה האמריקאים, אשר מתכננים לפעול מול תשתיות זרות, לבחון היטב את הקשרים בין התשתיות שבכוונתם לתקוף לבין תשתיות אחרות – במדינת היעד, בארצות הברית ובמדינות אחרות. זאת, על מנת למנוע פגיעה שתשפיע על התשתיות האמריקאיות, ולמנוע פגיעה – העלולה להיחשב כפשע מלחמה – בתשתיות נוספות.

מעורבותם של גופי מסחר בתחומי הלוחמה הקיברנטית

המרחב הקיברנטי מבוסס בחלקו הגדול על תשתיות, המקושרות זו לזו ונשענות על פעילותן של חברות ענק בין-לאומיות, דוגמת סיסקו, מיקרוסופט והדומות להן. לשוק האזרחי האמריקאי השפעה ניכרת על התפתחות המרחב הקיברנטי ועל יכולות ההתקפה וההגנה של סוכנויות הממשל והזרועות הצבאיות.

סייגים להפעלת כח קיברנטי

מאפייני התרבות והדמוקרטיה האמריקאית מציבים בפני קובעי המדיניות של ארצות הברית סייגים ובלמים כבדים מאוד באשר להפעלת הכוח הקיברנטי שלה במבצעי תקיפה על תשתיות אזרחיות. נראה, כי תקיפת מטרות צבאיות טהורות תוכל לצאת אל הפועל בקלות רבה יותר. עם זאת, ברור שיתקיימו פעולות שמטרתן לאסוף מודיעין, ואף להשיג נקודות גישה במערכות יריבים כהכנה לפגיעה בעתיד.

המסקנה העיקרית מתוצאות בחינה זו היא – "אין קינטי בלי קיברנטי". האסטרטגיה האמריקאית דוגלת בברור בשילוב פעולות קיברנטיות בפעולות הקינטיות, שכן פעולות מלחמתיות קונבנציונליות כשלעצמן אינן עוד הדרך הטובה והיעילה ביותר להשגת המטרות במערכה.

בהקשר זה יצוין כי ליכולת ההגנה תפקיד מכריע בהתמודדות ובניצחון בסביבה א-סימטרית, דוגמת זו שאותה חווים האמריקאים מול יריביהם במרחב הקיברנטי. יש צורך אקוטי ליצור איזון בין יכולות התקפה והכרעה לבין יכולות הרתעה והגנה על תשתיות ועל נכסים.

דרך הפעולה האמריקאית גורסת קיומה של מסגרת ועטיפה קיברנטית לכל תרחיש צבאי. השאיפה היא להגיע ליכולת נטרול מערכות ההגנה של הצד היריב טרם פתיחת הלחימה, ובמקביל לספק אבטחה למערכות המידע והתקשורת של הכוחות הלוחמים האמריקאים. כך, בצד הפגיעה ביכולותיהן של מערכות השליטה והפיקוד של היריב, ייפגעו גם מרכיבים קריטיים, ויכולתו של היריב להפעיל את מערכי הלחימה שלו תיפגע.

מחידושי מחקר זה יצוינו:

1. רצף הזמן של המרחב הקיברנטי שונה מרצף הזמן המוכר לנו בתחומים אחרים. פעמים רבות קשה ואף בלתי אפשרי לתזמן את השפעתה של פגיעה קיברנטית בדרך שבה אפשר לתזמן השפעה של תקיפה קינטית. לנתון זה סיבות רבות, למשל ריבוי וגוון של מערכות חומרה ותכנה ביעד המותקף, הקישוריות בין המערכות ביעד, המרחק בין המערכות ורוחב הפס, גיבוי המערכות הללו ועוד. דבר זה יצר צורך להקים מערכי גיבוי לתקיפה, קרי: אפשרות לבצע כמה תקיפות במקביל, במטרה להגיע לתוצאות הרצויות.
2. ניהול המערכה הקיברנטית מחייב חשיבה מחודשת וגיבוש הגדרות עדכניות למערכות מסורתיות, בעיקר באשר לקיומה של שדרת פיקוד סדורה ומוכרת המסוגלת לנהל את המערכה. הוקמו גופי לוחמה קיברנטית רבים כל כך במגזרים השונים, ולנוכח ריבוי הגופים עולה השאלה: מי ינהל את המערכה הקיברנטית? האם מצביא יחיד יוכל לנהל את שדה הקרב הווירטואלי במערכת המידע? מהו היחס הפיקודי בין הגופים הצבאיים-ביטחוניים לגופים האזרחיים? האם יתקיים שיתוף פעולה מסודר בין המפקדה לבין גורמים אזרחיים – התעשייה והמגזר הפרטי?
3. יותר מאשר בשדות הקרב המסורתיים, במערכה הקיברנטית נדרשת יכולת לקבל החלטות מהירות בתגובה לפעילות יריב במרחב הקיברנטי. אחת השאלות שיש לבחון היא, אם תגובה חייבת להיות דומה במאפייניה לתקיפה, כלומר

קיברנטית או קינטית. מתוך הבנה שאפשר להוציא את היריב משווי משקלו באמצעות פגיעה במערכות השליטה והפיקוד שלו, עולה למשל השאלה: האם לפגוע ישירות במערכות הקינטיות של היריב או לנסות לשבש את כלל מערכות ההפעלה שלו ואת מערכתיו הלוגיסטיות באמצעים קיברנטיים?

4. כל מערך תקיפה נדרש לדון בגבולות ובמגבלות התקיפה או התגובה לתקיפה, ובעיקר במצבים שבהם מדובר בהשבתה או בהשמדה של תשתיות ובפגיעה בגורמים אזרחיים.

כפועל יוצא מהמחקר, המסקנה המתבקשת היא, שהשאיפה האמריקאית היא לקיים פעילות קיברנטית תוקפת מקדימה לכל פעילות קינטית, ובמקרים מסוימים, לנסות ליתר את הפעילות הקינטית באמצעות הרס משאביו ותשתיותיו של היריב.

מס' מיון בספרייה:

005.8 מנש.של תשע"ד

מס' מערכת בספרייה:

002385029