את המאמר המלא ניתן למצוא בכתובת www.Grade.co.il. לשירות לקוחות ניתן לפנות info@grade.co.il.

תוכן עניינים

מבוא .....עמ' 2

פרק ראשון: מרחב קיברנטי -ביאור מושגים.....עמ' 3-4

פרק שני: רקע על טרור קיברנטי .....עמ' 4-7

פרק שלישי: טרור הסייבר כזירת לוחמה חמישית.....עמ' 7-12

פרק רביעי: ארגון הטרור דאע"ש ופעילותו במרחב הקיברנטי.....עמ' 12-23

פרק חמישי: התגוננות ישראל וארה"ב מפני טרור קיברנטי .....עמ' 23-29

סיכום .....עמ' 30

תקציר זה כפוף לתקנון אתר Grade.co.il ויחולו עליו התנאים הכתובים שם. העושה שימוש במסמך, לרבות קריאתו, מקבל על עצמו ללא סייגים את כל התנאים הקבועים בתקנון. מעבר לכך, אין להעתיק, לשכפל, לשנות, להפיץ, לפרסם, לשדר, להציג בפומבי, להעמיד לרשות הציבור, למסור או למכור לצד שלישי או לעשות שימוש מסחרי כלשהו במסמך זה ו/או כל חלק ממנו.

מבוא

בעשור האחרון מושגים כגון "מרחב הסייבר", "מתקפת הסייבר", "הטרור הקיברנטי" תופסים כותרות רבות ומטילים אימה על הציבור, בכל רחבי העולם. העולם הווירטואלי מפגיש בין חברים ליריבים, בין אויבים לידידים. עבור הטרור בעידן הסייבר לא קיימים גבולות מדינתיים או חברתיים. תהליכי הגלובליזציה הפכו את העולם ל"כפר גלובלי" אחד גדול, אשר המרחב הווירטואלי בו, הפך את השימוש באתרי האינטרנט לכלי יעיל, נגיש ונח לכל מטרה- גם עבור ארגוני הטרור (טל, סימן טוב, 2015).

בעבודה זו אנסה לספק תשובות אודות שאלת המחקר: אילו פעולות בתחום הטרור הקיברנטי עושים ארגוני הטרור, בדגש על ארגון הדאע"ש, בכדי לקדם את מטרותיהם, וכיצד מתגוננות ארה"ב וישראל עם הטרור הקיברנטי? העבודה הינה עיונית ומתבססת על מקורות אקדמיים ומקצועיים.

בפרק הראשון אסביר את המושגים והמונחים המגדירים ומרכיבים את מרחב הסייבר. בפרק השני אציג את הרקע להתפתחות הטרור במרחב הקיברנטי וכיצד מרחב זה משמש עבור ארוגני הטרור פלטפורמה להשגת מטרותיהם. בפרק השלישי אסביר כיצד השימוש במרחב הסייבר הפך הלכה למעשה למימד לוחמה חמישי, בנוסף לארבעת המימדים המקובלים: יבשה, ים, אוויר וחלל. אבהיר כיצד ומדוע מימד לוחמה זה מהווה איום על המדינות אליהן הוא מכוון, על כל הסכנות הגלומות בו, בתחומים כגון: כלכלה, תשתיות קריטיות, בנקאות, תהליכים הדמוקרטיים ועל אף חיי האדם.

מימדים סביבם מתנהל לרוב השיח במרחב הסייבר נעים סביב ציר ההגנה, ההתקפה, איסוף מידע מודיעיני. כפי שיעלה בעבודה זו- גם למימד ההשפעה במרחב הקיברנטי, שעד כה לא זכה לתשומת לב מספקת, תפקיד מכריע במרחב זה. אף על פי שעיקר ההתמקדות בעבודה זו היא הגנה מפני איומי הסייבר, אגע בקצרה גם במימד ההתקפה ובמימד ההשפעה, מה שיסייע להבין בהמשך כיצד מימד זה משרת את ארגון דאע"ש בהשגת מטרותיו.

בפרק הרביעי אציג כדוגמא את ארגון הטרור דאע"ש, אשר מנצל את מרחב הסייבר והרשתות החברתיות כבמה להטלת אימה על הציבור בעולם, בעיקר בארצות המערב, ארה"ב וישראל מחד גיסא, ומאידך משתמש בו לצורך הגדלת רשת תומכיו ומקורות המימון שלו. כך טרור הסייבר הפך למעשה לזירה בפני עצמה, בעוד שמדינות כלפיהן מכוון הטרור משקיעות משאבים עצומים בכדי להתגונן גם בזירה זו. בפרק זה אבחן גם את השערת המחקר שלי, לפיה ארגון דאע"ש משתמש במרחב הקיברנטי בצורה נרחבת יותר מארגוני טרור אחרים, ככלי נוסף לפעולות הטרור המוכרות, בכך מחזק את מעמדו כארגון טרור ומעלה את הסיכוי שלו לגיוס חברים חדשים ולגיוס משאבים כלכליים. בפרק זה אתייחס לשאלת המחקר שלי אשר בוחנת אילו פעולות בתחום הטרור הקיברנטי עושים ארגוני הטרור בכלל ודאע"ש בפרט. בפרק הבא אפרט את החלק השני של שאלת המחקר שלי המתמקדת בדרכי התגוננות של ארה"ב וישראל מפני איומי הטרור הקיבנרטי, בדגש על דאע"ש.

אנסה להסביר את הגורמים לעוצמתו של דאע"ש ואת המקורות למימון של ארגון טרור זה. בפרק החמישי, אציג שני מקרי בוחן -ישראל וארה"ב ואתאר כיצד מדינות אלה, העומדות בקדמת הטכנולוגיה, מתגוננות בפני איומי הסייבר בכלל ושל דאע"ש בפרט. בפרק השישי אציג את הסיכום.

תקציר זה כפוף לתקנון אתר Grade.co.il ויחולו עליו התנאים הכתובים שם. העושה שימוש במסמך, לרבות קריאתו, מקבל על עצמו ללא סייגים את כל התנאים הקבועים בתקנון. מעבר לכך, אין להעתיק, לשכפל, לשנות, להפיץ, לפרסם, לשדר, להציג בפומבי, להעמיד לרשות הציבור, למסור או למכור לצד שלישי או לעשות שימוש מסחרי כלשהו במסמך זה ו/או כל חלק ממנו.

פרק ראשון: מרחב קיברנטי -ביאור מושגים

בעשור האחרון, בשיח העולה סביב האיום הקיברנטי אנו נחשפים למושגים רבים אשר נשמעים לנו לא ברורים, לא מובנים ואף מאיימים. למונחים רבים בעולם הסייבר לא קיימות הגדרות ברורות וחד משמעיות. כך למשל, האם נכון לומר "מרחב הסייבר" או "המרחב הקיברנטי"(cyberspace)? מה ההבדל ביניהם? מסתבר כי לשני המושגים אותה המשתמעות, אך קיימות עברום מספר הגדרות. לפי טבנסקי (2011), צמד המילים "cyber space" מורכב ממילה space, שפירושה "מרחב" וממילה cyber (netics) (מקור המילה מיוונית- kybernetes), פירושה "הגיא". שימוש מודרני של המילה cybernetics הופיע לראשונה בספר אשר נכתב על ידי המתמטיקאי נורבטר וינר בשנת 1948, כדי לתאר "שליטה, בקרה ותקשורת בעולם החי או בעולם המכונות" (טבנסקי,2011,עמ' 66).

באופן תאורתי, מרחב הסייבר הינו מימד ווירטואלי המתייחס למרחב גאוגרפי, פילוסופי, חברתי, מתמטי ועוד. במטרה להבין את המושג, עלינו להתייחס אליו באמצעות התהליכים הקורים בעולם הממוחשב, תוך בחינת ההקשר שלהם לסוגיות הביטחון הלאומי. בניגוד למרחבים הטבעיים כגון יבשה, אוויר ומים, מרחב הסייבר הינו מלאכותי, פרי יצירתו של האדם אשר פיתח את הטכנולוגיות. המרחב מורכב למעשה מרשתות ממוחשבות בכל העולם (שם).

אודות לחיבור המרושת, מרחב הסייבר מאפשר זרימה חופשית של ידע, הון ושירותים עם חסמי כניסה נמוכים מאד, ובכך הוא משפר את הרווחה החברתית ומעודד חדשנות. פעילויות רבות עוברות להתקיים במרחב הסייבר דוגמת תשלומים דיגיטליים או שליטה ובקרה בתהליכי ייצור ותפעול. מהפכת המידע והתקשורת מובילה להפצה של מידע ומסחר מקוון. כתוצאה מכך ונוכח השפעתו הנרחבת על פעילותם של פרטים, ארגונים ומדינות, הופך מרחב הסייבר לבעל חשיבות אסטרטגית בהיבטים מדיניים, כלכליים, חברתיים וביטחוניים.

הסבר נוסף המוצע על ידי סוכנות האו"ם (ITU) , מתאר את מרחב הסייבר כ "מתחם הפיסי והלא פיסי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מחשבים, מערכות ממוכנות ורשתות, תוכנות, מידע ממוחשב, תוכן, נתוני תעבורה ובקרה " (אבן וסימן טוב ,2011,עמ' 16) .לפי הסבר זה, למרחב הסייבר שלושה רבדים: רובד אנושי בו האנשים משתמשים במערכות תקשוב, רובד לוגי המורכב מתוכנות והיבטים ורובד פיסי המכיל חומרה, תשתיות ניידות ונייחות.

מושג נוסף במרחב הסייבר הוא איום קיברנטי. מה הוא האיום, ממנו חרדות אפילו מעצמות המובילות בעולם? איום במרחב הקיברנטי היא תופעה חדשה יחסית בתחום אבטחת מידע, שנוצרה על ידי האדם ומתפתחת בקצב מסחרר. מדובר בשילוב טכניקות להונאה, התחזות, שכנוע או פריצה לצורך השגת מידע רגיש או פגיעה ברשת ממוחשבת בכוונות זדון. מרגע הגישה למידע, ניתן לשנותו, לנתבו או להשמידו, בהתאם לצרכי המתקפה. איומים קיברנטיים מהווים סכנה לא רק מצד גורמים חיצוניים אלא גם מצד הגורמים הפנימיים, מתוך הארגון עצמו. ביכולתם של אלה המסכנים את הארגון מבפנים, לחשוף את נקודות התורפה של הארגון כלפי חוץ ו/או לבצע מתקפה להדלפת מסמכים או מידע רגיש (מלכא, 2010 ,עמ' 161).

במסגרת המונחים בעולם הקיברנטי חשוב להסביר גם את המונח "מלחמה א-סימטרית" אשר מעלה את הלוחמה לרמה אחרת .בחרתי להציג את ההסבר של עמידרור (2007, עמ' 5). לפי הגדרה זו, מדובר על שימוש באמצעים לא שווים בין הצדדים הנלחמים, שימוש בעוצמה לא שווה ובאופן בו הם תופסים את שדה הקרב. מלחמה א-סימטרית מתקיימת בדרך כלל בין צבא סדיר של מדינה לארגוני טרור או גרילה בשטחים הנמצאים בדרך כלל בשטח שליטה של הארגון הצבאי. דוגמא למלחמה א-סימטרית בישראל היא מלחמת ישראל מול ארגוני הטרור, על גבולות המדינה בעזה,

תקציר זה כפוף לתקנון אתר Grade.co.il ויחולו עליו התנאים הכתובים שם. העושה שימוש במסמך, לרבות קריאתו, מקבל על עצמו ללא סייגים את כל התנאים הקבועים בתקנון. מעבר לכך, אין להעתיק, לשכפל, לשנות, להפיץ, לפרסם, לשדר, להציג בפומבי, להעמיד לרשות הציבור, למסור או למכור לצד שלישי או לעשות שימוש מסחרי כלשהו במסמך זה ו/או כל חלק ממנו.