**טופס הצעת מחקר לתזה – פורמאט מב"ל**

**שם התלמיד:** אל"ם שמואל בן עזרא

**נושא העבודה:**

הרתעה במרחב הקיברנטי – שינוי פרדיגמה או התאמות מקומיות?

**רקע:**

אסטרטגיית ההרתעה מהווה גורם משמעותי במרכיבי הביטחון של מדינות שונות בעולם. בישראל הוגדרה ההרתעה כאחד מארבעת רגלי הביטחון: התרעה, הרתעה, הכרעה והגנה. בעבר שימשה אסטרטגיה זו בשדה הקרב הקונבנציונלי כחלק מכלל מרכיבי המלחמה. בתקופת המלחמה הקרה התחדד מקומה של אסטרטגיה זו כמרכיב מרכזי לייצוב הסכסוך הלא קונבנציונלי בין המעצמות. חומרת האיום הגרעיני ותוצאותיו הפטאליות הובילו ליצירת מאזן אימה בו כל צד מורתע מהשלכותיו של השימוש בנשק מסוג זה. לאחרונה, עם התרחבות מגוון האיומים הותאמה אסטרטגיית ההרתעה לשמש ככלי גם כנגד תת מדינות, ארגוני טרור ועוד.

התפתחותו המואצת של המרחב הקיברנטי ותפוצתו הרחבה הפכו אותו למרכיב מרכזי בחייהם של יחידים כמו גם של מערכות ציבוריות רבות. בד בבד עם היתרונות הרבים הגלומים בתחום זה הופיע מרחב חדש של איומים – איומי הסייבר. פוטנציאל הנזק באיום זה מכסה מנעד רחב של רמות - החל מהצקה ליחיד, דרך נזק כספי משמעותי (תוכנות כופר) ועד ליכולת השבתה של מערכות אזרחיות מצילות חיים כמו גם מערכות צבאיות ממוחשבות. הצורך במתן מענה נגד איום זה הפך לחיוני, והוביל את ממשלת ישראל בשנת 2012 להקמתו של מטה סייבר לאומי. מסמך האסטרטגיה הישראלית להגנת הסייבר מפרט שלוש שכבות עיקריות העומדות בבסיס המענה לאיום במרחב הקיברנטי: 'עמידות משקית', 'חוסן חברתי' ו'הגנה לאומית'. אחד ממרכיבי שכבת 'ההגנה הלאומית' הוא ההרתעה בסייבר. יצוין כי ברמה של מדינת ישראל האתגר המרכזי הוא יכולת ההתמודדות עם איומי סייבר מקרב מדינות ומעצמות (כדוגמת אירן סין ורוסיה) ופחות לאלו המגיעים מקרב ארגונים תת מדינתיים (כדוגמת חמס וחיזבאללה) להם יכולות תקיפה פחותות באופן משמעותי.

השימוש הנרחב במושג ההרתעה במרחב הקינטי עשוי ליצור את הרושם שהנושא מובן מאליו גם במרחב הקיברנטי. בעיון מעמיק יותר מתברר שלא כן המצב. מאפייניו הייחודים של המרחב הקיברנטי מאתגרים את ישימות אסטרטגיית ההרתעה ומטילים ספק ממשי בעצם היכולת להשתמש בו. לדוגמה, אחד ממרכיביה הבסיסיים של ההרתעה הוא העברת אותות מאיימים (Signals) לגורם אותו מעוניינים להרתיע. במרחב הקיברנטי קיים קושי מהותי בנושא זה. כיצד ניתן לשדר אותות הרתעה לתוקף במרחב בו זהותו של התוקף לא תמיד ברורה?. אתגרים אלו והאופן בו נכון להתמודד אתם עומדים במרכזה של עבודת המחקר.

**מטרות העבודה:**

1. בחינה וניתוח של מושג ההרתעה במובנו המקובל במרחב הקינטי.
2. בחינת המרחב הקיברנטי ומאפייניו העקריים.
3. ניתוח מאפייניו הייחודים של האיום הקיברנטי בהשוואה לאיום הקונבנציונלי והעל קונבנציונלי (גרעין).
4. בחינת השפעת מאפייניו הייחודים של האיום הקיברנטי על עקרונות אסטרטגיית ההרתעה המקובלות באיומים הקונבנציונליים והעל קונבנציונליים.
5. גיבוש קריטריונים ייחודיים להרתעה במרחב הקיברנטי המותאמים למאפייניו של האיום בתחום זה.
6. ניסוחה של פרדיגמה לאסטרטגיית הרתעה במרחב הקיברנטי.

**שאלות המחקר:**

1. מהי הרתעה? ומהו המרחב הקיברנטי?
2. האם התפיסה של אסטרטגיית ההרתעה הרווחת כיום במרחב הקונבנציונלי והעל קונבנציונלי רלוונטית למרחב הקיברנטי, ומדוע.
3. האם נדרש שינוי מהותי בפרדיגמה של אסטרטגית הרתעה לאיום במרחב הקיברנטי ומהו השינוי, או שמא ניתן להסתפק בהתאמות מינוריות של התפיסה הקיימת ומהן התאמות אלו.

**תיחום המחקר:**

האיום במרחב הקיברנטי מתאפיין בתפוצה רחבה של תוקפים מסוגים שונים. ניתן לאפיין תוקפים אלו בהסתמך על חתכים שונים. החתך הראשון : עוצמת התוקף - החל מתקיפה ע"י האקרים בודדים, דרך ארגונים תת מדינתיים, ועד למדינות אויב ומעצמות על. חתך נוסף הוא תכלית התקיפה. תקיפה פלילית של ארגוני פשע במטרה להשיג רווחים כספיים (גניבת מידע, חשבונות בנק וכד') אל מול תקיפה בעלת היבטים ביטחוניים צבאיים. חתך שלישי אפשרי הוא נשוא התקיפה. מתקיפתו של אזרח בודד דרך חברה פרטית אזרחית קטנה ועד לחברות פרטיות או ממשלתיות גדולות כולל גופי הביטחון של מדינת ישראל.

במטרה להגביל את היקף המחקר הוא יצומצם לתקיפה **ביטחונית** של תוקף **מדינתי** כנגד גופים **מדינתיים** שכאמור הינו האיום המרכזי על מדינת ישראל. תקיפות פרטיות או של ארגון טרור כנגד בודדים או חברות קטנות במסגרת פשיעה לטובת הונאה כספית לא תכללנה במחקר זה.

**דרך הצגת הרעיונות במחקר (ראשי פרקים):**

1. מבוא - הצגת הנושא ורמות המחקר
2. בעיית המחקר
3. מאפייני איום הסייבר ואסטרטגיית ההרתעה בו – סקר ספרות
4. אתגר ההרתעה במרחב הקיברנטי
5. אסטרטגיית ההרתעה במרחב הקיברנטי – שינוי פרדיגמה או התאמות מקומיות
6. ייחודיות אסטרטגיית ההרתעה במרחב הקיברנטי
7. סיכום ומסקנות
8. נספחים

**חשיבות העבודה:**

התחום הקיברנטי נמצא בהתפתחות מתמדת בעשורים האחרונים. פוטנציאל הנזק העצום במרחב זה מעמיד את המדינות בפני צורך מידי בגיבוש מענה הולם לחומרת האיום. גופים שונים בארץ ובעולם הוקמו אד-הוק על מנת לגבש תוכניות נרחבות להתמודדות כוללת עם האיום. מרכיב ההרתעה במענה הכולל, כנגד האיום הקונבנציונלי והגרעיני הוכח כחיוני ובעל יעילות גבוהה, בייחוד בכך שהצלחתו בשדה הקרב חוסכת את הצורך בשימוש **בפועל** במרכיב הכוח. הרצון לממש מרכיב זה במרחב הקיברנטי מציף אתגרים חדשים הקשורים באופן ישיר למאפייניו הייחודיים של האיום. ברור סוגיה זו קריטי לביטחון הלאומי, שכן כישלון במציאת מענה לאתגרים אלו עלול לפגוע באחת מארבע הרגליים של הביטחון.

**יוזם העבודה:** הכותב

**מנחי העבודה:**

פרופ' יצחק בן ישראל (אוניברסיטת ת"א)

פרופ' גבריאל בן דור (אוניברסיטת חיפה)