|  |  |  |
| --- | --- | --- |
| המכללה לביטחון |  | Israel National |
| לאומי ישראל | Defense College |
| מחזור מ"ח | Class 48 |

**"מלחמת מחשבים" - הצעת מחקר**

ינואר 2021

אל"ם יואב טורחנסקי

אל"ם עומרי דור

אל"ם אוהד בוכריס

מנחה: פרופסור (אלוף במיל') יצחק בן ישראל

מלווה: מר אבי אלמוג

**נושא הפרויקט ומטרתו**

**העבודה תבחן את הצורך באסטרטגיה בתחום הסייבר ההתקפי כחלק ממרכיבי הביטחון הלאומי של מדינת ישראל . תהליך מרכזי המהווה חלק מהתפיסה והאסטרטגיה, הינו בניין כוח בתחום סייבר התקפי והמחקר יבחן גם היבט זה.**

המהפכה הדיגיטלית, שהגיעה לאחר המהפכה התעשייתית, הביאה במחצית השנייה של המאה העשרים את תחילתו של עידן המידע באמצעות המעבר מטכנולוגיה אלקטרונית-אנלוגית לטכנולוגיה דיגיטלית. החל מהמצאת המחשב ומשם לעידן האינטרנט, המהפכה הדיגיטלית שינתה וממשיכה לשנות ולהשפיע על האופן בו מדינות ומסגרות נדרשות להגן על היכולות שלהן ולפתח אותן, בו בזמן שהן נדרשות להתקדם טכנולוגית. בשנים האחרונות, אנו עדים ל**שימוש בנשק מסוג חדש בעל פוטנציאל לשינוי של זירת הלחימה באופן מהותי** – הסייבר.

נהוג לתאר את השימוש בסייבר בשלושה תחומים: מודיעין, הגנה והתקפה. **עבודה זו תעסוק אך ורק בתחום ההתקפי**. "סייבר התקפי" (Cyber warfare, CW) או במושגים דומים אחרים, "לוחמת הסייבר", "לוחמת רשת", "לוחמה קיברנטית" ולוחמת מידע (לוחמ"מ) היא פעולה מלחמתית אשר מבצעת מדינה או ארגון טרור, כדי לגרום נזקים לרשתות ומערכות המחשבים של האויב, או דרך מערכות המחשוב, למערכות אחרות שנשלטות ומבוקרות ע"י מערכות המחשוב הללו.

**מטרות העבודה:**

1. בחינת הצורך באסטרטגיה ואופן גיבושה ביחס לשימוש בסייבר ככלי התקפי עבור מדינת ישראל.
2. בחינת כלים ויכולות שישפרו וישדרגו את היכולת של מדינת ישראל להנחתת מהלומות קשות, מתחת ומעל לסף המלחמה.
3. בחינת ההבנה האסטרטגית בנוגע לנזק הפוטנציאלי כתוצאה ממאבק אלים מסוג זה (מבצעי, חברתי, כלכלי).

העבודה תנסה לאמוד את התהליך המתקיים כיום בתחום זה ואת איום ייחוס שעל פיו הוא מתעצב. בתוך כך האם בניין הכוח תואם, מתואם וצופה את המורכבות הטכנולוגית מצד אחד ואת האינטרסים הלאומיים ומרכזי הכובד של האויבים, הרלוונטיים מהצד השני.

בנוסף, תבדוק העבודה את הפוטנציאל האסטרטגי שבהתקפה בסייבר לתגבור הקטלניות, לשיפור האפקטיביות המבצעית וכמובן, את מידת ההשפעה על ההרתעה של מדינת ישראל ומימושה באמצעות בניין כוח מותאם ומתואם.

ממד הסייבר (cyber space) כולל בתוכו את החומרה, התוכנה ואת מערכות מידע, אך גם את בני האדם ואת האינטראקציות החברתיות שהם מבצעים באמצעות מערכות אלה. מרחב הסייבר הוא חלק אינטגרלי מכל אחת מזירות החיים שלנו. כמעט כל שירות ציבורי ופרטי שאנו מכירים תלוי ו/או עושה שימוש במחשוב, בתקשורת במחשבים ובמערכות מידע ממוחשבות: שירותי הטלפוניה, התקשורת במדיות השונות, מערכות הפיננסים והבנקאות, התחבורה; תשתיות המים והחשמל ועוד. לצד היתרונות והייעול, שמאפשרות המערכות הממוחשבות, הן יצרו גם איום חדש שמידת החשיפה לו גדלה ככל שההתפתחות הטכנולוגית גדולה יותר. לאיום הסייבר פנים שונות בתוכן: פשיעת סייבר, טרור וגרילה סייבר, ריגול סייבר, לוחמת סייבר ומודיעין עסקי.

בין הפעולות הכלולות כיום בלוחמת סייבר ניתן למצוא חדירה לרשתות מחשבים, ריגול, שאיבת מידע, פגיעה וגרימת נזקים למערכות (בעיקר תשתיות מדינה קריטיות), מתקפות על הרשתות או רשתות הנסמכות עליהן וכדומה.

קיים קשר חיובי בין היקף ורמת האמצעים ההתקפיים לפוטנציאל הנזק האפשרי. בשנים האחרונות אנו עדים למספר לא מבוטל של פעולות זדוניות מול תשתיות ונכסים בעולם (לא רק אלו המוגדרים כאסטרטגיים או צבאיים). פעולות אלו ברובן מבוצעות על ידי מדינות אל מול מדינות אחרות, אך גם ארגונים בעלי אינטרסים או כשליחים (פרוקסיז), אשר מעוניינים לקדם את האינטרסים שלהם. בעבר, היכולת לבצע נזק קריטי למערכות מסוג זה, היתה בידי מעצמות בלבד. כיום, ניתן לקנות יכולות שהאקרים וארגוני פשיעה עושים שימוש ביכולות, שכאמור, היו רק בקרב מדינות.

אירועי סייבר השפיעו על מערכות היחסים בין המדינות ואף הובילו ל"קפיצת מדרגה" בניהול ממד הסייבר באופן שניתן להגדירו כזירת לחימה לכל דבר. בשנת 2019 ביצעה איראן התקפות על כשמונה חברות מתחום הנפט. זאת, במטרה להשפיע על מחירי הנפט. בשנים האחרונות מתבצעים ניסיונות רבים כדי להביא לפגיעה או ליתרון בתחומים הקשורים ליחסים בין מדינות.

ניתן לתאר את השימוש **בסייבר ההתקפי כאמצעי נוסף,** באמצעותו יכולה מדינת ישראל לפעולו**להשיג את האינטרסים ואת המטרות מול יריביה ואויביה – לחזק את היכולות ההתקפיות ובהתאם כמובן את ההגנה, להגביר את ההרתעה ולייעל את המשאבים המושקעים לצרכים אלו**. ישראל צריכה לפתח את יכולותיה בהשגת עליונות סייבר באמצעות "עוצמה חדה".

תהליכי החשיבה והכלים לניתוח אסטרטגי של מערכות אויב נדרשים לכלול את כלל הפרמטרים הניתנים להבנה והשפעה על האויב. ממד הסייבר מצטרף לסל הכלים והיכולות האסטרטגיים המצויים בידי מדינת ישראל (ומדינות אחרות) והופך לשחקן מרכזי.

עולה השאלה, **האם יכולות ממד הסייבר ההתקפי משתלבות בסך השיקולים האסטרטגים והגיאופוליטיים בניתוח האויב ומהוות כלי המשתלב כחלק אינטגרלי ביכולות ה"קטלניות" של מדינת ישראל**?

הסייבר הינו עולם חדש יחסית, ה"לחימה" במימד זה אינה נושאת עמה היסטוריה של מאבקים, מתחים ולחימה. למלחמות "רגילות" יש כללים מסוימים. הסכמים נחתמו לאורך ההיסטוריה, כדי להקטין את הסיכוי לפגיעה בחפים מפשע. בשונה מכך, במלחמה בסייבר, נכון לכתיבת שורות אלה - לא נקבעו כללים אתיים. הסייבר אינו נראה, אך תוצאותיו בעלות פוטנציאל הרסני אם חוצים את קווי הלחימה כפי שהם מוכרים לנו היום. בשנים האחרונות ובדגש על השנה האחרונה, אנו עדים לשימוש הולך וגובר בלוחמת הסייבר, ככזה שמעסיק את מעצמות העולם, ללא גבולות ברורים של מותר ואסור, פוטנציאל נזק אשר עשוי ל"מחוק" יכולות נרחבות במדינות מסוימות או לגרום לכאוס **.**

על כן,ניתן לשאול האם ישנה הפניית משאבים מספקת לעיצוב מדיניות השימוש ביכולות השונות וניתוח הפוטנציאל (שלילי/חיובי). מדינת ישראל עלולה לעמוד בפני שוקת שבורה, ללא יכולת להגיב באופן ראוי בהגנה וביתר שאת באופן התקפי.

**חשיבות הנושא ותרומתו לביטחון הלאומי:**

על פי פרסומים, בשנת 2011 הוחדרה תולעת מחשב שפגעה בתכנית הגרעין האיראנית (STUXNET) באמצעות פגיעה במערכות בקרה תעשייתיות, מתוצרת חברת סימונס, ששולטות בצינטרפוגות במתקן ההעשרה בנתנז. מומחים בעולם מאמינים שישראל וארה"ב יצרו את התולעת כחלק ממבצע סייבר התקפי משותף. נראה כי ממד הסייבר ובוודאי שהחלק ההתקפי שבו, הפך להיות כלי מרכזי במאבק בין המעצמות הגדולות בעולם. זאת, על רקע היכולת והפוטנציאל שקיים בחובו. מורכב מאוד לתאר במילים את המידע הענק שניתן ל"גנוב" בסייבר, את פעולות ההשפעה והתודעה שניתן לבצע וכמובן את הפגיעה בנכסים וביכולות באמצעות הסייבר.

במפגש שהתקיים בניו יורק בדצמבר 2001 ,זמן לא רב לאחר מתקפת הטרור בארצות הברית, שטח הפילוסוף ז'אק דרידה את תפיסתו על התמורות שחוללו בעולם פיגועי ה11 בספטמבר 2001. לשיטתו, פיגועים אלו הם עדיין חלק מ"תיאטרון האלימות העתיק", העולם הממשי והנראה, שבו דברים עדיין מתנהלים ב"סדר ברור וגדול".

ואולם לדבריו, קיים מרחב פעולה , אשר מציב איום חמור יותר על עולמנו הפוליטי והפיזי, הוא- **מרחב הסייבר** **-** מרחב הסייבר, הנמצא בכל מקום ובשום מקום כאחד. מדיום המורכב ממיליוני יחידות של אינפורמציה, מדיום היוצר בבני אדם תחושה של הינתקות מהעולם הפיזי המוכר ומעבר למרחב גיאוגרפי מנטלי ודמיוני שבו הכול מותר. עולם לא חומרי, שבו אף אחד מן החוקים המוכרים בעולם "הרגיל" אינו מתקיים. הסכנות הטמונות בו משנות את היחס בין טרור, במובן הפסיכולוגי וההיסטורי של התקפה אלימה, לבין המושג טריטוריה.

כעת, בעידן הטכנו-מדעי החדש, האיום שהכרנו בעבר כממשי, נהפך לאיום בלתי נראה, שקט, מהיר, לא בהכרח בעל שפיכות דמים, שלדברי דרידה הוא גרוע יותר מפיגועי ספטמבר, שכוונו כלפי מקום ידוע בזמן מסוים. כעת אנו ניצבים נוכח אתגר המאיים על מרקם החיים החברתיים והכלכליים, מרקם שכולנו קשורים ותלויים בו, בכל נקודה ובכל רגע. ההתפתחויות והחידושים הטכנולוגים המהירים בשנים האחרונות במרחב הסייבר אכן יצרו שדה לחימה שבו חוברות ומאוגדות להן בו בזמן אוכלוסיות מגוונות ורבות, מקומיות ובינלאומיות, שהן יעד נחשק לפעילותם של אינטרסים שונים ומורכבים.

**הפוטנציאל השלילי שיש למלחמת סייבר ("מלחמת מחשבים") בין מעצמות ומדינות (אך לא רק), עלול להוביל לפגיעה ביכולות ובאתרים האסטרטגיים של מדינה, באופן שהחוסן יפגע באופן דרמטי וההתאוששות מפגיעה שכזו, תהיה קשה**. בשנים האחרונות, הממד הזה הפך לפעיל בצורה נרחבת ומכך גם מגוון היעדים אשר נתקפים בהתגוששות בין מדינות וארגונים

אם בעבר העיסוק בנזק הפוטנציאלי כתוצאה מתקיפה בסייבר היה תאורטי בלבד והתנהל במסגרת במשחקי מלחמה או בדיון על תרחישים, הרי שהשנים האחרונות, מלמדות אותנו הלכה למעשה, כיצד ניתן **להרוס תשתית** (בדצמבר 2015, דווחה פגיעה בהספקת החשמל של 27 **תחנות חשמל** באוקראינה, השלטון טען לפגיעת סייבר) או נכס לאומי כגון **נמל ימי** (על פי ה"וושינגטון פוסט", במאי 2020 נתקף נמל בנדר עבאס באיראן באמצעות סייבר ופעילותו נפגעה לאורך ימים ארוכים) , **לעצור פעילות של בית חולים** למספר ימים (במהלך מאי 2017, "נתקפו" עשרות בתי חולים באנגליה, העומדים מאחורי התקיפה, דרשו "כופר" על מנת להחזיר את הפעילות לסדרה) או "רק" להקפיא חברת ביטוח או חברה בסדר גודל בינוני. כל זאת, **מתחת לרף ההסלמה או אכיפה משמעותית**.

ניתן רק לדמיין את האפשרויות הגלומות ביכולות הקיימות בידי מדינת ישראל. זאת, על מנת להשיג את היעדים האסטרטגיים, כפי שהנחה הדרג המדיני הביטחוני וכמובן את היעדים האופרטיביים אל מול האויבים באופן פרטני. לא ניתן להתייחס לתחום כרכיב או ממד בודד, אלא כחלק בלתי נפרד מהיכולות האסטרטגיות, שמחזיקים בהן גורמי הפעלת הכוח במדינת ישראל לשם השגת מטרותיה.

**שאלת המחקר:**

לאור האמור לעיל ובחיבור לתהליכי בניין כוח נרחבים נוספים ברצוננו לבחון:

1. באיזו מידה **עיצוב מדיניות לאומית בתחום ה"סייבר ההתקפי"** עשוי לתרום ליצירת מכפיל כוח בהשגתם של אינטרסים לאומיים ושדרוג הביטחון הלאומי?
2. מהו פוטנציאל תרומתו של סייבר התקפי - כמימד הפועל כ**חלק ממענה התקפי שלם** ולאורה של **מדיניות סדורה** - לשיפור **ההרתעה** של מדינת ישראל, ואף ל**צמצום משאבים המופנים להגנה** כתוצאה מתהליכים התקפיים אחרים (בעיקרם)?
3. ככל שקיימת אסטרטגיה לאומית, מה נכלל בה בהיבטי **בניין כוח** התואמים את האינטרסים המדינתיים האזרחיים, שיוכל לספק הסייבר ההתקפי לצד שיקולי הגנה וצבא (בדגש על נושא "הקטלניות")? האם נדרש **מנגנון משולב** (אקוסיסטם) המאפשר **פעולה מתואמת ומסונכרנת** של בעלי העניין?

**שיטת המחקר**

1. העבודה תיערך כמחקר איכותני.
2. קריאה נרחבת של מידע נגיש בנושא, בדגש על מיקוד במלחמת סייבר או לחימה קיברנטית.
3. ניתוח אירועים מרכזיים בנושא שהתרחשו בעולם על פי פרסומים לא מסווגים.
4. פגישות עומק וראיונות עם גורמים אשר עוסקים בתחום ומוגדרים כמוקדי ידע, דמויות בכירות בעולם הביטחון הלאומי העוסקות בנושא מלחמת הסייבר.

**מבנה הפרויקט/ראשי פרקים**

1. מבוא
2. הגדרות ומושגים – פרק המתאר את תהליך התפתחות ממד הסייבר בדגש על סייבר ההתקפי, המושגים הרלוונטיים לנושא, באמצעות תאוריות.
3. ניתוח המצב הקיים – פרק המתאר את אבחון מצב הסייבר (בדגש ההתקפי) במדינת ישראל בהקשרי אסטרטגיה ומדיניות, תהליכי בניין כח והפעלת הכח מתוך כוונה להניח מצע לניתוח הפוטנציאלים הקיימים.
4. ניתוח התרומה הפוטנציאלית – פרק המתאר את הפוטנציאל הקיים לקטלניות ולהרתעה במב"מ ובמלחמה.
5. דיון, מסקנות, המלצות וסיכום.

**גבולות הפרויקט/במה לא יעסוק**

ממד הסייבר הינו תחום רחב בעל תתי נושאים רבים. העבודה לא תעסוק בשני תחומים מרכזיים הנוגעים באופן ישיר והם: סייבר לטובת מידע והגנה בסייבר.

העבודה תתאר ותנתח את הפוטנציאל שבשימוש נכון במימד הסייבר ההתקפי, כמימד הפועל כחלק ממענה התקפי שלם ותחת מדיניות סדורה ויכול **להביא לתגבור היכולת ההתקפית וההרתעה** של מדינת ישראל. זאת, ללא התייחסות ליכולות פרטניות או לחולשות שונות, מפאת רגישות הנושא.

אין המטרה להסביר על המבנה הארגוני הנדרש אלא לבאר ולהבהיר את ההשתנות שחלה בעולם והשפעתו על השגרה וכמובן על המלחמה.

**המשגה – רקע תיאורטי ומושגים מרכזיים**

1. **לוחמה קיברנטית** / **לוחמת סייבר-לוחמת מידע** של מדינות / ארגונים / פרטים מדינות/ארגונים/פרטים אחרים, המבוצעת מעל גבי תשתיות תקשוב, תוך מטרה לרגל ו/או לחבל בתשתיות אלו.
2. **מהפכת המידע** – תקופה בה המידע הופך לכוח המניע של הכלכלה, התרבות והפעילות האנושית, כולל המלחמה. טכנולוגיית המחשב היא שורש השינוי הזה. מחשבים הם מכונות ייחודיות; הם עוזרים להרחיב את כוח המוח. רובוטים ממוחשבים החליפו עובדי צווארון כחול; ייתכן שהם בקרוב יחליפו גם עובדי צווארון לבן. מחשבים היו בתחילה מכשירים העוקבים אחר סטים של הוראות הנקראות תוכנות מחשב, או תוכנה, אשר נכתבו על ידי אנשים המכונים מתכנתי מחשב, אולם כיום, עם כניסת הבינה המלאכותית (AI) הם מסוגלים לבצע גם פעולות "אינטליגנטיות. מהפכת המידע הובילה אותנו לעידן האינטרנט, שם רשתות תקשורת ממלאות תפקיד מפתח בהעברת כמויות אדירות של נתונים. האינטרנט ימשיך להתרחב עקב גידול אוכלוסיית המשתמשים וחדירת האינטרנט: אזורים גיאוגרפיים שלא היו נגישים בעבר באפריקה ובאסיה יגיעו לרשת.
3. **"עוצמה חדה"** – מתאר את היכולת של מדינה לכפות את רצונה על מדינה אחרת, וזאת באמצעות חדירה לסביבת המידע במדינה הנתקפת.
4. **"עוצמה קשה"** – מתאר את היכולת של מדינה להשיג את יעדיה באמצעות כפייה צבאית בשיטת "המקל והגזר".
5. **"עוצמה רכה"** – היכולת של מדינה לכפות את רצונה שלא באמצעות הפעלת כוח צבאי. עוצמה רכה פועלת על המוסדות הפוליטיים, תרבותיים וציבוריים – פעולה באמצעות השפעה כלכלית או "קירוב לבבות".

רשימת מקורות חלקית:

1. יצחק בן־ ישראל, ליאור טבנסקי (2011). **מבט בינתחומי על אתגרי הביטחון בעידן המידע.**
אוחזר מאתר INSS:https://www.inss.org.il/he/wp-
content/uploads/sites/2/2017/02/FILE1325967400.pdf
2. יצחק בן ישראל (2012). עידן הסייבר : **עקרונות ברמה הלאומית**. תל אביב : אוניברסיטת תל אביב - סדנת יובל נאמן למדע, טכנולוגיה וביטחון
3. גבי סיבוני וי"ר (2013). **מה עומד מאחורי לוחמת הסייבר של סין**, INSS מרחב הסייבר והביטחון הלאומי – מבחר מאמרים,39-52
4. ליאור טבנסקי (2013). **פשע קיברנטי – סכנה לביטחון הלאומי?** , INSS מרחב הסייבר והביטחון הלאומי – מבחר מאמרים, 69-88
5. אלסנדרו גוארינו ואמיליו אזיילו (2017). **אכיפת גבולות או חציית גבולות בסייבר: דילמת הריבונות**. INSS סייבר, מודיעין וביטחון. יוני 2017 כרך 2, 3-18
6. סימן טוב ד. והרשקוביץ ש (2017). **גישה "שיתופית" ביחסי מודיעין-קברניט ברמה הלאומית: האם יש לה תוחלת?** INSS סייבר, מודיעין וביטחון. יוני 2017 כרך 2, 77-93
7. שוייצר י, סיבוני ג, יוגב ע (2011) **המרחב הקיברנטי וארגוני הטרור.**
אוחזר מאתר INSS: https://www.inss.org.il/he/wp-content/uploads/sites/2/2017/02/FILE1325967384.pdf
8. **National cyber strategy of the United Utate of America September**
https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
9. דימה אדמסקי (2015), **אומנות אופרטיבית קיברנטית: מבט מזווית לימודית האסטרטגית ומפרספקטיבה השוואתית,** עשתונות גיליון 11.
10. **מערך הסייבר הלאומי, מדינת ישראל**
<https://www.gov.il/he/departments/israel_national_cyber_directorate>
11. HARVEY M. DEITEL, BARBARA DEITEL**,** [**The Information Revolution**](https://www.sciencedirect.com/science/article/pii/B9780122090059500060), in [An Introduction to Information Processing](https://www.sciencedirect.com/book/9780122090059/an-introduction-to-information-processing), 1986

<https://www.sciencedirect.com/topics/engineering/information-revolution>

1. רועי גולדשמידט ( 2013) **המרחב הקיברנטי וההגנה על תשתיות חיוניות**, מרכז המחקר והמידע של הכנסת. <http://www.knesset.gov.il/committees/heb/material/data/mada2013-05-13.doc>
2. עיונים בביטחון לאומי: לוחמת המידע – יצירת השפעה והתפתחות התאוריה הרוסית. נובמבר 2020, גליון 25, 9-24
3. Giovanna Borradori (2003) , **Philosophy in time of terror** with Jurgen Habermas and Jacques Derrida, University of Chicago

The conversation – **if two countries waged cyber war**
 https://theconversation.com/if-two-countries-waged-cyber-war-on-each-another-heres-what-to-expect-63544