



תא"ל אורי אורון < ראש להק מודיעין בחיל האוויר. בוגר מב"ל

# השפעת המרחב הקייברנטי על עיצוב של מערכות

השפעתו האפשרית של המרחב הקייברנטי על עיצוב וניהול מערכות היא רבה ומגוונת. לאור קצב השינויים הגדול סביבנו, הכרחי לקיים תהליך חשיבה ופיתוח ידע מתמיד על מנת לעצב, לבנות ולהשתמש במרחב זה בצורה המיטבית לצרכיה האסטרטגיים של מדינת ישראל



## מבוא

ההבנה כי למרחבים הקלסיים – יבשה, ים אוויר וחלל הצטרף מרחב לחימה חדש, המרחב הקיברנטי, היא היום נחלתם של רבים. לעומת זאת, לשאלה כיצד משפיע המרחב החדש הזה על עיצובה של מערכה יש תשובות מעטות ולא מעט מבוכה.

מרחב הסייבר, המתעצב לנגד עינינו, מאפשר פתיחה של מרחבי פעולה שלא היו קיימים בעבר, וזאת לאור אופיו השונה ממרחבי פעולה צבאיים קלסיים כמו ים, יבשה ואוויר. פעולה בו יכולה להשפיע על המערכה כולה ובוודאי על הממשקים בין המרחבים השונים. פעולות כאלו אף נעשו בעבר על ידי מדינות בכמה אירועים, לעתים כתמיכה במהלך צבאי, ולעיתים כמרכז הרעיון המערכתי לפתרון סוגיה אסטרטגית. מאמר זה מבקש לספק מתודולוגיה לשרטוט הממשקים האפשריים שבין סביבת הלחימה הקיברנטית לאתגרי השעה הביטחוניים, העומדים בפני מדינת ישראל. לצורך כך המאמר מנתח את מאפייניו של הסייבר כמרחב לחימה ומשווה אותו למרחבים הקיימים. תהליך בירור זה יאפשר לעצב עקרונות לדיון וללמידה, ומתוך כך להצביע על משמעותו של מרחב זה לעוצמתה הלאומית של ישראל. פיתוח שיח כזה חיוני לשיפור הבנתנו את המרחב הקיברנטי ואת היכולות והמשמעויות של פעולה בו. המאמר מבקש לתרום לשיח המקצועי באמצעות הצגת כלי המאפשר התבוננות על קשרים וממשקים בין עולם תוכן זה לבין ניהול מערכה ספציפית. כלי כזה יכול למשטר דיון ותהליך של עיצוב מערכה, שפעמים רבות אינו מוסדר, בוודאי בכל הקשור להשפעתו האפשרית של המרחב הצעיר והמתפתח הזה.



העובדה כי מרבית המחשבים והמערכות מבוססות המחשב פועלים על סמך פרוטוקולים זמינים וגלובליים הופכת את המרחב הקיברנטי למרחב אחד



האדם. על המרכיב הלוגי יופעלו כלי סייבר המשפיעים על הנתונים האגורים במערכות המחשב ועל האופן שבו מערכות ההפעלה מבצעות את חישוביהן.

מאפיין נוסף של המרחב הקיברנטי הוא העובדה כי זהו מרחב גלובלי, בו לגבולות הגיאוגרפיים יש משמעות

קטנה מאוד. יתר על כן, העובדה כי מרבית המחשבים והמערכות מבוססות המחשב פועלים על סמך פרוטוקולים זמינים וגלובליים הופכת את המרחב הזה למרחב אחוד.

המרחב הקיברנטי הוא מרחב דינמי הממשיך להתפתח באופן מהיר מאוד. ניתן לראות זאת גם במרכיביו הפיזיים, עם הגידול בכמות המערכות שבהן משובץ מחשב ובגיוון יישומיהן. גרף 1 מתאר ניתוח שעשתה חברת CISCO באפריל 2011, שבחן בין היתר את התפתחות המערכות המחוברות לאינטרנט ביחס לכמות האנשים בעולם. על פי ניתוח זה, בשנת 2020 יהיו לכל אדם על פני הגלובוס בממוצע 6.5 מכשירים המחוברים לאינטרנט - פי 3.5 ממספרם בתחילת העשור.

המרחב הקיברנטי מורכב, בין שאר מאפייניו, משחקנים רבים ומגוונים: ממדינות דרך ארגונים וקבוצות ועד לבודדים הפועלים ומשפיעים עליו. לפיכך, כאשר

ניגשים להתבונן על מרחב קיברנטי יש לבחון מיהם השחקנים, מה גודלם הקיברנטי מהי השפעתם במרחב ומהו טיב הממשקים בינם לבין שחקנים אחרים.

המרחב הקיברנטי הוא אם כן מרחב נוסף בעל מאפיינים משלו. טבלה 2 משווה את המרחב הזה למרחבי הלחימה הקלסיים במספר פרמטרים שלהם יש השלכות על הבנת השפעתו האפשרית על שדה הקרב.

### מאפייני סביבת הלחימה הקיברנטית

מאפייני סביבת הלחימה במרחב הקיברנטי נגזרים מאופיו של המרחב. כאן הם מנותחים בראייה מבצעית בדגש על היחס שבין מרחב זה לעולמות תוכן אחרים.

מרחב חשאי באופיו שבו ההסוואה וההסתרות קלות לביצוע ומרחב ההכחה נרחב. העמימות נשמרת בו בצורה טובה, ולרוב זהות התוקף אינה ברורה. בשנים האחרונות בוצעו במרחב הקיברנטי פעולות רבות, ועל אף אחת מהן לא נלקחה אחריות של מדינה או גוף רשמי כלשהו. כך היה בפעולות המיוחסות לרוסיה באסטוניה ובגיאורגיה, כך היה באירוע תולעת המחשב (סטוקסנט) באיראן, וכך גם בפעולות המיוחסות לארצות הברית מול צפון קוריאה.

מרכיב הזמן כפרמטר מבצעי הוא ייחודי בהשוואה לכל מרחב אחר. זמן המעבר במרחב הוא קרוב למהירות האור, והמשמעות המבצעית היא שפקודה יכולה להפוך לאפקט באופן מידי. אפילו בהשוואה למרחב האווירי, שבו נעשים הדברים במהירות



תרשים 1 - הסייבר כמרחב חמישי

### קווים לדמותו של המרחב הקיברנטי

המרחב הקיברנטי נוצר על ידי האדם, בסוף שנות ה-40 של המאה ה-20, כאשר החלו להיבנות מכונות המסוגלות לבצע פעולות חישוב, ומאז התפתח בצורה דרמטית. כיום זהו מרחב שלם, גדול ומתפתח המשפיע על כל אורחות חיינו, ובתוך כך על נושאי הביטחון הלאומי.

ברם, בניגוד למרחבים פיזיים ברורים, ההבנה כי אכן מדובר במרחב חדש אינה מובנת מאליה. דיונים רבים נסבו על הסוגיה אם אכן מדובר במרחב לחימה חמישי אם לאו. אולם, נראה כי המציאות וההתפתחות שחוה העולם בשנים האחרונות מותירות רבות מגדירה אותו כמרחב פעולה חמישי, השולטת במדינות רבות מאד ספק לגבי שאלה זו. התפיסה כזה המקיף באופן וירטואלי את שאר המרחבים<sup>1</sup>.

את היחס שבין המרחב הקיברנטי ליתר המרחבים הקלסיים ניתן לתאר בצורה גרפית כמרחב שיש לו ממשקים עם כל יתר המרחבים, אך אינו מקביל להם (תרשים 1). בדומה למרחב האווירי, המתקיים מעל המרחב היבשתי או הימי, גם הסייבר מתממשק ומתקיים בסביבתם, אך יש לו גם מרחב משלו, בו מתקיימות אינטראקציות וממשקים פנימיים.

למרחב הקיברנטי יש כמה מאפיינים המזהים אותו באופן ייחודי מיתר המרחבים הקלסיים. עמידה על מאפיינים אלו חיונית להבנת המרחב בכלל ולהבנתו כמרחב פעולה ולחימה בפרט.

המרחב הקיברנטי הוא יציר ידי האדם, וזאת בניגוד למרחבים הפיזיים הקיימים מאז ומעולם. יכולת הפעולה במרחבי הלחימה הקלסיים נגזרת משילוב בין הממדים הפיזיים הטבעיים בהם מראשית בריאתם בין השימושים שפיתח האדם. במרחב הקיברנטי נעדר כמעט הממד הפיזי ויכולות השימוש נגזרות בעיקר מהתפתחות הטכנולוגיה ודרכי השימוש בה בכל מדינה או ארגון.

מאפיין נוסף של המרחב הקיברנטי נוגע לקישוריות שבין המחשבים או המערכות שבהן משובץ מחשב. ניתן בהקשר זה לחלק את המערכות לשתי קבוצות, אלו הקשורות ברשת כלשהי ואלו המבודלות. מערכות מקושרות נמצאות בזמינות קבועה לעולם החיצון, באמצעות הרשתות, לעומת מערכות מבודלות, שבהן נדרשת פעולה חיצונית על מנת לחברן לעולם שסביבן.

המרחב הקיברנטי מורכב משלוש סביבות: הסביבה הפיזית שבה ימצאו מערכות, שרתים, חוטים וכבלים, היינו, כל דבר מוחשי; הסביבה האנושית - הקובעת את הדרישות לביצוע פעולות החישוב הללו, ואשר משתמשת בתוצרי הפעולות הללו לצרכיה השונים; והסביבה הלוגית - בה מתחברים ביטים לביטים ופעולות החישוב מתבצעות הלכה למעשה. מנקודת המבט של מרחבי פעולה צבאיים ניתן לתאר את ההבדל בין הסביבות האלו גם באמצעות הכלים שיכולים להשפיע על כל אחת מהן. על הרובד הפיזי יופעלו כלים קניטיים שונים - ממברג ופטיש ועד לחומר נפץ. על המרכיב האנושי יופעלו כלים מעולם הפסיכולוגיה, אשר שפיעו על התודעה ועל תהליכי הניתוח השונים שאותם מבצע

או מפעילים אותן. קיימות דוגמאות רבות בעולם הביטחוני והמסחרי לניצול החולשות של הטבע האנושי על מנת לעקוף הגנות היקפיות פיזיות ולוגיות הנראות לכאורה בלתי חדירות. אחת הדוגמאות המפורסמות לכך הוא סיפורו של אדוארד סנודן שגרם להיחשפותם של סודות רבים כתוצאה מנגישותו למידע מסווג רב ערך, ללא בקרה מספקת.<sup>2</sup>

קיים מגוון כלים שבאמצעותם ניתן לבצע פעולה במרחב הקיברנטי. העיקרון המוביל הוא שניתן לבצע פעולה על כל מערכת מבוססת מחשב באמצעות שימוש באחד או יותר מנתיבי החדירה הבאים: נגישות פיזית למערכת, התערבות ברשת, טיפול ברכיבים עצמם, או טיפול בשרשרת ההספקה אל המערכת. אולם, יש קושי רב בתחזוקת כלי תקיפה. לנוכח ההשתנות המהירה של המערכות והמורכבות הרבה שלהן, נדרשת השקעה רבה בתחזוקת הכלים. לדוגמה, שינוי גרסה מקרי או מתוכנן במערכת הפעלה הנעשה לעתים תכופות, או החלפה של אחד מהמרכיבים במערכת היעד, עשויים לחייב עדכון משמעותי בכלי התקיפה. מאפיין זה מקשה על התוקף, והנו כלי אפשרי בידיו של המגן.

הפגיעה יכולה להיות בצורות רבות ובמידת תחום גבוהה מאוד. ככל שמדובר במערכת יעד מתוחכמת יותר נדרש מודיעין מוגדר ומדויק והכרה טובה מאוד של המערכת המותקפת. בנוסף, מידת הנזק שיכולה להיגרם למערכת משתנות בהתאם לזמן שהיית הכלי במטרה, לרמת המודיעין עליה וליכולת לתחזק מתקפה כזו באופן שלא יאפשר את גילוייה. ככל שזמן השהייה בתוך המערכת הנפגעת יהיה ארוך יותר, כך ניתן יהיה להגדיל את מרחב הפגיעה האפשרי. בהשוואה לעולם קינטי, אפשר להציג אפשרות כזו כמטוס הנמצא מעל המטרה וחמוש במגוון כלים – ממקלע ועד

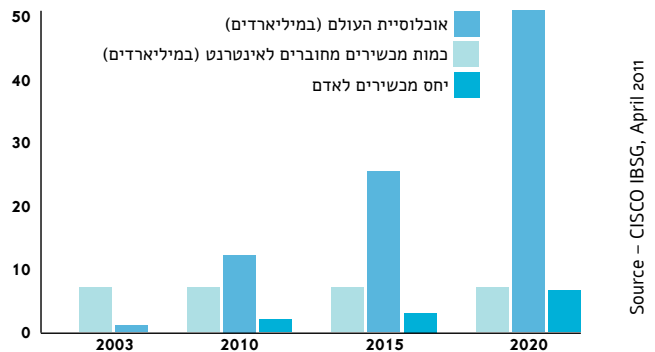
## במרחב הקיברנטי נערך כמעט המימד הפיזי ויכולות השימוש נגזרות בעיקר מהתפתחות הטכנולוגיה ודרכי השימוש בה בכל מדינה או ארגון

לפצצה רבת עוצמה.

הפעולה המבצעית במרחב הקיברנטי יכולה להיות בעלת יעוד הגנתי או התקפי כאחד, ובדומה למרחבים אחרים, היא יכולה להתבצע גם בשילוב פעילות מסייעת ממרחבים אחרים.<sup>3</sup> טבלה 3 מסכמת את אופני הפעולה השונים, בהקשר ליעוד ההשפעה ולמידת הנזק.

הקושי לחזות בצורה מדויקת את האפקט של פעולה במרחב, נגדנו או נגד יריב. קושי זה נובע מהקישוריות הרבה של מרבית המערכות, בינן לבין עצמן, וכן מההשפעה בתוך המערכת של מרכיב שפעילותו משתבשת. פעולה התקפית לא מבוקרת ולא מדודה עלולה להביא להסלמה בלתי נשלטת ובלתי רצויה, לאובדן יכולות ולפגיעה בפעילות האיסוף ואף לפגיעה במגננה. משמעות נוספת הקשורה לאפקט ולנזק הנגרמים כתוצאה מפעולה במרחב הקיברנטי היא מידת ההפיכות של הנזק. בעוד בעולם הקינטי, פגיעה במערכת משמעותה השבתה, בעולם הקיברנטי ניתן לעתים להחזיר את המערכת לפעולה תוך זמן קצר, כאשר הפוגען הוסר. מאפיין זה מאפשר גמישות מבצעית שאינה קיימת בכלים קינטיים.

הזמינות הגבוהה יחסית למרחב הלחימה היא מאפיין נוסף. על מנת לבצע פעולה התקפית ראשונית נדרשים אמצעים פשוטים



גורף 1 - התפתחות במספר המערכות המחוברות לאינטרנט ביחס לאוכלוסיית העולם

גבוהה, מדובר על סדרי גודל אחרים לחלוטין. משמעות נוספת לכך היא קצב השינוי בתמונת המצב שהוא גבוה מאוד. במידה רבה ניתן להתייחס אל תמונת המצב הקיברנטית כאל תמונה המשתנית באופן תמידי. עובדה זו מחייבת כלים ותהליכים משוכללים כדי לתמוך בביצוע הערכת מצב לשם פעולות בהגנה ובהתקפה. בנוסף, בשל המהירות הגבוהה בה יכולים דברים להשתנות, המעבר בין שגרה לחירום יכול להיות מהיר גם הוא, ומכאן מתחייבת יכולת תגובה מיידית, בדומה למרחב האווירי.

התייחס הגיאוגרפי של המרחב מטושטש מאוד, וניתן במידה רבה להתייחס אליו כאל מרחב נטול גבולות פיזיים. התופעה הזו מובהקת בעיקר בנוגע למחשבים ולמערכות המחוברים באופן קבוע לרשת כלשהי בדגש על האינטרנט, או אז ניתן להגיע מהם או אליהם מכל מקום. הדבר פחות מובהק

במערכות מבודדות וכאלו שאינן מחוברות לרשת. למערכות כאלו נדרשת גישה הקשורה למרחב הפיזי שלהן, בין אם על ידי הגעה פיזית אל המערכת, ובין אם בהתקרבות משמעותית אליה.

הגורם האנושי הוא במקרים רבים החוליה החלשה במערכות קיברנטיות - זו המאפשרת לא פעם את נתיבי החדירה אל מערכות מבוססות מחשב. הסיבות המרכזיות לחולשת הגורם האנושי הן חוסר מודעות, חוסר משמעת וחוסר מקצועיות של בני אדם הנמצאים בסמוך למערכות שהוגדרו כיעדים

מאפיין פיזי	יבשה	ים	אוויר	חלל	סייבר
מוצק	נוזל	גז	ריק	ללא	ללא
רגל/רכב	ספינה	מטוס	חללית	תוכנה	תוכנה
עשרות אלפי שנים	אלפי שנים	מאה שנים	עשרות שנים	שנים בודדות	שנים בודדות
כ-100 קמ"ש	כ-50 קמ"ש	עד 2,000 קמ"ש	עשרות אלפי קמ"ש	אלפי קמ"ש	מאות אלפי קמ"ש

טבלה 2 - השוואה בין מרחבים

תכלית	יעד להשפעה	מידת הנזק	הערות
ריגול	ללא שינוי	משתנה בהתאם לסוג המידע הנאסף	
לוחמת מידע	הרובד האנושי	משתנה. מנזק קצר ועד הונאה אסטרטגית	פעילות אפקטיבית לאור משקלן הגדול של מערכות מידע והשפעתן על התודעה
תקיפה קיברנטית - לוגית	הרובד הלוגי	משתנה. מנזק מוגבל ועד לפגיעה מהותית וקשה	למשל, פגיעה באמון הרשת יכולה להיות ארוכת טווח.
תקיפה קיברנטית - פיזית	הרובד הפיזי	משתנה. ממוגבל ועד לפגיעה קשה ביכולות, בתשתית וברכוש.	

**טבלה 3 - אופני הפעולה המבצעיים במרחב הקיברנטי**

העקרונות להתמודדות עם מרכיבי המערכת או קשרים אלו על מנת להשיג יעד חיוני, ותוכנית הביצוע מוציאה את הרעיון המסדר אל הפועל. במודל שיוצג להלן ייעשה שימוש במושגים "מענה מערכתי", ו"חשיבה מערכתית", הלקוחים מגישה רעיונית זו.

**המודל ודוגמאות ליישומו**

בניתוח הממשקים האפשריים בין המרחב הקיברנטי לאתגרים

הביטחוניים המרכזיים של ישראל ייעשה שימוש במודל המשלב בין ניתוח מערכתי של בעיה אסטרטגית לבין מאפייני מרחב הלחימה הקיברנטי שפורטו לעיל. המודל (טבלה 4) מפרק את המערכת למרכיביה המרכזיים ומולם מוצגים מאפייני סביבת הלחימה הקיברנטית שהוצגו לעיל. כל מרכיב במערכת נבחן מול כל מאפיין של סביבת הלחימה וניתן ציון לעוצמת הממשק ביניהם, המתוארת בצבעים כדלקמן:

- **ירוק - ממשק חזק** בו יש יתרון לסייבר על פני מרחבים אחרים;
- **צהוב - מתקיים ממשק**, אך ללא יתרון למרחב הקיברנטי;
- **ריק - אין ממשק** בין מרכיב במערכת למאפיין בסביבת הלחימה;
- **אדום - ממשק** שבו יש **חיסרון למרחב הקיברנטי** ביחס למרחבים אחרים.

עוצמת הממשק המוצגת נקבעה מעמדה סובייקטיבית, הנובעת הן מרמת הכרת המערכת הנבחנת, והן מהאופן שבו נתפס המרחב הקיברנטי על מאפייניו. ייתכן מאוד

כי אנשים שונים יציגו עמדות שונות בנוגע לעוצמת הממשק או למידת יתרונן של הסייבר על מרחב אחר. זו אינה מגבלה אלא יתרון - זהו לבו של תהליך הלמידה. המפה המתקבלת מאפשרת מחד גיסא הסתכלות על המערכת בכללותה ומאידך גיסא יכולת העמקה בפרטיה. תהליך בניית המפה והדיון הנוגע לעוצמת הממשקים מאפשרים למשטר את הדיון ואת פיתוח הידע.

את השימוש במודל אדגים על שני אתגרים אפשריים בהווה הביטחוני של מדינת ישראל. אתגרים אלו, גם אם הם שונים מהותית באופיים זה מזה, מחייבים התייחסות מערכתית כוללת

למדי, בוודאי בהשוואה לפעילות התקפית במרחב האווירי. אמצעים אלו לא יהיו מספיקים בידי תוקף פוטנציאלי לבצע פעולה משמעותית או מתוחכמת. שם תידרש השקעה במודיעין, בפיתוח ובאמצעים מבצעיים, השקעה שתעלה ככל שמדובר ביעד מוגן יותר. זמינות זו קורצת לשחקנים רבים, החל ממדינות, עבור ארגונים וכלה בבודדים שמאתגרים את מערכות ההגנה היקרות ממילא.

במרחב הקיברנטי יש יתרון לתוקף היוזם, המחפש והמזהה פרצה צרה שדרכה יוכל לחדור למערכת, על פני המגן המתקשה לסגור כל פרצה בקו ההגנה שלו. זאת בדומה אגב, למרחבים פיזיים. לתוקף יש יכולת לגרום לנזק משמעותי מאוד בעלות נמוכה יחסית להשקעת משאבים גדולה מאוד הנדרשת מהצד המגן. בנוסף, מגוון השחקנים הרב, והדינמיות הרבה של המרחב, מאפשרים לתוקף מגוון ערוצי חדירה. אולם, ישנם גם כמה יתרונות לצד המגן. קשה להבטיח את רציפות הפעולה ההתקפית בצורה מלאה, מאחר ששינוי במרכיב פיזי או לוגי, גם אם הוא מקרי, יכול למנוע את ההתקפה. המגן יכול גם לסגור את הפרצה, אך בניגוד למרחבים פיזיים, במרחב הקיברנטי סגירתה אינה כה גלויה לצד התוקף. דילמה נוספת, העומדת מול התוקף, היא שההתקפה שלו עשויה לחזק את הגנת היריב ולמנוע תקיפות נוספות בעתיד.

ניתן, אם כן, לומר כי בעולם הקיברנטי, בדומה למרחבי פעולה אחרים, יש יתרון לתוקף על פני המגן, אך זהו אינו יתרון מוחלט, וגם כאן הוא תלוי יריב, מודיעין והקשר.

**הגישה המערכתית לאתגר אסטרטגי**

תורת המערכות היא גישה מסדרת להתמודדות עם סביבות מורכבות מאוד, כגון ניהול מלחמות או אתגרים אסטרטגיים אחרים, שבבסיסה הרעיון של התבוננות על מערכת כעל שלם המורכב גם מסך חלקיו וגם מהיחסים והקשרים בין החלקים הללו.<sup>4</sup> על פי גישה זו, ניתן משקל גדול לשרטוט סביבה רעיונית בה מוצגים מרכיבי מערכת והקשרים ביניהם. הרעיון המסדר (אסטרטגיה) מציע את

**תורת המערכות היא גישה מסדרת להתמודדות עם סביבות מורכבות מאוד, כגון ניהול מלחמות או אתגרים אסטרטגיים אחרים, שבבסיסה הרעיון של התבוננות על מערכת כעל שלם המורכב גם מסך חלקיו וגם מהיחסים ומהקשרים בין החלקים הללו**



**תרשים 2 – מרכיבי מערכת בפרויקט פיתוח טכנולוגי מתקדם במעגל שלישי**

מהתשתיות, מהפיתוח ומהייצור עשוי להגיע מתוך יכולות פנימיות. הדבר מצמצם מצד אחד את החשיפה לגורמי חוץ, אך מצד אחר ממקד את הקשר עם העולם החיצון למספר מוגבל של מקומות ואנשי מפתח. מרכיב משמעותי מאוד בפרויקט הוא המידור הקפדני בכל הנוגע לעיסוק בו, המצמצם ומקשה מאוד על הגישה למרכיבי השונים, הנתונים תחת מעטפת הגנה ייחודית.

מרכיב נוסף הנו הריחוק הגיאוגרפי מתוקף העובדה כי הפרויקט מתקיים במדינה שלה אין גבול משותף עם ישראל. למרכיב זה משמעות בכל הקשור לגישה אל ועל מרכיביו השונים, והוא מגביל את מרחב האפשרויות והכלים בהם יכולה ישראל להשתמש. ניתוח הממשקים האפשריים של המערכת עם המרחב מוצג בטבלה 5.

על פי המודל, ניתן לראות כי למרחב הקיברנטי יש אפשרות רבה להשפיע בעת עיצוב וניהול מערכה נגד פרויקט כזה. המרכיבים במערכת, בהם יש לסייבר יתרון על פני מרחבים אחרים הם בראש ובראשונה היכולת הפוטנציאלית לתת מענה למרכיב הפיתוח של הטכנולוגיות המתקדמות בפרויקט. יתרון זה בא לידי ביטוי במאפייני סביבת לחימה הייחודיים של הסייבר, הרלוונטיים למרכיב זה ובראשם העובדה כי הוא נטול גבולות ואינו דורש הגעה פיזית מורכבת אל אזורי היעד. בנוסף, הגורם האנושי בתהליכי הפיתוח, שמאופיין בנקודת חולשה מאפשר חדירה פוטנציאלית, בנוסף למגוון אופני הפעולה והכלים המבצעיים. רמת התחכום של התקיפה, התלויה במודיעין, יכולה לאפשר פעולה שהנזק שלה יהיה <

ובהתמודדות עמם למרחב הקיברנטי יכול להיות תפקיד. האתגר הראשון הוא פיתוח מערכת נשק חדישה במדינה מרוחקת, מערכת נשק העלולה לאתגר את יכולותיה של ישראל. האתגר השני שאותו אבחן הנו איום הדה-לגיטימציה העומד בפני המדינה. אם בראשון ניתן להצביע בצורה טבעית על חשיבותו של המרחב הקיברנטי, הרי שמקומו של מרחב זה במענה המערכתי לאתגר השני אינו מובן מאליו. הניתוח המערכתי לכל אתגר מוצג ברמה כוללת וללא פירוט, אך בדרך המאפשרת את בחינת המרכיבים המרכזיים שבו.

מאפיין 4 של סביבת הלחימה הקיברנטית	מאפיין 3 של סביבת הלחימה הקיברנטית	מאפיין 2 של סביבת הלחימה הקיברנטית	מאפיין 1 של סביבת הלחימה הקיברנטית	
ממשק חזק. יתרון למרחב הדיגיטלי	ללא ממשק	קיים ממשק. ללא יתרון למרחב הדיגיטלי	ממשק חזק. יתרון למרחב הדיגיטלי	מרכיב א' במערכת X
ממשק חזק. יתרון למרחב הדיגיטלי	ללא ממשק	ממשק חזק. יתרון למרחב הדיגיטלי	קיים ממשק. ללא יתרון למרחב הדיגיטלי	מרכיב ב' במערכת X

**טבלה 4 – מודל למיפוי ממשקים בין המרחב הקיברנטי לאתגר האסטרטגי**

**פיתוח טכנולוגי מתקדם במדינה מרוחקת**

בחינה מערכתית של האתגר האסטרטגי של פיתוח מתקדם במדינה מרוחקת מציבה כמה מרכיבים שעמם נדרשת ישראל להתמודד (תרשים 2). בפרויקט כזה יש תפקיד מרכזי ומיוחד להכוונה ממוקדת של ההנהגה - החל מהגדרת היעד הנדרש, עבור דרך הקצאת המשאבים וכלה בהכוונת קצב הפיתוח. מרכיב זה במערכת מאופיין בקבוצת אנשים מצומצמת ובכירה המשקיעה מאמץ להגן על החלטותיה.

במהותו פרויקט כזה עוסק בטכנולוגיות מתקדמות, שהידע עליהן אינו נחלת הכלל. תפקידו המרכזי של המחקר והפיתוח בפרויקט מחייב גישה קבועה לידע ודורש עדכון לצורך התקדמות בפרויקט ופתרון בעיות תוך כדי מימושו. למרכיב זה מתחבר מרכיב נוסף והוא הסיוע החיצוני המוגבל לפרויקט. חלק ניכר מהידע,

קושי בהערכת האפקט	מודי פעולה מגוונים	זמינות מבצעית	הזמן המרכיב	יכולת פגיעה לוגית	א-סימטריה בין תוקף למגן	רמת תחכום גבוהה	נטול גבולות	הגורם האנושי	חשאיות	
-	+			+	+		++	+	+	מיקוד והכוונת הנהגה
-	++	+	+	++	++	++	++	++	+	טכנולוגיות מתקדמות
	+			+	++	++	+	+	++	מידור
-	+		++	++	+		++	+		ריחוק גיאוגרפי
				+	+	+	+	+	-	מאמץ פיתוח פנימי
	+		+	+	++		+	++	+	הגנה

מקרא:  
 ++ ממשק חזק. סייבר בעדיפות  
 + קיים ממשק. סייבר לא בעדיפות  
 - ללא ממשק  
 - חיסרון לסייבר

**טבלה 5 – מיפוי ממשקים אפשריים של המרחב הקיברנטי עם פרויקט פיתוח מתקדם**

▶ רב וממוקד מצד אחד, אך לא נרחב מדי, כמו בתקיפה קיבנית, שעשוי לגרום תגובת נגד משמעותית מצד היריב. במרכיבים אחרים במערכת יש לסייבר יכולת והוא יכול להיות חלק מהמענה, אך הוא איננו בהכרח עדיף על פני מענה ממרחבים אחרים. מתוך המודל בולט לעין תחום בו לסייבר יש חסרון מול מרחבים אחרים, הנובע מהקושי לחזות בצורה מדויקת יחסית את האפקט של שימוש בו כנגד מרכיבים במערכת. כלומר, פעולה קיברנטית, שמשמעותה המיידית אינה ברורה כמו פעולה קיבנית, יכולה במקרה כזה לגרום להסלמה, או לתגובת נגד לא צפויה.

### איום הדה-לגיטימציה



### תרשים 3 – מרכיבי מערכת הדה-לגיטימציה

מסע הדה-לגיטימציה המתנהל כנגד ישראל הוא איום מסוג אחר לחלוטין. הרעיון המוביל שולל את קיומה של ישראל כמדינה, ומגדיר את תכליתו בהוצאת הגופים הישראליים מחוץ למסגרות הפעולה הבינ-לאומיות. המערכה מנוהלת באמצעות איסוף מידע על פעולות ישראל והפצתו על מנת ליזום ולעודד פעולות נגד גופים ישראליים כגון מוסדות אקדמיים, גופי תרבות, חברות מסחריות, וגופים ממשלתיים. מדובר אם כן באתגר שבו המרכיב החשוב ביותר הוא מרכיב רך של תודעה, מידע ודעת קהל.

הצגת מרכיבי המערכת הזו נעשית באמצעות ההקשר הפונקציונלי של המרכיבים השונים ולא דרך שיוכם הארגוני או הגיאוגרפי (תרשים 3). כלי מרכזי במאמץ הוא חרם על גופים ישראליים שונים, או כזה המוטל על גופים המנהלים קשרים עם ישראל, כגון גופים מסחריים ותרבותיים. הקריאה לחרם מקודמת בין היתר באמצעות פרסום עובדת הקשר עם ישראל ויצירת דעת קהל נגד הגופים הקשורים עמה.

לוחמת המשפט היא מרכיב משמעותי מאוד במערכה נגד הלגיטימיות הישראלית. מרכיב נוסף הוא מאמץ למשיבת השקעות גופים כלכליים ויזמים מישראל. עיקר המאמץ של מובילי המאבק, הוא בזיהוי הגופים הללו והשחרת פניהם במדינות בהן הם פועלים. מאמץ נוסף מושקע ביצירת מיתוג שלילי לישראל כמדינה אלימה, המזלזלת בחיי אדם ובחוק הבינ-לאומי. לא פעם המיתוג נעשה באמצעי התקשורת השונים תוך פרסום מידע חלקי או שקרי. התקשורת הבינ-לאומית היא גורם מרכזי בגיבוש השקפת

העולם והתודעה של פרטים וארגונים ברחבי העולם. לפיכך משקיעים מארגני המאבק בלגיטימיות של ישראל מאמץ מיוחד בפרסום ובהפצת מידע רב על פעולותיה השונות.

המרכיב האחרון הנו קבוצה של גופים לא מדינתיים, אשר פועלים כל אחד ממניע משלו, אך גם בקשר מסוים ביניהם. גופים אלו אחראים לא פעם על איסוף ופרסום המידע לגופים המזכירים לעיל, ולכן מהווים מרכיב משמעותי במערכה.

המאמץ המופעל על מנת לייצר חרם וסנקציות על גופים ישראליים או כאלו שפועלים עם ישראל מציב בראש מעיניו את התודעה, והמידע כבסיס לפעולתו. עיקר המענה לאתגר נמצא אם כן במאבק נגדי אותו צריכה לנהל ישראל במישור הדיפלומטי וההסברתי, ולשם כך יכול הסייבר להוות מרכיב משמעותי מאוד באיסוף מידע מקדים שסייע למאמץ זה. מיפוי הממשקים בין המרחב הקיברנטי למרכיבי המערכת הפועלת לדה-לגיטימציה של ישראל בעולם מצביע על מספר מקומות בהם פעילות קיברנטית היא חלופה אפשרית (ראו טבלה 6 בעמוד הבא).

על פי המודל, יתרונו הגדול של המרחב הקיברנטי טמון בעובדה כי הוא נטול גבולות, ובעל גישה מיידית למוקדי המידע והנתונים שעליהם מבססים הגופים המובילים את מסע הדה-לגיטימציה. גם רמת התחכום הגבוהה של פעולה במרחב ומרכיב החשאיות מאפשרים לסייבר להיות מרכיב חשוב כגורם מסייע במענה. במרבית המקומות האחרים קיים ממשק בין המרחב הקיברנטי למרכיבי המערכת, אך יתרונו של הסייבר אינו מובהק.

ניתן לראות כי המרכיבים המרכזיים מולם יכול הסייבר לפעול הם הגופים העוסקים במיתוג, בתודעה, במידע ובלוחמת המשפט. אופני הפעולה על המידע יכולים להתמקד באיסוף מידע עבור הגופים המדיניים, מערכות ההסברה והגופים המשפטיים, כמו גם חשיפת מידע שיקרי באתרים וגופים הפועלים נגד ישראל. במאבקים רבים, חשיפת המידע של אתרים וגופים עשויה להשפיע רבות על הצלחת המאבק.

בהתמודדות מול אתגר הדה-לגיטימציה בולט נושא הדין הבינ-לאומי בנוגע לפעולה במרחב. מרבית הגופים והפעולות במסגרת מסע הדה-לגיטימציה נעשים במסגרות מערביות ובמדינות ידידותיות לישראל. יש להניח כי מדינת ישראל תפעל במקומות אלו על פי המקובל, גם ללא דין בין-לאומי ברור ומקובל, אך עם זאת פעולות איסוף מידע רבות יכולות להתבצע ולסייע רבות למאמץ העיקרי.

### תוכנות

המודל שהוצג והפעלתו על שני אתגרים אסטרטגיים למדינת ישראל מאפשרים דיון בעצם השימוש בו לפני העיסוק בתוכנות הנובעות ממנו. נקודת המפתח בשימוש במודל היא הדיון סביב עוצמת הממשק בין מרכיב במערכת למאפיין כלשהו של סביבת הלחימה הקיברנטית. זהו המקום שבו מתבצעת סינתזה בין הכרת המערכת היריבה לבין בירור היכולת הישראלית מולה. במילים אחרות, חוזקו של המודל הוא ברלוונטיות שלו לסביבה האסטרטגית הייחודית של ישראל ולעוצמתה הקיברנטית. השימוש בכלי בעל מאפיינים כמותיים, עם כל הקושי שבדבר, מאפשר לייצר תמונה נוחה של משמעות השימוש במרחב הקיברנטי אל מול מערכה נתונה.

המודל מציב קושי, בשלב הגדרת המרכיבים של מערכת מסוימת. נדרשת הכרה טובה מאוד של המערכת, הן מההיבט הטכני והן

	קושי בהערכת האפקט	מודי פעולה מגוונים	זמינות מבצעית	מרכיב הזמן	יכולת פגיעה לוגית	א-סימטריה בין תוקף למגן	רמת תחכום גבוהה	נטול גבולות	הגורם האנושי	חשאיית	
		+			+	+	++	++	+	++	חרם
	+	+			+	+	++	++	+	++	סנקציות על גופים מסחריים
	+	+			+	+	++	+	+	++	סנקציות על גופי ממשל
		+				+	++	++	+	++	משיבת השקעות מישראל
מקרא: ממשק ++	+	++			++	+	+	++	++	+	מיתוג שלילי לישראל
חזק. סייבר בעדיפות	+	++		++	++	++	++	+	++	+	תודעה בגופי תקשורת
קיים ממשק. סייבר לא בעדיפות		+			+	+	++	++	++	++	מידע בארגונים בי"ל
ללא ממשק	+	+			+	++	++	++	++	++	לוחמת משפט
חסרון לסייבר		+			+	+	+	++	+	+	גורמים לא מדינתיים

טבלה 6 – מפת ממשקים אפשרית עם אתגר הדה-לגיטימציה

הביטחוניים, העומדים בפני מדינת ישראל. תהליך הבירור מאפשר לעצב עקרונות לדיון וללמידה, ומתוך כך להצביע על משמעותו של מרחב זה לעוצמתה הלאומית של ישראל. פיתוח שיח כזה הכרחי לשיפור הבנתנו את המרחב הקיברנטי, את היכולות והמשמעותיות של פעולה בו.

המודל המוצג הינו כלי המאפשר דיון בין מומחים מסביבות שונות ומקבלי החלטות בכך תרומתו לשיח. המודל מתייחס לא רק לשני עולמות תוכן אלו, אלא מציג, בצורה גרפית, גם את היחס בין המרחב הקיברנטי למרחבי פעולה אחרים. ככל שהדבר פשטני, נותנת הצגה כזו תמונה בהירה יחסית על תפקידו האפשרי של הסייבר במענה לאתגרים ביטחוניים.

כמו מודלים רבים, גם לכלי זה חסרונות הנוגעים לאופן ההצגה, מוגבלות הניתוח והראייה הסובייקטיבית של מי שקובע בסופו של דבר את הנתונים המוצגים בו. שימוש נכון במודל, יכול להתקיים רק אם ישמש כבסיס לשיח בין הגורמים השונים, המגיעים מהקהילה הקיברנטית ומהקהילה האסטרטגית של מדינת ישראל.

מניתוח תוצאות הפעלת המודל על שני אתגרים לאומיים עולה כי לסייבר יכול להיות תפקיד מרכזי במענה המערכתי הניתן לאתגרים אלו. ניתוח התוצאות מראה כי תנאי למימוש הסייבר, הוא עליונותה של ישראל במרחב. השגת חופש פעולה קיברנטי מול יריב היא תנאי הכרחי למימוש פעולות בהגנה ובהתקפה. עליונות כזו נבנית לאו דווקא רק בגופים ביטחוניים והיא צריכה להיות חלק ממאמץ משולב בין גורמי ביטחון, אקדמיה, תעשייה וממשל.

לסיום, השפעתו האפשרית של המרחב הקיברנטי על עיצוב וניהול מערכות היא רבה ומגוונות. לאור קצב השינויים הגדול סביבנו, הכרחי לקיים תהליך חשיבה ופיתוח ידע מתמיד, על מנת לעצב, לבנות ולהשתמש במרחב זה בצורה המיטבית לצרכיה האסטרטגיים של מדינת ישראל.

מההיבט האנושי, ועם הקשרים ביניהם. הכרה כזו תהיה על פי רוב נחלתם של אנשי המודיעין. נושא נוסף, שעולה בשלב בניית המודל אל מול אתגר ספציפי, הוא הצורך בניתוח מקצועי של גודל המרחב הקיברנטי במערכת שעמה מתמודדים ושל מאפייניו.

בניית מפת הממשקים והדיון צריכים להתבצע באינטגרציה רחבה של גורמים שמכירים היטב את האתגר עם אלו שמכירים היטב את היכולות הקיברנטיות הישראליות בהגנה ובהתקפה, ועם אלו האמונים על חשיבה מערכתית. בשילוב כזה, הופך המודל לכלי שמאפשר לימוד הדדי ופיתוח ידע, אל מול תכלית מוגדרת. קיים יתרון בשימוש במודל כזה, "המאלץ" שיח בין הגורמים השונים. במילים אחרות, לא נדרש להיות מומחה טכני על מנת להגדיר צורך הנובע מניתוח המערכת היריבה, ולא נדרש להיות על מנת להצביע על אפשרויות לפעולה במרחב הקיברנטי מתוך ידע טכני.

תוצר נוסף מדיון כזה, וחשוב לא פחות, הוא הצבעה על מרכיבי בניין כוח שיש לפתח או לחזק בהתאם למענה המערכתי הנוצר. המודל יכול להציב בצורה בהירה נקודות חוזק או חולשה במרחב הקיברנטי הישראלי, ובכך לסייע לקבלת החלטות בתחום.

כמו בכל כלי ומודל תפיסתי נמצא גם במודל המוצע כמה מגבלות, שעיקרן בניסיון להתאים לתבניות ברורות נושאים שלא בהכרח קשורים אליהן. עצם ההתבוננות המערכתית על אתגר ופירוקו למרכיבים והערכת עוצמתם הם סובייקטיביים.

המאמר אינו נוגע בכמה נושאים מרכזיים בהשפעתו של המרחב הקיברנטי על ניהול המערכה, כמו סוגיית המודיעין או סוגיית תרומתו האפשרית של המרחב להתרעה. נושאים אלו אמנם קשורים באופן הדוק להשפעתו של המרחב הקיברנטי, הן על הרמה האסטרטגית והן על הרמה האופרטיבית, אך מפתא קוצר היריעה הם לא יידונו במסגרתו, אך יש לזכור שהתמונה המלאה כוללת גם אותם.

**סיכום**

מטרת מאמר זה הייתה להציג מודל לשרטוט הממשקים האפשריים שבין סביבת הלחימה הקיברנטית לבין אתגרי השעה

