

לעבר עליונות צבאית בממד הסייבר

תא"ל א', אל"מ ע', סא"ל איתי חימיניס ומר. א.שדות^[1]

פורסם לראשונה באוקטובר 2020

תוכן

- 1..... לעבר עליונות צבאית בממד הסייבר
- 2..... תקציר המערכת:
- 2..... מבוא
- 2..... פרק א' - עליונות צבאית בסייבר
- 4..... פרק ב' - התפתחות ממד הסייבר לזירת לחימה
- 5..... פרק ג' - השתנות בממד - צבאות המערב
- 6..... פרק ד' - השתנות בממד - המקרה הישראלי
- 7..... פרק ה' - לקחי העבר - התהוות הממד האווירי כממד לחימה
- 8..... סיכום והמלצות

תקציר המערכת:

צה"ל מהווה שחקן מעצמתי בממד הסייבר, אך מעמד זה עתיד להישחק. בשנים האחרונות מתרחב מעגל המדינות והשחקנים התת-מדינתיים הפעילים בממד זה כמרחב לחימה. צה"ל השכיל לזהות תופעה זו בראשיתה, אך טרם השלים את ההשתנות הנחוצה לשימור עליונותו הצבאית בממד. בעוד שבעשור האחרון זכו מאמצי איסוף המידע וההגנה בסייבר בצה"ל לתנופה, בסייבר ההתקפי נותר פוטנציאל רב לא ממומש. בכדי לשמר את עליונותו הצבאית בממד הסייבר על צה"ל לפעול בדומה לשאר מעצמות הסייבר העולמיות, ולאמץ תפיסות מבצעיות ומבנים ארגוניים חדשים. שינוי זה יאפשר לו להרתיע, להתריע ולסכל איומים קיברנטיים, ומתוך כך לשחוק את יכולות אויביו. רק כך ישיג צה"ל את "קפיצת המדרגה" הנדרשת וישמר את עליונותו בממד.

מבוא

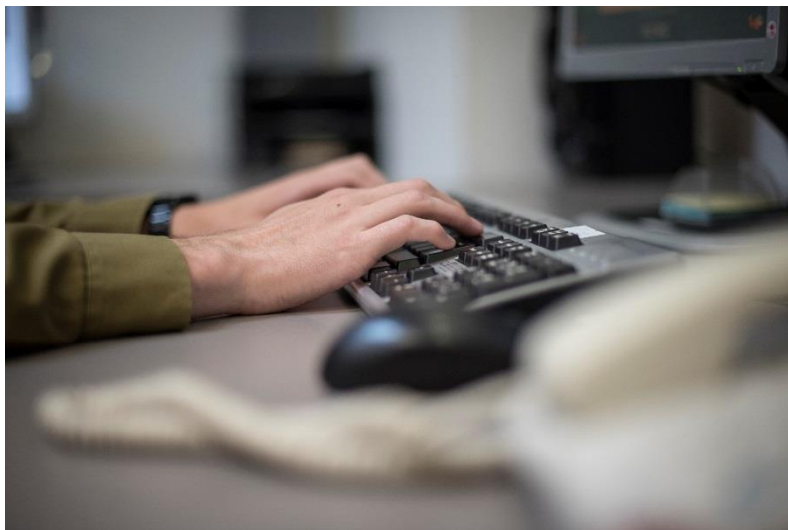
מאז הקמתה התבססה מדינת ישראל כמעצמה אזורית באוויר, בים וביבשה. עם זאת, רק בממד הסייבר התמקמה ישראל לצד מעצמות גלובאליות אשר קובעות תקדימים ומעצבות את הממד.

כבר היום משפיעה פעולתו של צה"ל בממד הסייבר באופן ניכר על מאזן הכוחות במזרח התיכון. אך מלוא הפוטנציאל טרם הושג: ברמה הטקטית, טרם מומש פוטנציאל שילוביות הסייבר בכוחות המתמרנים. במערכה מול האיום האיראני אמנם נעשה רבות, אך קיים עוד עושר הזדמנויות נרחב לפעולה בממד. ברמה האסטרטגית, טרם הופנם כובד משמעות מרחב הסייבר כאמצעי ל-"הקרנת כוח" ישראלית (Power Projection) בכל מקום בעולם.

מאמר זה יבחן את ההשתנות בשנים האחרונות בישראל ובעולם בתחום העליונות הצבאית בממד הסייבר^[2] וימליץ על הקמת חטיבת התקפה מטכ"לית בממד. זאת, לצורך שיפור האפקטיביות המבצעית הרב-זרועית של צה"ל ולטובת עליונותו המתמשכת בממד הסייבר.

בפרקים הבאים נברר את המגמות המרכזיות שמעצבות את הלחימה בסייבר. הפרק הראשון יבחן את מושג העליונות בסייבר במבט עולמי ויציע לראשונה הגדרה ישראלית של עליונות צבאית בממד. הפרק השני יגע בשינויים שחלו בממד ובמאפייניו, החל מ"עידן התמימות" של ראשית שנות האלפיים דרך שלבי ההבשלה של צה"ל ושל יריביו. הפרק השלישי יגע בהתפתחות התפיסתית שעברו צבאות וארגונים שונים בעולם, בעוד שהפרק הרביעי יעסוק בהתפתחות התפיסתית והארגונית בצה"ל. הפרק החמישי ידון בלקחים שניתן להפיק מהתהוות הממד האווירי בראשית המאה שעברה. הסיכום ידון בדרך קדימה עבור צה"ל בממד ויקרא לשינויים הנדרשים לטובת שימור כוחו והעצמתו.

פרק א' - עליונות צבאית בסייבר



כיצד נתפסת העליונות הצבאית בסייבר בישראל לעומת מדינות אחרות בעולם?

בישראל טרם נקבעה הגדרה רשמית למושג העליונות הצבאית בסייבר, אם כי מספר מסמכים רשמיים עסקו בנושא באופן עקיף.^[3] למשל, מסמך אסטרטגיית הסייבר שפורסם ב-2017 על-ידי מערך הסייבר הלאומי במשרד ראש הממשלה, מצייין, כי יש לרתום את ממד הסייבר להגשמת יעדיה של ישראל, לרבות בטחונה הלאומי.^[4] בתפיסת הפעלה החדשה של צה"ל שפורסמה ב-2020, עליונות בסייבר מוגדרת כיכולת חיונית להבטחת עליונות צה"ל בשאר ממדי הלחימה.^[5]

בארה"ב קיימות מספר הגדרות רשמיות. משרד ההגנה מגדיר עליונות צבאית בסייבר באופן הבא - "דרגת דומיננטיות בממד הסייבר על ידי צד אחד באופן המתיר לו ולכוחותיו באוויר, ביבשה, בים ובחלל לבצע מבצעים באופן בטוח, מהימן ובמסגרת מוגדרת של זמן ומרחב מבצעי, מבלי שליריבו תהיה היכולת למנוע ממנו."^[6] הגדרה צרה וממוקדת יותר מוצעת על ידי חיל האוויר האמריקאי: "עליונות בסייבר מייצגת יתרון מבצעי בממד הסייבר המאפשר ביצוע מבצעים בכל ממד בזמן מוגדר מבלי שליריב תהיה היכולת למנוע זאת."^[7] בצרפת, באופן דומה, הוגדרה עליונות בסייבר כמרכיב מרכזי בעליונות מבצעית^[8] והסייבר עצמו כממד לחימה מרכזי נוסף בשדה הקרב הרב-ממדי.^[9]

בבריטניה, מזהה משרד ההגנה את ממד הסייבר כחלק ממרחב גדול יותר של לוחמת מידע. משה"ג הבריטי מגדיר את העליונות במידע (Information Advantage) באופן הבא: "היתרון התחרותי המהימן המושג באמצעות הפעלה מתמשכת, סתגלנית, הכרעיתית ובעלת חוסן של מידע ומערכות מידע."^[10]

ברוסיה ובסין מסתמנת תפיסה דומה הרואה את הסייבר כחלק ממסגרת רחבה יותר של לוחמת מידע. במדינות אלו מיטשטשות הפרדות הנהוגות במערב בין לוחמת מידע ומחשבים, לוחמה פסיכולוגית או לוחמה אלקטרו-מגנטית.^[11] על פי דימה אדמסקי, הגישה הרוסית לעליונות במידע רואה בו אמצעי להכרעה של האויב. על פי גישה זו, עליונות במידע מהווה תנאי הכרחי ולעיתים אף מספק לניצחון במערכה, לעיתים באמצעות פגיעה משמעותית בקצב קבלת ההחלטות המערכתיות של היריב, באיכותן ובשיפור יכולות אלה בצד התוקף. מרכיב נוסף שמציג אדמסקי ביחס לגישה הרוסית הוא היחס להיבטי הזמן והמרחב. כך, לדבריו, הגישה הרוסית לעליונות במידע "אינה מבדילה בין עת שלום לעת מלחמה ומנהלת מערכה רב ממדית בלתי פוסקת. תפיסת הזמן... היא ארוכה יותר ואינה מוגבלת לאירוע מסוים, כשכל אירוע בה נתפס בהקשר רחב יותר."^[12]

קיים אם כך שוני רב בתפיסת הסייבר הצבאי בעולם. מגישה התופסת סייבר ככלי נוסף בארסנל הצבאי, בדומה ללוחמה האלקטרונית, אשר כוחה בשילובה עם כוחות האוויר, הים והיבשה; דרך גישה התופסת אותו כממד לחימה עצמאי, אשר בתוכו מתקיימת הלחימה בנפרד מממדי לחימה אחרים; ועד לגישה הרואה בו שיטה בעיקר ללוחמה פסיכולוגית ולהשפעה תודעתית אשר מתקיימת ברשתות המשמשות להעברת מידע. מהבדלי תפיסה אלה נובע גם שוני עמוק בהקשרי זמן ומרחב. בעוד שעימות קינטי או קיברנטי מצריך יתרון טכנולוגי-מבצעי בהקשר מוגדר ומתוחם, מהלך השפעה תודעתית מצריך אפקטיביות בתהליך ממושך.^[13]

על רקע זה, אנו מבקשים להציע להגדרה הבאה לעליונות צבאית בסייבר בצה"ל:

"היכולת לפעול ברציפות מבצעית וללא הפרעה בממד הסייבר למטרת פגיעה באויב, עליונות במידע והגנה מפני איומים בממד ומחוצה לו. זאת, תוך שימור יתרון איכותי מכריע על פני אויבים ומתחרים בממד."

הגדרה זו מגלמת מספר הנחות עבודה:

- "ברציפות מבצעית וללא הפרעה" – מצריכה השקעה ניכרת בפיתוח תפיסות, טכנולוגיות חדשניות ושיטות מבצעיות בכדי להתמודד עם ההשתנות המתמדת בממד.
- "בממד הסייבר" - צה"ל רואה בממד הסייבר ממד לחימה נוסף, בדומה לאוויר, הים והיבשה.

- "למטרת פגיעה באויב, עליונות במידע והגנה מפני איומים" - מצריכה יכולת פעולה בין-תחומית הכוללת מומחיות טכנולוגית, פסיכולוגית-תרבותית, לוגיסטית, התקפית והגנתית בדרגים המבצעים, כמו גם יכולת ניהול מערכה רב-תחומית בדרג האסטרטגי.
 - "בממד ומחוצה לו" - מצריכה שילוביות גבוהה והעצמה החדית עם כלל זרועות הצבא והגופים השונים במערכת הביטחון, בהתאם לתפיסת הנצחון של צה"ל.
 - "תוך שימור יתרון איכותי מכריע" - מצריכה השקעה ניכרת בתפיסות צבאיות ובהון האנושי בעולם תחרותי, משתנה וכזה המתאפיין באי-וודאות רבה.
- עד כאן דנו בשאלה מהי עליונות צבאית בממד הסייבר. אך מה מאפייני ממד הסייבר בשנת 2020? על כך נדון בפרק הבא.

פרק ב' – התפתחות ממד הסייבר לזירת לחימה

הבשלתו של ממד הסייבר לכדי זירת לחימה פעילה התרחשה בעשור וחצי האחרונים. משמעות המושג זירת לחימה היא שבתקופה זו הפכו תשתיות התקשורת והמחשבים המודרניות למוקד מרכזי נוסף של המאבק על מאזן העוצמה הגלובלי, אשר פועלים בו מעצמות, ^[14] צבאות וארגוני טרור. בד בבד, התפתח במרחב זה מאבק נוסף בין גורמי אכיפת חוק וארגוני פשע.

החוקר ג'ייסון הילי ^[15] מציע חלוקה של התפתחות ממד הסייבר ל-3 תקופות היסטוריות מובחנות בהקשר זה - ^[16] תקופת ההתהוות של האינטרנט (1980-1998); ותקופת הנסיקה (1998-2003), במהלכן נעשה שימוש בתקיפות סייבר בעיקר לצרכי איסוף מידע; ותקופת ה'מילטריזציה' שהחלה ב-2003. בתקופה זו ארה"ב אף הכירה בצורה רשמית בסייבר כמרחב לחימה, ^[17] ומעקב אשר בוצע על-ידי מפקד אמריקאים אחר תקריות סייבר מצביע על האצת קצב הלחימה בממד בשנים לאחר מכן. ^[18]

מהם המאפיינים האסטרטגיים, המערכתיים והטקטיים של ממד הסייבר כזירת לחימה פעילה? לשאלה זו תשובות רבות כמספר השחקנים הפועלים במרחב. ^[19] עם זאת, מספר מאפיינים משותפים לכולם:

יכולת ההכחשה (Deniability): התפוצה של טכנולוגיית מידע זולה ונגישה, לצד זליגת כלים מעצמתיים, העצימה שחקנים אזרחיים, ובתוכם ארגוני טרור ופשע, כמו גם פצחנים (האקרים) עצמאיים. ^[20] לשחקנים מסוג זה יש את היכולת לפגוע בביטחון ובשגשוג הכלכלי של מדינות וארגונים באמצעות ממד הסייבר, תוך הימנעות מעימות צבאי גלוי. ^[21] מבחינה טכנולוגית, קיים קושי רב לשייך פעולה במרחב הסייבר למקור שלה. לעיתים רבות, גם קשה לאבחן אם פגיעה במהימנות של מידע, תקלה טכנית או תאונה פיזית נגרמה כתוצאה מפעולת סייבר או שמקורה בטעות אנוש.

רב-תחומיות: תשתיות התקשורת המודרניות ובתוכם האינטרנט הוקמו למגוון רב של תכליות: כדי לשמש ככלי לתקשורת בין-אישית, או כמערכת לתקשורת המונים, אשר מחליף במידה רבה את מקורות המידע המסורתיים (רדיו, עיתון וטלוויזיה). בה בעת, משמשות רשתות אלה לטובת תקשורת בין רכיבים תעשייתיים כגון מכונות במפעל או אמצעי תחבורה. מצב דברים זה מאפשר לגוף הלוחם בסייבר לפגוע באויביו בדרכים שונות ולהסב נזק פיזי, כספי ותודעתי.

גלובאליות: בממד האינטרנט כמעט ואין משמעות למיקום הגיאוגרפי בעולם. מכך נובעות צורות לחימה חדשות וכלים "להקרנת כוח (power projection)" שטרם הורגלנו בהם בעבר בחשיבה הצבאית הישראלית. כך, גם לישראל מהווה ממד הסייבר פוטנציאל לקידום האינטרסים שלה בעולם באופן שאינו תלוי בקרבה גיאוגרפית.

ההגדרה שהוצעה לעליונות צבאית ישראלית בממד הסייבר, כמו גם ההשתנות המשמעותית במאפייני הממד, מחייבים בראייתנו לחשוב מחדש על הקשר שבין סוגית העליונות לפעילות ההתקפית של ישראל בממד. כך, להתרשמותנו, מדיניות התקפית ויזמת בממד ובאמצעות

הינה חיונית לצורך 'הקרנת עוצמה' צבאית; היא תוביל לאורך זמן לפגיעה באפקטיביות המבצעית של יריבים ואויבים באופן שיגביה את מחיר הפעולה בממד, ויחייב שיפור מגננותיהם; וכן, תתרום לאורך זמן לעיצוב 'כללי משחק' מועדפים בעבור ישראל בממד ומחוצה לו.

עד כאן דנו בהתפתחות ממד הסייבר לממד לחימה, כעת נבחן כיצד התאימו עצמם השחקנים המרכזיים במרחב להשתנות בממד?

פרק ג' – השתנות בממד – צבאות המערב

ניתן לסמן את שנת 2018 כנקודת מפנה באסטרטגיה האמריקאית בתחום הסייבר, שעיקרה פעולה מתמשכת ואגרסיביות בממד.

ברובד המדיניות, פורסמה דירקטיבה נשיאותית עדכנית (Presidential Policy Directive) אשר מעצימה ומגדירה מחדש את סמכויות הפעולה בתחום הסייבר ההתקפי בארה"ב.^[22] לכך יש להוסיף את פרסום מסמכי האסטרטגיה בסייבר של הבית הלבן^[23] ושל הפנטגון.^[24] הפרשנות המקובלת הינה שפרסום מסמכים אלה בעיתוי שבו פורסמו מצביעים על שינוי של ממש באסטרטגיה האמריקאית בסייבר.

ברובד הארגוני, באותה השנה זכה פיקוד הסייבר למעמד של פיקוד עצמאי, בדומה לפיקודים המרחביים האחרים (אירופה, אפריקה, חלל ועוד). הפיקוד גם זכה לתוספת משאבים ניכרת בתקציב וכ"א שמטרתה חיזוק היכולת ההתקפית בסייבר. שינוי ארגוני נוסף מתבצע בשנים האחרונות גם בדרג הטקטי, בדמות הקמת מסגרות חדשות שמטרתן לאפשר שילוב יכולות סייבר לצרכי איסוף, הגנה והתקפה בשילוב עם כוחות שטח. יתרה מכך, חל שינוי גם במאפייני הפעלת הכוח האמריקאי בסייבר, הבא לידי ביטוי בשימוש רב מבעבר ביכולות סייבר התקפיות נגד יריבים ברחבי הגלובוס לצורך חיזוק ההרתעה וסיכול איומים.

שינוי זה נבע, בראש ובראשונה, בעקבות חלחול התפיסה בארצות הברית שהיא מאבדת את עמדת ההובלה בתחום הסייבר ההתקפי וכך גם את יכולת ההרתעה והפעולה נגד פעולות אויב. לכך יש להוסיף את המיקוד האמריקאי הגובר בהגנה על כוחות לוחמים ברחבי העולם והצורך להעמיד לרשותם כלי לחימה נוספים בשדה הלחימה הרב-ממדי.

כלל השינויים הללו מלמדים על אימוץ גישה יוזמת יותר, פעילה יותר, מתמשכת, רציפה והתקפית יותר מבעבר. צמד מושגים הבולטים בשיח האמריקאי ואשר משקפים את השינוי הינם

' חינוך מתמיד (Persistent Engagement) 'ו- 'הגנה קדמית [25]. ' (Defend forward) תפיסה זו מבטאת הערכה ששלילה מתמשכת של יכולות אויב, באופן פעיל וקדומני, תוביל להשתנות בהתנהגות אויביה של ארצות הברית, לשינוי בחישובי העלות והתועלת שלהם ולנטישת הפעולות נגד ארצות הברית בממד.^[26]

בה בעת, לפחות מאז 2016 הצבא האמריקאי עושה מאמצים רבים לשלב יכולות סייבר לצרכי איסוף, הגנה והתקפה בדרג הטקטי, כחלק ממגמה רחבה יותר להעצים את קטלניות הכוחות הלוחמים באמצעות הפיכתם לבעלי יכולת רב-ממדית. בנוסף, הדבר משקף את ההכרה, כי מפקדי שדה צריכים להכיר בצורה טובה יותר יכולות סייבר לצורך שילובן במהלכיהם כמו גם לפתח הכרות עם איומי סייבר בכדי שיוכלו להתגונן מפניהם. לצורך כך, הצבא האמריקאי בוחן ומתרגל מספר צורות ארגוניות שבאמצעותן ניתן יהיה לשלב יכולות סייבר בדרג הטקטי.

במסגרת זאת, נבחנת למשל האפשרות להקים צוותי סייבר נפרדים שיפעלו לצד הכוח הלוחם כנכס מבצעי נוסף העומד לרשות מפקד החטיבה וגדוד רב-ממדי שישלב גם יכולות בתחום ה"ל"א, המודיעין והלוחמ"מ. לעיתים הכוחות יהיו בעלי יכולות סייבר אורגניות ולעיתים יהיו בכוח שדכנים אשר יוכלו לתכנן מבעוד מועד או לבקש אד-הוק את הפעלת הכוחות. בין המתארים המתורגלים על ידי כוחות הצבא האמריקאים: הפעלת כוח בממד במסגרת של תמרון יבשתי ותפיסת שטח, 'הכשרת הקרקע' לתקיפה אווירית במרחב רווי הגנ"א ומנגד, סיכול מתקפה קרקעית ותקיפה אווירית של האויב.^[27] בכל מתארים אלו הופעלו כוחות הסייבר לצורך שיבוש יכולות הגילוי וההרתעה והפז"ש של האויב, באמצעות פגיעה במגוון יעדים - ממערכות ההגנ"א ועד למערכות התקשורת והמדיעין שבהן נעשה שימוש. בנוסף, בחלק מהמתארים הכוח

הלוחם ביקש מרמה ממונה את הפעלת הכוח במקרה שבו היכולת הנדרשת לא הייתה בחזקתו או כאשר הפעלתה דרשה סמכות גבוהה יותר של אישור. בכל המתארים הללו הפעלת הכוח בממד לא הייתה בלעדית והינה חלק מהפעלת כוח בממדים נוספים על-ידי הלוחמים.^[28]

בבריטניה, הוכרז ב-2019 על הקמת סוכנות חדשה ללוחמת סייבר, National Cyber Force, המוקמת במשותף על ידי משרד ההגנה וה-GCHQ-סוכנות זו תתמקד בלחימה בממד הסייבר, בצורה יוזמת ורציפה, נגד אויביה של בריטניה ולצורך סיכול איומים מתהווים.^[29] גם הבריטים מציינים את חשיבות הפעולה בסמיכות למוצא האיום, כלומר ב-'שטח האויב'.^[30]

בצרפת חל שינוי דומה בתפיסה המבצעית. בחודש ינואר 2019 זכה תחום ההתקפה בסייבר למקום מרכזי במסגרת דוקטרינת הביטחון הצרפתית החדשה והוא אף הוגדר כחלק אינטגרטיבי מפעילותה הצבאית הקונבנציונאלית של צרפת, בין אם יכולות אלה יופעלו באופן עצמאי ובין אם בשילוב יכולות צבאיות בממדים אחרים.^[31]

לסיכום חלק זה, בשנים האחרונות בולטת מגמה בצבאות המערב להגדיר את לוחמת הסייבר ההתקפית כחלק חיוני מארגז הכלים הצבאי. זאת, מתוך מטרה ברורה לשמר את העליונות הצבאית שלהם בממד, ותוך הפרדה ברורה מבעבר ביחס לפעילות בסייבר לצרכי איסוף והגנה. בנוסף, ניכר שגוברת הלגיטימציה לשימוש בכלי סייבר לצרכי התקפה.

כעת, נדון במתרחש בישראל ונמליץ כיצד נכון לצה"ל להיערך לאתגרים העומדים בפניו.

פרק ד' – השתנות בממד – המקרה הישראלי

בשונה מצבאות המערב, מפת האיומים וההזדמנויות של מדינת ישראל הינה ייחודית. בעוד שארצות הברית, רוסיה, סין ואירופה מתמודדות בממד הסייבר כמעצמות, מדינת ישראל מתמודדת עם אויבים אשר נחותים ממנה טכנולוגית. אך דווקא מסיבה זו עשויים אויבים כמו איראן, חמאס וחזבאללה לנצל את הפגיעות של ישראל, הנובעת מהיותה כלכלת מידע מתקדמת, בכדי לייצר באמצעים א-סימטריים פגיעה ברציפות התפקוד שלה ושגשוגה, ולהצר את מרחב הפעולה המבצעי של צה"ל.

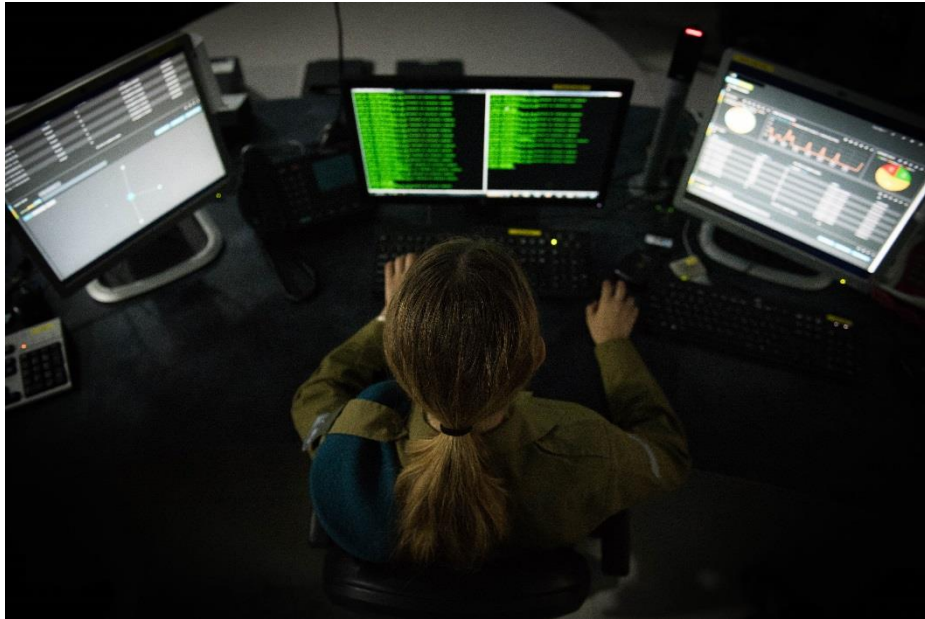
בשנים האחרונות, ניכרת התרחבות של מועדון המדינות המצומצם המפעיל כלי לחימה בסייבר. אם בעשור האחרון יכולות הסייבר ההתקפיות היו שמורות למספר מצומצם של מעצמות – ארצות הברית, רוסיה, סין, בריטניה וישראל. בחלוף השנים, כלים ויכולות מעצמתיים מוצאים את דרכם למדינות נוספות ואף לארגוני פשיעה באמצעות פיתוח עצמאי, העתקה או קנייתם בשוק החופשי. תהליכים אלו גורמים לשחיקה הדרגתית של בלעדיות המועדון המצומצם שנהנתה ממנו ישראל, באופן אשר עשוי לשחוק את יתרונה בסייבר ואף ליצור איומים חדשים כנגדה.

אך למרות התגברות איומים אלו, כמו גם הבנת ההזדמנויות בממד הסייבר, לא ניכרת התפתחות תפיסתית משמעותית בשנים האחרונות בצה"ל בתחום הסייבר כממד לחימה. בעוד שהנושא כן נכלל במסגרת יכולות ההתקפה הרב-ממדית שבהן עסק תר"ש "תנופה",^[32] לא גובשה בפועל תפיסת הפעלה כוללת או שינוי ארגוני משמעותי אשר בכוחם למצות את הפוטנציאל המגולם בממד הסייבר לפתרונות מבצעיים בידי צה"ל.

כבר ב-2009, הגדיר הרמטכ"ל דאז את הסייבר "כמרחב לחימה אסטרטגי ואופרטיבי עבור מדינת ישראל". בשנת 2015, כללה אסטרטגיית צה"ל התייחסות לסייבר כאחד מהאיומים הגוברים עימם על ישראל להתמודד.^[33] המסמך מגדיר את הלחימה בממד הסייבר כחלק מגישה רב-ממדית של לחימה בזמני שגרה, חירום ומלחמה, וכחלק מהמאמץ ההתקפי של צה"ל במלחמה בכל הרמות - אסטרטגית, אופרטיבית וטקטית. לצורך כך, קורא המסמך לבניין כוח משמעותי בסייבר - הקמת זרוע מטכ"לית (שלבסוף לא הוקמה) אשר תהיה אמונה על הממד ולצידה בניית יכולות הגנה על כלל המערכות המבצעיות והמסייעות.

מסמך אסטרטגיית צה"ל מ-2018 מבטא התפתחות נוספת בהבנה של צה"ל אודות ממד הסייבר כזירת לחימה. המסמך ממסגר את ההתפתחויות בממד כחלק מהתפתחות רחבה יותר של שינויים גלובליים ('מהפכת המידע'), הבחנה בין שחקנים מדינתיים ושחקנים לא מדינתיים והתייחסות ליכולות לחימה בסייבר כחלק ממאמץ המניעה וההשפעה בבט"ש וכמרכיב מרכזי במב"מ.^[34]

בדצמבר 2018 גם פורסם מאמרו של הרמטכ"ל לשעבר, רא"ל במיל' גדי איזנקוט בנושא הסייבר בצה"ל שבמסגרתו קבע, כי מעגל האיום הרביעי אתו מתמודד צה"ל הוא בממד הסייבר.^[35] המסמך מתאר תהליך למידה סביב השאלה כיצד לארגן את צה"ל בתחום לוחמת הסייבר. נבחנו חלופות שהיוו 'קפיצת מדרגה', כגון הקמת מפקדת סייבר שתכלול את כלל יכולות הסייבר של צה"ל, אך בפועל התגבשה לבסוף החלטה להמשיך ב-"התקדמות איטית וארגון פעילות הסייבר בצה"ל באופן מדוד.^[36]"...כך שבשונה מתחומי ההגנה והאיסוף, הוחלט שלא לפתח את תחום ההתקפה בסייבר תחת ארגון ייעודי מותאם. וזאת, כפי שראינו בחלקים הקודמים, בשונה ממרבית המדינות המובילות במערב.



פרק ה' - לקחי העבר - התהוות הממד האווירי כממד לחימה

אופיו הייחודי של ממד הסייבר מצריך פיתוח של תפיסות ושל מבנים ארגוניים ייחודיים ללחימה. התהוות הלחימה בממד האווירי מהווה מקרה בוחן חשוב לטענה זו. בתחילת מלחמת העולם הראשונה שימש ממד האוויר בעיקר לאיסוף מודיעין ומשימות סיור וקרבות אוויר הסתכמו בחילופי ריזות מנשק קל בין אנשי אוויר בעודם מסיירים. אך המלחמה האיצה את השימוש בממד ובמהלך 1918 הוקם לראשונה בעולם חיל-אוויר כגוף נפרד ועצמאי בבריטניה.^[37] כשניתנה בשנת 1921 ההגדרה הראשונה לעליונות אווירית היה קשה לדמיין כיצד יראה ממד הלחימה האווירי ב-1945 או ב-1967, אך היה ברור שהמגמה הטכנולוגית תלך ותעצים את שימושיות הממד ללחימה.^[38] כמעט מאה שנה לאחר מכן, בזמן כתיבת שורות אלה, קשה לדמיין כיצד תראה הלחימה בממד הסייבר ב-2045 או ב-2067, אך כן ברור שהמגמה הטכנולוגית תוביל להתרחבות הממד וכי האצת הדיגיטציה והחיבוריות בממד צפויה להמשיך ולשנות בעתיד את כל היבטי החיים, ובתוכם את הביטחון ואת הכלכלה.

ההחלטה על הקמת חיל האוויר הבריטי כגוף עצמאי התבססה של שני דו"חות רשמיים, שנקראו

^[39] The Smuts Reports המסמכים אלה חוברו בידי גנרל בשם Jan Smuts ונכתבו לבקשת ראש

הממשלה הבריטי דיוויד לויד ג'ורג. נושאם היה "התארגנות אווירית והגנה מפני פשיטות אוויריות". הדו"ח טען, כי "לא רחוק היום שבו מבצעים אוויריים נגד נכסי האויב כגון ריכוזי תעשייה ואוכלוסייה בקנה מידה גדול יהפכו לעיקר העיסוק המבצעי בלחימה, אשר מולם העיסוק המסורתי בלחימה יבשתית או ימית יהפוך משני ומוכפף.^[40]" לבסוף, הוחלט על הקמת חיל האוויר הבריטי מתוך זרוע האוויר של חיל היבשה (Royal Flying Corps) וזו של הימיה הבריטית, (Royal Naval Air Service) תוך התנגדות עזה של שתי הזרועות להקמתו. מצדדי הקמת החיל סברו, כי עליית מדרגה בממד האווירי מחייבת הקמת גוף ייעודי ועצמאי אשר חי ונושם את

הלחימה בממד ולא פועל בו כעיסוק משני או כנגזרת אגבית של עולמות תוכן אחרים. בחלוף השנים טענה זו התבררה כנכונה והועתקה על ידי כלל הצבאות. אך בעוד הצרפתים עשו זאת עשור וחצי לאחר מכן, הזיהוי המוקדם של ההשתנות המערכתית על-ידי הבריטים, תרם למובילות הבריטית המתמשכת בממד.

כמו באוויר כך גם בסייבר. אופיו הייחודי של הממד מצריך פיתוח של תפיסות ומבנים ייחודיים ללחימה, כמו גם חיכוך מתמיד עם המציאות בכדי להפוך תאוריה לפרקטיקה. כפי שעקרונות הלחימה באוויר שונים מהיבשה, כך גם ממד הסייבר שונה מקודמיו ומציב שאלות ייחודיות. כך, מה הערך של יצירת פעולה קינטית גדולה אחת בסייבר אל מול השקעה ביצירת מתח מצטבר למערכת היריבה ב"הרעשה סייברית" בלתי-פוסקות? אילו אפשרויות לוחמה כלכלית מאפשר הממד? כיצד נכון לשלב פעולה קיברנטית עם פעולה אווירית? או יבשתית? או עם מהלך דיפלומטי-מדיני? שאלות אלו ועוד מצריכות פיתוח דוקטרינות חדשניות בסביבה ייעודית, תוך חיכוך בממד עם מערכת יריבה לומדת.

באופן דומה, מימוש פוטנציאל השילוביות הרב-ממדי מצריך תרגול. ונכון היה לצה"ל לכלול היבטי סייבר בתרגילים מטכ"ליים. הערך יתבטא במספר מישורים. החל בדרג המתמך שיכול להיעזר בכלי סייבר לאיתור אויב, להפרדתו מאוכלוסייה אזרחית ואף כאמצעי תקשורת עמה. כך, גם בדרג האופרטיבי, החותר להשגת מטרות כמו שיבוש מערכות שו"ב ופז"ש של היריב בלחימה, וגרימת נזק קינטי בעורף האויב. כמו גם בדרג המערכתית, אשר לסל הכלים שלו יתווספו יכולות גרימת דיסאינפורמציה ובלבול בתשתיות הנתונים עליהן מסתמכת מערכת יריבה, ויכולת הדהוד מסרים אשר בכוחה להשפיע על ההסדרה המדינית בסיומו של עימות.

סיכום והמלצות

התקפה בסייבר מהווה התפתחות משמעותית בתפיסת הלחימה של השנים האחרונות. לצורת לחימה זו יש ערך הן ככלי עצמאי והן באופן משולב עם מאמצים צה"ליים אחרים. מתוך הבנת תרומתה הייחודית של ההתקפה בסייבר אל מול תרחישי לחימה ומעגלי הלחימה אשר מולו ניצב צה"ל, נכון לפתח בעת הזו שיח מערכתית-תפיסתי אודות ההזדמנויות והאיומים שמציע הממד. זאת, כפי שכבר מתרחש במדינות מובילות בעולם, כגון ארה"ב, בריטניה וצרפת.

גם במערכת הצבאית והמדינית בישראל חל עיסוק נרחב בנושא, כפי שהוצג בהרחבה במאמר. בפרט, תפיסת הלחימה כפי שהוצגה באופן מעמיק בסדנת הניצחון^[41] וכפי שמתבטא בתר"ש^[42] "תנופה" הפכה לאתגר רב-ממדי משולב, שבתוכו לסייבר מעמד ייחודי וחשוב.

בשנים האחרונות מתקדם המרכיב הדיגיטלי בקצב מואץ והופך לרכיב מרכזי בתפקודי הליבה של המערכת היריבה, באופן שמגביר את פגיעותה. מצב זה מעניק ללוחמת הסייבר פוטנציאל קטלניות ואפקטיביות מבצעית גוברת לצה"ל בעימות עתידי, באופן שיאפשר איגבור פעילות סימולטנית לפירוק מערכת האויב; לשינוי המאזן בין האויב לצה"ל בזמן לחימה; ליצירת פגיעה תודעתית; ומתוך כל אלה ליצירת הפתעה אסטרטגית.

צה"ל נדרש לבצע קפיצת מדרגה בתחום הלוחמה בסייבר כבר עכשיו. על מדינת ישראל וצה"ל להגביר את העיסוק בפיתוח תפיסות ותורות בצורת הלחימה בסייבר, באופן שימצה את פוטנציאל הפעולה שבו, ואת פוטנציאל השילוביות הרב-ממדית. אנו סבורים כי המשך פיתוחה ושכלולה של יכולת ההתקפה בממד הסייבר תעצים את יכולתו ההתקפית של צה"ל בממד הסייבר ובממדים אחרים, וכנגזרת מכך גם את עוצמתו בהגנה בממד, מתוך העתקת הלחימה בסייבר לשטח האויב.

בראייתנו, רק התארגנות עצמאית בדרג צה"לי משמעותי, שייעודה פיתוח ומימוש צורת לחימה זו, תאפשר לצה"ל את קפיצת המדרג הנדרשת. קיימים עוד סימני שאלה ומתחים רבים שיש לברר באשר למאפייני אותו ארגון שיש להקים. כך או אחרת, אנחנו סבורים כי הקמת חטיבת התקפה מטכ"לית אשר מרכזת את כלל יכולות ההתקפה וההשפעה בסייבר תחת סמכותה, תוך עיסוק מתמשך בבניין כח ובהפעלתו, היא ההתארגנות המיטבית לצרכיו המבצעיים של צה"ל בעת הזו. הקמתה תאפשר את שכלול יכולת הלחימה בממד, באופן שיבטיח את עליונותו הצבאית המתמשכת של צה"ל בממד הסייבר.

[1] תא"ל א' הוא מפקד יחידה 8200. אל"מ ע' הוא מפקד מרכז סייבר ביחידה 8200. סא"ל איתי חימיניס הוא רע"ן פיתוח ידע מערכתי במרכז דדו. א. שדות הוא יועץ ביחידה 8200. המחברים מבקשים להודות לתא"ל ערן אורטל, שמואל שמואל, סא"ל (במיל") דביר פלג, דן אנגלברג ולסא"ל ש' על הערותיהם המועילות.

[2] לדיון אודות מימד הסייבר מנקודת המבט של אומנות המערכה, לרבות אתגרי המימד לריבונות מדינות, הלימתו לכללי המשפט הבינ"ל והסיכונים וההזדמנויות המגולמות בפעולה במימד ובאמצעותו ראו גליון מספר 3 של כתב העת 'בין הקטבים אשר הוקדש לנושא. הגליון זמין לקריאה באתר האינטרנט של [כתבהעת](#).

[3] אין בכך כדי להצביע על כך שבישראל לא קיים עיסוק רב ומתמשך בנושא. כפי שמציג דימה אדמסקי בספרו, התרבות האסטרטגית הישראלית התאפיינה מאז ומעולם בעשייה רחבה וחדשנית שלא גובתה בבסיס תיאורטי מוצק שגובש, אם בכלל, רק לאחר מעשה או בעיצומו. אדמסקי, דימה. (2012). תרבות אסטרטגית וחדשנות צבאית. הוצאת משרד הביטחון.

[4] ISRAEL NATIONAL CYBER SECURITY STRATEGY.

[5] תפיסת ההפעלה לניצחון. (2020). מסמך פנימי.

[6] "the degree of dominance in cyberspace by one force that permits the" secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary".

[7] "the operational advantage in, through, and from cyberspace to conduct operations at a given time and in a given domain without prohibitive interference". Source - Bryant, William. (2013). "Cyberspace superiority: a conceptual model." Air & Space Power Journal, vol. 27, no. 6.

[8] FRANÇOIS, DELERUE, ALIX, DESFORGES, AND AUDE, GÉRY. (2019). "A CLOSE LOOK AT FRANCE'S NEW MILITARY CYBER STRATEGY". WAR ON THE ROCKS.

Isabelle Valentini. (2014). "Addressing the Cyber Threat— The French Defense Ministry's Approach", New Challenges to Global Security.

[9] FRANCH'S DEFENCE AND NATIONAL SECURITY STRATEGIC REVIEW, 2017.

[10] "the credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems". Source - Joint Concept Note 2/18 Information Advantage.

[11] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples From China and Russia.

[12] אדמסקי, דימה. (2015). "אומנות אופרטיבית קיברנטית". עשתונות, הוצאות המכללה לביטחון לאומי, גליון מספר 11, עמ' 43-44.

[13] השיח שונה גם בין מדינות מערביות. בגרמניה למשל נראה שהדגש ניתן לתחום החוסן הלאומי והרציפות התפקודית של המדינה הגרמנית ולתפקיד הכוחות המזויינים בגרמניה בשמירה עליו. לפרספקטיבה השוואתית רחבה על מדיניות בטחון סייבר של מדינות באירופה ראה Paul Ducheine, Frans Osinga, Joseph Soeters (eds.). Cyber Warfare: Critical Perspectives. Netherlands Annual Review of Military Studies 2012.

[14] לדיון השוואתי על המאבק המעצמתי במימד בין ארה"ב, סין ורוסיה ראו מאמרם של גיל ברעם ואופיר בראל בנושא 'לוחמת מידע בין המעצמות' בגליונות 22-23 של כתב העת 'בין הקטבים'.

[15] Jason Healey, ed. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Arlington, VA: Cyber Conflict Studies Association)

[16] בספרות המקצועית קיימת מחלוקת האם מבצעי השפעה ולוחמת מידע' ככלל מהווה נדבך בלוחמת סייבר. ביטוי לגישה זאת ראו למשל מדדריך המגזין האמריקאי "Wired" בנושא לוחמת סייבר.

מנגד, יש הרואים בלוחמת מידע דווקא את המרכיב החשוב ביותר של לוחמת סייבר עת הנוכחית. עמדה המיוצגת למשל ב-

Pollard Neal Et el. (2018). "Trust war: dangerous trends in Cyber conflict". *War on the rocks*.

[17] ב-2012 פרסם אף מזכיר ההגנה האמריקאי דאז, לאון פנטה, את אזהרתו הידועה מפני "פרל הרבור" בסייבר:

"The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability". Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.

[19] במהלך 2018-2019 פרסם פיקוד הסייבר האמריקאי מספר מסמכים השופכים אור על מימד הסייבר כזירת לחימה. על אף הבדלי נקודות המבט - אמריקאית לעומת ישראל - אנו מאמינים שניתן לאמץ רבות מהתובנות בהקשר זה גם לצורך הבנת סביבת הפעולה הנוכחית של צה"ל במימד. להרחבה ראו-

Paul M. Nakasone. (2019). "A Cyber Force for Persistent Operations". *JFQ* 92.

William T. Eliason. (2019). "An Interview with Paul M. Nakasone". *JFQ* 92.

US Cyber command. (2018). *Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command*.

[20] תחת הגדרה זו נופלים גם מומחי אבטחה הפועלים כ-"שכירי חרב" למרבה במחיר, וגם מומחי טכנולוגיה העוסקים באיתור ודיווח על פרצות אבטחה המאיימות על הציבור, המוכרים כבעלי "כובע לבן", או White-hat hacker.

[21] קטגוריזציה דומה של השחקנים העוינים במימד הסייבר מופיעה גם בדבריו של ראש ארגון הביון הבריטי, 'מטה התקשורת הלאומי', ה GCHQ-בנאומיו הפומביים ב-2018 וב-2019. בה בעת, מדבריו עולה, ראייה רחבה יותר של איומים הכוללת למשל פדופילים או סוחרי נשק ובבני אדם. המאמרים זמינים באתר האינטרנט של ה GCHQ-

[22] Borghard, Erica. (2018). "What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?". *CFR*.

[23] National Cyber strategy of the united states. (2018).

[24] Department of defense Cyber strategy. (2018).

[25] Nakasone, Paul. (2019). "A Cyber Force for Persistent Operations", *JOINT FORCE QUARTERLY*, 92:1, 10

“Persistent engagement of our adversaries in cyberspace cannot be successful if our actions are limited to DOD networks...To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well.”

^[26]Smeets, Max and Soesanto, Stefan. (2020). “Cyber Deterrence Is Dead. Long Live Cyber Deterrence!”. CFR.

במחקר שפורסם על ידי מכון RAND ב-2017 המליץ המכון על הרכב הכוח הטקטי הרב-מימדי בו משולבים תפקידינים בתחום הסייבר ובכלל זאת - 'לוחמי סייבר' בעלי הכשרה בתחום המאפשרת להם להפעיל אמל"ח בתנאי לחימה ברמת המחלקה; 'קצין סייבר' ברמת החטיבה בעל הכשרה טכנולוגית מעמיקה יותר והיכרות הן עם הצרכים המבצעיים של הכוחות בשטח והן עם מדיניות הפעלת הכוח ותהליכי האישור הנדרשים לצורך הפעלת כוח במימד; מספר מצומצם של 'מומחי סייבר' בעלי רקע מקצועי וניסיון רב בהפעלת ובניין כוח בתחום אשר יועמדו לרשות מפקד החטיבה על מנת להתמודד עם בעיות מורכבות שיצריכו רמת מומחיות אשר מצויה לרוב במטה. בנוסף, לכל חטיבה יהיה איש קשר במטה שהוא בעל הכשרה כמפתח/בונה כלים כמי שאמון על בניין הכוח של החטיבה בתחום. המחקר זמין ב-

Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, Drew Herrick. Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below. (Santa Monica, CA: RAND Corporation, 2017).

^[28]Mark, Pomerleau. (2018). "How the Army is improving tactical cyber operations". c4isrnet.

^[29]Dan Sabbagh. (2020). “UK to launch specialist cyber force able to target terror groups”. Guardian.

^[30]Jeremy Fleming. (2018). "Director's speech at Cyber UK 2018".

Jeremy Fleming. (2019). "Director's speech at Cyber UK 2019".

^[31] Arthur P.B. Laudrain. (2019). "France's New Offensive Cyber Doctrine". Lawfare.

Theresa Hitchens. (2019). "Tactical Cyber Weapons For Future French Battlefield Ops?". Breaking Defense.

^[32]הלר, אור. (2020). "מרחפנים ועד פיקוד איראן: תר"ש תנופה נחשפת". ישראל דיפנס.

^[34]המסמכים זמינים באתר צה"ל

^[35]איזנקוט, גבי. (2018). 'הסייבר בצה"ל'. סייבר, מודיעין וביטחון. גיליון 2.

^[36]שם, עמוד 93.

^[38]See: “Command Of The Air”, by General Giulio Douhet (Published in 1921)

^[40] And the day may not be far off when aerial operations with their devastation of enemy lands and the destruction of industrial and populous centers on a vast scale may become the principal operations of war, to which older forms of military and naval operations may become secondary and subordinate (17 Aug 1917).