גיליון 3 | טבת תשע"ה, דצמבר 2014

בלמ"ס

סוגיות עכשוויות באמנות המערכה

# בֵּין הַקְּטָבִים

## סייבר

אתגר והזדמנויות במרחבים חדשים

מרכז דדו
לחשיבה צבאית
בינתחומית

# מרכז דדו לחשיבה צבאית בינתחומית

## בֵּין הקְטָבִים

גיליון מס׳ 3

## סייבר

### אתגר והזדמנויות במרחבים חדשים

דצמבר 2014
טבת תשע״ה

**בין הקטבים**

**סוגיות עכשוויות באומנות המערכה**

גיליון 3 — דצמבר 2014
סייבר – אתגר והזדמנויות במרחבים חדשים

מרכז דדו לחשיבה צבאית בינתחומית
אגף המבצעים, חטיבת תורה והדרכה
צה"ל

**Bein Haktavim**
**Contemporary Issues in Operational Art**

Volume 3 — December 2014
Cyber – Challenges and Opportunities in New Spheres

Dado Center for Interdisciplinary Military Studies
Operations Directorate (GS/J3), Doctrine and Training Division
Israel Defense Forces

**מפקד כתב העת ועורך ראשי: אל"מ ערן אורטל**

**עורך: סרן ליאור לבד**

בשער הגיליון: גוף בלי ראש בחליפת עסקים, מסמלי ההתארגנות החתרנית 'אנונימוס'.
גוף האדם – כמערכת מורכבת, ללא ראש.

עיצוב העטיפה: אמ"ץ/תוה"ד, המדור לפרסומים ולמינוח, צוות הגרפיקה.

**גיליונות "בין הקטבים" זמינים באינטרנט באתר הוצאת "מערכות":**

**www.maarachot.idf.il**

# פתח דבר

"החשישיים של ימי הביניים הקימו "מדינה" אשר הכילה רשת של טירות ועמקי הרים מרוחקים, מופרדים באלפי קילומטרים, מוגנים אסטרטגית מפני חדירה, מחוברים בזרם מידע של סוכנים חשאיים, נמצאים במאבק מלחמתי נגד כל הממשלות, ומוקדשים לידע בלבד. הטכנולוגיה המודרנית, המגיעה לשיאה בלוויין הריגול, הופכת *אוטונומיה* מסוג זה לחלום רומנטי גרידא: לא עוד איים פיראטיים! בעתיד, אותה טכנולוגיה – משוחררת מכל סוג של שליטה פוליטית – תוכל לאפשר עולם שלם של *אזורים אוטונומיים*"

חכים ביי (פיטר למבורן וילסון), Temporary Autonomous Zone – TAZ, 1991.

"סייבר". המרחב הרשתי הדיגיטלי ששינה את עולמנו עד בלתי הכר, שיצר מהפכה כלכלית, תרבותית, חברתית מדינית וביטחונית, מרחב שהוא יציר ידי האדם, הוא גם, אולי באופן פרדוקסאלי, מרחב שהוא במידה רבה לא-נודע. אמנם קיימת ספרות מחקרית ענפה בנושא, אך זו, כך נראה, אינה מצליחה להדביק את קצב ההשתנות העצמי של הסייבר. קצב זה מוכתב על-ידי מאות מיליוני משתמשים אנושיים, חברות, ממשלות, תאגידים, מנועי חיפוש, פלטפורמות חברתיות, מכוני מחקר ושחקנים אחרים, החולקים את הסביבה המשותפת החדשה הזו ומשנים אותה מדי יום.

חכים ביי, או בשמו האמיתי פיטר למבורן וילסון, העמיד כבר ב-1991 בספרו TAZ – אזור אוטונומי ארעי, חזון אנרכיסטי-חתרני. לתפיסתו, המדינות הממוסדות הן שהיוו ומהוות בהיסטוריה האנושית את המקור לאי-צדק ולשעבוד בני האדם. בחזונו, המרחב הקיברנטי הטכנולוגי יוכל לספק תחליף למרחבים הגיאוגרפיים הלא-ממופים (Terra Incognita) שאפשרו בעבר (טרם הושלם מעשה הכרטוגרפיה[i] של הכדור) התאגדויות חופשיות של בני חורין, כמו זו של החשישיים בימי הביניים או קהילות של פיראטיים בוקאנירים (Buccaneers) במאות ה-16-17 באזורים הקאריביים ולחופי אפריקה. תופעת הרשת העולמית הרחבה (www) היא שתאפשר לאותם תאבי חירות אישית-

[i] כרטוגרפיה – תורת המיפוי והשרטוט של מפות גיאוגרפיות. יש הכותבים קרטוגרפיה.

קהילתית של דורנו, תנועה במרחבים הלא-ממופים של הרשת, חירות אינטלקטואלית מלאה, חופש מידע והגשמה עצמית, הרחק מהישג ידם של כוחות ממוסדים כמו מדינות הלאום והתאגידים הבין-לאומיים.

המרחב הקיברנטי, אם כן, הוא מרחב בעל השפעה מטשטשת על הגדרות העוצמה והכוח הקיימות. הוא מאפשר סוג של שוויון שאינו אפשרי בגיאוגרפיה המקובלת שלנו. מעצם טיבו הוא המרחב החתרני האולטימטיבי. יתר על-כן, שלא כמו האוקיינוסים העמוקים, או חגורות ההרים והמדבריות שבשולי הציביליזציות הידועות, מיפויו ומיסודו לטריטוריות מוגדרות ומשילות אינו תהליך סופי, שכן הוא משתנה, מתפתח ונע ללא הרף.

אם היו מי שסברו שניתן להפריד בין המרחב הוירטואלי לגיאוגרפיה המרחבית, באה לעולם תפיסת ה- **IOT** (**Internet of Things**), המגלמת חזון של רשתיות טכנולוגית מעשית יום-יומית. לפי חזון זה מכוניתנו תמצא לעצמה חניה מבעוד מועד באמצעות יישומון מבוסס רשת, ומכונת הכביסה שלנו תפעיל עצמה בעיתוי שפל בתעריף החשמל, וגם תזמין לעצמה חומרי כביסה בזמן. אך הפוטנציאלים רחבים ומשמעותיים מאשר תחומי הצריכה והנוחות האישית בלבד. למשל, שוו בדמיונכם עולם בו אדם מסוגל בלחיצת כפתור מצוקה לחבר את המכשיר הנייד שברשותו למוקד המשטרה, לרבות את שירותי הקול, הצילום והמיקום. האזרח הזה יוכל לא רק לקבל סיוע מהיר ואפקטיבי יותר בעת חירום, אלא גם להוות בעצמו גורם מתריע, ובהמשך גם מרתיע מפעילות פלילית בסביבתו, מעצם תפקודו כמצלמה משטרתית ניידת לעת מצוא[ii]. אמנם מדובר, מצד אחד, על הגברה משמעותית של נוכחות המושל (המשטרה), אך מהצד השני מתקיימת השתתפות והשפעה ישירה של האזרח במעשה המשילות. טשטוש גבולות.

השם "סייבר" (Cyber) הנגזר מהמילה היוונית "קיברנטיקה" (Cybernetics) משמעו נווט (או ליתר דיוק: "זה האוחז בהגה" - Helsman), ומכאן גם המילה העברית "קברניט". לשפה פרץ המונח במאה ה-19 על ידי פיסיקאי

[ii] מבוסס על רעיון טכנולוגי-תפיסתי שנמסר למשטרת ישראל.

צרפתי (Ampere) שהבחין בהיעדרו של תחום במדע העוסק בממשלות,[iii] ומאוחר יותר ב-1948 ע״י נ. וינר שייחס את המילה למדע העוסק בחקר העקרונות השולטים בהתנהגותן של מערכות – ובמיוחד תהליכי בקרה ותקשורת בתוכן.[iv]

הסייבר מוגדר, אם כן, כבר בעצם שמו, על ידי המתח שבין שליטה ומשילות – הקברניט, לבין תנועה ומורכבות – ניווט ומערכות מורכבות.

גיליון מספר שלוש של ״בין הקטבים״ לוקח אותנו למסע של התבוננות עצמית באמצעות חקירה משותפת של תופעת הסייבר. האם יש עתיד למוסד מדינת הלאום בעידן בו הגיאוגרפיה מאותגרת ומוגדרת מחדש? מהי המשמעות של מרחבי חתרנות ואנרכיזם בגיאוגרפיה החדשה שיצרה תופעת הרשת העולמית? האם נכון להבין בנפרד את תופעת הרשת הטכנולוגית האינטרנטית, תופעת הרשתות החברתיות שאנו חברים בהן, תופעת רשתות הטרור שאנו נלחמים בהן ותופעת רשתות השבטים-רעיונות-גיאוגרפיה (דאע״ש למשל) שהולכות ודוחקות את מוסד המדינה באזורנו? מה לכל זה ולמדינת ישראל? ולצה״ל?

למסע נצא באמצעות ארבעה כותבים:

**במאמר הראשון** עמית שיניאק, איש אגף התכנון בצה״ל, שחקר את הנושא מזווית ההסתכלות של מדעי-המדינה (במסגרת עבודת דוקטורט הנכתבת על ידו בימים אלה), מחפש ומוצא דפוסים היסטוריים חוזרים של איום על רעיון הריבונות המדינתית והסדר הבינלאומי והסרתו. המדינות, על-פי שיניאק, אותגרו תמיד על-ידי כוחות שפעלו בשולי הגיאוגרפיה הידועה. יכולתן של המדינות לשמר את ריבונותן היתה תוצאה של תהליך מתמשך, באמצעות מאמצים מאזנים כגון מיפוי כרטוגרפי והסדרה חוקתית המוזכרים במאמר בהקשר של המרחב הימי. על פי שיניאק צפוי, וגם רצוי, שהמדינות תסתגלנה לכך שהגיאוגרפיה הקיברנטית החדשה גם היא אתגר מתמשך, ותכרנה בתהליכים הדומים שכבר מתקיימים כדי לאזן אותו באמצעות מיפוי והסדרה – החלת חוקי המדינות והסדר הבינלאומי על המרחב הקיברנטי. מאמצים

[iii] ר׳ *קיברנטיקה*, אתר אינציקלופדיה בריטניקה.

[iv] יובל פורטוגלי, **מרחב זמן וחברה**, האונ׳ הפתוחה, ת״א.

אלה יש בהם כדי לישב, על פי הכותב, את המתח שבין מוסד המדינה לבין אופיו של התווך הקיברנטי.

**המאמר השני,** מאת מפקד קורס אפק לפיקוד ולמטה בצה"ל, שרון אפק, עומד על אתגרי הביטחון החדשים שמציב המרחב הקיברנטי בפני המדינות היום, מזווית המחקר המשפטית-חוקתית. אפק מעריך כי השנים הקרובות תהיינה מכוננות בתחום ההסדרה החוקתית הבינלאומית של הסייבר. אבחנה מעניינת נוספת שמעמיד המאמר היא העובדה שבעוד שכל המדינות מחייבות את החלת החוק הבינלאומי על מרחב הסייבר, לא כולן מסכימות לגבי מהות ערכי היסוד של החוק הזה. בעוד אחדות מהן רואות בחירויות הפרט ערך מוביל (המערב) אחרות רואות עדיפות לערכים של יציבות וריבונות (סין). זהו כמובן קושי עקרוני ובסיסי בתהליך ההסדרה החוקית של הסייבר. בין השורות ניתן להבין כי הסייבר מהווה זירה חדשה של התמודדות על סדר בינלאומי, התמודדות בה יש סיכוי חדש למעצמות מסדר שני ולמדינות קטנות יחסית לזכות בעוצמה יחסית גבוהה יותר מכפי שהיתה להם בעולם "הגיאוגרפי" הישן.

מאמריהם של אפק ושיניאק מאפשרים להיזכר באנלוגיה ההיסטורית של הפיראטים, ולהרהר לא רק באנרכיסטים הבוקאנירים שהקימו קהילות חופשיות עצמאיות באיים מרוחקים, אלא גם בפיראטים הפרייבטירים (Priveteers). אלה האחרונים היו שודדי ים ברישיון, שפעלו מטעם המדינות, אך תוך יכולת הכחשה. הידוע בהם, סר פרנסיס דרייק, פעל במאה ה-16, ותרם תרומה מכרעת להיחלשות האימפריה הספרדית ולעליית אנגליה כמעצמה. בתחילה עשה זאת דרייק באמצעות פגיעה בנתיבי המסחר הספרדיים באוקיינוס האטלנטי (שזה מקרוב ניפתח לשיט בזכות התקדמות טכנולוגיית הניווט), ושוד האוצרות שנשאו הספינות הספרדיות, ולבסוף באמצעות פיתוח עוצמה ימית שהפכה לצי האנגלי וניצחון על הארמדה הספרדית ב-1588.

במילים אחרות – החתירה תחת הסדר הבינלאומי הקיים אינה שמורה לאנרכיסטים בלבד. לצד האנרכיסטים, ולפעמים באמצעותם, מעצבות מחדש מדינות חלשות את יחסי העוצמה העולמיים לטובתן. בעידן בו ארה"ב

מאשימה את סין בריגול סייבר שיטתי לגניבת אוצרות הידע התעשייתי האמריקאי, ובימים בהם מתפרסמת מלחמת סייבר אפשרית בין ארה״ב לצפון קוריאה, לובשת האנלוגיה ההיסטורית משמעויות חדשות. הן מדינות קיימות והן ארגונים חתרניים, פועלים היום בסייבר למיצוי הפוטנציאל השיוויוני שלו ולשינוי יחסי הכוחות הבינלאומיים.

**המאמר השלישי,** שכתב ליאור לבד, עוזר מחקר במרכז דדו, בוחן את מרחב הסייבר באמצעות כלי הניתוח של תורת המערכות המורכבות. רק מי שמבין את הסייבר כתופעה מורכבת מסוגל להתמודד באפקטיביות עם הדינמיות העצומה המאפיינת אותו. לצורך ההמחשה דן לבד בתפיסות הגנה בסייבר, ולטענתו, היות ומימד ההגנה הוא המפותח ביותר (הן פרקטית, הן עיונית) הספיק מימד זה להתפתח מתפיסה פשוטה יחסית שעיקרה היה ״הגנה עמוקה״ (הדומה לשכבות ההגנה של העולם הצבאי) לתפיסה של הגנה קדמית, מניעה והתנגדות מקומית, הדומה יותר לאופן בו גוף האדם מתגונן מפני וירוסים. בהמשך, דן המאמר בתופעות של שליטה והשפעה במרחב – פרשיות ויקיליקס, אנונימוס, הדלפות סנודן ועוד, משמשות כדוגמאות לדיון במתח שבין חתרנות ואנרכיזם לבין ריבונות ומשילות במרחב הסייבר.

המסקנה העיקרית של הכותב היא שמורכבות מרחב הסייבר גוזרת מראש כישלון על המאמץ למשטר אותו ולשלוט בו. נדרשת פרקטיקה של הכלת מרחב הסייבר במרחב המדיני, ופיתוח דפוסי השפעה כאלטרנטיבה לשליטה ישירה. פרקטיקה כזו תאפשר לממסדים השונים להתמודד באופן נבון עם האתגרים הניצבים בפניהם, מבלי ״לשפוך את התינוק עם המים״.

**המאמר הרביעי**, פרי עטם של דניאל ברן, מפקד יחידת לוטם באגף התקשוב ויוסי לוי, מומחה לקולנוע ותקשורת המונית, מאפשר לנו התבוננות בעולם החדש והאמיץ של רשתיות טכנולוגית ואנושית באמצעות מקרה הבוחן של ארגון המדינה האסלאמית. הכותבים מצביעים על שלושת המימדים המקובלים בראיית העולם המערבי את מרחב הסייבר: מימד ההתקפה, מימד ההגנה ומימד האיסוף המודיעיני, וטוענים כי העיניים המערביות מפספסות (בגדול) את המימד האקוטי ביותר המאפיין את המרחב – מימד ההשפעה. באמצעות סקירה מקיפה על השימוש שעושה ארגון דאע״ש במרחב הסייבר,

מצביעים החוקרים על פוטנציאל ההשפעה הגלום במרחב זה, עליו עלה הארגון. באמצעות משחקי מחשב פופולאריים ושימוש בשפה דתית אפוקליפטית, פונים לוחמי הארגון אל לבו של המיעוט המוסלמי המפוזר בארצות המערב, וכך משיג תמיכה כלכלית, תמיכה אידיאולוגית וגיוס לוחמים חדשים. לטענת הכותבים, בהחמצה של המערב את מרכזיותו של היבט זה, גם אפקטיביות הקמפיין המתנהל כעת על ידי קואליציה של כוחות נגד המדינה האסלאמית, מוטלת בספק. טענתם היא כי היגיון התגובה המערבית תוקף את דאע"ש בדיוק במקום בו המערכת שלו צופה אותו, וכי "מלחמת דאע"ש" עלולה, בסופו של דבר, אף לחזק את הארגון והתמיכה בו במערב. בכך מצטרפים ברן ולוי לחוקרים שכבר הבחינו בפוטנציאל המהפכני של "גיוס המונים" קיברנטי, התשובה של המאה ה-21 להמצאת הגיוס הכללי של המהפכה הצרפתית[v].

מאמרם של ברן ולוי מאפשר גם עיון במפגש שבין הרעיון של רשת טכנולוגית-דיגיטאלית (www), הפוגשת את רעיון הרשת החברתית הוירטואלית (פייסבוק ודומותיה), שפוגש את רעיון הרשתיות הדתית-שבטית המסורתית (בו דנו גם בגיליון מס' 1). כל אלה מגדירים מחדש מרחב חתרני המוחק גבולות מוכרים בכרטוגרפיה הישנה (גבולות סייקס-פיקו) ויוצר מרחבים גיאוגרפיים חדשים - מרחב המדינה האסלאמית המתקיים במרחבים שונים ללא תלות ברציפות גיאוגרפית ביניהם.

הגיאוגרפיה הוירטואלית של הסייבר פוגשת, אם כן, את הגיאוגרפיה של היבשות. האם זהו הגילום האולטימטיבי של "האינטרנט של הדברים" (IOT) – גלישתו של מרחב הסייבר למרחב "החיים האמיתיים"?

הקורא, שאסף כלי עיון ודיון לאורך הגיליון, יוכל לשאול את עצמו שאלות נוספות על רקע מקרה הבוחן של ארגון המדינה האסלאמית. האם המדינה האסלאמית היא גלגול של הבוקאנירים האנרכיסטיים (ומכאן – זמניותה) או שמא היא התארגנות מדינתית חדשה המשנה את יחסי העוצמה האזוריים,

---

[v] כמו שהרחיבה בעניין אודרי קרונין בחיבורה מ – 2006.
Audrey Kurth Cronin, **Cyber-Mobilization, The New Levee en Mass**, 2006. spgia.gmu.edu

כמו המלכה אליזבת ופרנסיס דרייק במאה ה-16, האם אלה באמת, גם בימינו, שני מודלים נפרדים? האם יתכן שהאנרכיזם בן זמננו, שמייצגים (במידות שונות) אנונימוס וויקיליקס משרת גם, במודע או שלא במודע, גופים חתרניים מוכרים (צפון קוריאה, הג׳יהאד העולמי)?

מה משמעות התופעות שנסקרו כאן למושג אסטרטגיה במאה ה-21? כיצד מדינה כמו ישראל צריכה לנהוג ״בעולם החדש והאמיץ״ הזה? האם, כמי שחולקים את ערכי מדינת הלאום והסדר הבינלאומי, עלינו להצטרף למאמץ למשטר ולמסד את העולם הקיברנטי ולהחיל עליו את הסדר הקיים? אולי, כמדינה קטנה, עלינו למצות את ההזדמנות שמאפשר לנו הסייבר לעוצמה ״שוויונית״, שחורגת מהפרופורציות הטבעיות של מדינת ישראל? מכיוון שמדינת ישראל כבר זכתה להכרה כמעצמת סייבר, כיצד משמרים יתרון כזה בעולם כל כך דינמי? כיצד היתרון הישראלי כמעצמת סייבר עשוי לשרת אותנו בהתמודדות עם תופעות רשתיות כמו המימדים הקיברנטיים של הג׳יהאד העולמי בכלל והמדינה האסלאמית בפרט?

שאלות אלה ועוד, כולן ממשפחת ״הסייבר ואנחנו״, שנותרות בחלל, דורשות מאיתנו המשך חשיבה, עיבוד ופעולה.

ומי בצה״ל מוביל דיון זה?

בברכת קריאה מהנה ופורייה,

אלוף משנה ערן אורטל
ר׳ צוות חשיבה

# תוכן העניינים


| | | |
|---|---|---|
| עמית שיניאק | **התהוות המדינה במרחב הספר המקוון: השוואה תיאורטית והיסטורית** | 13 |
| שרון אפק | **שוברים את הכללים וכולם משחקים - על המפגש בין המרחב הקיברנטי לבין כללי המשפט הבינלאומי** | 45 |
| ליאור לבד | **מבוכו של המינוטאור או: פרדוקס הסייבר – עיון מערכתי באתגרים ובהזדמנויות של המרחב המקוון** | 77 |
| דניאל ברן ויוסי לוי | **תופעת המדינה האסלאמית – מה המערב לא מבין?** | 111 |

# התהוות המדינה במרחב הספר המקוון: השוואה תיאורטית והיסטורית

**עמית שיניאק**[i]

## מבוא

"On the Internet, nobody knows you're a dog"[1]

האם האינטרנט הוא המקום החדש המאפשר לנו להסתתר מאחורי המחשב מבלי שיגלו אותנו? האם זו תופעה חסרת תקדים המותירה את המדינה במבוכה? עצם ההתייחסות לרשת תקשורת ממוחשבת כאל מרחב מקוון (סייבר -Cyberspace),[ii] מעידה כשלעצמה כי האינטרנט כה נוכח בחיי היומיום המודרניים, עד שנתפתח לו תדמית ציבורית שיש המזהים אותה באופן אוטופי ככרוכה בערכים ליבראליים כגון חירות, שוויון וקידמה, או מנגד עם ערכים אנרכיים כגון היעדר שליטה, אנטי ממסדיות, טרוריזם ואינדיבידואליזם קיצוני. במסגרת מאמר זה, אני שואף לבחון את התדמית של האינטרנט כמרחב (מרחב מקוון), ואת ההנחה הסמויה הקיימת בקרב ציבורים רבים כי מדובר במרחב שאין למדינה ולממסד המדיני והביטחוני שליטה בו. שאלת המחקר העומדת בבסיסו של המאמר, היא האם ניתן להשוות בין התהליכים ההיסטוריים ליצירת ואכיפת הריבונות המדינית הביטחונית במרחבים הפיזיים (ים, אוויר ויבשה), לבין תהליכים אלו במרחב המקוון? לשאלה זו, שבוחנת את הניסיון המדיני ההיסטורי, השלכות נרחבות

---

[i] **רב-סרן עמית שיניאק משרת כראש מדור במחלקת שיתוף פעולה צבאי בינלאומי באגף התכנון.** עמית מסיים בימים אלה את עבודת הדוקטורט אותה הוא כותב במסגרת המחלקה למדע המדינה באוניברסיטה העברית בנושא "המרחב המקוון כאזור גבול: תהליך יצירת הריבונות ויכולת האכיפה במרחב המקוון בישראל, ארה"ב וסין", תחת הנחייתם של פרופ' אורן ברק ופרופ' ירון אזרחי. חלקים מעבודה זו מופיעים במאמר.

[ii] למרות שבחלק מהפרסומים בעברית מתורגם המונח"Cyberspace" למונח "מרחב קיברנטי" או "סייבר", במאמר זה אשתמש במונח "מרחב מקוון" כתרגום מדויק ונכון יותר בשפה העברית לאותו מונח באנגלית. יש לציין כי המושג "אינטרנט" תורגם רק לאחרונה למושג העברי החדש "מרשתת". משום שהשימוש במושג זה עדיין אינו רווח לא אעשה בו שימוש במאמר.

לגבי מדינאים, פקידי ממשל ואנשי צבא בבואם לקבוע מדיניות ומעשה במרחב המקוון.

ההשערה המרכזית שתיבחן היא כי ניתן למצוא קווים תיאורטיים מסוימים מקבילים בין תהליכי ההתפתחות, המיסוד ואכיפת מוסד הריבונות של המדינה במרחב המקוון ובין "אזורי ספר" אחרים. במילים אחרות, יכולת השליטה והאכיפה של המדינה במרחב זה דומה ליכולות שהיא הפגינה בעבר כלפי מרחבים "חדשים" אחרים בשלבי התפתחות דומים. המרחב המקוון יבחן אפוא כ"אזור גבול" (border zone), או כ"סְפָר", ותיערך השוואה בינו ובין ראשית החלת הריבונות במרחב הימי, כדוגמא לתקופה שבה ריבונות המדינה התקיימה באופן עמום במרחב אחר. לפיכך, מטרתו העיקרית של המאמר היא לבאר ולבסס את התשתית המושגית והתיאורטית, ולספק דוגמאות היסטוריות שיאפשרו ניתוח וקביעת מדיניות ביטחון של המדינה במרחב המקוון. זאת ועוד, מאז העלייה במרכזיות העיסוק במרחב המקוון במערכות הביטחון, נראה כי ישנו חסר מתמשך בתשתית סדורה והיסטורית שימושית לצורך תכנון מדיניות אסטרטגית, וישנה נטייה לטפל בסוגיה זו מתוך ראיה צרה שניתן לתאר אותה כטקטית או מודיעינית בלבד.

בניסיון לבסס את ההשערה שניתן ללמוד מהאינטראקציה ההיסטורית של המדינה במרחבים אחרים לבין המרחב המקוון, יחולק המאמר באופן הבא: הצגת המושגים התיאורטיים הנדרשים לניתוח האינטרנט (מרחב מקוון, ריבונות, גלובליזציה); הצגת התהליך ההיסטורי של התהוות המדינה; השוואת התנהלות המדינות במרחב הימי ובמרחב המקוון באמצעות ניתוח תהליך בניין המדינה במרחבים אלו בדגש למהלכי המיפוי והתיחום הטריטוריאלי ואכיפת המונופול המדיני על האלימות המאורגנת.

## א. מושג הריבונות המאותגרת והמרחב המקוון

היות ומאמר זה בוחן את האינטראקציה שבין המרחב המקוון לבין פעולתה של המדינה לצורך החלת ריבונותה הביטחונית וביסוס יכולת האכיפה, מובלעת בו הנחה סמויה שהמרחב המקוון מאתגר את המדינה. אתגר זה נובע מטבעו הבינלאומי של המרחב המקוון, המציב קשיים לאכיפת הסדר המדיני

הטריטוריאלי, לשלטון החוק ולהחלת נורמות בינלאומיות והמשפט הבינלאומי. תופעת השחיקה בריבונות המדינה היא תופעה מורכבת יותר מכפי שמתואר בחלק מהמחקרים המנתחים תופעות עדכניות התורמות למצב זה. מצד אחד, הגלובליזציה מהווה דוגמא עכשווית לאתגרים השוחקים את מוסד הריבונות, תופעות כגון ארגונים בינלאומיים (IO), ארגונים בינלאומיים לא ממשלתיים (NGO) והמרחב המקוון, מלבים את הפולמוס על עתידה של המדינה כישות הפוליטית הממוסדת המובילה במערכת הבינלאומית והאזורית היום[2]. מצד שני, מחקרים היסטוריים רבים מעידים כי אתגרים משמעותיים לריבונות המדינית כבר היו קיימים בעבר וישויות פוליטית חלופיות לסדר הריבוני המדיני שהתקיימו במקביל לריבונות המדינית, אך כשלו ביכולתם להחליפה[3]. בין הדוגמאות ניתן למנות אימפריות אזוריות ואתניות[4], ארגונים דתיים[5], איגודי סחר בינלאומיים וגילדות מקצועיות[6], יזמי אלימות עצמאיים כגון: פיראטים[7], שכירי חרב וחברות צבא פרטיות[8], ארגוני פשע[9], וארגוני טרור[10].

נוכח אתגרים אלה, ניתן לומר כי המערכת הריבונית המדינית שרדה, במיוחד במובן בו היא מקיימת המשכיות בלגיטימציה לריבונות טריטוריאלית ומונופול על הפעלת אלימות מאורגנת[11]. שרידותה של המדינה היא תוצר של מהלכים שנועדו לשמר את המונופול הריבוני. מהלכים אלו מעידים כי הריבונות המדינית היא סטאטוס יחסי שמושג בתוך מערכת של תשומות (לחצים, אתגרים והזדמנויות) פנימיות וחיצוניות, ומכאן שמושג הריבונות מבטא מצב סובייקטיבי תמידי של מאבק למול אתגרים - בין אם חברתיים או טכנולוגיים. לפיכך, מתקיימת המדינה באופן תדיר במצב של חיכוך ומשא ומתן מול גורמים, גופים, מוסדות ויחידים שונים המאתגרים אותה.

**הִסָּפֶר כביטוי למרחב בלתי נשלט**

הספר, או "אזור ספר", הינו מושג הניתן לפרשנויות שונות ומגוונות. ככאלה, נוח להגדירו באופן לעומתי מול המושג המוכר והרווח "גבול". מונחים אלו מהעולם הפיסי משמעותיים להבנת האינטראקציה של המדינה במרחב המקוון למרות היותו ווירטואלי. פירושו המילולי הלועזי של המונח סְפָר הוא

"גבול קדמי" (Front - Frontier) והוא מתייחס למרחבה הקדמי של מדינה (קדמי במובן של מרחק מהעורף או מהמרכז). לעומתו, המשמעות הלועזית של המונח גבול היא מכיל/מגביל (Bound - Boundary) והוא מתייחס למשמעות של תיחום המדינה הריבונית שהיא בעלת ריבונות משפטית בתוך טריטוריה מתוחמת[12]. המאפיינים של אזורים אלו שונים בהתאמה[13]:

אזור הספר הוא צנטריפוגלי/מכוון החוצה (Outer Oriented), הוא תופעה היסטורית חברתית עמומה וקשה להגדרה חד משמעית, המיועדת להוות בלם זעזועי למדינה ובו זמנית לשמש כאינטגרטור בין-תרבותי וכקטליזטור כלכלי. בדומה למונח "גבול רך", זהו מרחב המיועד לחצייה, בעל קיום משלו המוביל לכך שלמרות שהוא משויך ומזוהה עם מדינה מסוימת, הגורמים המעורבים בו הם בעלי אינטרס עצמאי שאינו חופף תמיד למדיניות של המרכז הפוליטי. כתופעה היסטורית, מושג הספר מזוהה עם קיומן של אימפריות בעלות גבול ארוך ורחב כגון רומא או סין[14], אך גם עם מדינות מודרניות יותר כגון ארה"ב.

הגבול, בניגוד לאזור הספר, הוא מושג בעל מהות המכוונת פנימה (Inner Oriented). הגבול הוא בדרך כלל ברור וקל לזיהוי (פיזית, חברתית ומנטאלית) ומהווה סמל להחלטות מדיניות טריטוריאליות המשקפות את גבולות השליטה האפקטיבית ואת הגבול הבינלאומי המוכר. מטרתו של הגבול היא לתחום את הקהילה הפוליטית, הוא אינו מיועד לחצייה אלא מהווה חסם ומשמש כאלמנט מפריד, ולכן הוא ביטוי של מדיניות הממשלה ו/או הממסד הפוליטי ומעוגן פורמאלית בחוק הבינלאומי. לכן, מהותו משתנה בהתאם למהות הפוליטית של המדינה והיא סובייקטיבית ותלוית הקשר חברתי פוליטי[15]. ישנה נטייה לראות הפרדה ברורה בין מצב הגבול למצב הספר, אך לאור תופעת הגלובליזציה ומהפכת המידע המדגישה את ההשפעה ההדדית שבין הפוטנציאל הכלכלי והחברתי הגלום ב"פתיחות" של אזור הספר (כמו גם את הסכנות הנובעות מפתיחות זו), גובר האינטרס של המדינה להגן על פוטנציאל זה ולהגדיר אותו כשייך לה ולנסות לייצר פתיחות בעלת בקרה גבוהה יותר[16]. בהמשך אדגים כיצד התנהלות המדינה בגבול היא כלי יעיל להבנת התנהלותה במרחב המקוון.

**המרחב המקוון: בין טכנולוגיה לתופעה חברתית**

המרחב המקוון, יוצג במאמר זה כמרחב חדש שהפך נגיש לאינטראקציה חברתית פוליטית ומדינית לאור התפתחויות טכנולוגיות והוא גם מהווה אתגר לריבונות המדינה. את המושג "מרחב מקוון" (Cyberspace) הגה וביאר הסופר ויליאם גיבסון (Gibson) במסגרת רומן בדיוני ידוע שפורסם ב-1984 בשם *Neuromancer*.[iii] העובדה שמקורו של המושג הוא בז'אנר הספרות הבדיונית, היא אולי אחת הסיבות לריבוי הפרשנויות למושג זה, ולקושי הקיים בקרב חוקרים, בירוקרטים ומדינאים לפרש אותו כבעל משמעות יישימה ובת השוואה למרחבים "פיזיים" כגון המרחב הימי. ביטוי מרכזי למחלוקת באשר לשאלה האם יש להשוות את המרחב המקוון למרחבים פיזיים, הוא בהבדלים שבין שתי קבוצות של ההגדרות המקובלות למושג ה"מרחב המקוון": ההגדרה הטכנית, שנתגבשה על בסיס הפיתוח הטכנולוגי של האינטרנט בקרב מומחי מחשבים ומשפטנים המתמחים בטכנולוגיה; וההגדרה החברתית - מרחבית, שנתגבשה לראשונה על ידי גיבסון ופותחה על ידי שורה של סופרי מדע בדיוני.

גיבסון, שהגה את המושג "מרחב מקוון" בראשית ימי המחשב הביתי והתקשורת מתווכת המחשב, ועוד בטרם פיתוחה של האינטרנט והתבססותם של יישומים כגון "הרשת העולמית הרחבה" (WWW), מבסס את ההגדרה החברתית - מרחבית באמצעות תיאורו את המרחב המקוון כביטוי גראפי של מטריקס (Matrix) מתמטי, המייצר חוויה חזותית ומקיפה, בקרב משתמשי מחשב שונים[17]. ההתייחסות של גיבסון למרחב המקוון, הוא כתופעה המאתגרת את כל המרכז החושי (Sensorium) של המוח, כפי שעולה מ"ההגדרה הספרותית" למושג "מרחב מקוון":

"A graphic representation of data abstracted from banks of every computer in the human system"[18].

[iii] לפרסום הספר קדם סיפור קצר שפורסם ב- 1982 בשם "Chrome Burning" בו הוזכר המונח לראשונה.

התייחסות של גיבסון לאינטרנט כאל מרחב (Space), נובעת מהחזון שלו על אודות היקף ההשפעה של רשתות מחשבים על בני האדם המשתמשים בהן, עד לכדי התחושה הקיימת בקרב ציבורים רבים היום של מרחב חדש ושל מציאות מדומה. ההגדרה "המרחבית" הזו עושה שימוש במטפורות גיאוגרפיות וחברתיות כדי לתאר את האינטרנט כמרחב המכיל בתוכו את כלל האפשרויות הגלומות באינטראקציה האנושית: רגש, אמונה, יחסי שיתוף פעולה, מלחמה טרור וכדומה. בעיניו, המשתתפים אינם "מִתקשרים", כפי שמתארים שיחה בטלפון, או "צופים" באופן פאסיבי, כפי שמתארים צפייה בטלביזיה. מי שעושה שימוש באינטרנט מקיים על פי הגדרה או גישה זו וכפי שרווח בהתייחסות הציבורית בימינו, אינטראקציה דומה לזו שבין בני אדם למרחב פיזי. לכן המשתמש "גולש", "נמצא ב..", "נכנס" או "יוצא" מבחינה מטאפורית מהמרחב המקוון. ההגדרה המרחבית היא זו המאפשרת לשוות את האינטרקציה החברתית במרחב המקוון, מבחינה מדינית וביטחונית למרחבים פיסיים אחרים.

לעומת ההגדרה המרחבית של גיבסון, ההגדרה המקובלת בחלק גדול מהספרות המחקרית, המשפטית מסמכי מדיניות וחקיקה, מתאפיינת בתיאור "טכני" של האינטרנט ומסתמכת על מונחים מקצועיים של מומחי מחשבים, המתמקדים בתיאור ההמצאה הטכנולוגית ולא במשמעויות הגלומות בה. כפי שעולה מהגדרתו של למלי:

"The internet is merely a simple computer protocol, a piece of code that permits computer users to transmit data between their computers using existing communications networks" [19].

ההגדרה הטכנית מבצעת הקבלה בין התיאור הטכני של המושג "אינטרנט", כיישום של תקשורת מתווכת מחשב, העושה שימוש בטכנולוגיות מידע ומבחינה מעשית מתקיימת במסגרת רשת המחשבים העולמית הרווחת היום (www), מצד אחד, לבין המונח "מרחב מקוון", הנתפס ככינוי או כמטפורה בלבד לאינטראקציה המתקיימת ברשת מחשבים, מצד שני. ההקבלה, מתבססת על דרך הפעולה של תקשורת המתווכת באמצעות מחשב (CMC),

המתייחסת בדרך כלל לתקשורת בין "יחידות מארחות" (Hosts). יחידות אלו, מוגדרות כחומרת מחשבים המחוברת לאינטרנט, בעוד שכל נקודת קצה (Node) נספרת כיחידה נוספת בפריסת הרשת[20]. חדשנותו של האינטרנט נובעת מהיותו רשת תקשורת המחברת רשתות מחשב פנימיות (Intranet) שכבר היו קיימות, באמצעות יישום של פיתוח טכנולוגי המאפשר העברה יעילה ומבוזרת של מידע אלקטרוני המכונה "מערך מיתוג מנות"[iv]. מערך זה מאפשר יַתִּירוּת לאחר תקיפה ופגיעה חלקית[21].

בין אלו המפרשים את האינטרנט כהתפתחות טכנולוגית תקשורתית גרידא, קיימים אלו הסוברים כי היא אינה יכולה להביא לשינוי משמעותי מעבר להשפעות המוכרות של אמצעי התקשורת המודרניים[22]. הסתירות הקיימות בין חקיקה ותוכניות מדיניות המסתמכות על תפיסה טכנית את האינטרנט, לבין התפיסה הציבורית המרחבית את המרחב המקוון הן אחת מבעיות היסוד המקשות על קידום מדיניות מקובלת ודינים בינלאומיים אחידים. לעומת זאת, בשנים האחרונות מעידות הגדרות למרחב המקוון במסמכים רשמיים עדכניים, אותם אני מאמץ לצורך מאמר זה, על הכרה במהותו הטכנית של המרחב המקוון אך גם על הצורך לפעול למולו כאל מרחב בעל השלכות חברתיות פוליטיות וביטחוניות מורכבות. כך למשל החלטת ממשלת ישראל 3611 על "קידום היכולת הלאומית במרחב הקיברנטי" מאוגוסט 2011 מגדירה את "המרחב הקיברנטי" כ: "מתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה"[23].

[iv] "מערך מיתוג מנות" נועד לאפשר שרידות של רשתות על ידי ביזור שליחת המידע באמצעות תהליך שבו "המסר הנשלח מחולק למנות. כל מתג מזהה את היעד הסופי של המסר, אבל מפצל אותו כך שכול מנה מועברת בנפרד בציר פנוי. המסר מאוחד שוב כאשר המערכת מאתרת את הגעתו של המסר לנקודת היעד". להרחבה ראו: ת. אשורי, **מהטלגרף עד המחשב: היסטוריה של אמצעי התקשורת**, (תל אביב: רסלינג, 2011), עמ' 134.

## ב. כיצד מדינות מתהוות במרחב?

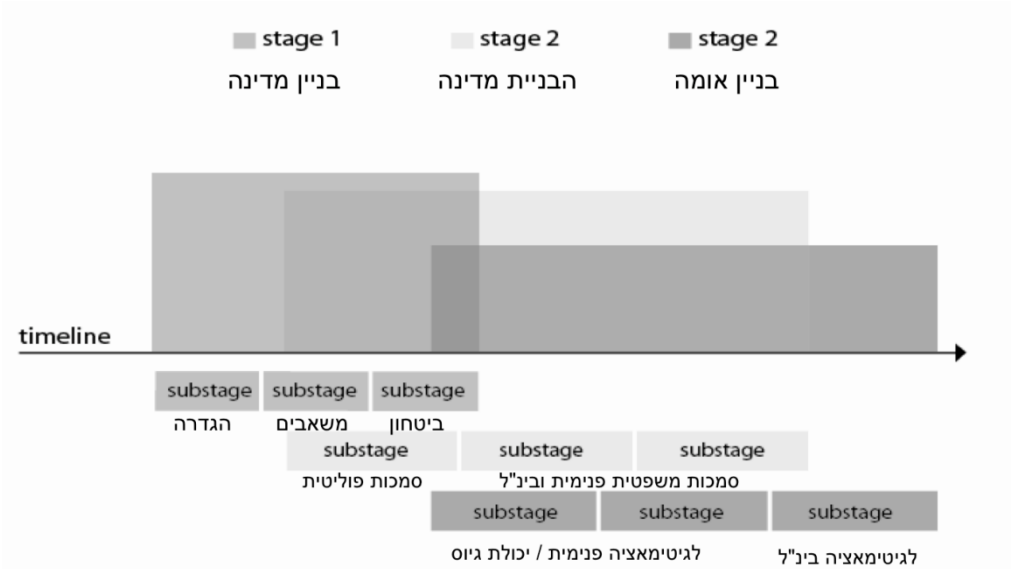
את התהליך המדיני להתמודדות עם תופעות השוחקות את ריבונותה של המדינה, ניתן לחלק לשלוש: 1) בניין המדינה (State Building) תוך התייחסות למהלכי תיחום הטריטוריה ויצירת יכולת האכיפה; 2) הבניית המדינה (State Construction), תוך התייחסות לביסוס הסמכות המשפטית המדינית והבינלאומית; 3) בניין האומה המכונה גם תהליך האינטגרציה הלאומית (Nation Building / National Integration), תוך התייחסות ליצירת הלגיטימציה הפנימית והבינלאומית.

**בניין המדינה** הוא התהליך המתאר את התהוות המימד הפיזי התשתיתי של המדינה ביחס למרחב בו היא מתקיימת, קרי הגדרה (טריטוריה, אוכלוסייה), ניצול ההון (משאבים וניהול כלכלי) והקניית ביטחון (מונופול על אמצעי הכפייה); **הבניית המדינה** הוא התהליך המתאר את התהוות המימד החברתי- מוסדי של המדינה, קרי המוסדות הפוליטיים שבהם עושה המדינה שימוש בכדי לשלוט במימד הפיזי בדגש לאמצעים הסימבוליים והנורמטיביים העומדים לרשותה (מוסד החקיקה, מערכת המשפט, התקשורת הרשמית, מערכת החינוך ועוד); **בניין האומה**, מתאר את תהליך התהוות המימד הערכי/ אידיאולוגי במדינה, המהווה תוצר של אינטגרציה לאומית בין החברה / אוכלוסייה בטריטוריה מוגדרת לבין הממסד המדיני. השילוב בין שלושת המרכיבים, מספק יכולת לפשט את התיאוריה לכדי תבחינים שבאמצעותם ניתן לבדוק את מקרי הבוחן ולאתר "עדויות" לתהליכים של ביסוס הריבונות ו/או שחיקה בריבונות[24].

כפי שממחיש תרשים מס' 1, התהליכים השונים משקפים שתי תנועות מנוגדות כביכול: הם משיקים זה לזה ויכולים להתקיים במקביל (גם אם תהליך אחד לא נסתיים)[25], אך גם משקפים סדרתיות, קרי שאין אפשרות שהתהליך השני יתקיים לפני הראשון. כך לדוגמא, הריבונות המדינית מתבטאת בהקמת מוסדות (ביטחון, משפט, כלכלה וכדומה); המוסדות מבוססים על סמכות; הסמכות מבוססת על לגיטימאציה שמשמעותה

הסכמה חברתית הרגישה להקשר[26]; ההקשר יכול במידה רבה להיות לאומיות.

**תרשים 1: תהליך ביסוס מוסד הריבונות בחלוקה לשלושה תהליכים החופפים בחלקם**




מאמר זה, כאמור, מתייחס רק לפן הביטחוני של הריבונות וביחסה של המדינה אל מרחבים חדשים כ"אזור גבול" או "ספר", מתוך ההנחה שתהליך ביסוס יכולת הכפייה במרחב (הפיזי והווירטואלי), הוא הבסיס לשורה של תהליכי משנה משמעותיים כגון: תיאור ביסוס הסמכות הפוליטית של המדינה; בניית יכולת המיסוי את הפעולות הכלכליות המתרחשות במרחב המקוון; ומהלכי המדינה למנוע פעילות לא רצויה ואף פלילית שאינה בגדר הפעלת אלימות, כגון הפרת זכויות יוצרים, צנזורה וחופש הביטוי, מימון פוליטי ושחיתות. לצורך המחשת הדמיון הרב בין סיפור התמודדותן של מדינות בעבר עם היפתחות המרחב הימי לבין המהלכים שבהן נוקטות

מדינות היום במרחב המקוון, אנתח במאמר רק את תהליך בניין המדינה תוך התמקדות במהלכים למיפוי ותיחום טריטוריאלי ולאכיפת המונופול המדיני על המרחב המקוון.

## ג. השוואה בין תהליך בניין המדינה: במרחב הימי ובמרחב המקוון

### כלכלה ביטחון וטריטוריה

תהליך בניין המדינה, מוגדר כצעדים המעודדים "גיבוש טריטוריאלי, צנטרליזציה, דיפרנציאציה של אמצעי הממשל, והשגת מונופול על אמצעי הכפייה"[27]. לפיכך, הוא מתקשר להיבטים החומריים או ה"גיאופוליטיים" של המדינה: טריטוריה, אוכלוסיה, משאבים וביטחון (פיזי)[28], ועוסק בתיאור תהליך של הקמה פיתוח, מיסוד תשתיות ו"חלוקת עבודה" במרחב בו המדינה מוקמת או שאליו היא מתרחבת. ניתן להגדיר היבטים אלו כביטויים לפן המכונן בריבונות, משום שהם מבססים את רכיבי היסוד המאפשרים למדינה באמצעות מוסד הריבונות, לפעול אחר כך לכינון תהליכי הבנייה חברתית וערכית, ולכן יש צורך בקיומו של תהליך זה טרם תהליכי הבניית המדינה ובניין האומה. לפיכך, שלושת תהליכי המשנה הבסיסיים המרכיבים יחד את תהליך בניין המדינה הם: ההגדרה והתיחום, המתבטאים בשני תהליכים מקבילים התלויים זה בזה, הגדרת הטריטוריה של המדינה או הישות הריבונית, וההסכמה על ההגדרה מי היא (ולכן גם מי אינה) האוכלוסייה המשוייכת לאותה טריטוריה; הביטחון, המושג באמצעות תהליכים של יצירת שליטה מוחלטת (Domination) / מונופול על אמצעי הכפייה ויכולת גיוס משאבים למניעת איומים חיצוניים ; ההון, המושג באמצעות תהליכים של צבירת משאבים חומריים וניצול שירותים, לצד התפתחות תהליכים של ניהול כלכלי. במאמר אתייחס, כאמור, רק לשני התהליכים הראשונים.

### טריטוריה: הגדרה, תיחום ושמירה על שלמות טריטוריאלית

תחום מרכזי בתהליך בניין המדינה, שהוא הביטוי הראשוני לשרידות בזמן ומרחב, הוא ההגדרה והתיחום של הטריטוריה והאוכלוסייה. הנחת המוצא

היא שהאלמנט המכונן הבסיסי ביותר הוא תהליך התיחום, הן של הטריטוריה והן של האוכלוסייה[v], שמוביל לקיבוע בזמן ובמרחב. רק לאחר השלמתו ושרידותו לאורך זמן, מבחינה פנימית ובינלאומית כאחד, קיימת למדינה העצמאות הריבונית לנצל את המשאבים ולבסס את המונופול על אמצעי הכפייה לצורך החלת הביטחון[29]. הנחה זו מתבססת על התהליך ההיסטורי של התפתחות המדינה המודרנית, בדגש לגיבוש הסדר הריבוני באירופה, שהתבטא במעבר מריבונות הטרמונית לריבונות טריטוריאלית המוגדרת כבידול יחידות טריטוריאליות מבחינה משפטית לעצמאות שיפוטית וערכית[30]. הסכם ווסטפליה מ- 1648 שסיים את מלחמת 30 השנים באירופה, שמשמעותו היא ההכרה בעצמאות הריבונית והשיפוטית של מדינות בטריטוריה המוגדרת להן, מצוין במחקרים רבים כאקט הסיום של תהליך זה או כמהלך פורמאלי בעל המשמעות הסימבולית ביותר[31].

מבחינה פרקטית, כלל הפעולות הריבוניות מתבססות על ההגדרה הטריטוריאלית, שמהווה את מערכת הכללים הראשונית שבאמצעותה המדינה פועלת ושבאמצעותה יש ביכולתה להחיל מדיניות והסדרים פוליטיים. מבחינה בינלאומית, רק באמצעות הכינון של מערכת של מדינות בעלות ריבונות עצמאית בטריטוריה מוגדרת, יכולה המדינה לייצר לעצמה את ההפרדה בין המערכת הבינלאומית לבין המערכת הפנים מדינתית וכתוצאה מכך לבסס תשתית לחקיקה וקבלת החלטות פנימית[32]. לכן, השאיפה של המדינה למונופול על אמצעי הכפייה מחייבת קודם כול את הגדרת הטריטוריה עוד לפני הרחבת המונופול לאלימות חוץ מדינתית[33]. לאחר תיחום הטריטוריה, השמירה על השלמות הטריטוריאלית היא האלמנט המכונן את המערכת הבינלאומית המודרנית מהמאה ה- 17[34], ובמיוחד במאות ה- 19 וה - 20 שהתבססה על מערכת של מדינות לאום והדגישה את משמעותה בעקרונות היסוד למוסדות הממשלתיים הבינלאומיים המרכזיים ביותר[35]. מגילת האו״ם מדגישה זאת[36]:

[v] אין בהכרח הקדמה של תיחום הטריטוריה לתיחום אוכלוסיה, ישנן דוגמאות היסטוריות לשני המקרים, המתבטאים למשל בתהליך השונה שבין מדינות לאום (קהילה קודמת להגדרה טריטוריאלית) למדינות הגירה (טריטוריה קודמת להגדרת האוכלוסייה).

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state"

מכיוון שמאמר זה עוסק ביחסים שבין מדינה ובין מרחב חדש המהווה אתגר לריבונות שלה, המנגנונים שמפעילה המדינה לצורך תיחום טריטוריאלי, דהיינו מהלכים של התפשטות והצטמצמות טריטוריאליים, הם משמעותיים להבנתם. יש לכך ביטוי במשפט הבינלאומי, בכללים ביחס לשינוי בהגדרות הטריטוריאליות של מדינות, המתבססות על תפיסת הטריטוריה כקניין של המדינה[37]. המשפט הבינלאומי מתייחס פורמאלית לחמש אפשרויות ("חוקיות") להרחבת הטריטוריה של מדינות המבוססים על פסקי דין תקדימיים: גילוי וכיבוש, ניצול, סיפוח, ירושה וצבירה[38]. תהליך המיפוי שתואר קודם לכן הוא ביטוי משמעותי למהלכים אלו, בדגש לצורך של מדינות להגיע להסכמה על שיטת המיפוי ועל תקופתה של "שפה גיאוגרפית משותפת" שרק באמצעותה ניתן לקיים סחר בינלאומי.

שאלה שכיחה בקרב מחקרים העוסקים במרחב המקוון, היא כיצד ניתן להתמקד בתהליכי התרחבות והצטמצמות, תיחום וסימון טריטוריאליים במרחב ווירטואלי? שאלה משמעותית זו, היא הסיבה לתהיות אודות סמכות השיפוט של המדינה במרחב המקוון[39]. הרלבנטיות לשאלה זו עולה בהקשר של תופעת הגלובליזציה המבטאת, לכאורה, שחיקה בריבונות המדינה ובמיוחד במשמעות של גבולותיה. התשובה לשאלה זו מתבססת על ההנחה כי מנגנוני ההתפשטות וההתרחבות של המדינה אל מרחבים חדשים נעשים בהיגיון של העתקת ריבונות טריטוריאלית, למשל באמצעות מיפוי וקביעת גבולות.

**גיבוש הגבולות במרחב הפיסי ובמרחב המקוון - תהליך המיפוי**

תהליך המיפוי ינותח כדוגמא ליכולתה של המדינה למסד ולעגן את תפיסתה על המרחב בו היא שולטת, או למרחב אליו היא מתרחבת, וכדוגמא ינותח תהליך המיפוי של המרחב הימי. המיפוי הוא ביטוי ליצירת סדר מוסדי על ידי מדינות, כתוצאה מנגישות חדשה למרחב בעקבות התפתחות טכנולוגית

המאפשרת לשוטט בו, למפות אותו, ובכך להנגישו ולהחיל עליו את החלוקה הגיאו אסטרטגית והפוליטית הקיימת. מתוך כך, לעתים, בשל תחרות וחוסר הסכמה פוליטיים, נובע גם שיש אלו שאינם מקבלים את הסדר הטריטוריאלי החדש שנוצר ועל המדינה המחילה את מיפויה החדש ישנה האחריות לאכוף אותו.

חשוב לציין את ההבחנה בין שלוש רמות או שלבים בתהליך ההבניה המרחבית אותה מבצעת המדינה במרחב חדש[40]: ראשית, גישה "צרה" לניתוח התנהלות המדינה, המתמקדת בתיאור של מהלכי מדיניות הנוגעים בהגדרת הטריטוריה באמצעות קביעת גבולות המדינה, באמצעים משפטיים כגון חקיקה, ואמצעים מוסדיים כגון הקמה ושינוי של מוסדות (למשל, חקיקת חוק פרלמנטארי לסיפוח שטח מסוים); שנית, גישה אינטגרלית, מתייחסת למשמעויות המוסדיות של תהליכי הטריטוריאליזציה הגוררים שינוי תודעתי בהתנהלות מוסדות המדינה והפנמת ה"מיקום" שלה במרחב. השינוי בא לידי ביטוי, ביכולת לגייס משאבים, להניע מהלכים כלכליים, ולייצר אמת מידה (Scale) לפעולותיה של המדינה (למשל, הנחת קווי מסילת ברזל וחיבורו של המרחב החדש הפריפריאלי בדרך כלל, למרכז); ושלישית, הגישה הייצוגית (Representational), המתייחסת למימד האידיאי, המדומיין, המיוחס למרחב החדש ולגבולות המדומיינים (למשל, הנפקת בול ממשלתי רשמי בו ישנה התייחסות למרחב החדש שסופח). גישה זו, מתייחסת גם להשלכות של מימד זה על התנהלות פוליטית פנים מדינית ובינלאומית ביחס לטריטוריות קיימות וחדשות (כולל מלחמה).

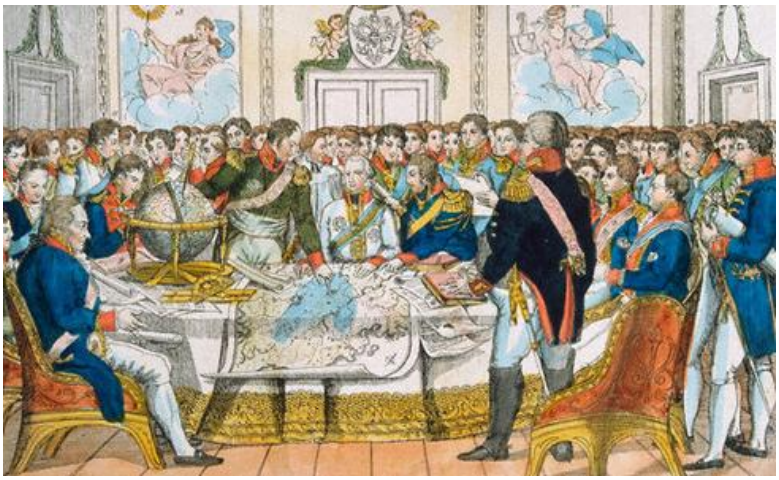
מצד אחד, שימור דפוסי הארגון המרחבי של המדינה במרחבים חדשים, תורם ליכולת לנצל אותם באופן מיטבי מבחינה כלכלית, ומצד שני הארגון של הסדר המרחבי מוגבל ולכן מדינות נדרשות לשכפל את עצמן למרחבים חדשים[41]. וכך, לצד השפעה לפרקים מתהליכי הגלובליזציה הגורמת לשחיקה בריבונותן וגבולותיהן הטריטוריאליים, מדינות הן אלו שמבנות את הפיתוח של המרחב הגלובלי באופן שימשיך להלום את החלוקה הריבונית הטריטוריאלית הקיימת, אך נדרשות גם להתרחב, אלו תהליכים של רה/דה טריטוריאליות[42]. חלוקה של מרחב חדש על פי טריטוריות מדיניות, היא

ביטוי משמעותי לסמכות המכוננת של מדינות במערכת הבינלאומית שמיושמת באמצעות מיפוי והסדרת הגבולות. המיפוי הוא פעולה בעלת מטען חברתי ופוליטי שפועלת להגדיר ולהדיר ישויות פוליטיות, אשר מבחינה היסטורית תרם לביסוס המערכת הבינלאומית הריבונית הקיימת בניגוד לרצף, ערי המדינה שהתקיים בימי הביניים[43]. זאת באמצעות שלושה מרכיבים: הומוגניות של היחידה הטריטוריאלית; המימד הלינארי הטהור של הגבולות הפוליטיים; העלמת ישויות אנטי טריטוריאליות (כגון פיראטים, האקרים וכדומה). עצם המהלך, להאחדת השימוש באותם כלי מדידה של רשת מיפוי, יצר למעשה שפה בינלאומית פוליטית אחידה וגרם למהפכה בתפיסת המרחב כהומוגני וטריטוריאלי[44].

עם זאת, יש לציין כי הסמכות לייצר מפות ולהנחיל באמצעותם תודעה מרחבית בינלאומית איננה נחלתה של כל מדינה באשר היא. למעמדה הגיאופוליטי של מדינה מסוימת בנקודת זמן (היסטורית או עכשווית) במסגרת מערכת של מדינות[vi], ישנה השפעה ישירה על יכולתה לפעול באופן מטא פוליטי שכזה. פעילות לחלוקת המרחב באמצעות מיפוי לטריטוריות מדיניות היא, אם כן, יישום של עוצמה "רכה" גדולה ביותר ולכן מביאה לידי ביטוי את ההיראַרכיה הבינלאומית, ומבדילה בין מעצמות גלובאליות לבין מדינות אחרות ובכלל זה מעצמות אזוריות ומדינות חסות ולווין. טענה זו, מבוססת על ההנחה כי לגיטימאציה בין מדינות היא הבסיס להיראַרכיה בינלאומית, ולכן, מצד אחד, המעצמות הגלובאליות הזוכות לתמיכת מדינות רבות (משיקולים שונים חומריים או אידיאולוגיים), הן המדינות בעלות הסמכות לקבוע את ה"גבולות הפוליטיים" במערכת הבינ"ל. ומצד שני, יש למעצמות גם אינטרס לשמר את מוסד הריבונות הבינ"ל, משום שהוא משמר את רעיון הסמכות המדינית ומקנה להן את הלגיטימאציה לפעול באופן מטה פוליטי לעיצוב המערכת המדינית העולמית[45]. זאת, בין היתר, באמצעות השפעה על החלוקה הטריטוריאלית ("שרטוט המפות")[46], ושימור המערכת הריבונית המדינית כביטוי פוליטי וממסדי לחלוקה זו.

[vi] מערכת מדינות ובמיוחד אלו שאינן מערביות מאופיינת כקבוצה מדינות הסובבות סביב מעצמה ומאופיינות במערכת יחסים של מרות או כפיפות ברמה מסוימת.

**תמונה 1: שרטוט מפת אירופה החדשה ע"י המעצמות המנצחות בקונגרס ווינה, 1814-1815**



ההשוואה בין תהליכים דומים במרחב המקוון ובמרחב הפיזי, שנתקיימו כאשר נוצר הצורך לתחם את הטריטוריה המדינית מחדש, ממחישה את תהליך התהוות המדינה שתואר לעיל. הדוגמאות ההיסטוריות במרחב הפיזי, ליישום של חשיבות התיחום וההגדרה הטריטוריאלית ניכרות במיוחד בתהליכי הקולוניזציה בעקבות ההתפתחות הטכנולוגית שאפשרה שינוע ימי ארוך טווח. יחד איתם, גם תהליכי הדה - קולוניזציה שעברו על העולם המודרני, במסגרתם הצטמצמו שליטתן של מעצמות בטריטוריות ונוצרו מדינות חדשות תוך שימור הגבולות הקיימים שנקבעו על ידי המעצמות ותיקופן בטיעונים לאומיים, מהווים גם הם דוגמא מאלפת[47]. שימור הגבולות הקולוניאליים בקרב מדינות שזה עתה השתחררו מעולה של הקולוניה, הוא ביטוי למשמעות השמירה על השלמות הטריטוריאלית של המדינה בנורמה שזכתה לכינוי "The Territorial Integrity Norm".[48] נורמה בינלאומית זו, זכתה לתשומת לב בינלאומית דווקא בשל הפוטנציאל הגלום בפירוק ויצירת מדינות לשינויים מהותיים בהגדרה ובתיחום הטריטוריאלי. הפוטנציאל לא מומש, ונראה כי גם מהלכים רביזיוניסטיים (כגון הפיכות צבאיות והכרה

במדינות חדשות) במערכת הבינלאומית אינם משפיעים באופן מהותי על קווי המתאר הבסיסיים של חלוקת המרחב הפוליטית. באופן דומה, לא מומשה האפשרות לייצר חלוקה שאיננה מדינית במרחב המקוון והוא נענה היום מבחינה תשתיתית לחלוקה המדינית הגיאו אסטרטגית המקובלת, כפי שעולה מהחלוקה במערכת הכתובות האלקטרוניות (DNS) עליה ארחיב בהמשך.

הנורמה שהתבססה בחצי המאה האחרונה של המאה ה- 20 בעקבות מלחמות העולם והתבססות הדמוקרטיה, איננה מייצגת תפיסה של הימנעות מוחלטת מחדירה לטריטוריה של מדינות אחרות, אלא את מוכנותן של מדינות לסדר בינלאומי הכולל שאיפה להימנעות מסכסוכי גבולות[49], מאוחר יותר עוגנו נורמות אלו במסגרת המשפט הבינלאומי תחת השם הלטיני "Uti Possidetis Juris" (בתרגום חפשי – "כפי שבחזקתך תחת החוק")[50].

העובדה שנורמות אלו יושמו גם במסגרת תהליכי דה קולוניזציה, וכחלק מעימותים בין מדינות[51], משמעותית להבנת תהליך תיחום הטריטוריה במרחב המקוון משום שגם הייצוג הטריטוריאלי של גבולות הקיים בו תוקף באמצעות חלוקה מחודשת של המרחב על ידי המעצמות (ארה"ב) ובעימותי סייבר בשנים האחרונות. חשיבותה של הנורמה, שתקפותה מבוססת על דוגמאות היסטוריות ועכשוויות מרחבי העולם (כגון תהליכי הדה-קולוניזציה באמריקה הלטינית ובמזה"ת), נעוצה בכמה טעמים: ראשית, היא מוכיחה את ההשפעה העמוקה של התפיסה הטריטוריאלית של הסדר הבינלאומי והמדינתי (ר' לעיל) על חלוקה פוליטית של מרחבים חדשים, גם כאשר החלוקה נתפסת כמנוגדת לשאיפות אידיאולוגיות, ל"גבולות טבעיים" או לשיקולים כלכליים גרידא; שנית, היא משקפת את הבסיס הנורמטיבי של המשפט הבינלאומי, המעיד למעשה על המשמעות של נורמות בינלאומיות לביסוס הסמכות המשפטית של מדינות במערכת הבינלאומית.

במרחב המקוון, באופן דומה לתהליכי הקולוניזציה מופו ועוגנו באופן טכני על ידי מעצמות (בדגש לארה"ב) גבולות בין מדינות על פי המודל הגיאופוליטי הקיים במרחב הפיסי ומוסדה ההיררכיה הבינלאומית ובראשה ארה"ב. המהלכים המרכזיים שנוצרו לצורך כינון מסד ליחסים בין מדינות שונות במרחב המקוון ובכלל זה קביעת קווי תיחום בין מדינתיים ("גבולות

וירטואליים") מבוססי טכנולוגיה, היו בעיקרם מהלכים פנים מדינתיים אמריקניים. חתירתה של ארה"ב, לביסוס השליטה בתשתיות העומק המרכיבות את "קווי המתאר" ("Grid") של המרחב המקוון מתבטאת בשלושה מנגנוני פיתוח טכנולוגיים שכבר זכו להתייחסות לא מבוטלת במחקרים בתחום[52]: 1) פיתוח טכנולוגי של "מערכת מיתוג המנות" ("Packet Switching"); 2) תהליך הפיתוח של הפרוטוקול הממוחשב האחיד (TCP/IP), המאפשר תקשורת מתווכת מחשב הפתוחה לשימוש של סוגי מחשב שונים; 3) כינון ומיסוד הניהול של מערכת הכתובות באינטרנט המכונה "מערכת שמות המתחם" (DNS- Domain Name System), המנוהלת על ידי ארגון אמריקני (ICANN), סמי ממשלתי הפועל בהנחיית משרד הסחר האמריקני תחת הסכמים רשמיים[53].

<u>שינוי תפיסתי</u>

התחזית לעליה חדה בכמות המשתמשים באינטרנט הובילה ליוזמה[vii] לבסס את החלוקה למתחמים בעלי שמות מילוליים בכדי לבסס "מרחב שמי" ("Name Space")[54]. עצם השימוש במונחים אלו, מעיד על השינוי התפיסתי בראיית העוסקים בתקשורת מתווכת מחשב הרואים את האינטרנט כבר כמרחב ולא כאמצעי תקשורת בלבד, ולכן גם הפתרון שנמצא הוא כלי לשליטה וניהול מרחבי, קרי לפקח על השמות שניתנים באמצעות הגדרת מתחמים שהם למעשה אדמיניסטרציות משנה שישמרו במאגר של כתובות[55].

מבחינה טכנית, ניתן להסביר את הפיתרון שניתן באמצעות הדמייתו לדואר רגיל, שהפרוטוקול שתואר לעיל מהווה את ה"מעטפה" המכילה את תוכן ההודעה (המכתב), ואילו הזיהוי הבינארי ו/או השמי המוצמד אליו מהווים את הכתובת הרשומה עליה. כתובת דואר כוללת מרכיבים קבועים: נמען

[vii] היוזמה פורסמה במסגרת RFC 882 בשנת 1983 ו RFC920 בשנת 1984 על ידי קבוצת העבודה לרשתות (NWG) שעדיין פעלה תחת פרוייקט APARANet של משרד ההגנה האמריקני.

אינדיבידואלי, חלוקה גיאו פוליטית מוסכמת (מספר בית ודירה, רחוב, עיר, מדינה) וקידוד מספרי (מיקוד). באופן דומה, גם מערכת שמות המתחם שנוצרה עקב צורך פרקטי בהעברת מידע (דואר אלקטרוני) לנקודת קצה "אינדיבידואלית", גם היא כוללת מרכיבים דומים, משקפת חלוקה גיאו פוליטית מוסכמת, ומקודדת באמצעות קוד מספרי ארוך (IP Addresses). המתאר בשפה בינארית את מיקומו של המחשב[56].

פענוח הקוד המספרי, מתבצע באמצעות קובץ פענוח מרכזי המכונה "קובץ השורש" (The File Zone Root), אשר מקשר בין הקוד המספרי לשמות "אזורים" המכונים שמות מתחם[57]. שמות המתחם המשמעותיים ביותר מבחינה כלכלית מכונים TLD (Top Level Domains),[viii] פורטו באופן מקיף בשנת 1994 במסמך RFC 1591 והם אלו המגדירים תחתם קבוצות גדולות של שמות מתחם אחרים ומאפשרים לנהל אותם ו/או לגבות מהמשתמשים בהם דמי שימוש[58]. ה- TLD מחולקים לשמות גנריים (gTLD) שהם בעלי המשמעות הכלכלית הגדולה ביותר (למשל הסיומות .NET, .COM, .ORG), ולשמות מדינות (ccTLD) המשקפים את החלוקה הגיאו פוליטית העולמית, ושהסימול שלהם מותאם לסימול הבינלאומי של מדינות על פי ארגון ISO המופקד על סטנדרטיזציה בינלאומית מטעם האו"ם. סטנדרט זה, המופיע במסמך שמספרו ISO 3166/1, גובש ביוזמת מדינות שונות בעולם והוא כולל סימול בן שתי אותיות לכול מדינה (כגון .UK, .FR, .IL וכו').

לסיכום באשר למיפוי ולתיחום הטריטוריאלי, למעט חריגות מעטות, מנגנוני הפיקוח הטכנולוגיים לעיל, תיקפו הלכה למעשה יישום מקוון של הגבולות הגיאו פוליטיים המקובלים, באמצעים טכניים ובירוקרטיים ועיגנו אותם על ידי מהלכים משפטיים פנימיים ובינלאומיים. באופן מפורט יותר ניתן למצוא קווי דמיון לא מעטים כאשר משווים את מערכת שמות המתחם לנורמות טריטוריאליות בתהליכי הדה קולוניזציה, שעיקרם הוא עדות לתהליך

[viii] בהקשר זה יש הטוענים להקבלה משפטית של שמות המתחם לסימנים כלכליים מוסכמים (Trademarks) המאוגדים תחת הסכמים בינלאומיים לשימור זכויות קניין.

התהוות המדינה במרחב, תוך יישום התיחום הגיאו אסטרטגי הקיים בקונצזוס הבינלאומי. מערכת שמות המתחם, בה עושים שימוש רוב המשתמשים בערוצי התקשורת מתווכת המחשב המקובלים, היא הביטוי הנוכח והברור ביותר לשכפול החלוקה הטריטוריאלית הגיאו פוליטית המסורתית למרחב המקוון. גם במקרה של דה קולוניזציה וגם במקרה של המרחב המקוון אין ניסיון ליצירת מערכת חלוקה חדשה, אלא לתקף את האחריות המדינית "טריטוריאלית" במרחב חדש וכתוצאה מכך ליצור תחושה של "מרחב לאומי" (מקוון או פיזי), המהווה ביטוי מקביל ונוסף לבסיס הטריטוריאלי של ריבונות המדינה. המשמעות לחלוקה זו, בין אם במרחב המקוון או הפיזי איננה רק טכנית, היא מהווה ממש כמו הגבולות שנוצרו בתהליך הדה קולוניזציה כלי מהותי ביצירת החיץ שבין יישות מדינית אחת לאחרת שעליו מתבססים כלל מהלכי המדיניות של המדינות במרחב המקוון (כלכלה, ביטחון וכדומה). הגבול החדש שנוצר מהווה מוסד כשלעצמו והוא בסיס לשינויים מוסדיים כגון הקמה של גופים בירוקרטיים חדשים, חקיקה ודוקטרינה ביטחונית.

**מונופול על אמצעי הכפייה - על פיראטים והאקרים**

הדוגמא ההיסטורית לפיראטיות (שוד ימי) תנותח כדוגמא ליזמי אלימות פרטיים המאתגרים את ריבונות המדינה במרחב שהנגישות אליו לא הייתה אפשרית לפני כן. "פיראטים" (Pirates), מוגדרים במחקר היחסים הבינלאומיים כ"אנשים חסרי מדינה שמעשיהם הימיים לא מתקיימים בשמה של מדינה כלשהי"[59]. המאפיין המרכזי שיש להתייחס אליו באשר לתופעת הפיראטיות, הוא היותם גורם הפועל באלימות לאורך זמן ובאופן נחוש כנגד המונופול המדיני על האלימות המאורגנת. למרות שפיראטיות כסוג של פשיעה התקיימה מראשית ימי הביניים ועד היום, נהוג להתייחס לשתי תקופות היסטוריות מובהקות של המאבק בין מעצמות הסחר לבין הפיראטים: הפיראטים הברברים שפעלו בים התיכון מחופי צפון אפריקה מהמאה ה- 16 ועד לתחילת המאה ה- 19; והפיראטים הבוקאנירים שפעלו בים הקריבי כנגד המעצמות הקולוניאליות בין המאה ה- 17 למאה ה- 18[60].

תופעות אלו ראויות להשוואה לתופעות השוחקות את הריבונות המדינית היום, משום שבזמנן הן היו פעולות במרחב שמדינות טרם יכלו לפעול בו באופן מלא.

המאפיינים הסוציולוגיים והאידיאולוגיים של הפיראטים בתקופות אלו היו משמעותיים, שכן מעבר לפעילות האלימה שבה נקטו, ההתארגנות בקבוצות עצמיות חסרות לאום, הייתה אבן שואבת לאינדיבידואלים וקבוצות שלא היו מקובלות באותה העת במדינות עצמן מסיבות שונות (דת, מגדר, גזע וכדומה). הן פעלו באופן דמוקרטי על פי קוד התנהגות וולונטרי שאותו גיבשו ולא היו תחת זהות או הגדרה לאומית כלשהי, פעולותיהן הונעו מאינטרסים כלכליים אינדיבידואלים וקבוצתיים בלבד ולא הייתה להן שאיפה להשתתף במערכת היחסים הבין מדינית באותה העת[61]. היחס של המדינות כלפיהם התאפיין בתפיסתם כתופעה ייחודית ומסוכנת, שאיננה מופנית כלפי מדינה מסוימת אלא כקריאת תיגר על כל המדינות כולן, קרי, כ״אויבי האנושות כולה״[62].

תפיסה זו, הובילה לגישה הרואה בטיפול ובחיסול הפיראטיות אינטרס משותף למעצמות ומדינות שונות, דבר שהקל על היווצרותן של שותפויות ביטחוניות ולאחר מכן כינון נורמות וכללי התנהגות שעוגנו בדין הבינלאומי (דיני הים ודיני המלחמה).

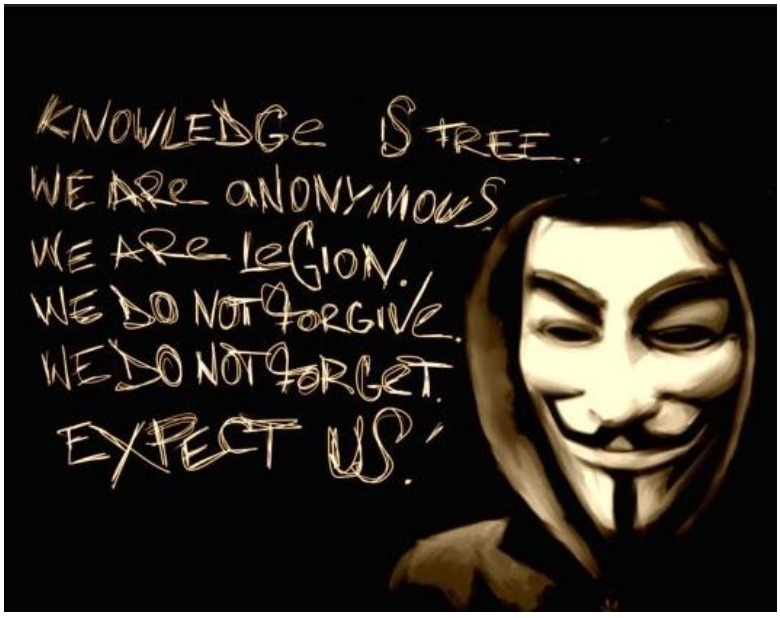
**תמונה 2: קפטן אדוארד טיץ', הוא שחור הזקן**

לאחר תיחום הקהילה הפוליטית במדינה, בדגש על התיחום הטריטוריאלי, הניסיון להשיג מונופול על אמצעי הכפייה או האלימות המאורגנת באותו "שטח מוגדר", הוא ההסבר השכיח ביותר לתהליך של ביסוס ריבונות המדינה וליצירת מערכת המדינות המודרנית. תהליך התגבשות זה של מונופול על הפעלת אמצעי האלימות המאורגנת מאפיין את המדינה המודרנית במערב אירופה מאז שלהי ימי הביניים[63]. מחד גיסא, התהליך ההיסטורי של האחדה וגיבוש של כל מפעילי האלימות המאורגנת תחת המדינה היה אלמנט הכרחי לביסוסה של המדינה המודרנית. מאידך גיסא, חל תהליך הבניה הדדי בין יזמי אלימות (Violent Entrepreneurs), אשר מצד אחד עוסקים בפשע ומנצלים את המדינה ומצד שני מהווים את מאתר כוח האדם שממנו המדינה מרכיבה את אלו האוכפים את המונופול על אמצעי הכפייה (מפיראטים לפרייברטירים, מפושעים לשכירי חרב ובסוף לחיילים), ואחר כך הם גם משוחררים על ידה בחזרה לשוק החופשי[64]. זהו תהליך היסטורי החוזר על עצמו במאות האחרונות מאז הקולוניאליזם: **יזמים כלכליים פועלים כחלוצים במרחב חדש ללא רגולציה מדינית; בעקבות כך הם נדרשים לבצע בעצמם רגולציה והסדרה בשל העלייה בפעילות הכלכלית; בסופו של דבר הם גוררים את המדינה למרחב החדש בכדי שתשית עליו את המונופול על אמצעי הכפייה. הדוגמאות ההיסטוריות מגוונות, מהקולוניאליזם האירופי באפריקה[65], ועד לציפיות ל"הסדרה עצמית" של יזמים כלכליים במרחב המקוון[66].**

באשר למרחב הימי, הוא מיישם באופן כמעט מלא את התהליך ההיסטורי שתואר. ההתפתחות הטכנולוגית משלהי ימי הביניים, אפשרה בניית כלי שייט מתוחכמים ועמידים מספיק כדי להרחיב את המרחב שבו התנהלו בני האדם, ובאופן ישיר את כינונן של קולוניות ומסחר ימי ער. העלייה במרכזיות שבאינטרסים הכלכליים בים והיעדרה של הסכמה בינלאומית באשר לדרכי ההתנהלות בים, הפכו את השוד הימי לכדאי ביותר ואת הפיראטיות לתופעה חריגה משום שהיא התקיימה באופן מאסיבי כמה מאות שנים ברציפות. פעילותם של הברברים בים התיכון לא נבלמה על ידי מעצמת הסחר דאז ספרד, משום שלא ניתן היה לייצר לגיטימציה מספקת למהלכים בינלאומיים

כנגדם, ומשום הימצאות פתרון אלטרנטיבי חלקי - ניתן היה "למשטר" חלקים מהפיראטים או באמצעות קניית נאמנותם (והפיכתם ל"פרייבטירים") או באמצעות הגעה להסכמות עם מדינות צפון אפריקה (תוניס, אלג'יר) שתיקחנה אותם תחת חסותן. לעומתם כמה מאות שנים מאוחר יותר, פעלו הבריטים להדביר את התופעה הן בים התיכון כנגד הברברים והן בים הקריבי כנגד הבוקאנירים. פעולה זו נתאפשרה בגלל היכולת לפעול במשותף עם מדינות נוספות והסירוב לאפשר לגיטימציה להמשך פעולתם באמצעות הסכמים ושוחד. אחד המהלכים המשמעותיים בהקשר זה, היה השימוש בפרייבטירים כדי להילחם בפיראטים[67].

**תמונה 3: קבוצת 'אנונימוס' וסיסמתה**




הלגיטימציה להפעלת כוח על ידי מדינות בזירה הפנימית והבינלאומית היא אם כן אחד ההישגים המרכזיים הנובעים מהמונופול על האלימות המאורגנת, אך אין הכוונה ששחקנים תת-מדינתיים או על-מדינתיים מפסיקים להפעיל אלימות, אלא להיפך: היא מאפשרת למדינה לקבוע איזו פעילות אלימה

נתפסת כזו שאינה מסכנת את המונופול של המדינה ומכאן שהיא "לגיטימית למחצה" ולא דורשת דיכוי מוחלט. למרות האמור לעיל, אינני טוען שהמונופול של המדינה על אמצעי הכפייה הוא מוחלט, לא מבחינה נורמטיבית בכלל ולא מבחינה אמפירית במרחב המקוון היום.

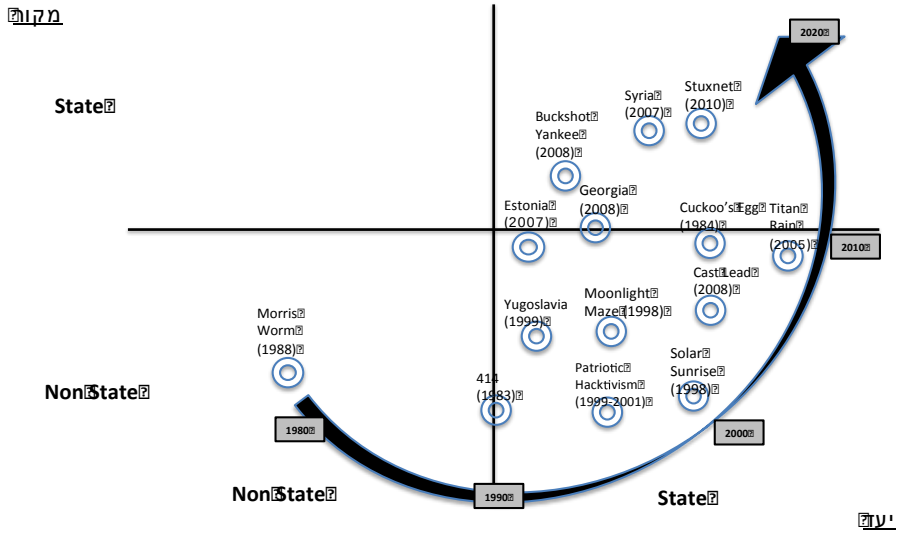
מבחינה נורמטיבית פעילות מוכרזת כלא לגיטימית, כאשר המדינה תחת סמכותה הריבונית מכריזה עליה כאסורה לאינדיבידואלים ומותרת רק למדינה[68]. בהקשר זה, בדומה לפרייבטירים יש להזכיר את השימוש שעושות מדינות ביזמי אלימות מתחרים כגון ארגוני פשע מאורגן, חברות צבא ואבטחה פרטיות, ארגוני טרור והאקרים, על ידי מיסודם והענקת לגיטימאציה לפעולתם כאשר היא מתקיימת תחת הכסות המדינית. **היכולת של מדינות, לעשות שימוש בגורמים שנתפסו קודם לכן כחותרים תחתיהן, מבטאת ומחזקת את סמכותה המטה-פוליטית של המדינה לקבוע את כללי המשחק, ולהפוך אלימות (Violence) לשימוש לגיטימי בכוח (Force)**[69].

מבחינה אמפירית, המרחב המקוון איננו שונה מהדוגמאות ההיסטוריות והעכשוויות שהציבו יזמי אלימות למול המדינה במרחבים הפיזיים. כפי שגורמים תת ועל מדינתיים המאתגרים את מונופול האלימות כגון צבאות פרטיים, פיראטים שכירי חרב וארגוני פשיעה פנים מדינתיים וטרנס לאומיים, הפכו למאתר כוח האדם הנדרש לשימור המונופול על האלימות כשהמדינה קנתה את שירותיהם, הכילה ומיסדה אותם לכדי צבאות מקצועיים ביבשה ובים ואף עשתה בהם שימוש להדברת יזמי אלימות סוררים (כמו במקרה של השימוש בפרייבטירים ללחימה כנגד פיראטים)[70]. באופן דומה, מהווים האקרים, וארגוני פשיעה העושים שימוש במרחב המקוון להשאת רווחים בניגוד לחוק, כוחות פוטנציאליים שפועלים למימוש האינטרס של מדינות ברמות שונות של תיאום עמה. תופעה זו המכונה "פעילים האקרים פטריוטיים" ("Patriot Hacktivists") התומכים במדיניות ובפעולות של מדינות (או ישויות פוליטיות אחרות) בתקיפות אתרים ומוסדות של מדינות אחרות ברמות שונות של תיאום והכוונה של המדינה[71].

על פי תרשים מס' 2, השינוי מפעילות אלימה המופעלת על ידי יזמי אלימות אינדיבידואליים שאינם פועלים מטעמה של מדינה כלשהי כגון "תולעת

מוריס״ ב - 1988 או מעצרה של כנופיית פשע מקוון בשם ״414״ בארה״ב ב - 1983, לפעולות מדינתיות וסמי מדינתיות הגיעה לשיאה בעשור הראשון למאה ה - 21. דוגמאות למהלכים אלו ניתן למצוא כבר בתקיפת אתרי נאט״ו וארה״ב כחלק ממבצע ״Allied Force״ בשנת 1999[72], אך במיוחד בתקיפת אתרי ממשל אסטוניים על ידי האקרים לאומנים רוסיים בשנת 2007[73], ובמהלך הפלישה הצבאית של רוסיה לגיאורגיה בשנת 2008[74]. דוגמא נוספת, הייתה בתקיפת אתרי מוסדות ציבוריים ישראליים על ידי תומכי ארגון החמאס במהלך מבצע ״עופרת יצוקה״ בעזה בדצמבר 2008[75].

**תרשים 2: השינוי בהפעלת אלימות במרחב המקוון**




חשיבות המונופול על הפעלת הכוח המאורגן, מדגישה את ההשלכות הבעייתיות למצב של היעדר ביטחון, המהווה את אחד הסממנים המרכזיים למדינות הנמצאות בתהליך קריסה[76], מצב של אוליגרכיה או ריבוי מונופולים של אלימות מאורגנת, הוא הבסיס למצב של היעדר משילות שמוביל לכישלון המדינה[77]. מבחינה היסטורית, נראה כי תהליך ארוך, ״מלמטה למעלה״,

שבמסגרתו המדינה פעלה למיגור מתחרים למונופול על יכולת האכיפה, כמו במקרה האירופי, הובילה למצב של "ריבונות חיובית" במרחב הימי. בעוד שמצב הפוך, שבו הריבונות ניתנת למדינה כתוצאה מהחלטה פורמאלית פוליטית משפטית בינלאומית, "מלמעלה למטה" כפי שקרה בתהליכי דה קולוניזציה, כאשר ישנם עדיין מתחרים משמעותיים השוברים את המונופול המדיני, מוביל למצב של "ריבונות שלילית" שיוצרת מצב של "מעין מדינות" ("Quasi States"). באופן לא מפתיע, במדינות כושלות מעין אלו עדיין מתקיימות תופעות כגון פיראטיות.

ניתן לסכם כי במדינות דמוקרטיות ליברליות היום, עדיין מתקיים מונופול של המדינה על אמצעי הכפייה והאלימות המאורגנת, לצד המשך קיומם של תופעות ושחקנים החותרים תחת מונופול זה, שהמדינה בדרך כלל אינה מרגישה צורך לגייס את המשאבים הנדרשים כדי למגר אותם לגמרי, משום שהם אינם נתפסים כמי שמסכנים את עצם קיומו של המונופול בו היא מחזיקה. כך גם המרחב המקוון המגלם בתוכו כמו במרחבים פיזיים, אתגרים לביטחון המדינה בדמות פשיעה מקוונת, פעילות מדינתית וטרור, לצד פעילות אינטנסיבית של מדינות לגבש יכולות ביטחוניות צבאיות ואחרות לאיסוף מודיעין, הגנה והתקפה המאזנות את תחושת האיום לתפקודה של המדינה ואיננה מובילה אותה בהכרח למצב של "מעין מדינה" במרחב המקוון.

## סיכום ומסקנות להמשך

היחסים שבין מדינה, מרחב והתפתחות טכנולוגית הן דפוס חוזר במערכת הבינלאומית המודרנית בכלל ובהתפתחות מערכות השליטה והביטחון המדיניות בפרט. ללא התפתחות פלטפורמות ימיות ואוויריות מודרניות, לא היו נוצר הצורך בהגדרת המרחב המדיני הטריטוריאלי גם באוויר ובים, תוך יצירת הסמכות החוקית הפנימית והבינלאומית ביסוס הנורמות והסדר הבינלאומי ופיתוח סמלים ליצירת לגיטימציה לאומית למרחבים אלו. לדעתי, **למרות שאלו טכנולוגיות חדשות, מדובר, בדפוסים חוזרים, הניתנים לניתוח על פי המרכיבים המוכרים מתהליך התפתחות המדינה ההיסטורי**. במאמר זה, בחרתי להמחיש זאת באמצעות תיאור מהלכי התיחום הטריטוריאלי

ואכיפת המונופול על האלימות המאורגנת, שלכול אחד מהם ביטויים אמפיריים במרחב המקוון ובמרחב הימי.

התחושה הקיימת אצל רבים בציבור וגם בקרב מקבלי ההחלטות בדבר אי היכולת לאכוף את ריבונות המדינה במרחב המקוון והפוטנציאל השלילי לביטחון המדינה שהוא משקף, נובעת גם מקשיי הסתגלות של מערכת התכנון המדינית ותפיסה נוקשה של מוסד ריבונות המדינה. קשיים אלו, הם בעצמם עדות לתהליכי ההסתגלות המדיניים לטכנולוגיות ולמרחבים חדשים שהיו מנת חלקן של מדינות משחר ההיסטוריה, ואינם צריכים לרפות את ידי המדינאים ופקידי הממשל. כפי שצוין, ריבונות המדינה היא דינאמית ומאותגרת תדיר כפי שהייתה גם במרחבים הנתפסים היום כנשלטים כגון הים. ההבנה שהמרחב המקוון הוא עוד אתגר נוסף שהמדינה מתנהלת למולו באותם מימדים, מחלחלת בשנים האחרונות ומתחילה אט אט לשנות את התפיסה בקרב הבירוקרטיה.

במאמר הצגתי קריטריונים לבחינת תהליכים מדיניים למול מרחב, המבוססים היסטורית על התיאוריה הריבונית מדיסציפלינת מדע המדינה והיחסים הבינלאומיים, שיכולים לשמש כלים לביצוע תהליך למידה מתמשך על המרחב המקוון ולספק כיוונים ראשוניים להתוויית מדיניות לגביו. האפשרות לעשות שימוש בהשוואה היסטורית אמפירית ותיאורטית, הוא מתודה נדרשת בכדי לבסס קריטריונים אלו, לפתח אותם ולהפוך אותם לכלים משמעותיים למקבלי החלטות. תקוותי, שמאמר זה יעודד שימוש בהשוואות היסטוריות מעין אלו בין המרחב המקוון למרחבים אחרים, ככלי לקידום יכולת האכיפה והריבונות של המדינה במרחב החדש.

דור חדש של פקידים, משפטנים, מדינאים ואנשי צבא נדרש כדי לאפשר התמודדות עם האתגרים שמציב המרחב המקוון. בעלי מקצוע המבינים מצד אחד את משמעותו של המרחב המקוון להמשך הביסוס הכלכלי החברתי והביטחוני של מדינות, ומצד שני אינם מוכנים להיכנע לתפיסה הרואה בו מרחב אנארכי ושלילי. יתכן כי אנו עדים לניצני התנהלות בירוקרטית ומדינית מחודשת מעין זו, הניכרת בהקמת מוסדות ביטחון ואכיפה ייעודיים בשנים האחרונות, ביניהם מטה הסייבר הלאומי בישראל ופיקוד הסייבר הצבאי בארה״ב. ככל שיקדם הזמן בו יופנם בקרב הזרוע המחוקקת,

המבצעת והשופטת כי ההיגיון המדיני הטריטוריאלי והביטחוני המוכר מהווה את הביטוי המרכזי להתהוות המדינה במרחב המקוון (כולל המאפיינים הטכניים הייחודיים לו), כן יקל על כלל המערכות המדיניות והמסגרות הבינלאומיות לשפר את פעולותיהן למולו, לאמץ אסטרטגיה מדינית דומה לזה המתקיימת מול המרחב הפיזי תוך ביצוע התאמות טקטיות למרחב המקוון.

## מקורות

[1]Peter Steiner, cartoon in *The New Yorker*, 5 July 1993, Pp. 61

[2]Krasner S.D. (2001). "Abiding Sovereignty". *International Political Science Review*. Vol. 22 No. 3 Pp. 245-247.

[3]Ibid, 239-245; H. Spruyt, **The Sovereign State and its competitors**. p. 4.

[4]Krasner, 2001; 240.

[5]Ibid. Pp. 243; D. Philpott "The Religious Roots of Modern International Relations," *World Politics*, Vol. 52, No. 2 (Jan. 2000), pp. 206-245; D. Philpott, **Revolution in Sovereignty**, (Princeton: Princeton University Press, 2001); J. R. Strayer, **On the Medieval Origins of the Modern State**, (Princeton: Princeton University Press, 2005).

[6]J. E. Thompson, "State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research". *International Studies Quarterly*. (June 1995) Vol. 39, No. 2, pp. 213-233; J. T. Mathews, "Power Shift". *Foreign Affairs*. Vol. 76, No. 1 (Jan. - Feb. 1997). pp. 50-66; R. Rosecrance, .**The Rise of the Trading State**. (New York: Basic Books, 1986); C. Tilly, **Coercion, Capital, and European State AD 990-1990**, 1995.

[7]O. Lo¨wenheim, **Predators and Parasites: Persistent Agents of Transnational Harm and Great Power Authority**, (Ann Arbor: The University of Michigan Press, 2007) (Lo"wenheim 2007 (1)); O. Lo¨wenheim, ""Do Ourselves Credit and Render a Lasting Service to Mankind": British Moral Prestige, Humanitarian Intervention, and the Barbary Pirates". *International Studies Quarterly*. Vol. 47, No. 1 (Mar. 2003), pp. 23-48; J. E. Thompson, **Mercenaries, Pirates and Sovereigns: State Building and Extraterritorial Violence in Early Modern Europe**. (New Jersey: Princeton University Press, 1994).

[8]D. Avant, "From Mercenary to Citizens Armies: Explaining Change in the Practice of War". *International Organization*, Vol. 54. No. 1. (Winter 2000). pp. 41-72; T. Lynch and Walsh A.J., "The Good Mercenary?," *The Journal of Political Philosophy*, Vol. 8 No. 2. (2000) pp. 133-153; L. W. Serewicz, "Globalization, Sovereignty and the Military Revolution: From Mercenaries to Private International Security Companies". *International Politics*, Vol. 39. (March 2002), pp. 75-89.

[9]O. Lo¨wenheim, 2007 (1); V. Volkov, "Violent Entrepreneurship in Post-Communist Russia", *Europe-Asia Studies*, Vol. 51.No. 5, 1999. pp. 741-754.

[10]B. R. Barber, **Jihad vs. McWorld: How Globalism and Tribalism are Shaping the World**, (New York: Times Books, 1995); M. Van Creveld, **The Rise and Decline of the State**. (Cambridge: Cambridge University Press, 1999).

[11]J. A. Pemberton, **Sovereignty: Interpretations**. (Hampshire: Palgrave Macmillan, 2009).

[12]L. K. D. Kristof, "The Nature of Frontiers and Boundaries," *Annals of the Association of American Geographers*, Vol. 49. No. 3. [Part 1] (Sep. 1959), pp. 269-271.

[13] Ibid. pp. 271-274

[14] S. D. Krasner, "Sovereignty: An Institutional perspective," *Comparative Political Studies*, Vol. 21, 1988. pp. 87-88; F. Kratochwil, "Of Systems, Boundaries, and Territoriality: An Inquiry into the Formation of the State System". *World Politics*, Vol. 39. No. 1 (Oct. 1986). pp. 27-28.

[15] L. K. D. Kristof, 1959; 281-282.

[16] M. B. Salter, "Passports, Mobility, and Security: How smart can the border be?," *International Studies Perspectives*. Vol. 5. Pp. 86-88, 2004.

[17] W. Gibson, **Neuromancer**, (New York: Ace Books, 2000 [1984]), pp. 61-62.

[18] Ibid. Pp 60

[19] M. A. Lemley, "Place and Cyberspace" .*California Law Review*. Vol. 91, No. 2, (March 2003). pp 523.

[20] יש לציין כי נקודות קצה אינן בהכרח שוות, הן יכולות להיות משתמש בודד או ארגון שלם.
C. R. Kedzie, "The third Wave," in: B. Kahin and Nesson C. (eds.), **Borders in Cyberspace**. (Cambridge: MIT Press, 1997). pp. 111.

[21] ת. אשורי, **מהטלגרף עד המחשב: היסטוריה של אמצעי התקשורת**. (תל אביב: רסלינג, 2011). עמ' 133-38.

[22] כך למשל טוען גולדסמית' במאמרו שכבר קיבל מעמד קאנוני בקרב חוקרי האינטרנט:
"Activity in cyberspace is functionally identical to transnational activity mediated by other means, such as mail or telephone or smoke signal" (Goldsmith, 1998: 1240)

[23] החלטה 3611 של הממשלה ה- 32. קידום היכול הלאומית במרחב הקיברנטי. (2011)

[24] ניתן להשוות את כל התהליך של ביסוס הריבונות למושג ה "Stateness" שטבע נטל (Nettl,1968) ואת השחיקה בריבונות למושג ה "Statenessless" ולקריטריונים למדינה מתפקדת לעומת מדינה בתהליך התמוטטות. ראה:
W. I. Zartman, "Introduction: Posing the Problem of State Collapsed," in: W. I. Zartman (ed.), **Collapsed States: The Disintegration and Restoration of Legitimate Authority**, (Colorado: Lynne Rienner Publishers Inc., 1995), p. 5.

[25] על פי סוז'ה הממדים מחוברים (Interrelate) וחופפים. ראה:
E. W. Soja, **Postmodern Geography: The reassertion of space in critical social theory**, (London & New-York: Verso, 2001), pp. 120.

[26] T. J. Biersteker, **State Sovereignty and Territoriality**, 2002. pp. 168-169.

[27] C. Tilly, "Reflections on the History of European State-Making" in: C. Tilly (ed.) **The Formation of National States in Western Europe**. (Princeton: Princeton University Press, 1975), Pp. 42.

[28] אני מסתמך על הגדרת המושג ביטחון של בני מילר (תרגום שלי): "חופש מאיומים וסכנות... המתקיימים כאשר אין איום ערכי קודמים... וכשיש יכולת התגוננות במחיר סביר"
B. Miller, "The Concept of Security: Should it be Redefined?," *Journal of Strategic Studies*. Vol. 24 No. 2, 2001. pp.16.
ביטחון זה מתבטא בהקמת מוסדות (גבול, משטרה, צבא). איני מתייחס בחלק למשמעויות הנורמטיביות של מוסדות אלו (על כך יורחב בהמשך) ולא לפולמוס האקדמי לגבי הגדרת

מושג הביטחון לכדי הכללה של מוסדות נוספים כגון מערכת חינוך, או אינדיקטורים לאיכות חיים.

[29] C. Tilly, **Coercion, Capital, and European State AD 990-1990**, (Cambridge: Basil Library, 1990), Pp. 1-2; M. Van Creveld, "The Fate of the State," *Parameters,* Vol. 26.No. 1, 1996. pp. 4; E.S. Finer, "State-building, state boundaries and border control : An essay on certain aspects of the first phase of state-building in Western Europe considered in the light of the Rokkan-Hirschman model," *Social Science Information*, Vol. 13 No. 79, 1974. pp. 79-80.

[30] J.G. Ruggie, "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis Theory of International Politics.by Kenneth N. Waltz," *World Politics* Vol. 35, No. 2 (Jan. 1983). pp. 280.

[31] Ibid; D. Philpott, "Westphalia, Authority and International Society," *Political Studies*, XLVII, 1999. pp. 566-589; A. Osiander, "Sovereignty, International Relations, and the Westphalian Myth", *International Organization* Vol. 55. No. 2 (Spring 2001), pp. 251-287.

[32] J. E. Thompson, **Mercenaries, Pirates and Sovereigns: State Building and Extraterritorial Violence in Early Modern Europe**, (New Jersey: Princeton University Press, 1994) Pp. 17-18.

[33] J. E. Thomson, "Explaining the regulation of transnational practices: a state building approach," in: James N. Rosenau and Ernst-Otto Czempiel (eds.), **Governance without Government: Order and Change in World Politics**, (Cambridge: Cambridge University Press, 1992) pp. 208-210.

[34] M. W. Zacher, "The Territorial Integrity Norm: International Boundaries and the Use of Force," 2001. Pp. 216-234.

[35] A. Osiander,2001; 281.

[36] The Character of the United Nations, (1945). Article 2.

[37] P. K. Menon, "The Acquisition of Territory in International Law: A Traditional Perspective," *The Korean Journal of Comparative Law*, Vol. 22, 1994. pp. 125.

[38] Ibid. pp. 127-129.

[39] D. R. Johnson and D. G. Post, "The rise of Law on the global network," in: B. Kahin and C. Nesson (eds.), **Borders in Cyberspace**, (Cambridge: MIT Press, 1997) pp. 3-48; J. Goldsmith and T. Wu, **Who Controls the Internet? Illusion of Boderless World**, (Oxford: Oxford University Press, 2006)

[40] N. Brenner et al., "Introduction: State Space in Question," in: N. Brenner et at. (eds.) **State/Space A Reader**, (Oxford: Blackwell Publishers, 2003), pp. 6-21.

[41] D. Harvey, "The geopolitics of capitalism," in: D. Gregory and J. Urry (eds.), **Social Relations and Spatial Structures**, (London: Macmillan, 1985), pp. 150.

[42] N. Brenner, "Beyond State-Centrism? Space, Territoriality, and Geographical Scale in Globalization Studies," *Theory and Society*. Vol. 28. No. 1 (Feb. 1999), pp. 41.

[43] J. Branch, "Mapping the Sovereign State: Technology, Authority and systematic change".*International Organization*. Vol. 65, (Winter 2011). pp. 15-16.

[44] Ibid. pp. 7-8, 12-13, 20-21, 27-38.

[45]O. Lo¨wenheim, 2007 (1); pp. 31-32.

[46]R. H. Kaplan, "The Coming Anarchy," in: P. Williams, D. M. Goldstein and J. M. Shafritz (eds.), **Classic Readings of International Relations**, (2nd Ed.), (Pittsburgh: Harcourt Brace College Publishers, 1999), pp. 667.

[47]Zacher, 2001; 216-234.

[48]Ibid. 215-216.

[49]Ibid. 244-248.

[50]R. Silfen, (2009). "Uti Possidetis Juris: Same Same but Different". Paper presented at the International Law Forum, HUJI, pp. 13-17.

[51]להרחבה ר' טבלה הסוקרת את כלל העימותים בהם תוקפו הגבולות הקולוניאליים בין השנים 1946-2000 (Zacher, 2001; 225-228).

[52]ר' למשל Abbate, 1999; Franda, 2001; Drezner, 2004.

[53]להרחבה ר' סיכום פסגת ה WSIS של האו"ם בתוניס מ 2005, במסגרתה הוחלט למעשה להותיר את ארגון ICANN כגוף המנהל את מערכת שמות המתחם העולמית ולייסד את פורום ה IGF במסגרתו פועלות מדינות להשפיע על מדיניותו (United Nations. 2006: §8).

[54]P. Mockapetris, "Domain Names - Concepts and Facilities," *RFC 882*, 1983. pp.1-2.

[55]J. Postel and J. Reynolds, "Domain Requirements," *RFC 920*, 1984. pp. 1; P. Mockapetris, "Domain Names - Concepts and Facilities," *RFC 882*, 1983. pp.5

[56] H. Feld, (2003) "Structued to Fail: ICANN and the 'Privatization' Experiment". In: A. Thierer and W. C. Clyde Jr., **Who Rules the Net? Internet Governance and Jurisdiction**. (Masochist: Cato Institute, 2003), Pp. 345.

[57]E. Rony and P. Rony, **The Domain Name Handbook: High Stakes and Strategies in Cyberspace**. (Kansas: R&D Books, 1998.)

[58]J. Postel, "Domain Name System Structure and Delegation," *RFC 1591*, 1994. §2.

[59] "Stateless persons for whose acts on the high seas no state would be held accountable" (Thompson, 1994; 144)

[60]O. Lo¨wenheim, 2007 (1); 18-19.

[61]חכים ביי, TAZ - אזור אוטונומי ארעי, (ירושלים: רסלינג, 2002), עמ' 61-59.

[62]O. Lo¨wenheim, 2007 (1); 81-82.

[63]E. S. Finer, "State-building, state boundaries and border control : An essay on certain aspects of the first phase of state-building in Western Europe considered in the light of the Rokkan-Hirschman model," 1974. pp. 85; C. Tilly, "War Making and State Making as Organized Crime," in: P. B. Evans, D. Rueschemeyer and T. Skocpol, **Bringing the State Back In**, (Cambridge: Cambridge University Press, 1985). pp. 171-175.

[64] Tilly, 1985; 173.

[65]Thompson, 1995; 216.

[66] M. L. Mueller, **Networks & States: The Global Politics of Internet Governance**, (MA: MIT Press, 2010).

[67]O. Lo¨wenheim, 2007 (1); 14-16.

[68] Thomson, 1992; 217.

[69] C. Tilly, **The Politics of Collective Violence**, (United Kingdom: Cambridge University Press, 2003), pp. 27.

[70] להרחבה ר' בספרו של לווינהיים ((1) 2007 ,Lo"wenheim).

[71] J. Healey (ed.), **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. (CCSA Publication, 2013), pp. 44.
טיפולוגיה של רמת שיתוף הפעולה בין מדינות לפעולות של האקרים עצמאיים ניתן למצוא אצל הילי בטבלה 3.

[72] Ibid.

[73] Ibid. Pp. 62

[74] Ibid. Pp. 63

[75] J. Carr, **Inside Cyber Warfare**. (CA: O'reilly Media, 2009), Pp. 47-50.

[76] R. I. Rotberg, **State failure and state weakness in a time of terror**, (Whashington DC: Brookings Institution Press, 2003), pp. 1-11.

[77] H. R. Jackson and C. G. Rosberg, "Why Africa's Weak States Persist: The Empirical and the Juridical in Statehood," *World Politics*. Vol. 35, No. 1 (Oct. 1982), p.3.

# שוברים את הכללים וכולם משחקים - על המפגש בין המרחב הקיברנטי לבין כללי המשפט הבינלאומי

**שרון אפק**[i]

*"אז נבקעו החומות ונפתח לרווחה את השער.*
*אצו רבים לעזרה, גלגלים למפלצת ישימו,*
*גם את ערפם נתנו למושכות להזיז את הרכש.*
*אט צעדה המכונה אל הדביר הרת-נשק וחרב.*
*יחד יצאו במחול בחורים ובתולות וישירו*
*זמר-תודה לאלים וישישו לנגע בחבל.*
*ככה חדרה המכונה אל טבור הקריה לאידנו"*

מתוך: וירגיליוס, אינאיס, ספר שני, תרגם: שלמה דיקמן.

## מבוא - המרחב הקיברנטי והמשפט הבינלאומי

סיפורם של הדינים, המסדירים את הלחימה בין בני אדם, הוא סיפור של מעבר בין ממדים או מרחבים. הלחימה החלה על פני היבשה, עברה אל גלי הימים, נמשכה אל המרחב האווירי ואף חדרה לחלל החיצון. אין ממד או מרחב, ממנו התעלמו מדינות ומנהיגים בשאיפתם להשיג עוצמה מדינית, כלכלית וצבאית.

סיפורה של המלחמה ודיניה הוא גם סיפור של התפתחויות טכנולוגיות. זאת החל מעידן הכלים (המצאת הגלגל), דרך עידן המכונות (למשל השימוש בארטילריה), עידן המערכות (כגון רדאר ומטוסים ארוכי טווח) ועד עידן האוטומציה והמידע (מערכות תקשורת ומחשוב מתוחכמות)[1].

את הלחימה המודרנית מרבים לתאר כלוחמת מידע, לאור המקום הנכבד שתופס בה השימוש בטכנולוגיית מחשבים[2]. במאה העשרים ואחת, רשתות תקשורת ומחשבים הם מרכיב משמעותי ביותר בביטחון הלאומי של מדינות.

---

[i] **אלוף משנה שרון אפק מכהן כיום כמפקד קורס פיקוד ומטה (פו"ם) 'אפק' במכללות הצבאיות.** מאמר זה נשען על פרסומו "ההתקפה הקיברנטית - קווים משפטיים לדמותה, יישום כללי המשפט הבינלאומי על לוחמה במרחב הקיברנטי", בבמת הפרסום של מרכז המחקר של המכללה לביטחון לאומי, *עשתונות*, גיליון מס' 5, אוקטובר 2013.

הם מעצימים את כוחן של מדינות ופותחים בפניהן אופקים חדשים, אך בה בעת, התלות בהם מחדדת את הפגיעות והרגישות של מדינות להתקפות עליהן במרחב המכונה 'קיברנטי'[3].

מהו 'המרחב קיברנטי', אותו מרחב יציר אדם, אשר התפתח במהירות כה גדולה ועלול להפוך לשדה לחימה מודרני? זהו מונח מורכב, לו הגדרות רבות. כך למשל, ההגדרה של משרד ההגנה האמריקני היא:

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers"[4].

הגדרה זו מקיפה עולם רחב, הכולל את רשת האינטרנט והרבה מעבר לכך, לרבות רשתות תקשורת, חומרה ותוכנה, מחשבים, טלפונים ניידים, לוויינים, גלי רדיו, סיבים אופטיים ועוד.

בלבו של המרחב הקיברנטי מצויה רשת האינטרנט ('מרשתת', בעברית תקנית). האינטרנט, אסופה של רשתות המקושרות ביניהן, פותחה בשנות השישים בארצות הברית כ-ARPANET, תוכנה צבאית שנועדה לקשר בין הרשתות של משרד ההגנה האמריקני, קבלנים שעבדו עמו ורשתות שנפרשו במספר אוניברסיטאות[5]. הרשת, שנשענה בראשיתה על מספר קווי טלפון שחיברו מחשבים בודדים, היא כיום ענק גלובלי, המקשר חלק נכבד מהאנושות[6]. במציאות המודרנית, למרחב הקיברנטי חלק משמעותי בכל תחום כמעט של חיינו, ומגמת ההרחבה של השפעתו צפויה להתעצם.

רשת האינטרנט נשאה עמה בשורה חדשה. היא תוכננה במטרה להיות פתוחה, מינימליסטית וניטראלית[7]. מבחינה טכנולוגית היא חסרת גבולות, חוצה גבולות וגלובלית[8]. אדם הניצב מול מסוף מחשב, עשוי בלחיצת כפתור לבצע פעולה, שתהדהד במקום הרחוק ממנו אלפי מילין. הוא עשוי לתרום בכך לידע, לרפואה, לכלכלה ולחברה, אך לפעולתו עלולה להיות גם תוצאה מזיקה. לצד היתרונות העצומים של המרחב הקיברנטי, והאפשרויות הבלתי

מוגבלות של שימוש בו לתכלית טובה, הוא משמש גם כר פורה לריגול, פגיעה בזכויות אזרח, פשיעה, גרימת נזק וטרור[9].

כאשר התפתח המרחב הקיברנטי, היו שציירו אותו כ-'מערב פרוע' נטול סדר וחוקים[10]. למעשה, אופיו החתרני והפתוח של המרחב היה אחד ממוקדי המשיכה אליו. עם הזמן, לצד הפיכת המרחב למרכזי כל כך בהוויה האנושית, הולך ומתפתח שיח בעניין יצירת 'משטר קיברנטי'[11]. על רקע האופי הגלובלי וחוצה הגבולות של המרחב, ברור שהסדרה תחייב מעורבות של שחקנים רבים ושיתוף פעולה בינלאומי.

יצירת משטר קיברנטי כרוכה, בין השאר, בגיבוש כללי משחק מתחום המשפט הבינלאומי. כללים שיגדירו את המותר והאסור בין שחקנים בינלאומיים, ובין השאר, יפתרו את סימני השאלה ביחס לפעילות התקפית במרחב הקיברנטי.

## א. התקפה במרחב הקיברנטי

אחד מאתגרי העיסוק המשפטי במרחב הקיברנטי הוא הצורך לגשר בין המונחים המקצועיים (הקיברנטיים), לבין עולם המושגים המשפטי. הדבר בולט ביחס למונח מרכזי, אשר עתיד לעמוד בלב ההסדרה המשפטית - 'התקפה' (Attack)[12].

התקפות קיברנטיות הפכו כבר לשגרה, אך טרם התגבשה הבנה מוסכמת ומקובלת בזירה הבינלאומית ביחס להגדרתן. הדבר אינו כה מפתיע, שכן מונחים משמעותיים אחרים, כמו 'טרור', טרם זכו להגדרה בינלאומית מוסכמת[13].

הניסיון להגדיר התקפה קיברנטית מחדד את פערי היסוד והמחלוקות האסטרטגיות בין המעצמות הקיברנטיות. בפרט, קיימים קיטוב וחשדנות הדדית, על רקע שוני באינטרסים ובתפיסות, בין ארצות הברית ומדינות המערב לבין רוסיה וסין.

בארצות הברית, לאחר שהוקם פיקוד ייעודי למרחב הקיברנטי[14], החלו להתפרסם, משנת 2011, הגדרות רשמיות להתקפה קיברנטית. בהכללה, ההגדרות שאומצו על ידי ארצות הברית, נאט"ו ומדינות מערביות אחריות,

כוללות שלושה רכיבים: אמצעי התקיפה (פעולה באמצעות מחשבים ורשתות); גרימת נזק; והתשתית המותקפות (מחשבים, מידע ורשתות של הגורם המותקף).

העמדה של רוסיה וסין, מנגד, שמה דגש על כך שפעולות מסוימות במרחב הקיברנטי הן פסולות. ניתן למשל ללמוד עליה מתוך גישת Shanghai Cooperation Organization.[15] הארגון שולל הפצת מידע, שנועדה להזיק למערכות חברתיות, פוליטיות וכלכליות, ומבקש לאסור שימוש במרחב הקיברנטי, באופן המערער את היציבות הפוליטית[16]. למותר לציין שגישה זו אינה מתיישבת עם ערכים מערביים, הנתפסים כאבן יסוד של המרחב הקיברנטי, כגון חופש הביטוי, הזכות לקבל מידע ולהחליף מידע בזמן אמת ועוד [17].

הספרות המשפטית מנתחת על פי רוב שלושה סוגים מרכזיים של התקפות קיברנטיות[18]:

הראשונה, *Distributed Denial of Service* (DDoS בקיצור, ובעברית: 'שלילה מבוזרת של שירותים') - דרך פעולה נפוצה בשנים האחרונות. בסוג התקפות זה, מוחדר וירוס לאלפי מחשבים, המאפשר שימוש בהם לצרכי הגורם החודר. בהמשך, באופן מתואם, אותם Botnets - אלפי מחשבים ש'נחטפו' - משבשים את השרתים המותקפים, באמצעות כניסה שיטתית והמונית לאתרים מסוימים. זאת, עד לנפילת האתרים כתוצאה מהעומס ומניעת פעילות באותם אתרים. היתרון בשיטה הוא השימוש באלפי מחשבים 'תמימים' מסביב לעולם, תוך שמירת אנונימיות התוקפים. כיום ניתן לרכוש מגורמים עבריינים את השירות של ביצוע התקפת DDoS.

השנייה, *שתילת מידע שגוי* - התוקף מחדיר מידע שגוי למערכת מחשב, כאשר זו ממשיכה לכאורה לפעול בצורה תקינה, גם כאשר היא סוטה ממשימותיה[19]. כך למשל, נטען כי ארצות הברית תכננה בשנת 1999 להזין מידע שגוי במערכת ההגנה האווירית של סרביה ולנטרל כך את יכולתה לפגוע במטוסי נאט"ו[20].

השלישית, *חדירה לרשת מחשבים וביצוע פעולות באמצעותה* - להתקפה מסוג זה פוטנציאל לשבש מערכות רגישות, למשל כאשר מערכות מחשבים שולטות

על מפעלים גדולים ותשתיות כמו חשמל ומים (מערכות SCADA - Supervisory Control and Data Acquisition).

## ב. התקפות הדגל הקיברנטיות בזירה הגלובלית

מלחמה קיברנטית, יום הדין הטכנולוגי, נתפסה בעבר כמדע בדיוני. בשנים האחרונות, התקפות קיברנטיות מדווחות, לא אחת, בראש מהדורות החדשות[21], כפי שארע לאחרונה ביחס לחילופי המהלומות הקיברנטיים בין צפון קוריאה לבין ארצות הברית, על רקע סרט שעסק בשליט צפון קוריאה. כותבים מצביעים על תרחישים מטרידים, בהם התקפות אלו מסיטות רכבות נוסעים ממסילותיהן, מחשיכות ערים, מפוצצות צינורות נפט וגז ומשביתות שדות תעופה[22]. הדעה הרווחת היא שסכסוכי העתיד (ולמעשה כבר במאבקי ההווה), יכללו גם לחימה קיברנטית, שמטרתה פגיעה בתשתיות, במידע, בכלכלה וברוח האנשים[23]. אין זה מפתיע שביטחון המרחב הקיברנטי הוכתר על ידי האו"ם כאחד האתגרים המשמעותיים במאה העשרים ואחת[24].

במרחב הקיברנטי טרם התרחשו אירועים מכוננים (טרם ארע "9/11 קיברנטי"), ששינו באופן דרמטי את התודעה המדינית והצבאית העולמית. ועדיין, בשנים האחרונות המחישו התקפות קיברנטיות את הפוטנציאל ההרסני הטמון בכלים וביכולות קיברנטיים. להלן יוצגו בקצרה כמה מהמקרים הידועים והבולטים ביותר.

### ההתקפה על אסטוניה

באפריל - מאי 2007 נערכו התקפות מסיביות על רשת המחשבים של אסטוניה[25]. זאת בתגובה לכוונת ממשלת אסטוניה להעביר אנדרטת זיכרון למלחמת העולם השנייה ממרכז עיר הבירה, טאלין, לבית קברות צבאי בפרברי העיר. ההתקפות נמשכו כחודש וכוונו נגד תשתיות אינטרנט ציבוריות וכלכליות, לרבות של הנשיא, ראש הממשלה, הפרלמנט, מפלגות, בנקים, גופי תקשורת וספקי אינטרנט[26]. ההתקפות היו מסוגים שונים - DDoS, השחתת אתרי אינטרנט, הרס מידע ממוחשב ועוד, והובילו לנפילת שרתים ואתרי אינטרנט.

**תמונה מס׳ 1: אנדרטת הזיכרון בטאלין**[27]

באסטוניה מהווה האינטרנט כלי משמעותי בתחומים רבים, והמדינה אף תוארה כמדינה הפגיעה ביותר להתקפות קיברנטיות[28]. חצי מהאוכלוסייה השתמשה בשנת 2007 באינטרנט לקבלת שירותים ממשלתיים; הממשלה פעלה ׳ללא נייר׳; 95% מהפעילות הבנקאית נוהלו באופן דיגיטלי ו-98% משטח המדינה היה מרושת קיברנטית[29]. בהתאם, להתקפות היו השלכות משמעותיות: יכולת הפעולה האפקטיבית של שני הבנקים המרכזיים במדינה שותקה למספר ימים, חצי מסוכנויות החדשות המרכזיות נתקלו בקשיים[30], נפגעה גביית המסים, נותקו קווי החירום במדינה למשך שעה, ניזוקה התקשורת הפרטית והציבורית, ולא פחות חשוב - נפגע האמון בכלכלת המדינה. הנזק הכלכלי של התקיפות נאמד בין 27.5 ל-40 מיליון דולרים.

בהתקפות נגד אסטוניה נוצלו כמיליון מחשבים. חלקם הקטן בשימוש ישיר ורובם כ׳זומבים׳, לאחר שהוחדרה בהם תוכנה זדונית. התקפות רבות בוצעו מרוסיה, אך העקבות הובילו ל-177 מדינות לפחות[31]. רוב ההתקפות בוצעו ממחשבים בעלי כתובת (IP) פרטית, אך אותרו גם מחשבים בשליטת מוסדות ממשלתיים רוסיים.

החשד לביצוע ההתקפות נפל, מטבע התפתחות האירועים, על רוסיה. יש הטוענים כי רוסיה הפעילה לשם כך ארגוני חסות. עם זאת, לא הוצגו הוכחות

חזקות וחד משמעיות שממשלת רוסיה ביצעה את ההתקפות או עמדה מאחוריהן. אסטוניה עצמה קבעה שההתקפות בוצעו על ידי קבוצות פטריוטיות של פצחנים (האקרים) רוסיים, מבלי שייחסה אותן ישירות לממשלת רוסיה[32]. אסטוניה הגיבה בעיקר בפעולות כמו הרחבת פסי התקשורת, ובמאמץ דיפלומטי משותף עם גורמי נאט"ו.

חשיבותן של ההתקפות על אסטוניה בהיותן 'קריאת השכמה', המבשרת על העידן החדש. לראשונה, מדינה מצאה עצמה מתמודדת עם התקפה רחבת היקף ומשמעותית, שבוצעה, ככל הנראה, בחסות מדינה אחרת, במרחב הקיברנטי.

**ההתקפה על גיאורגיה**

בקיץ 2008 פרץ סכסוך בין גיאורגיה לבין רוסיה, לאחר שכוחות גיאורגים חדרו לחבל דרום אוסטיה. מבחינה משפטית, היה זה סכסוך מזוין בינלאומי (International Armed Conflict), כלומר כזה המתקיים בין מדינות וחלים עליו דיני המלחמה. המאבק הפיזי לא היה ממושך והוכרע במהרה לטובת רוסיה.

עוד בטרם החלה תנועת כוחות הצבא הרוסי, בוצעו התקפות קיברנטיות רחבות היקף נגד גיאורגיה[33], לרבות תקיפות DDoS על אתרי אינטרנט ממשלתיים והשחתת מידע באופן קיברנטי. התקיפות ארכו כחודש ונמשכו גם לאחר שהושגה הפסקת אש בשדה הקרב.

גיאורגיה אינה אסטוניה מבחינת משקל המרחב הקיברנטי, ולכן הפגיעה בה הייתה, באופן יחסי, פחות חמורה. עדיין, נפגעו שירותים ממשלתיים, זמינות הבנקים ואמינות המערכות הממוחשבות במדינה[34]. מטרות ההתקפות לא היו רק פיזיות, אלא גם (ובעיקר) יצירת לחץ על האוכלוסייה בגיאורגיה[35].

גם במקרה זה, לא נמצאו ראיות חד משמעיות, שאפשרו לייחס לרוסיה אחריות להתקפות או מעורבות בהן. הסברה המקובלת היא שרוסיה לכל הפחות עמדה מהצד, שעה שפצחנים (האקרים) רוסיים ביצעו את ההתקפות נגד גיאורגיה[36].

חשיבות ההתקפות על גיאורגיה בכך שהדגימו לראשונה את האופן בו שזורות פעולות במרחב הקיברנטי במלחמה מודרנית. הן חידדו את ההבנה, כי לצד המערכה הצבאית, תתקיים מערכה קיברנטית משלימה.

**התקפת Stuxnet באיראן**

בשנת 2010 נפגעה התכנית הגרעינית של איראן, כתוצאה מפעולת וירוס, המכונה Stuxnet, במתקן להעשרת אורניום בנתנז. תולעת (Worm) שחדרה למערכות במתקן, גרמה לצנטריפוגות להסתובב במהירות גבוהה מהרצוי, מבלי שמנגנוני השליטה במתקן יאתרו את התקלה, דבר שהוביל לכך שהצנטריפוגות נהרסו[37].

פעולה זו מתוארת בכתיבה המשפטית כתקדים משמעותי (יש אף הרואים בה 'שינוי של כללי המשחק'). זהו וירוס המחשבים הידוע הראשון, שגילם יכולת להתקיף באופן ספציפי מערכת תעשייתית[38] (מהסוג המכונה - SCADA, Supervisory Control and Data Acquisition) ולגרום לה נזק רב. אם עד אז, התקפות קיברנטיות גרמו לשיתוק מחשבים ולאובדן מידע, לראשונה גרמה התקפה כזו הרס פיזי לרכוש[39]. הדבר חידד את הפוטנציאל של התקפות קיברנטיות כאמצעי של יצירת אפקט הרס ליריב.

גורמים באיראן ובמדינות אחרות ייחסו את ההתקפה לארצות הברית ולישראל[40], אך לא הוצגו ראיות של ממש למעורבות של מדינה כלשהי בפיתוח הווירוס או בהפצתו.

וירוס ה- Stuxnet התאפיין במורכבות וברמת תחכום גבוהה. בשנים שלאחר גילויו, הופצו וירוסים נוספים ברמת פיתוח גבוהה, כגון אלו המכונים Flame, DuQu ו- Gauss, אך אין מידע חד-משמעי לפיו הללו גרמו, באופן ישיר, נזק לתשתיות.

**התקפות סיניות בארצות הברית**

בשנים האחרונות הצטברו סימנים לקיומה של תכנית רחבת היקף, במסגרתה נערכות התקפות קיברנטיות בחסות ממשלת סין[41]. חברות אבטחת מחשבים בארצות הברית שבות ומדווחות כי 'שחקן מדינתי' (הכוונה לסין), מבצע במשך שנים התקפות נגד גופי ממשל וכלכלה רבים בארצות הברית. כך למשל, אחת ההתקפות הידועות, אשר בוצעה כבר בשנת 2005, כונתה "Titan Rain"[42].

בחשיפה משמעותית לכאורה, פרסמה בפברואר 2012 חברת האבטחה Mandiant, כי יחידה בצבא סין שמספרה 61398 פרצה את מערכות המחשוב של שלוש חברות ענק אמריקניות לפחות (קוקה קולה, ענקית האבטחה הממוחשבת RSA, וחברת לוקהיד-מרטין - יצרנית מטוסי הקרב הגדולה במערב). בנוסף, בוצעו התקפות סיניות משמעותיות נגד חברות אמריקניות ומערביות אחרות, לרבות כאלו המפעילות תשתיות קריטיות בתחומי האנרגיה והמים.[43]

חשיבותן של ההתקפות הקיברנטיות הסיניות בכך שהן מרכיב במימוש אסטרטגיה של מעצמה, הרואה בהן תרומה לאינטרסים רחבים של ביטחון לאומי. לפי הפרסומים, בלב פעילות זו עומדים שיקולים כלכליים, אך היא מהווה בהחלט גם פלטפורמה לפעילות עתידית בעלת אופי ביטחוני וצבאי.

## ג. מבט להמשך - האטרקטיביות של התקפות קיברנטיות

התקפות במרחב הקיברנטי מאתגרות את כללי המשחק הקיימים והתפיסות המקובלות. במובן זה, הן מזכירות סוג אחר של התקפות, אשר מצאו את הקהילה הבינלאומית בלתי מוכנה - הטרור העולמי, בעיקר מאז שנת 2001. באופן לא מפתיע, ארגוני טרור מוצאים במרחב הקיברנטי כר פורה לפעילות, בין נגד גופים ממשלתיים ובין נגד גורמים מהמגזר הפרטי[44].

למרבה הצער, דרך הטרור אומצה כדרך פעולה מועדפת על ידי קבוצות ופרטים רבים, והשפעתה על הזירה האזורית והגלובלית רבה. ניסיון לנתח את ההתפתחויות ביחס להתקפות קיברנטיות, מוביל למסקנה כי גם הן נתפסות

וצפויות להמשיך ולהיתפס בקרב מדינות, ארגונים ופרטים כאטרקטיביות. בהתאם, היקפן ועוצמתן עלולים לצמוח.

טעמים רבים עומדים בבסיס המשיכה אל התקפות קיברנטיות כדרך פעולה[45]. להלן יוצגו, על רגל אחת בלבד, חלק מאותם טעמים[46].

ראשית, יכולת ההסתרה של פעולות קיברנטיות. שחקן מתוחכם יכול להסתיר את זהות מבצע ההתקפה ומקורה הגיאוגרפי, ולעיתים אף את עיתויה, אמצעיה והשפעותיה. פעולות קיברנטיות ניתנות גם לביצוע באופן מקוטע, כמארג של פעולות נפרדות, כך שתיתפסנה כאירועים מבודדים, מבלי שניתן להתחקות אחר 'התמונה הגדולה'[47].

בנוסף, ניתן להפעיל גורמים פרטיים בעלי ידע לביצוע ההתקפות, בין אם גורמים עבריינים הפועלים בתשלום ובין אזרחים הפועלים מתוך רגש פטריוטי[48]. הדבר מסייע למסך את מעורבות הגורם היוזם. לעיתים, פעולות שנתפסות כוונדליזם או פיראטיות במרחב הקיברנטי, הן בעצם יוזמה מדינתית.

מעבר לכך, גם אם הגורם המותקף מגלה את מקור ההתקפה, הנזק שנגרם על ידי התקפה בודדת אינו שווה תמיד את המחיר הכרוך בתגובה, בפרט תגובה בכוח צבאי 'מסורתי'[49].

שנית, עלותה של הטכנולוגיה הנדרשת לביצוע התקפה היא נמוכה (באופן יחסי), זמינותה גבוהה ואין היא מחייבת כוח אדם בהיקף רחב. זאת ועוד, התקפות קיברנטיות אינן מוגבלות בשיקולי זמן ומרחק או בגבולות מדיניים פיזיים. מבחינה טכנולוגית, באופן בו המרחב הקיברנטי התפתח, ההתקפה במרחב תהיה ככל הנראה תמיד חזקה מההגנה, והגנה מושלמת אינה קיימת[50].

שלישית, התקפה קיברנטית היא כלי משמעותי מול יריב חזק, אשר נהנה מיתרון משאבי וטכנולוגי, אך סובל מפגיעות במרחב הקיברנטי. היתרון הטכנולוגי של מעצמות עלול להפוך לחרב פיפיות, כאשר תלותן בתשתית מחשבים תנוצל לשם פגיעה בהן. המרחב האינטרנטי יכול לשחק תפקיד משווה (מלשון שוויון), במובן שהוא מאפשר פגיעה ביתרונותיו של יריב בעל עוצמה צבאית וטכנולוגית.

רביעית, התקפות קיברנטיות עשויות לאפשר פגיעה בהתפתחות התעשייתית, הטכנולוגית, הכלכלית והחברתית של היריב. אלו תחומים שפגיעה קונבנציונלית או קינטית בהם מצויה מחוץ לכללי המשחק. ליכולת, למשל, להשיג באמצעים קיברנטיים את הפיתוחים הטכנולוגיים העדכניים ביותר של היריב, עשויים להיות יתרונות כלכליים וצבאיים, שלא ניתן להפיק בדרך אחרת וקשה להפריז בחשיבותם[51].

הנקודה האחרונה לא נעלמה מעינם של קובעי המדיניות ומנסחי התפיסות במדינה כמו סין (שם גם נעשה שימוש במינוח מתחום הביטחון הלאומי: סין כ- "Cyber Power")[52]. בראייה הסינית, הפעילות הצבאית היא חלק מתחרות אסטרטגית רב תחומית, המתקיימת בממדים כמו לוחמת מידע, מסחר, מטבע ומדיה[53]. מדינות המבקשות להיאבק בממדים אלו ביריביהן, בעצימות נמוכה ומבלי לחצות את הסף שיוביל לתגובה צבאית, ימצאו במרחב הקיברנטי מגרש מהמעלה הראשונה לקידום מטרותיהן[54].

חמישית, כשם שהמשטר המשפטי בתחום ההתמודדות עם טרור טרם הבשיל לכדי הסדרה מלאה, כך טרם הוסדר הפן המשפטי של המרחב הקיברנטי. היעדר משטר משפטי בינלאומי אפקטיבי וחוסר מורא מענישה, מעודדים בחירה באמצעי של התקפות קיברנטיות ואת אי-היציבות העלול להיגרם מכך. המשך המאמר יעסוק בכינון המשטר המשפטי ואתגריו.

### ד. עיצוב כללי המשחק

בשנים האחרונות הלכה והתחדדה תשומת הלב של מדינות למרחב הקיברנטי, תוך הפנמת חשיבותו הגדולה של המרחב וחיוניותו לביטחון, לכלכלה ולחברה. זהו תהליך הדרגתי, המונע על ידי מספר גורמים, כמו הבנת משקל המרחב על חיי היום יום והאינטרסים הכלכליים הטמונים בו; הרצון של ממשלות מסוימות להגביר את הפיקוח על מידע 'מערער יציבות' ברשת האינטרנט; ההתקפות הקיברנטיות שכבר התרחשו ב'זירת הלחימה' החדשה והחשש מהתקפות עתידיות וחמורות יותר.

השנים הקרובות צפויות להיות תקופה מכוננת ורבת חשיבות בעיצוב המשטר העתידי שיחול במרחב הקיברנטי. קצרה היריעה מלספק, במסגרת זו, ניתוח

עמוק של ההקשר האסטרטגי הרחב והגורמים המעצבים והמשפיעים. עם זאת, דומה שראוי להצביע על מספר מהלכים המצויים בעיצומם: במישור המדינתי - גיבוש מדיניות בהקשר הקיברנטי; השיח באו"ם בתחום בקרת הנשק הקיברנטי; והחתירה ליצירת כללי משחק משפטיים.

**גיבוש מדיניות קיברנטית**

אשר למישור המדינתי, בהכללה, ההתפתחות המהירה של המרחב הקיברנטי תפסה את מדינות העולם בלתי מוכנות להתמודד עם אתגרי השעה. מדינות רבות, בעיקר במערב, נדרשו לפתח, תוך זמן קצר, מדיניות חוץ וביטחון בהקשר הקיברנטי; לנסח דוקטרינה; להקים גופי מטה ומבנים ארגוניים; להקצות משאבים; ואף לגבש מדיניות משפטית[55] ולקדם משטר משפטי.

המדינה המובילה את העיסוק בנושא, ארצות הברית, פרסמה במאי 2010 את מסמך האסטרטגיה הביטחונית הלאומית, בו תואר האיום הקיברנטי כ"אחד האיומים הרציניים ביותר לביטחון הלאומי, ביטחון הציבור והכלכלה, שאנו מתמודדים עמם כאומה"[56]. הממשל האמריקני מודע היטב לכך שההישענות על טכנולוגיה מודרנית ועל המרחב הקיברנטי, עלול להיות עקב אכילס של ארצות הברית[57]. בהתאם, זוהה הצורך בריסון השימוש ברשת, שיסכן את העליונות הכלכלית והצבאית האמריקנית. נשיא ארצות הברית עצמו התייחס לכך ביולי 2012:

"It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill. This is the future we have to avoid"[58].

ציטוט נוסף מלמד על האינטרס האמריקני:

"Having some effective limits on what nations actually do with their cyber war knowledge might, given our asymmetrical vulnerabilities, be in the U.S. national interest"[59].

במסגרת ההיערכות האמריקנית למציאות החדשה, פרסם משרד ההגנה בשנת 2011 את המסמך שכותרתו: Strategy for Operating in Cyberspace. במסמך הוגדר המרחב הקיברנטי כממד אופרטיבי, בדומה לממדים המסורתיים - יבשה, ים, אוויר וחלל[60]. מעבר לכך, הוקם לראשונה פיקוד קיברנטי, האחראי על הפעילות בממד זה. הקמת הפיקוד אינה סמלית בלבד, אלא מדובר בצעד משמעותי של ריכוז כל היכולות והסמכויות האמריקניות במסגרת ארגון אחד, אשר יוכל להוביל ספקטרום רחב של פעילות מבצעית במרחב הקיברנטי[61].

בארצות הברית מתקיים דיון ער במיוחד, שעניינו הנורמות שיחולו במרחב הקיברנטי. מורכבות הדיון נובעת, בין השאר, מהמתח הנעוץ בהיות המרחב שדה לקידום האינטרסים של ארצות הברית, אך גם לפגיעה קשה ב'בטן הרכה' שלה[62].

בדומה לארצות הברית, הנושא זוכה לעיסוק נרחב גם בבריטניה, בארגון נאט"ו, ואף במדינות שאינן מערביות כמו סין ורוסיה[63]. רוסיה, למשל, פרסמה בשנת 2011, באופן חריג, מסמך תפיסתי, המנחה את הכוחות המזוינים של המדינה ביחס לפעילות במרחב המידע[64].

**הפעילות באו"ם**

צמיחת המרחב הקיברנטי, ההתקפות שבוצעו, הסיכונים הכרוכים בכך והתפתחותו של מעין מרוץ חימוש קיברנטי - כל אלו צפויים היו להוביל לדיונים בעלי אופי משפטי באו"ם[65]. כך קרה בפועל, תחילה באופן מהוסס ובשנים האחרונות היקף הדיונים הולך וצובר תאוצה.

בהכללה, הדיונים באו"ם מתקיימים בשני הקשרים מרכזיים: הפוליטי-צבאי, בו דנים בלוחמה קיברנטית, לעתים תחת הכותרת של בקרת נשק

(בעיקר במסגרת הוועידה הראשונה של האו״ם); וההקשר הכלכלי, בו דנים בעיקר בפשיעה במרחב הקיברנטי[66]. בהקשר הפוליטי-צבאי, לב הדיון הוא בשאלות, כיצד טכנולוגיות וכלים במרחב הקיברנטי, עלולים לשמש למטרות שאינן מתיישבות עם שמירת היציבות והביטחון הבינלאומיים ולסכן את הביטחון של מדינות, וכיצד הקהילה הבינלאומית נדרשת להגיב לכך.

זירת האו״ם היא מיקרוקוסמוס, ממנה ניתן ללמוד על מרוץ החימוש שמתרחש במרחב הקיברנטי, ועל האינטרסים השונים במסגרתו. באופן אירוני, רוסיה היא שמובילה קריאה בינלאומית לבקרת נשק במרחב הקיברנטי, ואילו ארצות הברית נתפסת לעיתים כמי שחוסמת מהלך כזה[67]. מבלי להרחיב, בשלב זה מוקדם להעריך את כיווני ההתפתחויות של היוזמות המקודמות במסגרת האו״ם והאם תבשלנה למשטר מחייב בהובלת הארגון.

**כינון המשטר המשפטי**

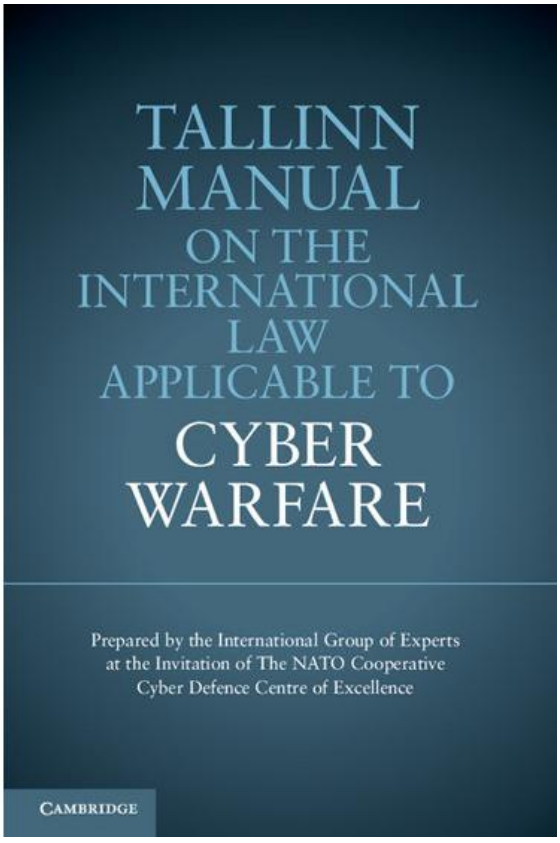
בעת הזו מצוי המשטר המשפטי הבינלאומי, שיסדיר את המרחב הקיברנטי, בשלבי התהוות ראשונים (Norm Emergence, במונחי אחד המודלים, המתאר התפתחות נורמות ביחסים בינלאומיים[ii]). זהו שלב של עיצוב כללי משחק משפטיים, בו גורמים שונים מנסים ליזום הצעות למשטר עתידי ולשכנע כמה שיותר מדינות וארגונים בינלאומיים לאמץ את הצעותיהם, בדרכים שונות. חלק מהיוזמות ממוקד בניסיון לפתח משטר משפטי, המכונה Soft Law, כלומר כזה שאינו מחייב ואינו ניתן לאכיפה. זהו משטר הכולל נורמות ועקרונות לא מחייבים, שמטרתו הסמויה, ולעתים המופגנת, היא להשפיע על הפרקטיקה של מדינות[68]. מסלול משפטי זה, המשולב בדיפלומטיה ציבורית ובשיח אקדמאי, מבקש לעצב גרסאות 'רכות' יותר של המשטר המשפטי העתידי, במטרה לעודד התקדמות בעיסוק המשפטי, כשלב מוקדם בתהליך רב שלבי[69].

תהליך משמעותי ברוח זו היה ניסוח מדריך טאלין (להלן גם - המדריך)[70]. המדריך נוסח על ידי קבוצת מומחים, בהובלת פרופ' מייקל שמיט מארצות הברית. התהליך שהביא לניסוח המדריך קודם על ידי גוף הפועל בחסות

[ii] מודל שפותח על ידי Finnemore & Sikkink, לא יורחב לגביו במסגרת זו.

נאט״ו, שעניינו שיתוף פעולה בהגנה במרחב הקיברנטי - NATO Cooperative Cyber Defence Centre for Excellence (NATO CCD COE). זהו גוף צבאי בינלאומי, שמקום מושבו בטאלין, אסטוניה. לפני מספר שנים, הוזמנה על ידו קבוצת מומחים בינלאומית לשם הפקת מדריך בנושא הדין החל על לוחמה קיברנטית[71]. עם קבוצת המומחים נמנו משפטנים בעלי ניסיון פרקטי רב, אקדמאים ומומחים טכניים[72]. התהליך שהחל בשנת 2009, הבשיל בקיץ 2012, אז הושלם המדריך ופורסם, תחילה באופן מקוון, ובמארס 2013 גם בדפוס[73].

**תמונה 2: מדריך טאלין**



**ד. המרחב הקיברנטי והמשפט הבינלאומי - ביחד או לחוד?**

הדיון המשפטי הראשון בחשיבותו, עניינו שאלת יסוד: האם כללי המשפט הבינלאומי המקובלים והקיימים מסדירים בכלל את המרחב הקיברנטי?

המענה לשאלה זו אינו חד משמעי. הדבר נובע, בראש ובראשונה, מכך שאותן אמנות בינלאומיות, המהוות את עמוד השדרה של כללי המשפט הבינלאומי, נוסחו בעידן שבו המרחב הקיברנטי היה בגדר מדע עתידי, ואינן מתייחסות כמובן ישירות למרחב זה. יתר על כן, לא קיימת פרקטיקה של מדינות, ממנה ניתן לגזור את הכללים שמנחים אותן בפועל בהתמודדות המשפטית עם המרחב[74].

עוד חשוב לציין, כי הגישות השונות לנושא מבטאות לא רק שיקולים משפטיים 'טהורים', אלא גם שיקולים רחבים יותר - אסטרטגיים ואידיאולוגיים. כך, המענה לשאלה עשוי להשתנות בהתאם למקום מגוריו של המשיב - בייג'ינג, מוסקבה או וושינגטון.

לאור האמור, נדרשות צניעות וביקורתיות ביחס לכל יומרה להציג, ברמה גבוהה של ודאות, את המצב המשפטי במרחב הקיברנטי.

אם בכל זאת נבקש להתחקות אחר עמדות בשאלת היסוד האמורה, נראה כי העמדה הסינית מכירה בצורך להחיל כללים בינלאומיים במרחב הקיברנטי, לרבות כללים המיועדים למנוע מיליטריזציה של המרחב, לעודד פתרון סכסוכים בדרכי שלום ולאסור שימוש בכוח[75]. סין מדגישה את היותה קורבן להתקפות במרחב הקיברנטי, בפרט מצד ארה"ב, יפן וקוריאה הדרומית[76], ומגנה את ניסיונות המערב למנוע ממנה פיתוח יכולות קיברנטיות.

אשר לגישה הרוסית, זו מכירה בכללי המשפט הבינלאומי הקיימים כנקודת מוצא לדיון במרחב הקיברנטי, אך מציגה להם פרשנות החורגת מפרשנותם המקובלת במערב, לצד דרישה להכללת עקרונות משפטיים נוספים[77].

סין ורוסיה ממוקדות בקידום אסטרטגיה שתיצור מרחב, המתאים יותר לאינטרסים שלהן. בראייתן, השליטה הדומיננטית של המערב במידע היא חלק מאסטרטגיה גדולה יותר של הגמוניה, האינטרנט בסגנונו המערבי מהווה איום על המשטרים שלהן, והמידע הוא נשק שחובה לפקח עליו[78].

אשר לעמדות במערב, ניתן להצביע על קשת של דעות, החל מכאלה המצדדות בהחלה מלאה של כללי המשפט הבינלאומי במרחב הקיברנטי; דרך דעות

לפיהן ההחלה מחייבת שינויי פרשנות ותפיסה; וכלה בדעה החולקת על תחולת הדין הקיים ביחס לפעולות קיברנטיות[79].

העמדה הדומיננטית בקרב גורמים רשמיים בממשלת ארצות הברית, כמו גם בקרב כותבים מובילים במדינה, היא שיש ליישם את כללי המשפט הבינלאומי גם על המרחב הקיברנטי[80]. עמדה זו באה לידי ביטוי במסמך האסטרטגיה הבינלאומית למרחב הקיברנטי, שפורסם בשנת 2011. שם נכתב:

"[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behaviour - in times of peace and conflict - also apply in cyberspace"[81].

דברים דומים נאמרו בנאום חשוב שנשא היועץ המשפטי של מחלקת המדינה בארצות הברית (להלן - נאום Koh) בספטמבר 2012.[82]

לצד הקביעה העקרונית, המקובלת בארצות הברית ובמדינות מערביות, כי יש להחיל את כללי המשפט הבינלאומי במרחב הקיברנטי, קיים מגוון של דעות בעניין מידת ההתאמה של הכללים למרחב הקיברנטי והקלות בה ניתן ליישמם. במסמך האסטרטגיה שהוזכר לעיל, נכתב כי נדרשת עבודה משפטית, במטרה לקבוע כיצד בדיוק הכללים חלים ומה נדרש כדי להשלים אותם. הכותבים מדגישים, כי ישנה אי בהירות ביחס לאופן בו ראוי ליישם את כללי המשפט הבינלאומי ביחס להתקפות בתחום הקיברנטי[83], וכי נדרשת בחינה משמעותית של כללי המשפט הבינלאומי לאור ההתפתחויות הקשורות לפריחת המרחב הקיברנטי[84].

### ה. האתגר בהחלת כללי המשפט הבינלאומי במרחב הקיברנטי

גם המאמינים ההדוקים ביותר בתחולתם הרחבה של כללי המשפט הבינלאומי, יסכימו לקביעה שהחלתם ויישומם במרחב הקיברנטי מאתגרים, בלשון המעטה[85].

המרחב הקיברנטי חותר תחת פרדיגמות מסורתיות של המשפט הבינלאומי. מספיק לאזכר חלק מהמאפיינים של כללי המשפט הבינלאומי והאופן בו התפתחו, כדי לעמוד על המורכבות של החלתם במרחב הקיברנטי.

כך למשל, המשפט הבינלאומי התפתח כאמצעי להסדרת יחסים בין מדינות, להן גבולות, טריטוריה וריבונות. במרחב הקיברנטי, לעומת זאת, פועלים שחקנים משמעותיים שאינם מדינות, בהם גופי ענק כלכליים כמו גוגל (Google), פייסבוק (Facebook) ואחרים, ארגונים כמו הקבוצה המכונה אנונימוס (Anonymous) ולהבדיל - ארגוני טרור, פצחנים (Hackers), גופים לא רשמיים המופעלים על ידי מדינות ועוד. יתר על כן, קשה להתייחס לפעילות קיברנטית במונחים כמו 'טריטוריה' 'הפרת ריבונות', 'כבוד לגבולות גיאוגרפיים', 'פעילות מדינתית' וכו'[86]. מונחים מרכזיים אלו מתחום המשפט הבינלאומי, כמעט זרים למרחב הקיברנטי, הפתוח והגלובלי.

אחת ההתפתחויות החשובות במשפט הבינלאומי בעשורים האחרונים היא הטלת אחריות על מדינות ועל פרטים, למשל במקרה של ביצוע פשעי מלחמה. הטלת אחריות במישור המשפטי מחייבת זיהוי של המדינה או הגורם שביצע את הפעולה וייחוס הפעולה לו, בהתבסס על ראיות. המרחב הקיברנטי, כפי שכבר הודגש, לא תוכנן על מנת לאפשר זיהוי של הפועלים בו. שחקנים מתוחכמים לא יותירו עקבות למעשיהם, ימנעו ייחוס (Attribution) של התקיפות אליהם[87] ואף יוכלו 'להפליל' גורמים תמימים. תקיפות הדגל במרחב הקיברנטי לוו אמנם בשלל ספקולציות ביחס לגורמים האחראים, אך ההשערות הללו לא נתמכו בראיות והוכחות של ממש, ולא בכדי.

כללי המשפט הבינלאומי, המסדירים לחימה, מבוססים על מספר עקרונות, בהם עקרון האבחנה (Distinction). העיקרון מחייב, בין היתר, להבחין בעת תקיפה בין לוחמים ומטרות צבאיות של האויב לבין אזרחים ורכוש אזרחי, תוך הימנעות מפגיעה באחרונים. עמידה בדרישת האבחנה מאתגרת בלחימה המודרנית בכלל, ועלולה להיות קשה ליישום פי כמה וכמה במרחב הקיברנטי. במרחב הקיברנטי שורר טשטוש כמעט מוחלט בין 'אזרחים' לבין 'לוחמים' ('לוחמים' עשויים להיות אזרחים, בלבוש אזרחי ובמשרד אזרחי, שנשקם מקלדת ומחשב)[88]. קיימת מזיגה כמעט מלאה של תשתיות אזרחיות ותשתיות

צבאיות, ללא הפרדה של ממש בין רשתות, מתקנים ומוסדות צבאיים לבין אלו האזרחיים[89]. מונחים כמו 'לוחם', 'מטרה צבאית', 'פרופורציונאליות' ו-'נזק אגבי', מחייבים, לכל הפחות, מחשבה חדשה ויצירתית בהקשר הקיברנטי.

בראייה רחבה יותר, ניתן לומר כי הכללים המשפטיים, באופן מסורתי, מבוססים על הפרדות ואבחנות: בין מדינות לבין גופים שאינם מדינתיים; בין תשתית צבאית לבין תשתית אזרחית; בין התקפה לבין הגנה עצמית וכיו"ב. המרחב הקיברנטי, לעומת זאת, אינו עולם של סיווג ברור ודיכוטומי. זהו מרחב של עמימות טבועה ומכוונת, מרחב פתוח לכולם, דינמי ומשתנה. המיזוג בו בין צבאי לאזרחי, בין מדינתי לפרטי, בין אינטרסים ותכליות פעולה שונים, רק יתגבר עם הזמן.

המרחב הקיברנטי מאיים לשבור (ואולי כבר שובר) את האבחנות המשפטיות המסורתיות, אינו מיישר קו עם הרציונל שבבסיס הכללים המקובלים, וחותר תחת דרך המחשבה המשפטית (והצבאית) האופיינית[90].

מאפיין נוסף של המרחב הקיברנטי, מעבר לשבירת הכללים (או מתיחתם לכיוונים חדשים), קשור בעובדה ש'כולם משחקים'.

בשעה שיש למשל מעט מדינות, אם בכלל, המסוגלות לאיים (באופן ריאלי) בתקיפה קינטית משמעותית על מדינות המערב, הרי שעם ההתפתחות הטכנולוגית, מדינות, ארגונים וגופים רבים הם תוקף פוטנציאלי (או הלכה למעשה) של מדינות המערב. במרחב הקיברנטי גם לשחקנים 'קטנים' יכולת להשפיע באופן משמעותי, הרבה מעבר לגודלם היחסי[91], על הביטחון הלאומי של מדינות אחרות.

זאת ועוד, מדינות המערב היו בעבר המעצמות הדומיננטיות שהובילו את עיצוב כללי המשפט הבינלאומי. הסדרה משפטית עתידית של המרחב הקיברנטי אינה צפויה להיות פריבילגיה של המערב. יתר השחקנים לא יהיו חותמת גומי ושותפים סבילים. סין ורוסיה הן מעצמות קיברנטיות ובעלות אינטרסים ומשקל בכל תהליך של הסדרה עתידית. ניתן להניח כי גם למדינות אחרות הפעילות במרחב (הודו ואיראן למשל) תהיה השפעה בתחום זה.

אכן, המשפט הבינלאומי כבר נדרש להתאים עצמו להרחבת הלחימה לממדים נוספים (ים, אוויר וחלל) ולהתמודדות עם תופעות חדשות ומשמעותיות (כמו נשק גרעיני וטרור). עדיין, המרחב הקיברנטי, על מאפייניו הייחודיים והאפשרויות האינסופיות הגלומות בו, עשוי להוות אתגר חסר תקדים בכל הקשור לישימות הכללים הקיימים. כדי לא להותיר את הדברים כלליים מידי, הדבר יודגם בהקשר אחד בלבד - הזכות להשתמש בכוח כהגנה עצמית כתגובה ל'התקפה מזוינת'.

**ו. הזכות להשתמש בכוח כהגנה עצמית כתגובה ל'התקפה מזוינת'**

אחד העקרונות החשובים במשפט הבינלאומי הוא איסור השימוש בכוח. האיסור מעוגן בסעיף 2(4) למגילת האו"ם, ונחשב, כפי שקבע בית הדין הבינלאומי בהאג, אחד מאדני היסוד של המגילה[92]. הסעיף קובע, בתרגום חופשי: "כל חברי האו"ם יימנעו ביחסיהם הבינלאומיים מאיום או משימוש בכוח נגד שלמותה הטריטוריאלית או עצמאותה המדינית של מדינה כלשהי, או בכל דרך אחרת שאינה מתיישבת עם מטרות האו"ם".

אם נעשה שימוש בכוח נגד מדינה מסוימת, עלולות להיות לכך השלכות מרחיקות לכת. כאשר השימוש בכוח חמור מספיק, ונחשב בגדר 'התקפה מזוינת' (Armed Attack), קמה למדינה המותקפת זכות לעשות שימוש נגדי בכוח, כהגנה עצמית[93]. מכאן, המרחק למלחמה עלול להיות קצר וכואב.

האם עקרונות וכללים אלו, שנולדו מתוך מחשבה על הפעלת נשק קונבנציונלי, כלומר קינטי, חלים גם על שימוש ב'נשק' המחשבים וברשתות התקשורת? הדעה המקובלת היא חיובית.

בית הדין הבינלאומי בהאג כבר פסק ביחס לאיסור השימוש בכוח, כי זה חל על כל שימוש בכוח, בלי קשר לשאלה באיזה נשק נעשה שימוש. היועץ המשפטי של מחלקת המדינה האמריקנית הצהיר, כי ארצות הברית תממש את זכותה להגנה עצמית, גם במקרה שתותקף באמצעים קיברנטיים, אם הפעילות נגדה תגיע לכדי 'התקפה מזוינת'[94].

אם כך, השאלה המתבקשת - אילו פעולות קיברנטיות עלולות להוות 'התקפה מזוינת'?

העמדה הדומיננטית במערב היא שהתקפה קיברנטית תהיה 'התקפה מזוינת' כשיהיו לה מאפיינים ותוצאות, המזכירים 'התקפה מזוינת' קינטית[95], כלומר גרימת מוות או פציעה של אנשים או פגיעה ברכוש.

גישה זו אומצה למשל במדריך טאלין, ובאה לביטוי במסגרתו בכלל מספר 13. בקרב מחברי המדריך היה קונצנזוס, כי פעולות קיברנטיות עלולות להיות כה חמורות, עד שיוצדק להגדירן כ'התקפה מזוינת'. הם הוסיפו, כי לא כל שימוש בכוח יהווה 'התקפה מזוינת'. נדרשים היקף וחומרה מסוימים ('Scale and Effects'), על מנת ש'שימוש בכוח' יגיע לכדי 'התקפה מזוינת'[96].

הגישה הרשמית האמריקנית הוצגה בספטמבר 2012 על ידי היועץ המשפטי של מחלקת המדינה (נאום Koh). לפי עמדה זו, התוצאות הפיזיות של הפעולה הקיברנטית הן המפתח להגדרתה: אם התוצאות הן מוות, פציעה או הרס רכוש משמעותי, התקיפה תיתפס כשימוש בכוח המהווה 'התקפה מזוינת' ומצדיק הגנה עצמית בכוח. כך למשל יהיה, כאשר התוצאות הפיזיות של התקפה קיברנטית תהיינה שקולות לתוצאות של הטלת פצצה או ירי טיל. כדוגמאות לפעולות קיברנטיות מסוג זה, הוצגו תרחישים תיאורטיים של גרימת התכה במתקן גרעיני, פריצה של סכר באזור מיושב או נטרול של בקרת תעופה.

האם פגיעה במידע היא פגיעה ברכוש? הפרשנות המקובלת היא שאיסוף מידע קיברנטי, גניבת מידע ואפילו השמדת מידע או שינויו, אינם 'התקפה מזוינת' בפני עצמם[97].

הגישה האמריקנית והמערבית מבטאות תפיסה מסורתית של עולם המלחמה. לאורך ההיסטוריה, שיבשו מדינות את הסדר העולמי באמצעות פגיעה בבני אדם וגרימת נזק לרכוש. תוצאות פיזיות אלו נתפסו כהרסניות ליציבות העולמית ולביטחון המדינות, ולכן הקהילה הבינלאומית הסכימה לאמץ כללים שימנעו את התרחשותן[98].

האתגר שמעורר המרחב הקיברנטי קשור למצבים בהם נגרמת למדינה, כתוצאה מהתקפה קיברנטית, פגיעה קשה ומשמעותית שאינה מתבטאת בנזק פיזי ישיר לאדם או לרכוש. דמיינו למשל התקפה קיברנטית על הבורסה בניו יורק, שתגרום לפגיעה קשה בזרימת המידע ובאמינותו ולהתרסקות הבורסה.

הפגיעה בכלכלה האמריקנית והעולמית תהיה קשה מאוד. לכאורה, נגרם נזק כלכלי גרידא, אין לפעולה מאפיינים של פגיעה פיזית ישירה, ולכן אינה בגדר 'התקפה מזוינת'.

הבעיה, אם כך, היא שבמרחב הקיברנטי ניתן לערער את היציבות של מדינות באמצעות פעולות שאינן קינטיות, באמצעות הקשה על לוח המקשים של מקלדת מחשב או מסך מגע. כלים ויכולות קיברנטיים, שאיש בעבר לא חשב לאסור, עלולים לגרום תוצאות קשות, שייתפסו על ידי מדינות כ-Casus Belli (עילה למלחמה).[99]

במילים כלליות יותר, המרחב הקיברנטי מנתק את החפיפה בין המשטר המשפטי הקיים לבין התוצאות שהמשפט מבקש למנוע. המשטר המשפטי הבינלאומי אמור לאפשר למדינות להגן על עצמן ולמנוע תוצאות שנתפסות כחמורות מאד בראייתן[100]. בעולם המודרני, המשפט אינו יכול להסתפק באיסור על פגיעה פיזית ותו לא. מדינה שבה האזרחים לא יוכלו לגלוש באינטרנט, האמון במערכת הבנקאית ייפגע, הבורסה תשותק ושירותי הממשלה הממוחשבים לא יתפקדו, תראה זאת בחומרה רבה. היא תחוש פגיעה שאינה נופלת מזו של התקפה קינטית-צבאית. מדינה שתיפגע כך, תרצה להגיב ותחוש הצדקה מלאה לכך. המשפט יהיה חייב לתת מענה גם לסוג ההתקפות הקיברנטיות הללו[101]. גם אם הדין ימלא פיו מים, הפרקטיקה של מדינות תכתיב כללי משחק חדשים.

הקושי בהשלמה עם המצב המשפטי כבר זכה לביטוי, בעיקר בכתיבה האקדמית. כותבים רבים סבורים שלא האופי הפיזי של תוצאות התקיפה (פגיעה גופנית או הרס רכוש בלבד) צריך להיות המבחן הקובע בהקשר שתואר לעיל. לגישתם, למשל, צריך לבחון בצורה רחבה יותר את היקף האפקט הנגרם מהתקיפה, כך שהתקפה קיברנטית שתוצאותיה הכלכליות קשות, תיחשב 'התקפה מזוינת'[102]. בראייה זו, התקפה קיברנטית הגורמת, למשל, שיבושים קשים ברשתות תקשורת וברישומים פיננסיים, מצדיקה שימוש נגדי בכוח כהגנה עצמית.

כך, השוואה מעניינת שעלתה בכתיבה היא בין חסימת גישה למידע דיגיטלי לבין חסימת נתיבי שייט, הנחשבת ככלל אסורה לפי המשפט הבינלאומי[103].

לפי הקבלה זו, התלות המודרנית בתשתית דיגיטלית אינה פחותה מהתלות בתשתית פיזית, ויש לאסור על פגיעה בשני סוגי התשתיות.
המורכבות בהחלת הכללים המשפטיים בעניין הזכות להשתמש בכוח בהגנה עצמית כתגובה ל'התקפה מזוינת' במרחב הקיברנטי, היא דוגמה אחת בלבד מני רבות לקושי רחב בהרבה. גם ניסיון להחיל עקרונות משפטיים אחרים במרחב הקיברנטי יוליד פערים וסימני שאלה דומים.

**סיכום**

ביטחון המרחב הקיברנטי הוגדר על ידי ארגון האומות המאוחדות ועל ידי מדינות רבות כאחד האתגרים המשמעותיים של המאה הנוכחית. ראש ממשלת ישראל רואה בו את אחד מארבעת האיומים הגדולים ביותר על ישראל[104].
תפיסות אלו התגבשו על רקע ההתקפות שכבר בוצעו ומבוצעות במרחב הקיברנטי, ויותר מכך - על הבנה כי השימוש בהן ילך ויגבר ועל מודעות לפוטנציאל הנזק הטמון בהן. התקפות קיברנטיות הן דרך פעולה אטרקטיבית עבור מדינות, ארגונים ופרטים. הן ניתנות להסתרה בקלות יחסית, זולות, זמינות, קשה להתגונן מפניהן, בכוחן לאיין יתרונות טכנולוגיים וכלכליים של יריבים ולתרום לביטחון הלאומי של התוקף. בנוסף הנורמות המשפטיות ביחס אליהן טרם עוצבו, כך שהתוקף אינו מסתכן בפעילות המצויה 'מחוץ לכללי המשחק'.
השנים הקרובות צפויות להיות תקופה מכוננת בעיצוב המשטר המשפטי העתידי, שיסדיר את המרחב הקיברנטי. כיום, כבר שוררת הסכמה רחבה למדי (הן במערב והן בסין וברוסיה) כי יש להחיל את כללי המשפט הבינלאומי במרחב זה. בד בבד, קיימת תמימות דעים כי החלה זו היא מאתגרת, בלשון המעטה.
מה מקור האתגר? המרחב הקיברנטי חותר תחת פרדיגמות מסורתיות של המשפט הבינלאומי. מונחי המשפט הבינלאומי (כמו גבולות, טריטוריה, מדינות, לוחמים ועוד) כמעט זרים למרחב הקיברנטי; קשה לייחס אחריות משפטית לפעילות קיברנטית; המשפט הבינלאומי נשען על אבחנות

דיכוטומיות בין אזרחי לבין צבאי, ואילו המרחב הקיברנטי מאופיין בעמימות טבועה ומכוונת.

המרחב הקיברנטי מאיים 'לשבור' (ואולי כבר החל לשבור) את האבחנות המשפטיות המסורתיות, אינו מיישר קו עם הרציונל שבבסיס הכללים המקובלים, וחותר תחת דרך המחשבה האופיינית למשפט הבינלאומי.

בנוסף, במרחב הקיברנטי 'כולם משחקים' - גם שחקנים קטנים באופן יחסי עלולים להשפיע באופן משמעותי על הביטחון הלאומי של מדינות. זאת ועוד, עיצוב כללי המשחק המשפטיים לא יהיה פריבילגיה של מדינות המערב, אלא מהלך מורכב, לו שותפים שחקנים רבים.

כדוגמה לאתגר של המשפט הבינלאומי הוצגה הזכות שהוא מעניק למדינה, להשתמש בכוח כהגנה עצמית בתגובה ל'התקפה מזוינת' (Armed attack) עליה. לפי הכללים הקיימים, זכות זו מוקנית רק למדינה שהותקפה בפעולה שגרמה נזק פיזי ישיר לאדם או לרכוש (שאינו מידע). עם זאת, במרחב הקיברנטי ניתן לערער יציבות של מדינות ולגרום להן פגיעה כלכלית אדירה, מבלי לתקוף אותן פיזית.

הרחבה ביחס לכיווני הפעולה הנדרשים מחייבת חריגה מהיקפו של מאמר זה. ברור כי המשפט הבינלאומי יצטרך להשתנות ולהתפתח כדי לתת מענה למציאות החדשה. אם הדבר לא יקרה, מדינות יחושו מוגבלות על ידי המשפט הקיים ונטולות מענה אפקטיבי לאיומים עליהן[105]. שמירה על כללי המשפט הבינלאומי 'המסורתיים' עלולה לעמוד בניגוד לאינטרסים שלהן בתחום הביטחון הלאומי ולעורר דילמות קשות ביחס לדרך הפעולה. ככל שהטכנולוגיה תצעד קדימה וירבו התקפות קיברנטיות, מדינות תידרשנה בתדירות גבוהה לקבל החלטות, האם להגיב באמצעות שימוש בכוח, קיברנטי או פיזי. על המשפט הבינלאומי להמציא עצמו מחדש ביחס למרחב הקיברנטי ולספק כללים שיסייעו בשמירה על היציבות והביטחון. ימים יגידו האם המשפט עמד בהצלחה באתגר זה.

## מקורות

[1] William Owens, **Lifting the Fog of War** (2001).
לעניין ההקבלה בין התפתחות המרחב הקיברנטי לבין התפתחות הכוח האווירי, והצורך בשני המקרים לפתח תיאוריה צבאית מתאימה:
Brett T. Williams, "The Joint Forces Commander's Guide to Cyberspace Operations", 73 *Joint Forces Quarterly* 12 (2nd Quarter 2014).
המונח "עידן המידע" לקוח מספרו הידוע של אלווין טופלר, הגל השלישי.

[2] Martin C. Libicki, "What is information warfare?," *ACIS Paper* 3 (August 1995). Available at:
http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

[3] Rex Hughes, "Towards a Global Regime for Cyber Warfare", in: Christian Czosseck and Kenneth Geers, eds., **The virtual battlefield: perspectives on cyber-warfare** (2009), pp. 528-529.

[4] להרחבה ביחס להגדרות המרחב:
Clifford S. Magee, "Awaiting Cyber 9/11", 70 *Joint Forces Quarterly* 76 (3rd Quarter 2013).

[5] George K. Walker, "Information Warfare and Neutrality", 33 *Vand. J. Transnat'l L.* 1079 (2000), pp. 1094-1095.

[6] Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places", 51 *Naval Law Review* 132 (2005). pp. 135-136.

[7] Joseph S. Nye, "Cyber Power", Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010), p.3.

[8] אם כי בפועל, הרשת מוגבלת לעתים על ידי מדינות, חוקים לאומיים וטכנולוגיות שונות. להרחבה:
Tim Maurer, "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-security", Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School (September 2011). p. 8.

[9] Ibid. p. 16.

[10] Ibid. p. 14.

[11] Ibid. p. 9.
משטר במובן מכלול עקרונות ישירים ועקיפים, נורמות, חוקים ופרוצדורות לקבלת החלטות, שסביבם מתלכדות ציפיות של שחקנים בתחום היחסים הבינלאומיים. המחבר מפנה להגדרתו הידועה של Krasner משנת 1983.

[12] להרחבה בקושי שקשור למינוח:
Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in: Czosseck Christian, Ottis Ryan & Ziolkowski Katharina eds., **Proceedings of the 4th International Conference on Cyber Conflict** 283 (2012).

[13] המונח 'טרור' נטבע לראשונה כבר בשלהי המאה השמונה עשרה, במהלך המהפכה הצרפתית, אך עד היום טרם נמצאה לו הגדרה מחייבת ומקובלת, שזכתה לקונצנזוס עולמי. להרחבה:

Ben Saul, **Defining terrorism in International Law** (2006).

[14] הפיקוד הוקם במאי 2010, מתוך הכרה בחשיבות הממד הקיברנטי כממד חמישי, על מנת לתאם את הפעילות של כל הזרועות בתחום הקיברנטי. מטרתו לשמר את היכולת של ארצות הברית לפעול באופן חופשי במרחב הקיברנטי, לשם קידום האינטרסים הביטחוניים הלאומיים. בישראל טרם הוקם פיקוד קיברנטי. להרחבה:

Sean Watts, "Low Intensity Computer Network Attack and Self-Defense", 83 *International Law Studies series*, U.S. Naval War College 59 (2011). p.59.

[15] ארגון שיתוף פעולה ביטחוני, המורכב מסין, רוסיה, רפובליקות אסיאתיות (שהיו בעבר בברית המועצות) ומשקיפות כמו איראן, הודו ופקיסטן.

[16] להרחבה בעניין מאמצים סיניים ורוסיים להפעיל מנגנוני פיקוח ושליטה:

Tom Gjelten, "Seeing the Internet as an 'Information Weapon'," Sep. 23 2010. Available at:
http://www.npr.org/templates/story/story.php?storyId=130052701

[17] להרחבה בעניין ההשקפות השונות של מדינות בהקשר הקיברנטי, כמבטאות סיכונים והזדמנויות אסטרטגיים:

Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law*, Vol. 36, 421 (2011).

[18] Oona A. Hathaway, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William and Spiegel Julia, "The Law of Cyber-Attack", *California Law Review*, 100, 4 (2012); Yale Law & Economics Research Paper No. 453; Yale Law School, Public Law Working Paper No. 258.
Available at:
http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf

[19] ראו: Libicki, 1995; 77.

[20] פעולה שלא יצאה לפועל. להרחבה:

Arkin M. William, "The Cyber Bomb in Yugoslavia", Wash. Post (Oct. 25, 1999). Available at:
http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.html

[21] William Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber War", 89 *Int'l L. Stud.* 157 (2013), pp. 157-158.

[22] Richard A. Clarke & Knake Robert K., **Cyber War: The Next Threat to National Security and What to Do About It** (2010), pp. 64-68.

[23] Waxman, 2011; 423. המחבר מצטט דו"ח של מכון המחקר הבריטי, ה-IISS, לשנת 2010.

[24] שם, עמ' 424; המחבר מצטט את דו"ח האו"ם:

Rep. of the Grp. of Governmental Experts on Dev. in the Field of Info. & Telecomm in the Context of Int'l Sec., 65th Sess., 1, U.N. Doc. A/65/201 (July 30, 2010).

[25] Eneken Tikk, Kaska Kadri & Vihul Liis, **International Cyber Incidents: Legal Consideration** (2010).pp. 14-33.

[26] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, Vol. 56, 569 (2011). p. 569. (Schmitt 2011 (1))

[27] צילום: סוכנות AP

[28] Li Sheng, "When Does Internet Denial trigger the Right of Armed Self-Defence?", 38(1) *Yale Journal of International Law* (November 15, 2012), p. 200.

[29] Tikk, 2010; 17.
על הקדמה הטכנולוגית של אסטוניה יעידו, למשל, העובדה שבה פותחה אפליקציית Skype ונערכו בה בחירות באופן מקוון.

[30] Katharine C. Hinkle, "Countermeasures in the Cyber Context: One More Thing to Worry About", *Yale Journal of International Law Online*, 37 (2011), p. 13. Available at: http://www.yjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf

[31] Charles Glover, "Kremlin-Backed Group behind Estonian Cyber Blitz", Fin. Times, March 11, 2009.

[32] Tikk. 2010; 23.

[33] Ibid. pp. 66-90.

[34] Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", *Naval War College International Law Studies* (2011). p. 113. (Schmitt, 2011 (2))

[35] Richard M. Crowell, **War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare**, (2012), p. 14.

[36] Hathaway, 2012; 838.

[37] Marco Roscini, "Cyber Operations as Nuclear Counterproliferation Measures", *Journal of Conflict and Security Law*, Vol. 19 (2014), p . 137.

[38] Hathaway, 2012; 819.

[39] Banks, 2013; 157-158. Kenneth Geers, "Pandemonium: Nation States, National Security, and the Internet", *The Tallin Papers*, Vol. 1 No. 1 (2014). pp. 5-6. Available at: https://www.ccdcoe.org/publications/TP_Vol1No1_Geers.pdf

[40] לדוגמה:
"Iran blames U.S., Israel for Stuxnet malware", AP, April 16, 2011 http://www.cbsnews.com/2100-202_162-20054574.html

[41] בתוכנית טלוויזיה אף צולמה, בזמן אמת, התקפה קיברנטית (בשיטת DDoS), על ידי צבא סין, נגד אתר של תנועת Falun Gong בארצות הברית:
Ellen Nakashima & Wan William, "China's Denials About Cyberattacks Undermined By Video Clip", *Wash. Post* (Aug. 24, 2011).

[42] Crowell, 2012; 16.

[43] להרחבה:
http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=0

[44] Banks, 2013; 159.

[45] Watts, 2011; 72.

[46] ראו גם: יצחק בן-ישראל וליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", *צבא ואסטרטגיה*, 3(3), 2011, עמ' 19.

[47] Antoine Lemay, Fernandeza José M. & Knight Scott, "Pinprick Attacks, a Lesser Included Case?", in: Czosseck Christian & Podins Karlis eds., **Conference on Cyber Conflict, Proceedings** , 183 (2010) .p. 191.

[48] Rain Ottis, "From Pitchforks to Laptops: Volunteers in Cyber Conflicts," in: Czosseck & Podins, 2010; 97.

פרנק ג' צ'ילופו, קרדאש שרון ל' וסלמואירגי ג'ורג' ס', "תוכנית להרתעת סייבר: בניית יציבות באמצעות כוח", *צבא ואסטרטגיה* 4 (3), 2012, עמ' 3.

[49] הגורם התוקף מנסה לא אחת לפעול מתחת ל'סף התגובה' של מדינות, ולייצר לעצמו מעין 'חסינות קיברנטית' מפני תגובה.

Watts, 2011; 72-75.

[50] John N.T. Shanahan, "Achieving Accountability in Cyberspace - Revolution or Evolution", 73 *Joint Forces Quarterly* 20 (2nd Quarter 2014). p. 25.

וגם: בן- ישראל וטבנסקי, 2011.

[51] Lemay, 2010; 190.

[52] Li Zhang, "A Chinese Perspective on Cyber War", *International Review of the Red Cross*, Vol. 94, (2012).

[53] ספר משמעותי שנכתב בסין בנושא ופורסם כבר בשלהי המאה הקודמת:

Liang Qiao & Wang Xiangsui, **Unrestricted Warfare** (1999).

[54] Watts, 2011; 74.

[55] כך למשל, בחודש פברואר 2013 התפרסם כי בארצות הברית נערך legal review בעניין הפעלת הסמכויות בתחום ההתקפות הקיברנטיות, בין השאר במטרה להגדיר את סמכויות הנשיא, ראו:

"Broad Powers Seen for Obama in Cyberstrikes", *NY Times*, February 3, 2013. Available at:
http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0

[56] The White House, National Security Strategy 27 (2010)
www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[57] Andrew F. Krepinevich, **7 Deadly Scenarios: A military Futurist Explores War in the 21st Century** (2009). p. 194.

[58] ראו:
http://www.whitehouse.gov/blog/2012/07/20/taking-cyberattack-threat-seriously?utm_source=related

[59] Richard D. Clarke, שהיה אחראי לתיאום ביטחון קיברנטי בבית הלבן עד שנת 2003, כפי שצוטט ב:

Maurer, 2011; 5.

[60] Department of Defense, Strategy for Operating in Cyberspace (2011).

[61] להרחבה ראו דברים שפרסם משרד ההגנה האמריקני בעת הקמת הפיקוד החדש:
http://www.defense.gov/news/newsarticle.aspx?id=59295

[62] Maurer, 2011; 5.

[63] להרחבה:

Vladislav P. Sherstyuk, "Summit must play a part in creating a safer global information space", *BRICS New Delhi Summit* 86 (2012).

עוזר מזכיר המועצה לביטחון לאומי הרוסית, בתוך פרסום של ארגון BRICS, המתייחס, בין השאר, לתפיסה הרוסית בנושא ריבונות במרחב הקיברנטי. לעניין העמדה הסינית ביתר הרחבה: Zhang, 2012.

[64] Russian Federation, Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space (2011).
תרגום לאנגלית:
http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

[65] Waxman, 2011; 425. המחבר מציע ללמוד מלקחי ההיסטוריה ומהדיונים שנערכו בעבר בסוגיות דומות באו"ם, ובפרט מהדיונים בנושא משמעות 'שימוש בכוח' בתקופת המלחמה הקרה.

[66] Maurer, 2011; 6. המחבר מרחיב אודות זירות הדיונים באו"ם והזיקה בין הדיונים להתפתחויות הגלובליות.

[67] Clarke & Knake, 2010; 218-219. יש לציין שהיחסים בין המעצמות אינם רק מנוגדים ויש גם סימנים לשיתופי פעולה, לדוגמה פורסם דבר קיומו של "קו חם" בין ארה"ב לבין רוסיה בהקשרים קיברנטיים, ראו: Geers, 2014; 13.

[68] להרחבה:
Alan E. Boyle, "Some Reflections on the Relationship of Treaties and Soft Law", *The International and Comparative Law Quarterly* 48.4 (1999), p. 901-902.

[69] Maurer, 2011; 14.

[70] Tallinn Manual on The International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.
(להלן: "מדריך טאלין" או "המדריך").

[71] המחשבה הייתה שהמהלך יוביל להפקת מסמך משפטי, אשר יתרום באופן משמעותי להתהוות המשפט הבינלאומי המנהגי, ברוח San Remo Manual on International Law Applicable to Armed Conflicts at Sea.

[72] לא היה ישראלי בקרב המומחים.

[73] הכללים המופיעים במדריך נוסחו על בסיס של קונצנזוס בקרב המומחים, ככאלו שמבטאים לדעתם את המשפט הבינלאומי הקיים. השאיפה להגיע להסכמה על דעת כל המומחים, כרוכה לעתים בפשרה וביצירת מכנה משותף רחב. מנסחי המדריך אינם מציעים, למשל, פרדיגמה חדשה להסדרה המשפטית של המרחב הקיברנטי, כגון אמנה חדשה או החלה סלקטיבית של כללים קיימים, אלא מבקשים, בהכללה, לספק מענה לאתגרי המרחב באמצעות פרשנות לכללי המשפט הקיימים.

[74] מדריך טאלין, 5.

[75] להרחבה: Zhang, 2012.

[76] הסינים מוטרדים ממלחמה נגדם במרחב הקיברנטי. לטענתם, נכון לשנת 2012, מבוצעות נגדם כ- 80,000 תקיפות בחודש. ראה: Zhang, 2012; 805.

[77] הדבר עולה למשל מטיוטת אמנה בנושא ביטחון מידע בינלאומי, מספטמבר 2011, שהציג מזכיר המועצה הרוסית לביטחון לאומי, ניקולאי פטרושב. בסעיף 7 לטיוטה, נכתב שבמהלך מלחמות מידע יש לציית לדין ההומניטרי הבינלאומי.
http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

[78] לואיס ג'יימס א', "להגנת וירוס הסטקסנט", *צבא ואסטרטגיה*, 4 (3), 2012, עמ' 57.

[79] מדריך טאלין, 3. במדריך מצוטטת, בין השאר, עמדת ארגון הצלב האדום הבינלאומי, לפיה הדינים חלים במרחב הקיברנטי. לדעה מעניינת, לפיה המשפט הבינלאומי צריך להתפתח כדי להסדיר את התחום הקיברנטי, ואף לעודד פעילות התקפית קיברנטית כתחליף למלחמה קונבנציונלית, ראו:

Jeffrey T.G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", 106/7 *Michigan Law Review* 1427 (2008).

[80] מדריך טאלין, 5. ראו גם הוגה אסטרטגי חשוב:
Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly* (Spring 2011).

[81] למסמך המלא:
The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World 9 (2011).
Available at:
http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdfpace.pdf

[82] Harold Koh Honhgu, "Legal Advisor of the Dep't of State, International Law in Cyberspace Address to the USCYBERCOM Inter-Agency Legal Conference," (Sept. 18, 2012)
Available at:
http://www.state.gov/s/l/releases/remarks/197924.htm

[83] לדוגמה:
James A. Lewis, "Multilateral Agreement to Constrain Cyberconflict", *Arms Control Today* (June 2010). p. 16.

[84] לדוגמה:
Duncan B. Hollis, "Why States Need an International Law for Information Operations", 11 *Lewis & Clark L. Rev.* 1023 (2007), pp. 1027-1028.

[85] Hathaway, 2012; 840.

[86] Luciano Floridy, "The Ethics of Cyber-Conflicts in Hyperhistorical Societies", in: Ludovica Glorioso & Anna-Maria Osula eds., **1st Workshop on Ethics of Cyber Conflict 3**, (2014). p. 4.

[87] Larry Greenemeier, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers", *SCI. AM.,* June 11, 2011.
Available at:
http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.
בתקיפות DDoS ניתן לעיתים להציג ראיות נסיבתיות לעניין הגורם האחראי, אך לא בטוח שהדבר מספק. להרחבה:
Sheng, 2012; 202-203.

[88] להרחבה בדבר טשטוש מעמד הלוחמים במרחב הקיברנטי:
Maurizio D'urso, "The Cyber-Combatant: A New Status for a New Warrior", in: Glorioso & Osula, 2014.

[89] מתי יו קרוסטון, "'דילמת דוקו': הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרילית", *צבא ואסטרטגיה*, 5(1), 2013, עמ' 99.
המחבר מדגים את חוסר היכולת להבחין בין צבאי לבין אזרחי תוך ניתוח וירוס DuQu. לגישתו אין במרחב הקיברנטי תשתית אזרחית 'טהורה'.

[90] ואכן יש הכופרים באפשרות לגבש משטר משפטי ראוי למרחב הקיברנטי, ושמים את יהבם על אסטרטגיה של הרתעה, כמו: קרוסטון, 2013.

[91] צ'ילופו, קרדאש וסלמואירגי, 2012.

[92] Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda) 2005 I.C.J. Rep. 168, 223.

[93] בהתאם לסעיף 51 למגילת האו״ם, מוקנית זכות להגנה עצמית, אינדיבידואלית או קולקטיבית, למדינה כאשר בוצעה נגדה 'התקפה מזוינת' (Armed attack). זאת כל עוד לא נקטה מועצת הביטחון אמצעים החיוניים לשמירת השלום והביטחון הבינלאומיים. זו אחת מזכויות היסוד החשובות במשפט הבינלאומי.

[94] נאום Koh, 4.

[95] Sheng, 2012; 188.

[96] מונח שלקוח מפסק הדין של בית הדין הבינלאומי בהאג בפרשת ניקרגואה.

[97] יש הטוענים שאחרת, המשמעות תהיה שכמעט כל הפעולות במרחב הקיברנטי תהיינה 'התקפה מזוינת' - פרשנות בלתי סבירה שתוצאותיה קשות. יש המוסיפים בכל זאת חריג, במקרה בו נפגע מידע, המיועד להיהפך באופן מיידי לחפצים מוחשיים, כגון מחיקת חשבון בנק ששקול לכסף מזומן. במקרה כזה, הפגיעה במידע עשויה, לפי פרשנותם, להיחשב פגיעה ברכוש. להרחבה: Schmitt, 2011 ; 589.

[98] Schmitt, 2011 (1); 603.

[99] הדברים עלו גם מפי נשיא ארה״ב, שציין שמתקפות קיברנטיות אשר אינן פיזיות, עודן עלולות לגרום משבר פיננסי ומצבי חירום רפואיים:

Barack Obama, "Taking the Cyberattack Threat Seriously", *WALL ST. J.,* July 19, 2012.

[100] Schmitt, 2012; 287.

[101] Ibid, pp. 288-289.

[102] מדריך טאלין, 56.

[103] Sheng, 2012.

[104] ״מי יגן על ישראל ממתקפות מחשב? נתניהו העדיף את מטה הסייבר על פני השב״כ״ (״הארץ״, 21 בספטמבר 2014). להרחבה:

http://www.haaretz.co.il/news/politics/.premium-1.2439777

[105] להרחבה: Watts, 2011 ; 76.

# מבוכו של המינוטאור
# או: פרדוקס הסייבר – עיון מערכתי באתגרים ובהזדמנויות של המרחב המקוון

**ליאור לבד**[i]

"אתם חייבים לשמוע מה אחיין שלי עשה אתמול!" צעק לפני כמה שבועות מכר שלי בכניסתו לבית. "נו, מה?" שאלתי באדישות, מוכן לעוד סיפור על חיתולים ונפלאות המגבונים הלחים. "הוא ישב ממושכות מול החלון והביט בנוף, אחר כך דידה לעברו, הושיט יד, והחליק כמה פעמים את אצבעו על החלון משמאל לימין, כאילו מנסה להחליף את הנוף על גבי מסך האייפד!" התלהב הדוד. כולנו צחקנו, לא עברו רגעים ספורים ועלתה בי המחשבה – "העתיד" כבר כאן.

על פי נתונים שהציג מולי אדן, נשיא אינטל ישראל, בכנס הסייבר הבינלאומי האחרון שנערך באוני' ת"א, בזמן שקראתם על סיפורו של אורי והחלון בפסקה הראשונה, באתר יוטיוב הועלו מעל 30 שעות של סרטוני וידאו, בטוויטר פורסמו מעל מאה אלף טוויטים, ובסביבות השישה מיליון דפים נצפו ברשת הפייסבוק. אורי לא הספיק להושיט ידו את החלון ומעל 20 מליון תמונות נסרקו בפליקר, כ- 47,000 אפליקציות הורדו לסמארטפונים שונים, וכ- 45 תוכנות זדוניות (Malware) חדשות הועלו לרשת. בכל דקה שעוברת, היקף תנועת המידע המועבר על פני הרשת יכול למלא 230,000 דיסקים – מספר יחסית קטן, לעומת התחזיות המביטות אל עבר שנת 2015 (!), בה צפויים להיות 15 מיליארד מכשירים שונים מחוברים לרשת האינטרנט, היקף תעבורת התקשורת הניידת (סמארטפונים, טאבלטים ודומיהם) צפוי לזנק פי 11, ואילו היקף כלל התקשורת העולמית צפוי לגדול פי שלושה.

---

[i] **סרן ליאור לבד משרת כעוזר מחקר במרכז דדו.**

הגידול האקסטנסיבי הצפוי בנפח תעבורת המידע איננו פועל יוצא רק של גידול בכמות המשתמשים על פני הגלובוס כולו, אלא בשינוי מן היסוד הצפוי בחוויית התקשורת בקרב משתמשים בעולם המפותח. חזון ה"אינטרנט של הדברים" (IOT - Internet Of Things), או "האינטרנט של הכל" – (IOE Internet Of Everything), אשר הואץ במיוחד במהלך השנה החולפת, צפוי להתממש הרבה יותר מהר מכפי שדמיינו אותו. בקרוב, נוכל להציץ על הולוגרמה שקופה על ידנו ולדעת את רמת הסוכר בדם או אחוזי שומן הגוף, המקרר שלנו יזמין בעצמו קניות בסופר, הרכב שלנו יאותת לבית שלנו שאנחנו מתקרבים והכניסה לחניה תחכה פתוחה, או שהקומקום כבר ירתח, ואילו העיר שבה נגור תנתב אותנו הרחק מפקקים באמצעות מערכת רמזורים חכמה ותדע לנצל חשמל ומים ביעילות מרבית.

כיום, כ – 85% מכלל המכשירים החשמליים בעולם אינם נכנסים לקטגוריית ה – IOT, שכן הם אינם עומדים בשלושת תנאי הסף – יכולת חישוב, תקשורת וחיבור לענן מידע (Data Cloud). עם זאת, כבר בשנת 2020 צפויה האנושות להשתמש בכ – 50 מיליארד מכשירים מבוססי עיבוד ותקשורת, אשר יהיו מחוברים לענן מידע עצום. אגב, כבר ישנם התוהים על השמות שינתנו ליחידות המידה הגדולות יותר שתבואנה לאחר היוֹטה-בייט (יוטה-בייט אחד שווה לאלף מיליארד טרה-בייט, או בקיצור, $10^{24}$ בייטים, בשיטה העשרונית). הנוחות הדיגיטאלית הזו, כאמור, תהיה ככל הנראה חלק בלתי נפרד מעולמנו ושגרת חיינו בעוד לא זמן רב כלל. אך כגודל ההבטחה אותה מביאה קדמה זו, כך גם גודל הסיכון הטמון בחובה. הסיכון אינו קיים רק בכך שהמקרר שלי יזמין מהחנות שבעים טון פסטרמה, או בכך שהרכב שלי יתעקש שוב ושוב להביאני לביתה של חמותי (שתחיה) במקום לזה שלי. הסיכון אף אינו טמון כולו רק בשדות הריגול, גניבת הזהויות ואיסוף המידע כפי שאנו, אנשי הצבא, עלולים לחשוב.[ii] מהותו של הסיכון במסירת השליטה על הסדר בכל מישור

[ii] הגנרל דיוויד פטראוס, בשעתו כראש ה – CIA, כבר התבטא בעניין "שינוי תפיסת הסודיות" לה אנו נדרשים לאור העידן הדיגיטאלי אליו אנו צועדים, בהקשר ליכולות הצפויות שתהיינה לארגוני ביון שונים. להרחבה ראו:

המוכר לנו, הוא באבדן השליטה על תפיסת העצמי – כפרט, כחברה, כאומה, ומרחיקי הלכת יאמרו – כאנושות.

עם זאת, אין בכוונתי לגזול את מנת לחמם לא של פילוסופים, לא של פסיכולוגים, וגם לא את זו של חברות הביטוח. על כן, במאמר זה אתמקד, באמצעות גישת המערכות המורכבות, בהבניית מערכת מושגית שתאפשר, כך תקוותי, להאיר ולבאר את חוסר הנוחות המאפיין את "בעיית הסייבר". חוסר נוחות זה נובע משלל המתחים המתקיימים וגוברים ככל שהולך וגדל מספר הילדים שמנסים להחליף נוף בחלון. פרטיות מול נוחות, אישי מול משותף, חשאיות מול אפקטיביות מבצעית– כל אלה, ועוד רבים נוספים, הם מתחים ודילמות איתם אנו מתמודדים כבר היום הן בחיינו הפרטיים, הן בעבודתנו במערכת הביטחון. העדר הגבולות והפוטנציאל האינסופי הטמונים במרחב הסייבר מביאים עמם אולי את השאלה הפרדוקסאלית שטרם נענתה – כיצד חובתה של מדינה לפעול במרחב חדש מתיישבת עם אופיו החותר, לכאורה, תחת עצם קיומה?

אופיו הכאוטי, אינספור הגורמים המרכיבים אותו, נטייתו להתארגנות עצמית, ומאפיינים נוספים, מעמידים את ניתוח מימד הסייבר כמקרה בוחן טוב לחקירה של מערכות מתהוות. על כן, המתודולוגיה המוצעת במאמר זה לניתוחו היא מתודולוגיה הוליסטית – מערכתית, המבוססת על תורת המערכות המורכבות, עליה ארחיב בחלק הראשון.

חלקו השני של המאמר יפתח בהרחבה על מימד ההגנה בסייבר. באמצעות סקירה של תהליך למידה שנעשה בחיל הים האמריקני לצורך פיתוח תפיסה מערכתית להגנה בסייבר והרחבה על התפתחות תפיסת 'מחשוב ענן' והגנתו, יראה הפרק את המעבר המתבצע בימינו ממש ממודל חשיבה של "הגנה בעומק" למודל חשיבה של "הגנה קדמית" בתחום אבטחת המידע. שאר מרכיבי מרחב הסייבר, כגון איסוף, הרתעה, השפעה ומלחמה בהאקרים יידונו, בהקשר ניתוח מערכתי, באחריתו של החלק. נדבכים אחרים בפעילות במרחב הסייבר נעדרים ממאמר זה עקב מגבלות שונות.

---

Spencer Ackerman, "CIA Chief: We'll Spy on You Through Your Dishwasher," *Wired*, 15.03.2012. http://www.wired.com/2012/03/petraeus-tv-remote/

**א. תורת המערכות המורכבות – התפתחות ומאפיינים**

בתחום חקר החברה והדינאמיקות החברתיות המאפיינות חברות שונות, קיימות גישות רבות ואסכולות מנוגדות זו לזו בפירוש התופעות הנצפות. עם זאת, במשך מאות שנים קיימת הסכמה בסיסית אחת לגבי התנהגות "החברה"- בהסתמך על חוקיות כזו או אחרת, ניהול חברתי נבון הינו בר השגה. אי ההסכמה סבבה תמיד סביב מהות החוקים הללו. תפיסה זו, ניתן לתמצתה בנוסחה פשוטה: פעולה מוגדרת בהכרח תביא לתוצאה מוגדרת. כך עולה מתפיסת העולם הלינארית הקרטזיאנית[1].

כמות המידע האינסופית המעשירה את עולם המחקר, מורכבות הניתוח והמבנים התיאורטיים הרבים אליהם נדרשים חוקרים בעבודותיהם, הופכים את המדע המודרני לגלגל הולך וגדל המכיל יותר ויותר תחומים מחקריים חדשים ומחודשים. כך, מוצא עצמו המדע מתחלק שוב ושוב לכמות עצומה של ספירות המתפצלות לתת- ספירות וכן הלאה. עם זאת, סקירת התפתחותו של המדע המודרני מעלה את העובדה המפתיעה לפיה, למרות היעדרותה של המשגה כללית ועצמאותם של תחומים אלה מאחרים, בעיות, תהיות ותפיסות עולם דומות, ולעיתים אף זהות, מועלות באופן נרחב בתחומי מחקר שונים, שלכאורה אינם משתפים בינם שום מאפיינים דומים.[2] גישה אנליטית-מכניסטית ישנה זו הולידה במהלך המאה העשרים ספקנות בקרב הקהילה המדעית באשר ליכולתה לענות על האתגרים אותם מציבה חדשות לבקרים מורכבותן של החברה והטכנולוגיה המודרניות. כתוצאה מכך גברה ההכרה בדבר הצורך בהבנה חדשה, המבוססת על גישות מערכתיות כוללות ובעלות אופי בין- תחומי נרחב.[3] אחד מחלוצי ומפתחי גישת המערכות הכללית, פון ברטלנפי, כתב בספרו המרכזי בתחום כי "מדובר בשינוי בקטגוריות החשיבה הבסיסיות, ומורכבותה של הטכנולוגיה המודרנית הינה רק אחת מגילויו ואולי לא החשוב שבהם. אנו נאלצים, בצורה זו או אחרת, להתמודד עם מורכבויות, עם מכלולים או מערכות, בכל תחומי הידע. דבר זה מחייב אוריינטציה מחודשת לחשיבה המדעית."[4] התפתחותה של הבנה מערכתית חדשה זו הולידה את הצורך בניסוחה של תיאוריה כללית למערכות, אשר לא בהכרח תבטל את התיאוריות הקודמות למערכות ספציפיות, אלא תפעל במקביל להן, אם לא תאגדן תחת המשגה מחקרית אחת, על בסיס עקרונות

אוניברסאליים. כך, בתחילת שנות החמישים חברו לודוויג פון ברטלנפי (ביולוג), אנטול רפופורט (מתמטיקאי), קנת בולדינג (כלכלן) וראלף ג׳רארד (פיסיקאי) כדי לייסד את התחום המדעי החדש. למעשה, גישתם אינה מהווה תשובה נגדית לדרך המחשבה הקרטזיאנית שהוצגה לעיל, אלא מהווה תשובה מודרנית, או ביטוי מודרני, לאותו הלך הרוח.

ברטלנפי מגדיר מערכת כמכלול של אלמנטים אינטראקטיביים. לכן, הבעיות אשר בפניהן ניצבת מערכת כלשהי הינן, לשיטתו, בעיות של יחסי גומלין בין מספר רב של משתנים, הקיימים בתחומי הפוליטיקה, הכלכלה, התעשייה, המסחר, הניהול הצבאי, וכו׳. ברטלנפי מציע כלי חשיבה לצורך הערכה וביקורת של מערכות, בהתבסס על שלושה פרמטרים: הראשון הינו הפרמטר הכמותי, העוסק במספר האלמנטים המרכיבים את המערכת; השני הינו החומר, שכן הוא עוסק באופי האלמנטים; והשלישי הינו הפרמטר האיכותי או, ליתר דיוק, מהותי, והוא מתמקד בתכונות היחסים שבין האלמנטים השונים במערכת.[5] בעקבות זאת מגדיר ברטלנפי שתי קטגוריות בסיסיות של מערכות אוניברסאליות, מערכות פתוחות ומערכות סגורות: ״אנו מבטאים זאת על ידי האמירה שמערכות חיות הינן למעשה מערכות פתוחות. מערכת פתוחה מוגדרת כמערכת המצויה במצב של חילופי חומר עם סביבתה, כולל יבוא ויצוא, בניה והריסה של מרכיביה החומריים... מערכות סגורות הינן כאלה שניתן להחשיבן כמבודדות מסביבתן.״[6]

במרוצת השנים ידעה תורת המערכות הכללית פיתוחים, שינויים ו״תיאוריות נגזרות״ שהתפתחו ממנה. בשל קוצר היריעה לא ארחיב כאן על כל שלבי ההתפתחות, אך לא ניתן שלא להזכיר את תיאוריית הקיברנטיקה שהתפתחה בשנות הארבעים, תחום הדינאמיקה המערכתית שהחל להתפתח בשנות השישים, ותיאוריית הכאוס שהפכה פופולארית במיוחד בשנות התשעים.[7]

כאמור, תורת המערכות הכללית משנות החמישים לא ייצגה אלטרנטיבה לצורת החשיבה הקרטזיאנית הדטרמניסטית, אלא היוותה ביטוי מודרני לדרך החשיבה הישנה. לאורך הזמן, ועם ההתפתחויות התיאורטיות במהלך העשורים האחרונים, התפתחה גישה אלטרנטיבית, ״מדעי המורכבות״ או "Complexity Sciences", אשר הולכת וחודרת יותר ויותר למדעי החברה. ליבת

הגישה היא בהכרה בעובדה שישנן מערכות (פיזיות, ביולוגיות וחברתיות)[8] שאופן התנהלותן אינו עומד בקנה מידה אחד עם התפיסה הלינארית המאפיינת את התנהלות המערכות לפי ברטלנפי. המערכות המורכבות נקראות כך מעצם אופי התנהלותן- מורכבת ואי-ליניארית. לפי תיאוריה זו, ובניגוד לתפיסה הקרטזיאנית, הקשר בין פעולות לתוצאותיהן נע על פני רשת (Network[9]) בה מתקיימים אינספור קשרי גומלין שונים בין מכלול רב של אלמנטים. במילים אחרות, במערכת נתונה הכל משפיע על הכל – מעין "אפקט הפרפר". בשל כך, גירוי מזערי ביותר בחלקה האחד של המערכת, עשוי להוביל לתוצאות מרחיקות לכת בחלקיה האחרים, ואף עלול לפגוע ביציבות המערכת כולה או להביא להשמדתה. כך, לדוגמא, פגם גנטי זניח, הגורם למחסור באנזים מסוים בגוף, שבלעדיו האדם אינו מסוגל לעכל מרכיב מזון כלשהו, עלול לגרום למותו עם אכילת מזון המכיל מרכיב זה. כך גם שריפתו העצמית של אדם מן הישוב בתוניסיה בדצמבר 2010 הביאה דרך סדרת אירועים בלתי צפויים לשרשרת אירועים היסטוריים במהלך השנים האחרונות, המכונים "האביב הערבי" או "הטלטלה האזורית". הקשר הבלתי- קווי (הפעלה שולית שעשויה להביא לשינוי משמעותי או להפך) עושה את המערכות המורכבות לבלתי צפויות פר הגדרה[10].

כדי להבין התנהגותן של מערכות מורכבות יש צורך בהבנה לא רק של התנהגות החלקים המרכיבים את המערכות, אלא בהתנהגותם המשותפת המעצבת את התנהגות הכלל. **איננו יכולים לתאר את הכלל בלא לתאר כל מרכיב ממנו, ואין אנו יכולים לתאר כל מרכיב שהוא אלא ביחס לשאר המרכיבים**.[11] על כן, תמציתה של המערכת טמונה יותר ביחסי הגומלין בין מרכיביה מאשר בכל דבר אחר.

תכונה נוספת של המערכות המורכבות היא קיומן המתמיד "על סף התוהו". משום שהשינויים הבלתי צפויים במערכות מורכבות הם באופן התפקוד הנורמטיבי שלהן, המערכות תמיד מתנהלות "על הקצה". כלומר, לא ניתן לצפות ממערכות מורכבות שתתנהגנה על פי תכנית כלשהי, ותגובתן תמיד תהא פרטיקולארית, ובהתאמה לנסיבות הנתונות לאותו מצב ורגע. כך, לדוגמא, מבלי להתכוון לכך, כבר במאה ה- 18 ניסח קלאוזביץ טענה

מערכתית מורכבת בקביעתו כי שדה הקרב הינו ממלכת אי הודאות, בו לעולם לא יקרו הדברים כפי שתוכננו מבעוד מועד.

אופיין הכאוטי של המערכות המורכבות, והתהייה על השאלה "אם כך, אז איך זה בכל זאת עובד?", נענו בתשובה- מחקר בתחום המערכות המורכבות מראה שכנגד הכאוס והאי-סדר המובנים בתוכן, עומד כוח מאזן ומסדר המכונה "**התארגנות עצמית**".[12] כוחה של ההתארגנות העצמית גדול ולא נחות מכוחו של אי-הסדר. לדוגמה, הדמוקרטיה החברתית היא צורה של התארגנות עצמית המהווה ערך תרבותי המקודש לחברה המערבית. דוגמא נוספת מתבטאת במיליציות אזרחיות המתארגנות לצורכי הגנה עצמית בשעת מצוקה והיחלשות השלטון המרכזי. כבר מאז "מצב הטבע" של תומאס הובס והתארגנותם העצמית של הפרטים לכדי חברה אחת, ספרות אקדמית ענפה מתארת מקרים המדגימים כיצד מתוך קבוצות מבוהלות של פרטים (תמיד) צומחת מנהיגות המפחיתה את הכאוס ואי-הסדר.[13]

התארגנות זו נעשית על פי עקרון המשיכה ל"מוקד כוח" (Attractor) החזק ביותר מבין כלל הגורמים האחרים הפעילים בהקשר קונקרטי. המושג "מוקד כוח", בו משתמשת תורת המערכות המורכבות יכול להיות מקורב במידה מסוימת למושג "מוטיבציה". אלא שמוקד הכוח מושך אליו כמו מגנט, וזאת משום שהוא נתפס על ידי המערכת כמוקד "ההצלה" החזק ביותר בעת הנתונה. מאחר והמערכת כולה נמצאת על סף קריסה מתמדת, היא נעה ללא הרף בין "מוקדי כוח" שונים. התחלופה הקבועה בין מוקדי הכוח נובעת מהעובדה כי התנהגות זו היא פועל יוצא של השפעתם הבלתי פוסקת של כוחות חיצוניים ופנימיים רבים, מגוונים ועצמתיים, באופנים שונים ובקשרים רשתיים (בלתי- קוויים) על מרכיבי המערכת המורכבת. אך גם כאן חל עקרון התזה והאנטי-תזה - פרט למוקדי הכוח, אלמנט נוסף אשר משפיע על התנהלותה של המערכת ותמרונה בין מוקדי כוח, הוא אלמנט מוקדי הדחייה (Repulsion)[14]. מוקדי הדחייה משפיעים על המערכת בצורה הפוכה מהשפעת מוקדי הכוח, ובמקום למשוך את מרכיבי המערכת להתארגנות עצמית סביבו, הם דוחפים אותה מעצמם ובכך משפיעים על עיצובה העצמי של המערכת. אגב, לפי גישה זו, סוד הצלחתו של ארגון דאע"ש, הוא בהיותו

גורם 'מושך' היוצר סדר (לפי ראיית עולמו) במערכת הכאוטית הנקראת 'המזרח התיכון של ימינו'. וכמו כל גורם מושך אחר, הוא מצוי בתחרות מול גורמי מושכים ודוחים אחרים, המעצבים את המערכת האזורית לא פחות ממנו.[15]

כאמור, מערכות מורכבות מתאפיינות בכמות אינסופית של אלמנטים, ובכמות אינסופית של קשרים בין האלמנטים הללו. מצב זה מקשה עד מאוד, ויש האומרים עושה לבלתי אפשרי[16], את יישום שיטת המחקר המדעית הבסיסית ביותר- הפשטה ("רדוקציה"). באופן מסורתי, בהתבסס על השקפת העולם הדטרמיניסטית, הפשטה לצורך מחקר נועדה בכדי לאפשר את למידתו והבנתו של חלק כלשהו מן השלם, למען הכללת התובנות הנגזרות מן הניתוח, על השלם כולו. אולם בשל הכמות האינסופית של חלקים וקשרים במערכות המורכבות, **הן אינן בנות הפשטה**.[iii] לכן, במהלך העשורים האחרונים התפתח מספר רב של מתודולוגיות מודרניות להתמודדות עם מערכות מורכבות.

**על זהירות, צניעות ומתודולוגיות יישום**

"המערכת המורכבת" כשמה היא- מורכבת, בלתי צפויה בעליל, ובלתי ניתנת לחקירה והבנה על ידי שיטות המדע המסורתיות. בהשאלה מן העולם הצבאי – מתודולוגיית "הערכת המצב" המסורתית אולי רלוונטית ומתאימה ללמידת מצבה הפיסי של דיביזיית האויב שמעבר לגבעה, אך כשמדובר בלמידה על ארגון דאע"ש, למשל, או על התפתחות איומי טרור בחבלי ארץ שוממים – הערכת המצב עלולה לספק מענה חלקי בלבד, שיכול להיות רלוונטי לגיבוש מידע, אך לא תורם לפיתוח הידע. חשוב לציין, כי ליישומה בפועל של תורת המערכות המורכבות קיימות מתודולוגיות יישום רבות. הקלות היחסית בה נופלים שבי, פרקטיקנים ומומחים כאחד, בידי מתודולוגיית יישום אחת בה הם רואים חזות הכל, ומוצאים עצמם לעתים "דוחסים" מציאות אל

[iii] כאמירתו המפורסמת של העיתונאי והסופר הנרי לואיס מנקן:
"For every complex problem there is an answer that is clear, simple, and **wrong**."

מידותיה של השפה אליה הם מורגלים, מקנה חשיבות לזהירות וביקורתיות עצמית.

במרוצת העשורים האחרונים התפתחו פרקטיקות שונות לניתוח מערכות מורכבות ולהתמודדות עמן. כנראה בגלל התחרות הקשה וההתמודדות היומיומית עם מציאות של "על סף תהום", התחום העיקרי בו התפתחו פרקטיקות אלו הוא התחום העסקי. במסגרתו, פורסמו במהלך השנים עשרות רבות של ספרי ייעוץ על התמודדות "נכונה" של ארגונים עם המציאות המשתנה הסובבת אותם.[iv] למשל, פרקטיקה בולטת העולה מהררי ההמלצות, היא כי מתוקף אופיה הרב-תחומי של גישת המערכות (שכן מערכת מורכבת מאופיינת באלמנטים משלל תחומים מגוונים), הבכיר הארגוני או הדירקטוריון אינו עוסק ב"קבלת החלטות" ובניית תכניות ליניאריות ארוכות טווח, אלא ב"עיצוב" (Design) מתמשך, הער לשינויים המתרחשים תוך כדי תנועה, ומנווט את ספינת הארגון דרך המים הגועשים של המציאות המתהווה.[17]

פרט לארגונים עסקיים, גם צבאות מודרניים אימצו את גישת העיצוב המערכתי. כנראה בשל רוח התקופה המהפכנית, הנחשון בתחום היה הצבא הסובייטי, אשר אימץ את הגישה ופיתח את התחום עוד בשנות השלושים של המאה הקודמת ובתקופת מלחמת העולם השנייה.[18] מתודולוגיות של חשיבה מערכתית לתכנון (עיצוב) מערכה נוצרו בהמשך גם בצבאות הישראלי והאמריקאי, ובראשם ה- SOD (System Operational Design – עיצוב מערכתי אופרטיבי). פיתוחים נוספים לתפיסה זו נוצרו בהמשך השנים.

ידיעת העקרונות של חשיבה מערכתית איננה מבטיחה שאכן נחשוב מערכתית. במהלך השנים התפתחו מתודולוגיות שונות לניתוח מערכתי, אשר באו מגישות שונות לתורת המערכות. עם זאת, כל המתודולוגיות השונות

---

[iv] בין רבים אחרים, ראו למשל:

Senge, Peter M. **The Fifth Discipline: The art and practice of the learning organization**, Doubleday, New York, 1990; Russell L. Ackoff, **Systems Thinking for Curious Managers**. Triarchy Press, 2010; Jamshid Gharajedaghi, **Systems Thinking: Managing Chaos and Complexity - A Platform for Designing Business Architecture**. Butterworth-Heinemann, 2005;

כוללות שיטה לניתוח מערכות, איתור הבעיה/ תהליך למידה והתאמת פתרונות למצבים נתונים. בברירה שבין המתודולוגיות השונות, ניתן להפעיל שלושה מבחנים של ישימות בתהליך העבודה על פי מתודולוגיה: א. האם ביחד עם המתודולוגיה אנו מפעילים גם חשיבה מערכתית? ב. האם בחרנו את המתודולוגיה המתאימה למערכת אותה אנו חוקרים? ג. האם המתודולוגיה נגישה גם למי שאינו מומחה מקצועי בשימוש בה?[19]

ייתכן כי מתודולוגיה טובה אכן לא מחייבת נוכחות של מומחה למתודולוגיה בחדר, אך הבחירה במתודולוגיה מתאימה להקשר הנתון הנלמד – כדאי שתיעשה לאחר מחשבה רבה.

### ב. התבוננות מערכתית במרחב הסייבר

בחלק זה של המאמר טמון פרדוקס. כפי שתואר בפרק הקודם, ניתוח בעיות מורכבות לפי מאפייני תורת המערכות המורכבות מחייב גישה הוליסטית – מערכתית ללא פירוקה של הבעיה למרכיביה השונים. מדוע, אם כך, ימצא הקורא התוהה בפרק זה פירוקו של מרחב הסייבר לכדי מרכיביו המוכרים? ולא, נאמר, ניתוח מערכתי של מרחב הסייבר כמערכת-על מורכבת? היות ומטרתו של המאמר היא להציע מבט אחר על קטגוריות הייחוס המקובלות למרחב הסייבר, ולהעניק לאיש המקצוע כלים להתמודדות טובה יותר עמו, ימצא הקורא פרשנות מערכתית על כל אחת מקטגוריות מרחב הסייבר בנפרד. עבודת הבנייתה של מערכת-על אחת, הכוללת את כלל הקטגוריות כנדבכים מרושתים זה בזה, יכולה להיות בת מימוש על ידי אנשי מקצוע בלבד, "אמני סייבר", בעלי הסתכלות מערכתית, וכתוצאה מתהליך למידה מבנה.

### על מלחמה בוירוסים – ממערכות הגנה בסייבר למערכת החיסונית של גוף האדם

בעיית ההגנה בסייבר היא הנדונה, המנותחת והפופולארית ביותר הן בעולם הפרקטיקה של חברות אבטחת מידע וארגונים ממשלתיים, הן בעולם האקדמי. יתכן כי בזכות שיח ער זה, מימד ההגנה הוא גם המפותח ביותר

מבחינה תיאורטית (לפחות במקורות גלויים) ועל כן גם תפיסות ההפעלה הנוצרות בקרבו מתקדמות יותר לעומת תחומי סייבר אחרים.

כניסתו המהירה של מרחב הסייבר כמעט לכל נדבך בחיינו (וכפי שתואר בפתיח – כניסה שצפויה לגדול ולהעצים עד מאוד) הינה הגורם המרכזי לחשש מפני השתלטות עוינת והשפעה זדונית על מערכות בהן אנו נעשים תלויים יותר ויותר. תוכנות זדוניות קיימות מזה ארבעים שנים[v], אך לפי דו"ח חברת אבטחת המידע הספרדית Panda Security כ – 20% מכלל התוכנות הזדוניות הקיימות נוצרו רק במהלך שנת 2013.[20] בסיכום שנת 2013 הציגה החברה נתונים לפיהם מדי יום נוצרות בממוצע 82,000 תוכנות זדוניות המופצות ברשת,[21] אך בדו"ח הרבעון השלישי של 2014 מספר זה מאמיר לכמעט 230,000 תוכנות מדי יום, כאשר רק בין החודשים יולי – ספטמבר 2014 נוצרו למעלה מ – 20 מליון תוכנות זדוניות חדשות.[22]

במהלך שלושת העשורים האחרונים נכתבו והופצו לשוק עשרות תוכנות אנטי וירוס אשר התפתחו ושודרגו במקביל להתפתחותם ושדרוגם של האיומים השונים על הרשת. תפיסת האבטחה כמובן השתנתה עם השנים, ותוכנות אבטחה מתקדמות ביותר הופצו לשוק, אך, לרוב, מדובר היה בתוספת שכבות הגנה על אתרי הרשת השונים ומשתמשיהם. תפיסת שכבות ההגנה שואבת מעוגנה המרכזי של תפיסת ההגנה המקובלת - אסטרטגיית ה"הגנה לעומק" ("Defence in Depth") השאולה מהתחום הצבאי הטקטי - מערכתי.[vi] לפי

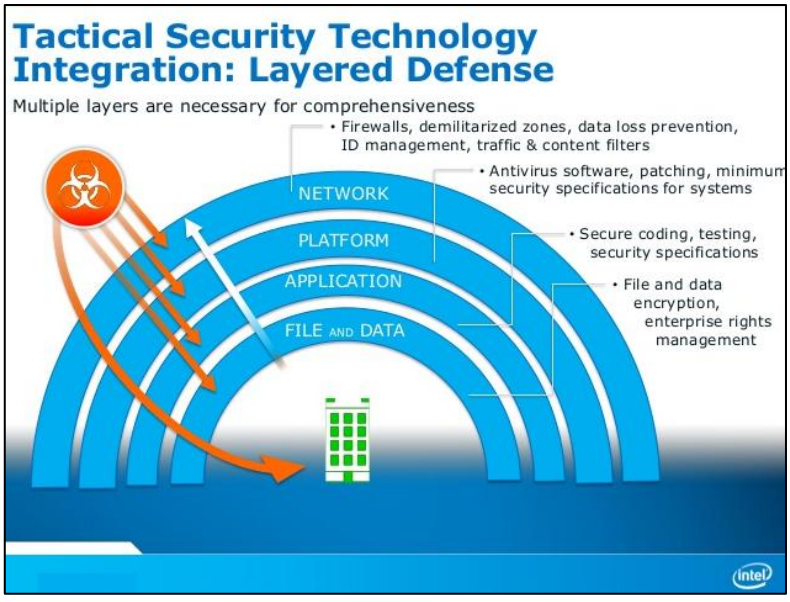
---

[v] ההנחה הרווחת היא כי התכנות הזדוניות הראשונות היו "The Creeper System" מ - 1971 ו – "Rabbit" או "Wabbit" מ – 1974.

[vi] ה"**הגנה בעומק**" הוא מושג בו השתמש ההיסטוריון ומדען המדינה אדוארד לוטוואק בספרו המכונן "האסטרטגיה רבתי של האימפריה הרומית". אחת השאלות המרכזיות עמן מתמודד ספרו היא "כיצד הרומים שמרו על גבולותיהם?" לטענתו, במאה השלישית ובתחילת המאה הרביעית לספירה עברה האימפריה הרומית מאסטרטגיה של "**הגנה קדמית**", המונעת כל חדירה של כוחות זרים לשטחי האימפריה ומנטרלת אותה בשטחי האויב, לאסטרטגיה של "הגנה בעומק", המתייחסת לחדירת כוחות זרים כמצב נתון, אותו ניתן לנצל לטובת הכוחות המגנים באמצעות הכלה, ארגון כוחות ותקיפה. לצורך ההמחשה, ניתן לטעון כי אסרטגיית ההגנה של מדינת ישראל, על פי תפיסת הביטחון לבן גוריון, היא תפיסת "הגנה קדמית", מתוקף דוקטרינת העברת המלחמה לשטחי האויב, ואילו תפיסת ההגנה של סוריה (טרם מלחמת האזרחים, כמובן), בהתאם לדוקטרינה הסובייטית, היא תפיסת "הגנה בעומק", במסגרתה חגורת הביטחון הרחוקה ביותר ממרכז העצבים (דמשק) היא גם החלשה ביותר, ועל כן הדיפת כוח פולש תהיה על אדמת סוריה ובאמצעות הכוחות ההולכים וחזקים עם ההתקרבות לבירה. המקרה הסורי הוא גם ההמחשה לכך שתפיסת "הגנה בעומק" היא בהכרח תפיסה של שכבות הגנה.

גישה זו, מיקוד ההגנה הוא אינו במניעת הפגיעה כליל, אלא בעיכובה ככל הניתן, בעיקר באמצעות יתירות מבנה, וזאת לשם מתן זמן זיהוי ותגובה הולמת למערכת המגנה. מכשולי נ"ט, לדוגמא, הם ביטוי לגישת "הגנה לעומק" – הם אינם מונעים כניסת טנקי אויב, אלא מעכבים ודוחים אותה. גישת "שכבות ההגנה" היא המקובלת כיום על ידי רוב חברות אבטחת המידע, ומהותה ביצירת מענה אבטחתי לכל רובדי התנועה המקוונת – החל מעמדת המחשב הפרטי בביתנו ('עמדת הקצה') וכלה בספקית האינטרנט. ביטוי ויזואלי אופייני ניתן, למשל, לראות בהצגת תפיסת ההגנה של חברת אינטל, כפי שהוצגה בינואר השנה בועידת "CyberStart14 Security Conference" בהלסינקי:[23]

**תמונה 1: גישת "שכבות הגנה" באבטחת המידע של חברת אינטל**




אדוארד לוטוואק, **האסטרטגיה רבתי של האימפריה הרומית**, (הוצאת מערכות, 1982).
המונח "הגנה בעומק" הפך, כאמור, משמעותי בהקשר מימד ההגנה בסייבר. להרחבה על התפיסה ומימושה במרחב אבטחת המידע ראו הסבר באתר הסוכנות לביטחון לאומי (ה - NSA):

https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

רוס אשבי, פסיכיאטר בריטי ואחד מאבות תחום הקיברנטיקה וגישת המערכות המורכבות, גרס בספרו הנודע "An Introduction to Cybernetics" משנת 1956 כי מערכת מנהלת מוכרחה להיות מורכבת יותר מהמערכת שהיא מנהלת בעצמה.[24] כך, ניסו במשך העשורים האחרונים חברות האבטחה לשמור על קצב התפתחות זהה, ובשאיפה – מהיר יותר, מקצב התפתחות ושדרוג התוכנות הזדוניות על שלל סוגיהן. בשנים האחרונות נשמעים בשיח האקדמי (והמעשי) בתחום ההגנה בסייבר קולות שונים, המבקשים לבחון דרכים אחרות לפיתוח נוסף של "גישת השכבות". הולכת ומתעצבת הבנה כי אם כבר היום ההגנה בסייבר מאותגרת יותר מפעם ומתקשה להתמודד עם כמות רבה כל כך של תקיפות (מתוחכמות במיוחד בחלקן), הרי שעל אחת כמה וכמה יאותגרו מערכות אלו בעתיד, כאשר היקף תעבורת המידע במרחב יגדל בעשרות מונים. נשמעים קולות לחשיבה 'אחרת' ולשינוי תפיסתי בגישה הבסיסית, עד כדי כך שמייסד חברת האבטחה נורטון אנטי וירוס, בריאן דיי, הכריז השנה חגיגית על "מותו של האנטי וירוס", בהתייחסו לתהליך שינוי גישה מערכתית בה נוקטת החברה.[25]

על רקע השינוי בשיח חוגי הפרקטיקנים בהגנה במרחב הסייבר, ואף עוד לפני שהנושא הפך פופולארי במיוחד, שיתוף פעולה מחקרי[vii] בין ה- Chief of Naval Operations Strategic Studies Group (SSG) של חיל הים האמריקני (Navy) לבין מכון ניו אינגלנד למערכות מורכבות (New England Complex Systems Institute) בראשותו של פרופ' יניר בר ים, הוביל למסקנות מערכתיות מקוריות:[26]

> הנחת המוצא של סטייסי (עמית מחקר במכון) ובר ים היא כי גישות מסורתיות להגנה בסייבר הופכות לרלוונטיות פחות ופחות עם התגברות האיומים, תחכומם, והקצב בו הם משתנים. בנוסף, כך הם

[vii] שיתוף הפעולה המדובר התקיים במהלך שנת 2008, ולכן אין ספק כי מימד ההגנה בסייבר ידע שינויים והתפחויות מאז. היות ואין עניינו של המאמר בהעלאת חידושים ומהפכנות, אלא בהצעת כלים לחשיבה אחרת, תיאור תוצאות המחקר מובאות בתור דוגמא לתהליך למידה פתוח שאפשר הכנסת מושגים לכאורה לא קשורים, כגון המערכת החיסונית האנושית, אך הוביל לפיתוח תפיסות מקוריות וחדשניות.

גורסים, בעולם האבטחה ניתן לזהות דפוסי פעולה כלליים דומים, וכי זיהוי מאפייני מערכות אבטחה כלליות יעילות יכול להועיל בהתמודדות עם אתגרים מורכבים חדשים ברשתות טרור גלובאליות ובאבטחה בסייבר. בנייר המסכם את תהליך הלמידה המשותף עם ה - SSG, משתמשים החוקרים במערכת החיסונית האנושית כהשראה למערכת המתמודדת עם אתגרים ואיומים מקבילים לאלה הקיימים במרחב הסייבר.

השוואה זו מתאפשרת, לטענת החוקרים, עם הפיכתה של תקשורת המחשבים למתפתחת, מתמשכת ומהירה. המערכת החיסונית האנושית מורכבת ממיליארדי תאים המתואמים ביניהם להגיב על אתגרי אבטחה בגוף האנושי. לדידם, הפעילות של המערכת החיסונית אינה יכולה להיות מובנת כמערכת ריכוזית הנשלטת על ידי "מוח" אחד, אלא מתקיימת באמצעות מספר רב של קשרים מקומיים בין מרכיבים "יעודיים לצורך ביצוע תגובת חירום מיידית. הברירה הטבעית האבולוציונית הביאה את המערכת החיסונית לכדי שכלול כזה שהיא משיגה תוצאות טובות, היא גמישה, מדידה, ומסוגלת להבחין תוך כדי פעולה בין "ידיד" ל"אויב".

את פעילותה של המערכת החיסונית ניתן לחלק לשלוש שכבות: הראשונה, מורכבת מחסמים בין 'אזורי אבטחה' לסביבתם – שכבות העור המפרידות בין גוף האדם לסביבתו החיצונית, כמו גם חסמים פנים גופניים המפרידים בין סביבות שונות. בשכבה השנייה מתבצעת תגובה לפגיעות במערכת המשפיעות על מספר רב של תאים, וכוללת איחוי רקמות ו"החלפת" חסמים. השכבה השלישית, "חוד החנית", היא המערכת החיסונית הסתגלנית (Adaptive immune system), מגיבה לאתגרים המשמעותיים ביותר הפוגעים במערכת, ואחראית על איתור תאים ומולקולות המופצים במערכות הגוף, בדגש על זיהוי וירוסים ובקטריות המסוגלים לשכפל עצמם לכדי כמויות גדולות תוך פרק זמן קצר, ותגובה מיידית לנטרולם. לכל אחת מהשכבות הללו, כך

טוען בר ים, יש את המקבילה שלה במימד ההגנה בסייבר, ואילו השכבה השלישית – היא החשובה והמתוחכמת ביותר, ועליה נרחיב.

התכונות החשובות ביותר של שכבת המערכת החיסונית הסתגלנית הן הזיהוי והתגובה, מה שנכון לגבי כל מערכת אבטחה באשר היא. הזיהוי מושג באמצעות מיפוי המרחב המאובטח על תכולותיו והתנהגויותיו השגרתיות – מה שמאפשר בשעת התקפה את היכולת להבדיל בין איום ל'לא איום' (בין "ידיד" ל"אויב"). כאשר מאובחן "אויב" שחדר לסביבה המאובטחת, מופעלת תגובת נגד מיידית. הזיהוי והתגובה הן שתי פונקציות נפרדות של מרכיבי המערכת, הדורשים רגולציה עדינה שתאפשר פעולה מסונכרנת. ניתוח מעמיק של מערכות התקשורת המתקיימות בין האלמנטים השונים של המערכת החיסונית מגלה דפוסים המאפשרים למערכת 'ללמוד מחיכוך' ולהגביר את יכולתה להגיב במהירות לאיומים חדשים. מערכת תקשורת זו מפיצה בגוף את ידע 'מנגנוני הגילוי' שנשארים או נשכחים בהתאם ליעילותם בברירה הטבעית.

החוקרים ממשיכים וטוענים כי מערכות ההגנה בסייבר הקיימות היום גם הן חולקות מרכיבים דומים עם המערכת החיסונית האנושית. תפיסת החסמים וההגבלה המאפיינת את שכבת ההגנה הראשונה של המערכת החיסונית באה לידי ביטוי ב'חומות אש' (Firewalls) והפרדת רשתות. השכבה השנייה של ההגנה, בה מתבצעת התגובה לפגמי המערכת מתבטאת, למשל, באמצעות קיום "רשימות שחורות" של שמות תחום (DNSBLs) לצורך חסימת מפיצי ספאם. השכבה השלישית, היא תוכנות האנטי וירוס ומסנני דואר אלקטרוני המזהים תוכנות זדוניות וחוסמים אותם. בעוד שכאמור, מתקיים דמיון בין המערכת החיסונית לתפיסת ההגנה בסייבר הקיימת היום, עם ההשוואה למערכת החיסונית מתגלים שני פערים משמעותיים בארכיטקטורה של הרשת, המונעים ממנגנוני אבטחתה את הרלוונטיות לאתגרי המחר. ראשית, לא מתקיים מנגנון הפצה של הידע הנוצר מהתגובה לזיהוי תוכנות זדוניות, למנגנוני אבטחה אחרים. הפצת הידע הזו היא

אופציונאלית, המתאפשרת רק עם רישום פעיל של משתמשים בודדים למערכות אבטחה. בעוד שתוכנות זדוניות מקיימות מנגנוני שכפול והפצה עצמית ברשת (וחלקן אף 'לומדות תוך כדי' ומתחזקות ככל שתנועתן נמשכת), הידע שנוצר מחסימתן בעמדות קצה שונות אינו מופץ ואינו 'מלמד' עמדות קצה אחרות, מה שמיידית מציב את ההגנה בעמדת נחיתות לעומת התוקף. שנית, התפיסה המקובלת של מערכות ההגנה איננה תפיסה מערכתית משום שהיא איננה מערכת הגנה קולקטיבית. המיקוד הוא בהגנה של מרכיבים בתוך האינטרנט (בין אם אתרים ספציפיים או עמדות קצה של משתמשים) ולא בהגנה על האינטרנט כמערכת שלמה. ללא מערכת הגנה קולקטיבית, הפתרון היחידי להתמודדות עם אתגרים מתגברים ומשתנים, היא הקשחת כל מרכיב נפרד של האינטרנט, מלאכה לא פשוטה בפני עצמה. כתוצאה מכך, מסיקים החוקרים, מרחב הסייבר נעדר מנגנוני חסימה של תקיפות עם כניסתן למרחב המשותף, אלא ממוקד בחסימתן בנקודות תקיפה רבות "בסוף מסלול ההתפשטות".

על אף ההשראה הותיקה של האיומים על המערכת החיסונית האנושית לעולם ההגנה בסייבר (שהרי לא סתם מחשב הנגוע בתוכנה זדונית כלשהו הוא מחשב "עם וירוס"), רק חמש השנים האחרונות הביאו עמן בשורה של הגנות מערכתיות. המניע המרכזי להתפתחות שיח של גישה מערכתית לאבטחת מידע היה התפתחות תפיסת וטכנולוגיית מחשוב הענן ( Cloud Computing). תפיסת מחשוב הענן, המהווה בסיס מרכזי לבשורת ה"אינטרנט של הדברים" (IOT) אותה הזכרנו בתחילת המאמר, מציעה בפנינו מציאות עתידית בה המסמכים, התמונות, התוכנות, ולמעשה – כל מה ששמור לנו במחשב הפרטי בבית, יהיה נגיש לנו באמצעות "ענן" מידע עליו הם יישמרו. במקום שנצטרך לקנות תוכנה ולהתקינה על המחשב הפרטי (או הרשת המקומית), ניתן יהיה להשתמש במידע או בישום הנשמר בחוות שרתים מרוחקת, ולשלם (אם בכלל) רק עפ"י שימוש. ניתן, למשל, להקביל את השימוש המעודכן באינטרנט עפ"י טכנולוגיה זו לשימוש ברשת החשמל - המשתמש תמיד מחובר לרשת אך משלם על פי השימוש בחשמל. למעשה, כל

מי שמנהל, למשל, חשבון פייסבוק ושומר עליו תמונות, משתמש כבר היום בשירות אחסון מידע בענן.[27] טכנולוגיית מחשוב הענן מעמידה דרישות חדשות, מחמירות יותר, בכל הנוגע לאבטחת מידע. כעת, כשהמשתמש (או החברה) מאבדים את היכולת ל"קשר פיסי" עם המידע האישי או העסקי שלהם (שהרי כבר לא יהיה "דאבל קליק" על 'המסמכים שלי'), החשש מפני התערבות גורמים זרים ועוינים, ומפני אבדן המידע, רק מעצים. שינוי בסיסי מעין זה מוביל כעת לחשיבה מחודשת על עקרון ה"הגנה בעומק" שהוביל את עולם ההגנה בסייבר שנים כה רבות. ספקי תשתיות כבר לא יכולים להרשות לעצמם "הכלה בשטחנו", היות והם מעמידים בסיכון מידע שהם אמונים על שמירתו. על כן, תפיסת "הגנת הענן" (Cloud Security) המתפתחת, נוטה יותר ויותר לכיוון תורת ה"הגנה הקדמית", המיועדת למניעת חדירה של גורמים עוינים עוד בטרם יגיעו ל'גבול'.[28] עם זאת, לפולמוס הער המתרחש היום סביב מהות הגנת הענן, מבנהו ואופן פעילותו (גם נוכח בעיות משמעותיות של הגנה על פרטיות) יש עוד מרחק רב לעבור עד שיחול קונצנזוס כלשהו סביב 'תפיסת הפעלה' על ידי קהילת אבטחת המידע והמשתמשים.[29]

**לוחמת מידע וחופש מידע – התבוננות מערכתית על מרכיבי מימד הסייבר**

> "בכל רחבי העולם, אנשים מבחינים בחלקים שונים ממה שמתרחש בסביבתם. אחרים מקבלים מידע ממקור שני. באמצע נמצאים אנשים שמעורבים בהעברת המידע מהצופים לאנשים שיפעלו על סמך המידע. אלו שלוש בעיות נפרדות שכרוכות זו בזו.
>
> הרגשתי שקשה לנתח נושאים ולהפיץ את הניתוח באופן יעיל, כך שהמידע יגיע לאנשים שבסופו של דבר יפעלו על פיו. אפשר לטעון שחברות כמו גוגל, למשל, מעורבות בעסקי ה'תיווך' האלה, של העברת מידע מאנשים שהמידע מצוי אצלם לאנשים שמעוניינים בו. הבעיה שזיהיתי היתה שהשלב הראשון, ולפעמים גם השלב האחרון, מוגבלים כשמדובר במידע שממשלות נוטות לצנזר.
>
> אפשר להסתכל על התהליך הזה כעל צדק שנעשה על ידי הרשות הרביעית. [...] היה נראה לי שצוואר הבקבוק מצוי בראש ובראשונה בהשגת מידע, שימשיך וייצר שינויים צודקים. בהקשר של הרשות הרביעית, אנשים שמשיגים מידע הם בגדר מקורות; אנשים שמעבדים את המידע ומפיצים אותו הם עיתונאים ומפרסמים למיניהם; ואנשים שעשויים לפעול על סמך המידע הם כולם. זה תיאור ממעוף הציפור אבל הוא מסתכם באופן שבו מהנדסים מערכת שתפתור את הבעיה, ולא סתם מערכת טכנית אלא מערכת כוללת. ויקיליקס היתה, ועודנה, ניסיון – אם כי ראשוני מאוד – להיות מערכת כוללת כזאת."[30]
>
> ג'וליאן אסאנג'

בין ה – 18 בפברואר 2010 ל – 1 בספטמבר 2011 חווה העולם את מה שכונה אחר כך "ההדלפה הגדולה בהיסטוריה", או בשמה הרשמי – "פרשת קייבלגייט". במשך 19 חודשים פרסם אתר ויקיליקס 251,287 מסמכי תכתובות מסווגים שונים שנשלחו במקור אל מחלקת המדינה האמריקאית מ-274 הקונסוליות שלה, השגרירויות שלה, וכן הנציגויות שלה ברחבי העולם, הכוללים ניתוחים מדיניים וציטוטים של מנהיגים ושרים שונים ברחבי העולם אשר נאמרו במקור בדלתיים סגורות. מסמכי התכתובת שהודלפו במסגרת הפרשה נוצרו במקור החל מדצמבר 1966 ועד לפברואר 2010.

המסמכים מכילים ניתוחים מדיניים ממנהיגי העולם, וכן הערכותיהם של דיפלומטים אמריקנים במדינות המארחות ושל הפקידים שלהם.

קשה להגזים בתיאור ההשפעה של ויקיליקס על מרחב הסייבר. בספרו, מצטט אסאנג' את המוציא לאור של העיתון התוניסאי "נוואת", סמי בן ע'רביה שכתב כך: "עשרים יום חלפו בין פרסום התכתובות המודלפות על תוניסיה ב – 28 בנובמבר 2010, לבין תחילתו של האביב הערבי ב – 17 בדצמבר 2010. ביום ההוא, רוכל עני בשם מחמד בועזיזי הצית את עצמו. בצ'אט עם עיתונאי בריטי שנערך השנה הודה שר התעמולה של בן עלי, אוסאמה רומדאני, כי '**ההדלפות היו מכת החסד, הקש ששבר את גב הגמל מבחינת המערכת של בן עלי.**' לא היה זה המידע על השחיתות ועל העדפת המקורבים, התוניסאים לא היו זקוקים להדלפות כדי לדעת שארצם מושחתת. [...] ההבדל היה בהשפעה הפסיכולוגית של ממסד שנאלץ להתעמת באופן פומבי כל כך עם בבואתו העכורה. [...] ומי שסיפר את הסיפור לא היה מורד או רוחש-רעה פוליטי. זו היתה מחלקת המדינה של ארצות הברית, בעלת ברית לכאורה."[31] רבים נוספים מייחסים להדלפות ויקיליקס תפקיד משמעותי, אם לא מכריע, בפרוץ המרידות ברחבי העולם הערבי נגד משטריהם האוטוקרטיים,[32] אך גם אם נשאיר להיסטוריה לשפוט בעניין זה, הרי שההצלחה המשמעותית ביותר של ויקיליקס היא ביצירת שיח ציבורי חסר תקדים בהיקפו, על פתיחות המידע.

בענייננו, מעניין לראות כי תגובתם הראשונה של גופי סייבר, בין אם פרטיים או ממסדיים, להדלפות ויקיליקס הייתה ניסיון 'להשתלט על המערכת'. אתרי ויקיליקס השונים ספגו אש ארטילרית מכל הכיוונים, האתר הופל והועלה מספר פעמים, ומלחמת חורמה נפתחה נגד ספקי השרתים שעבדו עם אסאנג' ונגד חברות אשראי שסיפקו דרכים לתמיכה כספית בפרוייקט. התקיפות על ויקיליקס נעשו כנראה על רקע רצון בנקמה או בפגיעה באתר, שהרי ברור לכל איש מחשבים בינוני שברגע שמידע כלשהו עולה לאינטרנט – הוא נשאר בו. ולראייה, גם היום ניתן להיכנס לאתר ויקיליקס באין מפריע ולראות את כלל הפרסומים שנעשו בתקופה ההיא, כמו גם הדלפות חדשות שיוצאות מדי פעם.

סיפור ויקילקס לא מובא במאמר זה רק כקוריוז פיקנטי להמחשת הסכנות באינטרנט. ויקילקס, ובמיוחד פרשת קייבלגייט, מהווים דוגמא קלאסית לניצחונה של מערכת מורכבת על מערכת מורכבת פחות. ויקילקס לא רק נבנתה באופן מורכב טכנולוגית כדי לעמוד בפרץ ההתקפות על אתריה, אלא **היא נבנתה בהיגיון שממוטט את היגיון הפעילות של המערכת ה'יריבה' לה.** מחלקת המדינה האמריקנית, בתפקודה השגרתי מול נציגויותיה בעולם ובאמצעות שימוש בעקרון כה נושן הנקרא "סיווג בטחוני" למסמכים, לא הייתה בנויה לעמוד בפני התקפה שכזו.

באותו האופן, הבנוי על פעילות בהיגיון הממוטט את מבנה המערכת ה'יריבה', פועלת גם קבוצת אנונימוס. אנונימוס החלה להתארגן אי שם בשנת 2003 כקבוצת צ'ט בפורום 4chan. כבר בהתחלה פעלו הגולשים בפורום באופן משותף על מנת 'להטריל'[viii] פורומים אחרים ומשחקי און ליין שונים. אט אט החלה פעילות משותפת זו לעבור לתחום ה'האקטיביזם' תוך חתירה תחת הממסד. ככל שהתרבו פעילות ההאקינג שלהם – כך גברה הפופולאריות של הקבוצה. עם הזמן, הוכרה הקבוצה כ'תופעה אינטרנטית' והיא נתפסת היום כקבוצה בעלת יכולות פריצה מתקדמות ביותר (בשנת 2012 קבוצת אנונימוס הפילה את אתר משרד המשפטים של ארצות הברית, אתר הבולשת הפדרלית (FBI) והאתרים של חברות בידור ומוזיקה שונות כגון חברת יוניברסל מיוזיק, במחאה על סגירת אתר ההורדות Megaupload וצעדי הממשל האמריקאי כנגד אתרים פיראטיים). אחד מסמליה של הקבוצה, חליפת איש עסקים עם סימן שאלה במקום ראש, הוא אחד הביטויים הגראפיים להיגיון פעילותה – פעילות סייבר אלימה ומאסיבית ללא גוף שניתן 'לאחוז בו', ללא דוברים, מייצגים, או כתובת למשלוח מכתבים. באתר ויקיפדיה מסווג אנונימוס כ'ארגון'.[33] ככזה, זוכה העמוד למסגרת ("בוקס") של "תעודת זהות" אותה מקבלים כלל הארגונים המתוארים בויקיפדיה, על פי אמות המידה המקובלות ל'מהו ארגון' (מדינת מקור, מייסדים, מיקום

[viii] 'להטריל' – (מהמילה טרול) לפעול בצורה תוקפנית וטורדנית כלפי גולשים אחרים ברשת האינטרנט, למשל בפורומים, רשתות חברתיות, שליחת הודעות וכד'. *מילוג* – המילון העברי החפשי ברשת.
http://milog.co.il/%D7%9C%D7%94%D7%98%D7%A8%D7%99%D7%9C/s

המטה, בעלות...). בדקו בעצמכם כמה אנונימוס עונה להגדרות 'מקובלות' בתמונה המצורפת, וראו בכך דוגמא חיה ליכולתן של מערכות ממסדיות "להכיל" תופעות שכאלה.

אין כוונתי כאן, להביע תמיכה או גינוי כלפי גופים, ארגונים או פרטים הפועלים במרחב הסייבר. ללא ספק ישנם גם האקרים המנצלים לרעה את הכישרון הניתן להם ופוגעים פגיעות קשות בפרטיותם של גולשים, בפיתוח כלכלי של חברות מדינות, בקניין רוחני של אמני וכו'. אך עם זאת, להאקרים, כפי שטוענת המומחית לאבטחת מידע קרן אלעזרי, ישנו גם הפוטנציאל להיות מערכת החיסון של מרחב הסייבר, ביכולתם לזהות פרצות אבטחה וכשלי מערכות, ולהתריע מפניהם.[34]

השימוש במרחב הסייבר לצרכי השפעה על ידי ארגוני טרור גם הוא תופעה הראויה לניתוח בראייה מערכתית. על פעילותו של ארגון דאע"ש במרחב הסייבר כבר העמיקו בגיליון זה ברן ולוי, אך קיימות עדויות ומחקרים רבים גם לפעילות מקוונת לצרכי השפעה, וגיוס תמיכה ומשאבים על ידי מדינות כמו איראן[35] וארגוני טרור כמו חמאס וחזבאללה[36].

ארגוני הטרור, כמו גם ארגוני פשע ועבריינים, מנצלים גם את האנונימיות

**תמונה 2: "תעודת הזהות" של ארגון אנונימוס באתר ויקיפדיה**

שב"רשת האפלה" (Darknet)[ix] על מנת ליצור התקשרויות בינם לבין עצמם, ובינם לבין רשתות קרימינליות ולקוחות פוטנציאליים, וכל זאת מתחת לרדאר ובעילום שם.

אין ספק בלבי כי ארגוני הביון המערביים מודעים לתופעה זו, שהרי סערת ויקיליקס לא הספיקה לשכוח ומיד צצה פרשה חדשה, בדמות ההדלפות של אדוארד סנודן. סנודן, עובד לשעבר בסוכנות לביטחון לאומי (ה - NSA), העביר ביוני 2013 לעיתונים "הגארדיאן" ו"הוושינגטון פוסט" חומר מסווג על תוכניות סודיות ביותר של הסוכנות לביטחון לאומי, כולל תוכניות המעקב PRISM (המופעלת ע"י ה - NSA) ו – Muscular (המופעלת בשיתוף פעולה ע"י ה- NSA וה – GCHQ, סוכנות הביון הבריטית).

על פי המסמכים שהודלפו, PRISM היא תכנית חשאית לאיסוף מידע מודיעיני מחברות טכנולוגיה אמריקאיות, הפועלת מאז שנת 2007. החברות הכלולות בתוכנית הן מיקרוסופט (מאז 2007), יאהו (Yahoo) (מאז 2008), גוגל, פייסבוק ופאלטוק (Paltalk) (מאז 2009), יוטיוב (מאז 2010), AOL וסקייפ (Skype) (מאז 2011) ואפל (מאז 2012), כאשר 98% מהמידע המופק בתוכנית מקורו ביאהו, גוגל ומייקרוסופט.[x]

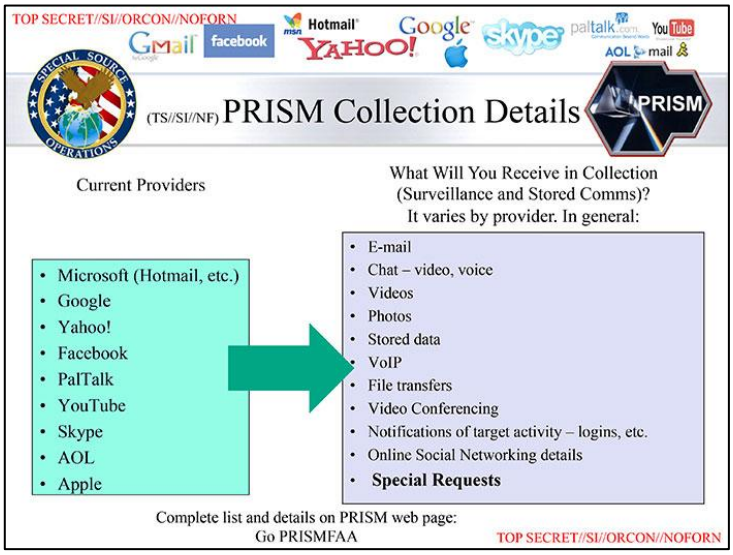
Muscular, היא תוכנה שפותחה על ידי סוכנות הביון הבריטית (GCHQ) ומייצרת גישה באמצעות פרצה אל מאגרי המידע של החברות גוגל ויאהו, בדומה לתוכנה ששימשה את ה – NSA בתכנית המעקב שלה.

---

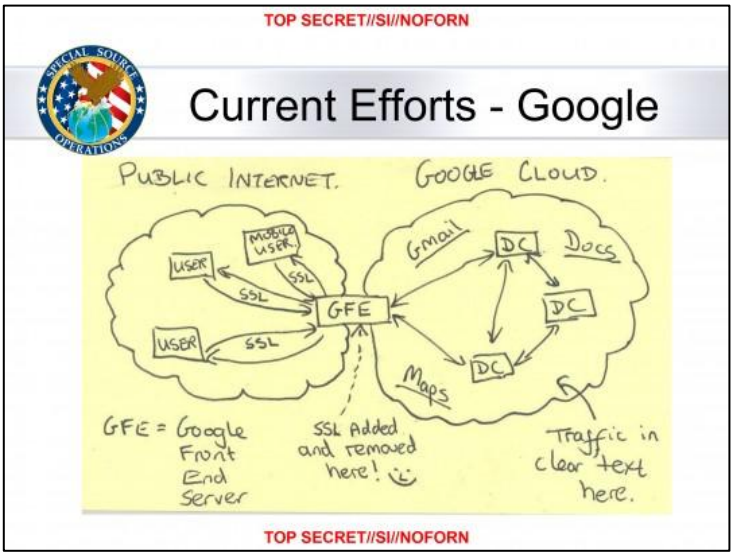
[ix] "רשתות אפלות" ("Darknets"), הוא שם כולל לרשתות תקשורת אנונימיות ומוצפנות, המבוססות על תשתית אינטרנט. רשתות אלה אמנם משתמשות ב"נתיבי התעבורה" של רשת האינטרנט, אך הן פועלות על פי פרוטוקולי תקשורת שונים ומאפשרות רמת אנונימיות ופרטיות מידע מוגברת.
הכנסת. מרכז המחקר והמידע, רועי גולדשמידט, "שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה," מוגש לוועדת המדע והטכנולוגיה, 1 בינואר 2012.
http://www.knesset.gov.il/committees/heb/material/data/mada2012-01-02.doc

[x] לפירוט מלא על ההדלפה, פרטי התכנית והשלכות הפרסום:
http://www.theguardian.com/us-news/the-nsa-files

**תמונה 3: תכנית PRISM- שקופית "פרטי האיסוף" מתוך אחת המצגות המסווגות שהודלפו**




**תמונה 4: תוכנת Muscular- שקופית ארכיטקטורת המאמץ על גוגל מתוך אחת המצגות המסווגות שהודלפו**



מאמצן של סוכנויות הביון בבניית תוכנות איסוף מידע שכאלה ותוכנות ניתוח לכמויות כה גדולות של מידע היה ללא ספק עצום. אך במקביל עלה החשד להפרה גסה של זכויות אזרחיות המעוגנות בחוקת ארה״ב, כפי שטענה במאמרה גם פרופ׳ לורה דונהיו מאוני׳ ג׳ורג׳טאון.[37] נשיא ארצות הברית בעצמו, ברק אובמה, בנאומו ביום למחרת פרסום החומרים המסווגים אמר [ההדגשות שלי]:

> "You can't have 100 percent security and then also have 100 percent privacy and zero inconvenience. **You know, we're going to have to make some choices as a society**."[xi]

במאמר צד ניתן רק לתהות על השימוש שנעשה במידע הצבור עלינו על ידי חברות התקשורת עצמן. אם סוכנויות הביון היו צריכות למצוא פרצות כדי לשים ידן על מידע כה יקר ערך, הרי שבמקרה של חברות התקשורת– הן שומרות הסף של המידע הזה. בהקשר זה קישר ג׳וליאן אסאנג׳ בספרו בין ציטוט של העיתונאי טום פרידמן, בעל הטור בניו יורק טיימס, משנת 1999: ״ידו הנעלמה של השוק החופשי לא תצלח ללא אגרוף נעלם. מקדונלדס לא תשגשג ללא מקדונל-דאגלאס, מתכנן ה – F15. והאגרוף הנעלם שמאפשר לטכנולוגיות של עמק הסיליקון לשגשג בעולם נקרא הצבא, חיל האוויר, חיל הים וחיל הנחתים של ארצות הברית.״[38] לבין ציטוט המופיע בספרם של אריק שמידט, מנכ״ל גוגל, וג׳ארד כהן, ראש חטיבת Google Ideas, משנת 2013: **׳מה שלוקהיד-מרטין היתה עבור המאה העשרים, הטכנולוגיה וחברות לאבטחת מחשבים יהיו עבור המאה העשרים ואחת.״**[39]

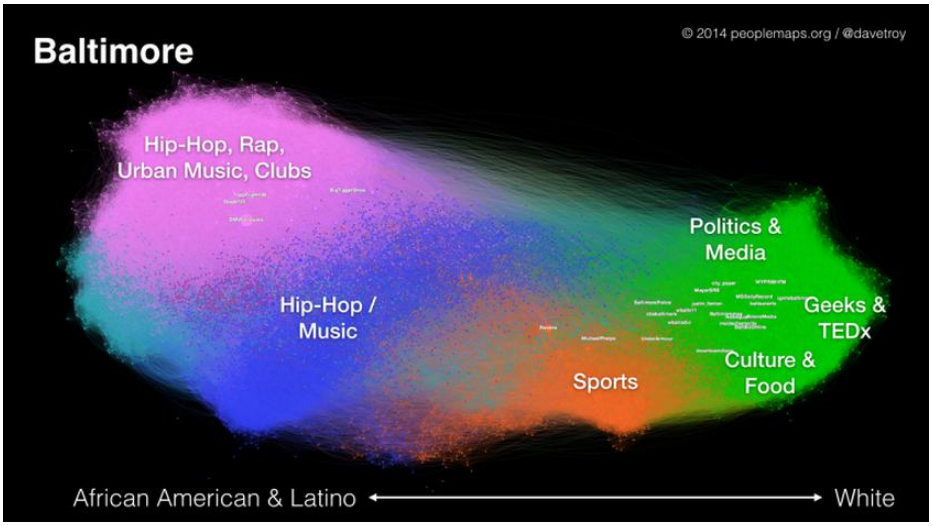
כוונותיהן השאפתניות של סוכנות הביון ״לשבת על הברז״ של תעבורת כמות מידע כה עצומה בכדי לאתר איומים פוטנציאליים (או קיימים) על שלום המולדת מעידות על גישה הנדסית, לפיה ככל שתהיה לך כמות גדולה יותר של מידע – כך גוברים סיכוייך לגלות איום חבוי. יתכן וגישה זו נכונה לצורך

[xi] Peter Baker and David E. Sanger, "Obama Calls Surveillance Programs Legal and Limited," *The New York Times,* June 7, 2013. http://www.nytimes.com/2013/06/08/us/national-security-agency-surveillance.html

גילוי, למשל, רשתות טרור קטנות המתכננות פעולה כזו או אחרת (בהנחה ורשתות כאלו אכן משתמשות בכלים כגון ג׳ימייל, פייסבוק או יוטיוב), אך באשר לזיהוי מגמות או למיפוי מערכות חברתיות מורכבות – הרי שהרשתות החברתיות מלאות במידע שהאזרח המוגן משתף מרצונו החפשי. ניתן כמובן להשתמש בניתוחים מדעיים מעמיקים בתחום זיהוי גורמים משפיעים (attractors) על מערכות מורכבות,[40] אך ניתן גם להשתמש במגוון חברות אזרחיות המפתחות אלגוריתמים אשר סוקרים את הרשתות החברתיות ומספקים מיפוי מוצלח למדי של המערכות על מרכיביהן.

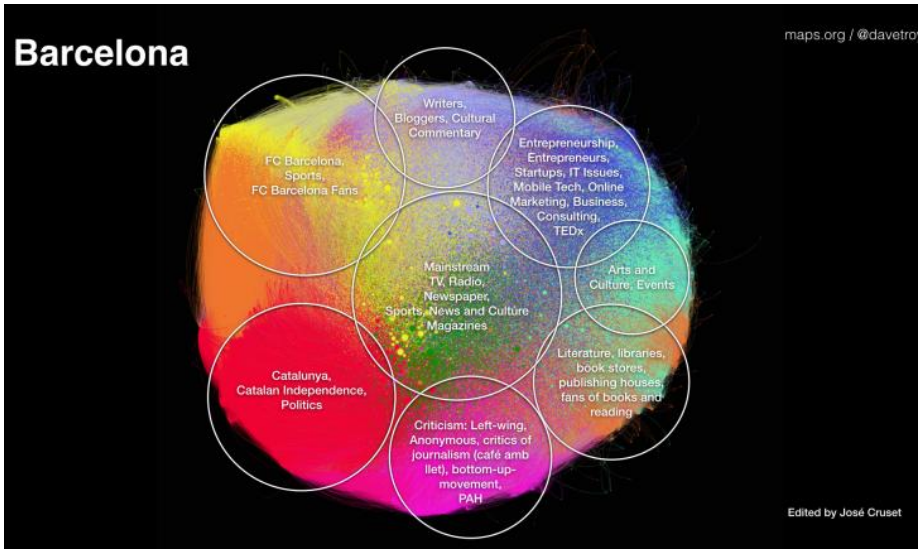
למשל, פרוייקט ״People Maps״ שבראשו עומד דייב טרוי, הוא פרוייקט שמטרתו לחשוף קשרים חברתיים, קבוצות וקהילות באזור גיאוגרפי תחום.[41] המפה החברתית הנוצרת איננה בהכרח גיאוגרפית, אלא בעיקר מלמדת על שונות חברתית ותחומי עניין נפרדים או משיקים בין קבוצות אוכלוסייה שונות. למשל, נעיף מבט אל עבר מיפוי תחומי העניין הבולטים בעיר בולטימור, באמצעות פילוח הנושאים הפופולאריים העולים ברשתות החברתיות של תושבי העיר:

**תמונה 5: פילוח חברתי של העיר בולטימור, לפי שיטת אתר ״People Maps״**



במפה, כל נקודה מסמלת אדם (או שם משתמש), כל קו מסמל קשר בין אנשים, ואילו כל קבוצת צבע מסמלת קהילה בעלת תחום עניין משותף.
במפה החברתית של בולטימור ניתן לראות סגרגציה גזעית מובהקת. המפה כמעט מחולקת לשניים – בצד שמאל של המפה נמצאים בעיקר תושבים ממוצא אפרו-אמריקאי ולטיני, ומימינה – בעיקר לבנים. ניתן לראות גם את תחומי העניין המאפיינים את שני הקצוות, כמו גם את העובדה כי לא קיים תחום עניין ברור המקשר בין השניים.
לעומת זאת, המפה החברתית של ברצלונה נראית אחרת לגמרי:

**תמונה 6: פילוח חברתי של העיר ברצלונה, לפי שיטת אתר "People Maps"**




מעבר לגיבוש החברתי היחסי הניכר מצורת התפזרות תחומי העניין (כדורית), ניתן גם לזהות בבירור נושאים "חמים" עליהם סוערות הרשתות. למשל, ביטויים פוליטיים לעצמאות קטלוניה היא תחום עניין משמעותי המאגד קבוצה גדולה של אנשים סביבו, המקושרים, באופן לא מפתיע, לקבוצה גדולה של אנשים המזוהים יותר עם אוהדי מועדון הכדורגל ברצלונה (FCB). כלל הקבוצות סובבות סביב תרבות מיינסטרימית (ומכאן שמה...) וסביב

חדשות היום. כמו כן, ניכר מהמפה כי למתעניינים בטכנולוגיה, סטארטאפים ועסקים יש מעט מן המשותף עם אוהדי הכדורגל מחד, ועם תושבים המזוהים עם השמאל הפוליטי ותנועות חברתיות (bottom-Up-movement) מאידך.
ניטור קבוע של מפות מסוג זה מאפשר זיהוי היווצרותן של מגמות ופערים, ומאפשר זיהויים של הנעדרים מן השיח המרכזי. מיפוי דעותיה ומחשבותיה של חברה מאפשר לפרקטיקן (הן הממסדי הן אחר) במרחב הסייבר את היכולת **להשפיע** בצורה אפקטיבית על קהלי יעד רצויים – בין אם לצורך ניווט מגמות ובין אם לצורכי הגנה.

כלל הגורמים והתופעות שנסקרו בחלק זה - ויקיליקס, אנונימוס, האקרים פרטיים, השימוש שעושים באינטרנט ארגוני טרור ומדינות, תכניות PRISM ו-Muscular, ושיטות למיפוי רשתות חברתיות, למעשה מבטאים שני צידי מתרס של המלחמה המתחוללת בתקופתנו על המידע. שלל התופעות שנסקרו מתחלקות לשתי קטגוריות – האחת, היא יצירת השפעה במרחב הסייבר. השנייה, היא הניסיון להתמודד עם יצירת ההשפעה ולהשתלט עליה. שתי הקטגוריות מייצגות גם שתי תפיסות המנוגדות זו לזו. הראשונה, "נשקו של הקטן", מציעה גישה רכה להפעלת כוח במרחב הסייבר, ואילו הגישה השנייה, המדינית, היא הקשה והטוטאלית בתפיסתה. מיותר לציין פעם נוספת כי זירת מרחב הסייבר היא מערכת מורכבת שלא ניתן להשתלט עליה אלא לכל היותר לתרום את כלי הנגינה שלך בסימפוניית הביטים. ואכן, על אף תקציבי עתק המועברים מדי שנה לפיתוח טכנולוגיות שיאפשרו שליטת הממסד ב"בן הקיברנטי הסורר" – נראה דווקא כי השפעת הכוחות הלא מדינתיים, האזרחיים, על פתיחות מרחב הסייבר רק עולה.

## סיכום

> ״ידוע לי כי בני האדם סבורים שענייני העולם נשלטים על ידי המזל ואלוהים, וכי האנשים, עם כל כישרונותיהם, אינם מסוגלים לשנות את מה שקבעו אלה. מכך עלולה לנבוע המסקנה כי אין טעם לטרוח ולשנות דברים ומוטב להניח להם להתגלגל בנתיב גורלם. [...] דומה הדבר לאותם נהרות הרסניים, אשר עולים על גדותיהם ושוטפים עצים ומבנים העומדים בדרכם, מעבירים אדמה מאזור לאזור, מבריחים כל מי שמסוגל להימלט, ללא כל יכולת לעצרם. למרות שכך הוא הדבר, בני האדם, בזמנים כתיקונם, מסוגלים לצפות את הדבר מראש ולהתקין תעלות וסכרים באופן שבעת השיטפונות המים יוטו לתעלות ונזקם לא יהיה כה רב. כך הם פני הדברים גם בכל הקשור למזל. הוא מפגין את עצמתו במקום שבו לא נמצאה תושייה לנקוט באמצעים כדי לעמוד בפניו, והוא מכוון את מכותיו לאותם מקומות שבהם לא הקימו סכרים ותעלות כדי לרסנו.״[42]
>
> ניקולו מקיאוולי

בנותנו עצות חכמות (אם כי שנויות במחלוקת) לשליטי איטליה לדורותיהם, העניק לנו מקיאוולי עצה חכמה להתמודדות עם מרחב הסייבר. בעידן שיטפון המידע בו אנו חיים, שיטפון שרק ילך ויגבר, נראה כי הדרך הנכונה להתמודדות ראויה עמו היא לא בניסיון לשלוט בימים ובנהרות, אלא בבניית סכרים ותעלות, בהשפעה ולא בהשתלטות.

השינוי התפיסתי שחל בקרב קהילת אבטחת הסייבר, שתואר בתחילת חלקו השני של המאמר, היא סנונית ראשונה ומבורכת להתמודדות מערכתית מורכבת עם אתגרי המחר. המעבר מתפיסת ״הגנה בעומק״ המורכבת משכבות שכבות של מגנים לתפיסה של ״הגנה קדמית״ מקיפה נבע מההבנה כי אין באפשרות חברות האבטחה לשלוט בתעבורת המידע לכלל עמדות הקצה המצויות בכל בית ולהבטיח כשרותה, אלא יש לווסת את תנועת המידע לכדי אזור מוגדר ומאובטח באמצעות שכבת הגנה קדמית אחת חזקה.

בהמשך, תיארתי מגמות, תופעות ופרקטיקות שונות המאפיינות את הפעילות במרחב הסייבר של ימינו. "במאבקי הכוח הללו", כפי שכתבה פרופ' קרין נהון בהקדמה לספרו של אסאנג', "יש צדדים למאבקים, אולם הסתכלות על מאבקים אלה כמאבקים של טוב נגד רע, אנרכיסט נגד קונפורמיסט, לוחם חופש המידע אל מול תאב השליטה, היא פשטנית ומתעלמת מהמורכבות של מאבקים אלו".[43] מדובר במאבק מרתק בין תפיסות עולם שונות (למרות שבכולן הקידמה הטכנולוגית מוצבת כאידיאל דטרמניסטי בהתפתחותו), המיוצגות, אמנם, על ידי גופים וארגונים ענקיים, אך בסופו של דבר, המחזיקים בהן בני אדם. כל גולש אינטרנט, בבחירות שהוא עושה מדי 'לייק' (אם הוא בחר להיות בפייסבוק), הוא בעל פתק הצבעה לתפיסות העולם השונות הללו.

תורת המערכות המורכבות, שהוצגה בקיצור נמרץ בחלקו הראשון של המאמר, היא אחד הכלים להבנת העולם הסבוך בו אנו מתפקדים מדי יום. ההכרה בהיעדר סופיות המידע והאפשרויות, ובטבע המשיכה החברתית ל'מעצבים' זמניים הינם כלים חשובים מאין כמותם במימוש אחריותנו כאנשי צבא (בחשיבתנו על האתגרים וההזדמנויות הביטחוניים והשלומניים של המחר), כאזרחי מדינה (המעצבים כל אחד בחלקתו את האקוסיסטם החברתי בו ילדנו יגדלו), וכשותפים למערכת אמונות ועקרונות חובקי עולם (כבעלי קול, שבעוצמתו כבר שינה סדרי עולם בעבר).

בטרם אסיים, חש אני חובה בפני הקורא להסביר, סוף סוף, את שמו של המאמר. ובכן, האגדה, מהמיתולוגיה היוונית, מספרת כך: לפני שמינוס היה למלך כרתים, הוא התפלל לאל פוסידון, וביקש סימן שיאשש שהוא זה שצריך לקבל את כס המלכות, ולא אחיו. בתמורה, הוא הבטיח להקריב לפוסידון את היצור שייצא מהים. פוסידון שלח לו פר לבן ויפהפה, אך מינוס, שרחמיו נכמרו על היצור המופלא, הקריב במקומו שור רגיל. פוסידון, נזעם מהפרת ההבטחה, גרם לפסיפאה, אשתו של מינוס, להזדווג עם הפר, וכתוצאה מכך נולד המינוטאור - יצור כלאיים של שור ואדם. המינוטאור היה יצור אכזר ופראי שהטיל את חיתתו על תושבי כרתים, ולכן מינוס, בעצתו של האורקל מדלפי, כלא אותו בלבירינת (מבוך).

באותה תקופה הכריז מינוס מלחמה על אתונה, כיוון שרצה לנקום באתונאים שרצחו את בנו. אתונה נוצחה במלחמה, וכעונש, נדרשה לשלוח, מדי תקופה קבועה, שבעה נערים ושבע נערות אל תוך הלבירינת, כדי שיהיו טרף עבור המינוטאור. בהמשך, תסאוס, בנו של מלך אתונה, התנדב להישלח אל תוך המבוך, במטרה לשים קץ ליצור ולהורגו. למרבה מזלו של תסאוס, לפני שהוא נשלח ללבירינת, אריאדנה, בתו של המלך מינוס, התאהבה בו וגמרה אומר לסייע לו להשמיד את המינוטאור. היא העניקה לו פקעת חוטים, כדי שיוכל לשוב על עקבותיו ולצאת מן המבוך. תסאוס אכן הרג את המינוטאור, והוביל את שאר האתונאים החוצה מן הלבירינת.

מינוס, בזעמו על תסאוס שהצליח לברוח מן הלבירינת, החליט להעניש את דדלוס על כשלונו בבניית הלבירינת כמקום ללא מוצא, וכלא אותו ואת בנו איקרוס במבוך. עם זאת, בזכות תושייתו וכושר המצאתו של דדלוס, הצליחו השניים לברוח לחופשי, בכך שהם בנו לעצמם כנפיים מנוצות ומשעווה.[44]

בראייתי, קווי דמיון רבים נמתחים בין האגדה על מבוכו של המינוטאור לבין סיפור מרחב הסייבר של ימינו. שניהם מעשה ידי אדם, בשניהם מתקיים מאבק, ובשניהם ניתן ללכת לאיבוד. סוד נצחונו של תסאוס לא היה רק בגבורתו על המינוטאור, אלא בשבירתו את היגיון המבוך עם פקעת החוטים. יתכן ואהבה ונועזות הם כלים לא רעים להתמודדותו של כל אחד, עם המינוטאור שלו.

ואם פקששת ונכלאת במבוך – אל תאמר נואש. שבירת הפרדיגמה תבוא גם מחזון הנישא על כנפיים.

## מקורות


[1] K. A. Richardson, Mathieson, G. & Cilliers, P. "Theory and practice of complexity science: Epistemological considerations for military operational analysis," *SysteMexico*, vol. 1, No. 1, 2000, pp. 25-66.

[2] L. von Bertalanffy, **General System Theory- Foundations, Development, Applications**, (New York: George Braziller, 1968), p. 30.

[3] שמעון נוה, **אמנות המערכה- התהוותה של מצוינות צבאית**, (תל אביב: "מערכות"/ משהב"ט, 2001), עמ' 24.

[4] שם. (תרגום הציטוט מתוך .3 ,1968; Bertalanffy).

[5] שם, עמ' 24- 25.

[6] שם. (תרגום הציטוט מתוך. 38 ,14 ,1968; Bertalanffy).

[7] אבי אלטמן, "גישת המערכות – היסטוריה, עקרונות ופרקטיקות של חשיבה מערכתית," *חשיבה מערכתית – חומר עזר מקצועי*. צה"ל/אמ"ץ- תוה"ד/ מרכז דדו לחשיבה צבאית בינתחומית. אוקטובר 2014. מסמך פנימי.

על הקיברנטיקה ראו:

Norbert Wiener. **Cybernetics: Or Control and Communication in the Animal and the Machine**. (Paris: (Hermann & Cie) & Camb. Mass. MIT Press, 1948).

על ייסוד גישת הדינאמיקה המערכתית ראו:

Jay W. Forrester, **Industrial Dynamics**. (Waltham, MA: Pegasus Communications, 1961)

על ייסוד תיאוריית הכאוס ראו:

James Gleick, **Chaos: Making a New Science**, (New York: Viking Penguin Inc., 1987).

[8] M. A. Boden, "Autopoesis and life," *Cognitive science quarterly*, Vol. 1, 2000, pp. 117-145;

[9] Y. Bar- Yam, **the Dynamics of Complex Systems**, (Westview Press, 1997).

[10] C. Gershenson & Heylighen, F., "How can we think complex?" In: A. K. Richardson (Ed.*),* **Managing organizational complexity: Philosophy, theory, and applications- A Volume in Managing the complex**, (Greenwich, Connecticut: Information Age pub., 2005), pp. 47-61.

[11] Bar- Yam, 1997; 1.

[12] L. M. Rocha, "Selected self-organization and the semiotics of evolutionary systems," In S. N. Salthe, Van de Vijver, G., Delpos, M. (Eds.), **Evolutionary Systems: Biological and Epistemological Perspectives on Selection and Self-organization**. (Boston, Mass.: Kluwer Academic Publishers, 1998), pp. 341-358.

[13] S. Guastello, "Self-organization and leadership emergence in emergency response teams," *Nonlinear Dynamics, Psychology, and Life Sciences,* Vol. 14, No. 2, 2010, pp. 179-204.

[14] V. Dimitrov, **A New Kind of Social Science- Study of Self- Organization of Human Dynamics,** (Morrisville, NC: Lulu Press Morrisville, 2005), p. 22.

[15] Felix Lebed & Michael Bar-Eli, **Complexity and Control in Team Sports – Dialectics in Contesting Human Systems,** (London, New York: Routledge, 2013, 2014). pp. 11-18.

[16] L. Biggero, "Sources of complexity in human systems," *Nonlinear dynamics, psychology and life sciences*, Vol. 5, No. 1, 2001, pp. 3-19.

[17] לדוגמא, ראה ספרו של הפילוסוף האמריקאי צ'רצ'מן, שפורסם כבר בשנת 1971:
C. West Churchman, **The Design of Inquiring Systems: Basic Concepts of Systems and Organization**. (New York: Basic Books, 1971).

[18] להרחבה יתרה, ראו: נווה, 2001; רפי רודניק, "אבולוציית המערכה הצבאית – הזיקה בין הפעלת הכוח הצבאי למאפייני סביבת המלחמה," *בין הקטבים*, גיליון 2 – שינוי והשתנות, יולי 2014, עמ' 135-133.

[19] אלטמן, 2014.

[20] http://mediacenter.pandasecurity.com/mediacenter/wp-content/uploads/2014/07/Annual-Report-PandaLabs-2013.pdf

[21] Ibid.

[22] http://mediacenter.pandasecurity.com/mediacenter/wp-content/uploads/2014/11/Quarterly-Report-PandaLabs_Q3.pdf

[23] Intel® Cyber Security Briefing: Trends, Challenges, and Leadership Opportunities. Matthew Rosenquist, Cyber Security Strategist, Intel Corp January 2014.
http://www.slideshare.net/MatthewRosenquist/cyberstrat14-helsinki-matthew-rosenquist-2014-public

[24] W. R. Ashby, **An Introduction to Cybernetics,** (London: Chapman & Hall LTD., 1957) [2nd Ed.], pp. 219-259.

[25] Brad Chacos, "Antivirus is dead, says maker of Norton Antivirus," *PCWorld*, 5 may 2014. http://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html

[26] כלל תיאורי תוצאות המחקר מובאים מתוך:
Blake Stacey and Yaneer Bar-Yam, "Principles of Security: Human, Cyber and Biological," New England Complex Systems Institute, reported to William G. Glenney IV, Chief of Naval Operations Strategic Studies Group, June 1st 2008.
http://necsi.edu/research/military/cyber/netsecurity.pdf

[27] דני דניאל, " טכנולוגית מחשוב ענן: 'באזז' בעולם ה-IT, אז מה זה בעצם?," *ביזפורטל*, 21.01.2010.
http://wallstreet.bizportal.co.il/articles.php?id=110427
להסבר קצר אך תכליתי על מהות מחשוב הענן ראו:
http://www.davidchappell.com/CloudPlatforms--Chappell.pdf

[28] להרחבה ראו:
Vic Winkler, **Securing the Cloud: Cloud Computer Security Techniques and Tactics**, (Elsevier, 2011).
אתר האינטרנט של "ברית הגנת הענן":
https://cloudsecurityalliance.org/

[29] ראו למשל:
Rajiv Gupta, "Why cloud security requires multiple layers," *USA Today*, 25 Nov. 2013. http://www.usatoday.com/story/cybertruth/2013/11/25/why-cloud-security-requires-multiple-layers/3683171/; Cliff Saran, "Cloud security remains a barrier for CIOs across Europe," *ComputerWeekly.com*, 9 December 2014, http://www.computerweekly.com/news/2240236318/Cloud-security-remains-a-barrier-for-CIOs-across-Europe ; Mark Wilson, "Has Microsoft found the answer to cloud security?," *ITProPortal,* 3 December 2014, http://www.itproportal.com/2014/12/03/haven-answer-cloud-security-problems/

[30] ג'וליאן אסאנג', **כשגוגל פגשה את ויקיליקס,** (תל אביב: הוצאת דיונון, 2014), עמ' 71-70.

[31] שם, עמ' 16.

[32] ראה למשל:
Brett van Niekerk, Kiru Pillay, Manoj Maharaj, "The Arab Spring| Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," *International Journal of Communication*, vol. 5 (2011); Benedetta Brevini, Arne Hintz, Patrick McCurdy, **Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society,** (Palgrave Macmillan, 2013); June R. Klein, "Wikileaks, Arab Uprisings, English Riots and Occupy Wall Street: Implications for Internet Policy and Practice from a Business and Industry Outcome Perspective," *Information, Communication & Society Journal*, No. 14.6, 2012; Theresa Sauter & Gavin P. Kendall," Parrhesia and democracy : Truthtelling, WikiLeaks and the Arab Spring", *Social Alternatives*, 30(3), pp. 10-14;
ועוד רבים נוספים.

[33] http://goo.gl/4bXrc7

[34] Dan Smith, "Hackers are the immune system for the information age," *Weird,* 13 June 2014. http://www.wired.co.uk/news/archive/2014-06/13/keren-elazari
ראו גם הרצאתה ב – TED:
https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

[35] גבי סיבוני וסמי קרוננפלד, "התפתחויות בלוחמת הסייבר של איראן 2013-2014," *צבא ואסטרטגיה*, כרך 6, גיליון 2, אוגוסט 2012.

[36] המרכז למורשת המודיעין (מל"מ) - מרכז המידע למודיעין ולטרור, "האינטרנט כזירת מאבק עם ארגוני הטרור: השימוש שעושים חזבאללה וחמאס באינטרנט במלחמה על התודעה ודרכי ההתמודדות עם התופעה," 25 ביולי 2007.
http://www.terrorism-info.org.il/data/pdf/PDF_07_084_1.pdf

[37] Laura K. Donohue, " NSA surveillance may be legal — but it's unconstitutional," *The Washington Post,* June 21 2013. http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html

[38] Thomas Friedman, "A Manifesto for the Fast World," *New York Times,* 28 March 1999. archive.today/aQHvy

[39] Eric Schmidt and Jared Cohen, **The New Digital Age,** British paperback edition (John Murray, 2013), p. 98.

[40] ראו, למשל:

Maksim Kitsak, Lazaros K. Gallos, Shlomo Havlin, Fredrik Liljeros, Lev Muchnik, H. Eugene Stanley & Hernán A. Makse, "Identification of influential spreaders in complex networks," *Nature Physics* vol. 6, 2010, pp. 888–893.

[41] http://peoplemaps.org/

ראו גם הרצאתו ב – TED:

http://www.ted.com/talks/dave_troy_social_maps_that_reveal_a_city_s_intersections_and_separations

[42] ניקולו מקיאוולי, **הנסיך**, (בתרגום גאיו שילוני), (תל אביב: זמורה ביתן, 1988). פרק 25.

[43] קרין נהון, הקדמה לג'וליאן אסאנג', 2014; עמ' iii.

[44] ויקיפדיה. *מיטאורוס*. http://goo.gl/f3T20e

# תופעת סייבר המדינה האסלאמית - מה המערב לא מבין?

**דניאל ברן ויוסי לוי**[i]

**"דאע"ש מומחים בתקשורת ובהפחדות, אין מה לפחד מהם"**[ii]; כך טען בתחילת השנה האלוף במיל' עמוס ידלין, ראש אמ"ן לשעבר וראש מכון ה-INSS היום.

מנגד, בעצרת האו"ם בספטמבר השנה, הכריז הנשיא האמריקאי כי "יש להרוס את דאע"ש... נמשיך במאמץ הצבאי נגד הארגון". ה"ניו יורק טיימס" דיווח כי בעוד הכוחות האמריקנים תוקפים מן האוויר את אנשי המדינה האסלאמית, כוחות הקשורים לאיראן פועלים על הקרקע, נגד האויב המשותף לשתי המדינות.

בראיון שהעניק לאחרונה, הודה הנשיא אובמה כי גורמי המודיעין האמריקאי לא העריכו נכונה את עוצמתו של הארגון בסוריה. בנוסף, כ- 35 שנה לאחר המהפכה האסלאמית באיראן נפגשו בשולי עצרת האו"ם בניו יורק, ראש ממשלת בריטניה ונשיא איראן, למפגש היסטורי ראשון במטרה להדק את הקשר בין שתי המדינות[iii].

במהלך מסע הבחירות לנשיאות, הצהיר נשיא ארה"ב ברק אובמה לא אחת, כי הוא מתנגד ללחימה בעיראק ולכשיבחר יסיג את הכוחות האמריקאים משם. ואכן, ב-19 באוגוסט 2010 האמריקאים נסוג צבא ארה"ב מעיראק. על רקע החלטה זו, ועל רקע הקו המדיני הברור בו נקט אובמה, תמוהה החלטת הממשל האמריקאי והבריטי, ארבע שנים מאוחר יותר, לאחד קואליציה למאבק באותו מקום ממנו נסוגו ב-2010, שעל פי ראש ממשלת בריטניה ויו"ר

---

[i] **תת-אלוף דניאל ברן מכהן היום כמפקד יחידת "לוטם" – היחידה הטכנולוגית לתקשוב מבצעי באגף התקשוב. מר יוסי לוי הוא מומחה לקולנוע ולתקשורת המונים.**
הכותבים מבקשים להודות לאלוף משנה (במיל') עינת גפנר – גולדשטיין, חוקרת מרכז דדו, על תרומתה וסיועה בכתיבת המאמר.

[ii] האלוף במיל' עמוס ידלין, ראש אמ"ן לשעבר, בכנס על ארגון הטרור הסוני הקיצוני דעא"ש – 5.1.2014.

[iii] "שעה של דיאלוג מעשי", צייץ רוחאני. "היסטוריה קטנה נעשתה", אמר קמרון.

המטות המשולבים של ארה״ב ייקח שנים, וידרוש נוכחות של עשרות אלפי חיילים על הקרקע.

מה הצליח לאחד את מנהיגי המערב לפעולה נגד ארגון טרור, שהיה אנונימי יחסית עד לאחרונה ולפעול באופן המחזק את מה שהוגדר עד לא מזמן על ידם כ״ציר הרשע״? במשך למעלה משלוש שנים התנהלה מלחמת אזרחים בסוריה שגבתה למעלה מ - 170,000 הרוגים ובמשך כל תקופה זו ארה״ב ומדינות המערב עמדו מנגד. כיצד אם כן, הצליח בפרק זמן כה קצר ארגון טרור שקיומו נחשף רק לאחרונה, ומונה פחות מ-40 אלף טרוריסטים מצוידים בנשק בסיסי ורכובים על טנדרים, להיות מוגדר על ידי ארה״ב כ״איום על המולדת״?

## תופעת ״המדינה האסלאמית״

**מהו הדבר שהמערב לא מבין בתופעת המדינה האסלאמית? כיצד חוסר ההבנה יוצר פחד בקרב מנהיגי המערב? מדוע חוסר ההבנה לא רק הופך את ההתמודדות עם המדינה האסלאמית ללא אפקטיבי, אלא אולי, באופן פרדוקסאלי, מגביר את הצלחתו, לפחות נכון לעכשיו?**

ארגון המדינה האסלאמית, IS (Islamic State), או כפי שנקרא במקור – דאע״ש (אל-דולה אל-אסלאמיה פי אל-עראק ואל-שאם – ׳המדינה האסלאמית בעראק ובשאם [סוריה]׳), הוא ארגון טרור אסלאמי סוני קיצוני, שהתפצל מארגון אל-קאעדה בשנת 2014, בעקבות חילוקי דעות בין ההנהגה המרכזית למפקדי השטח של הארגון. שינוי שמו של הארגון מדאע״ש ל״מדינה האסלאמית״, מלמד על שאיפותיו המתרחבות אשר אינן מוגבלות עוד מבחינה גיאוגרפית. בסוף יוני 2014 הכריז הארגון על הקמת ח׳ליפות אסלאמית עצמאית בשטחים שבשליטתו.

הארגון הוקם על ידי אבו מסעב א-זרקאווי ב - 2003 ונקרא ג׳מאעת א-תוחיד ואל-ג׳האד, ומטרתו הוגדרה להילחם בכוחות הקואליציה שחדרו לעיראק כדי להפיל את שלטונו של צדאם חסין. ב- 2004 נשבעו לוחמי הארגון אמונים לאל-קאעידה והפכו לשלוחתו בעיראק. מנהיג הארגון אבו מוסעב א-זרקאווי נהרג ב- 8 ביוני 2008 בהפצצת חיל האוויר של ארצות הברית

בעיראק, לאחר ניסיונות התנקשות קודמים שכשלו. אבו איוב אל-מסרי, שהחליף את א-זרקאווי כראש הארגון, חוסל אף הוא ב- 18 באפריל 2010 בפעילות אמריקאית-עיראקית. מנהיגו הנוכחי של ארגון "המדינה האסלאמית", אבו בכר אל-בגדאדי, עומד בראשו ממאי 2010. תחת הנהגתו שינה הארגון את היגיון פעולתו והחל להשתלט על אזורים בעיראק ולהשליט בהם שלטון אסלאמי קיצוני, עם שאיפה להמשיך ולהתרחב.

ההיגיון האסטרטגי של הארגון מתמצה בתנועה להתפשטות במרחב, תוך יצירת מרחב הולך וגדל לח'ליפות אסלאמית, כאשר זו תבנה בהדרגה דרך שלושה מעגלי השפעה. המעגל הראשון מגדיר את גרעין ייסודה של הח'ליפות האסלאמית בעיראק, סוריה ואפגניסטן. זהו המרחב האופרטיבי בו ייווצר המודל הפוליטי החדש שישמש בסיס להתארגנות מוסדית כמו מדינתית[iv] ואשר ישמש השראה להתרחבותה העתידית. המעגל השני, על פי תפישת העתיד של הארגון, הוא המדינות המוסלמיות הכופרות שאיבדו את דרכן, ואילו המעגל השלישי אליו מכוון ארגון "המדינה האסלאמית" את יעדיו הוא המערב. אמנם המערב מוגדר כיעד הרחוק בסדר עדיפויותיו להשפעה והשתלטות, אך בל נטעה, המעגל הזה, כפי שיוצג גם בהמשך המאמר, איננו מחכה בתור. ארגון המדינה האסלאמית בונה את יכולות השפעתו עליו סימולטנית למעגלים האחרים.

התקדמותם של צבאות כובשים בעבר לוותה בקריאות קרב וצלילי הלמות תופי מלחמה מהדהדים בשדה הקרב. הטכנולוגיה והאבולוציה הרשתית העבירה אותנו לעידן הלחימה החדש, בו למכשיר הסלולרי הנייד, למחשב האישי ולרשת החברתית תפקיד משמעותי במימוש האסטרטגיה הצבאית. אל-קאעדה היה מראשוני ארגוני הטרור שהשתמש בהצלחה ברשת, בעיקר כאמצעי תקשורת, פו"ש והדרכה לרכישת יכולות ולקראת ביצוע משימות. אולם, ארגון המדינה האסלאמית עושה שימוש חסר תקדים בתחכומו, בהיקפו ובטקטיקות שלו בשימוש ברשתות החברתיות.

[iv] החליפות האסלאמית אינה מבטאת רעיון של מדינת הלאום כפי שאנו מכירים, אך עם זאת יש באסטרטגיה של המדינה האסלאמית ניסיון לייצר מסגרת פוליטית עם מאפיינים מוסדיים המוכרים לנו (ארגון חברתי, הגדרה טריטוריאלית, כלכלה וכו').

בראי ההיסטוריה, התעמולה כצורת תקשורת להפצת רעיונות בקרב ציבור רחב, במטרה להשפיע על התנהגותו או עמדותיו - קיימת מאות ואלפי שנים. מנגנון מרכזי בתעמולה מבוסס על שימוש בריבוי וחזרה של המסרים המועברים, וזאת על מנת להעצים את חשיפת הפרט אליהם תוך ניצול החשיבה הלא-מודעת של הפרט. עוצמתה של התעמולה בשתי המדינות הטוטליטריות הגדולות של המאה ה-20 - ברית המועצות וגרמניה הנאצית, מוכרת היטב. המניע האידיאולוגי התחבר לצורך ליצור בקרב אומות אלו תחושת קולקטיב רעיוני - המוני - מלכד - חובק כל. התעמולה כללה שימוש באמצעים טכנולוגיים חדישים לזמנם - הרדיו והקולנוע, כמו גם בעצרות המונים, בדגלים ובסמלים, ליצירת שפה חזותית ורעיונית ייחודית, שמטרתה השלטת אורח המחשבה הרצוי על כל הכפופים וההולכים אחרי המשטרים בכל היבט של חייהם.

ארגון "המדינה האסלאמית" שהבין לעומק את משמעות מימד הסייבר ופוטנציאל השפעתו על הפעילות האנושית, יצר מסע תעמולה מקוון מתוחכם, רב השפעה ומתוזמן היטב המקיף את כלל האספקטים של מימד זה, ובדגש על הרשתות החברתיות השונות (וואטסאפ [WhatsApp], פייסבוק [Facebook], טוויטר [Twitter] ויוטיוב [YouTube]), לטובת הפצתו וקידומו של "מותג" הג'האד שלו על פני הגלובוס.

בתחילת שנות האלפיים זיהו חוקרים[v] את השימוש הנעשה על ידי ארגוני הטרור ברשת האינטרנט כמאופיין בחמש קטגוריות עיקריות: תעמולה ולוחמה פסיכולוגית, גיוס מימון, גיוס חברים, רישות (Networking) ואיסוף מידע. המודלים הללו דיברו על דרך פעולה שבדרך כלל נחבאה אל הכלים ונצמדה לאמצעים וערוצים מסורתיים (דוא"ל, אתרים, פורומים). עם התחוללותה של מהפכת ה – Web 2.0 כל כללי המשחק השתנו ובארגון "המדינה האסלאמית" הבינו לעומק את הפוטנציאל וההזדמנויות הנובעים מהתפתחות הרשתות החברתיות והגלובליזציה הרשתית, כפלטפורמה

[v] Muara Conway, "Terrorism and the Internet New Media – New Threat?," *Parliamentary Affairs,* Vol. 59 (2), pp. 283-298.

לתשתית קידום רעיון החי'ליפות המבוזרת והרחבה, בעולם שלאחר ה"אביב הערבי".

פעילותו של ארגון 'המדינה האסלאמית' נשענת על אידיאולוגיה מוגדרת, סדורה וברורה ובניגוד לתפיסה הרווחת, לא מדובר בהתארגנות שצצה לאחרונה "משום מקום". הנהגת הארגון זיהתה מוקדם מאוד (שנתיים לפחות בטרם ההכרזה הרשמית על ייסוד החי'ליפות ביוני 2014) את קהל היעד שלהם, והגדירה אסטרטגיה ודרכים למימושה. הקריאה האידיאולוגית היא ל"מרד" מוסלמי אזרחי עולמי - Rise of the Ummah. זהו מרד הניזון מתחושות נרדפות, ומדיכוי חברתי וכלכלי.

הארגון, ששם לעצמו מטרה להחזיר את החי'ליפות המוסלמית על כנה, עושה שימוש מושכל, מתקדם וחדשני בכל אפיקי התקשורת בעולם המודרני. הוא ניכס את הפלטפורמה הרשתית ליעדיו ולתוכניתו ארוכת הטווח, ונראה כי יש לו את הסבלנות ואורך הרוח הנדרשים כדי להוציאם לפועל.

בספטמבר 2004, חטף מייסד דאע"ש, אבו מסעב א- זארקאווי, שלושה אזרחים מערביים (בריטי ושני אמריקנים), ודרש שחרור אסירים תמורתם. שני האמריקאים הוצאו להורג וראשם נערף בהפרש של יומיים זה מזה, תוך ניצול מופע ההרג של הבריטי ליצירת סרטוני לוחמה פסיכולוגית. הסרטונים הועלו לרשת האינטרנט ועד מהרה מצאו את דרכם גם לרשתות הטלוויזיה ששידרו את הסיפור באינטנסיביות ובהרחבה.

עשור לאחר מכן, שיחזר הארגון בדיוק רב את אותה הטקטיקה שעבדה אז, אך הפעם תחת פיקודו של אבו בכר אל בגדאדי. הארגון הוציא להורג, בזה אחר זה, את הצלם האמריקאי ג'יימס פולי, העיתונאי האמריקאי סטיבן סוטלוף, ועובד הסיוע הבריטי דיוויד היינס, והשתמש בעיתונאי הבריטי ג'ון קנטלי לסדרת סרטוני לוחמה פסיכולוגית. ישנם מוטיבים חוזרים ברורים בסרטונים שקשה להחמיצם, כמו הבגד הכתום (שמתקשר עם לבושם של אסירי הכלא האמריקאי גוואנטאנאמו), הדגל השחור ברקע וכן שיטות הפעולה; עם זאת, ניתן לזהות בבירור את ההבדל העיקרי והוא המיצוי של המדיום האינטרנטי. בשנת 2004 הארגון היה נתון לחסדיה ותשומת ליבה של התקשורת העולמית המוסדית כדי להעביר את המסרים שלו באופן נרחב,

ואילו בשנת 2014 הארגון אינו תלוי עוד בחסדיהם של גורמים חיצוניים. עליית כוחן ומרכזיותן של הרשתות החברתיות בחיי היום-יום, אתרי שיתוף הווידאו ולידתה של "הבלוגוספירה" פטרו אותו מכל תלות שהייתה לו בגורמים חיצוניים. בעת הזו ארגון "המדינה האסלאמית" פעיל בכל מישורי המדיה (כתובה, מודפסת, שמע ווידאו) באופן עצמאי לחלוטין. הוא מעסיק מומחים בתחומי השיווק, יחסי ציבור והפקת תוכן חזותי, תוך שימוש בכלים "משחקיים", כדוגמת ה- gamification[vi], והוא מנצל (בציניות רבה) את מאפייני דור ה- Y ודור ה- Z במערב, תוך רומנטיזציה של האידיאולוגיה שלו.

בין הכלים המופעלים על ידי אנשי הארגון ניתן למנות את ה- #Hashtaghijacking[vii], גניבת חשבונות אישיים באמצעות אפליקציות mobile רשמיות (על כך יורחב בהמשך), שימוש ברשתות BOT אליהן הם הסתננו, ושימוש בכל אלו להפצת קמפיינים (בעיקר כנגד המערב), להעברת מסרים לעוקבים (באמצעות הרשתות השונות), להפצת משחקי מחשב, סרטי תודעה ועוד.

באמצעים אלו מנסה הארגון לגייס חברים חדשים (בדגש על מערביים), להפיץ ולנטוע פחד בקרב אויבים ויריבים (בעיקר במערב), לגייס לגיטימציה וכספים, כאשר נראה כי כלל המטרות מושגות באופן עקבי ומהיר.

החוט המקשר בין כל מישורי הפעולה של הארגון הוא הנעה והתקדמות, לפחות למראית עין, לעבר חזון קץ הימים על פי המסורת הסונית. במסגרת המאמץ לזרוע פחד בלב האויבים והיריבים משחרר הארגון, כבר מראשית שנת 2012, עשרות סרטונים, כשהבולטים ביניהם, באורך הקרוב לשעה, הם סדרה של ארבעה סרטי וידאו המכונה "Clanging of the Swords". בשלושת

---

[vi] השימוש בטכניקות עיצוב משחקים, משחקי חשיבה ומכניקת המשחק, נעשה במטרה לעודד אנשים לאמץ אותם או על מנת להשפיע על אופן השימוש בהם. המשחוק פועל באמצעות הפיכת הטכנולוגיה למרתקת יותר, על ידי עידוד המשתמשים לעסוק בהתנהגויות רצויות, על ידי הצגת הדרך להשגת שליטה עצמית ואוטונומיה.

[vii] ה- Hashtag הוא תווית תוכן ברשתות חברתיות. העוזרת לאחרים המתעניינים בנושא מסוים, למצוא את התוכן באותו נושא במהירות. "Hashtagehijacking" הוא 'גניבת' תוויות לצורך ויסות הקשב של גולשי הרשתות החברתיות. לדוגמא, תווית בשם #ILovelsrael תוביל לציוצים וסטאטוסים התומכים בישראל. הצפה של תווית זו בתכנים אנטי-ישראלים תגרום, למעשה, ל'גניבתה', וכך כל מי שילחץ על תווית זו יגיע בעיקר לתכנים אנטי-ישראלים.

הסרטים הראשונים ישנה התפתחות במסרים ובוויזואליזציה והם מוכוונים בעיקר לגיוס האוכלוסייה דוברת הערבית. עוברים בהם כחוט השני מוטיבים "אפוקליפטיים" וסמליים הלקוחים מהחדית'[viii], המבשרים את ביאת ה"מהאדי" (המשיח המוסלמי) בשנת ההיג'רה 1435 (היא 2014). האלמנטים הבולטים בסדרה הם הדגל השחור (המוכר כמותג הארגון), מגזין מקוון בשם dabiq[ix], שימוש במונח Ummah והדגל האדום המייצג את המאהדי (המשיח המוסלמי), שבואו מבשר את אחרית הימים. בחלק מהסרטים משולבות סצנות אלימות המצולמות בהשראת משפחת משחקי המחשב הפופולאריים GTA ו – Call Of Duty.

לסרט הרביעי והאחרון שהוציא הארגון בסדרה- " Clanging of the Swords IV" אפשר ליחס קפיצת מדרגה ביחס לשלושת קודמיו. הוא מציג את חזון ה-Ummah, את הישגי המאבק והניצחונות בקרבות, את קריעת הדרכונים על ידי הלוחמים החדשים (המגויסים מרחבי העולם) וגם הפעם משולבים בסרט קטעים המצולמים בהשראת המשחק הפופולארי GTA IV. הסרט מסתיים במשפט "...והלהבה הוצתה לה בעיראק. חום הלהבה ורצון האל יתגברו עד שישרפו את נושאי הצלב ב- Dabiq ...".

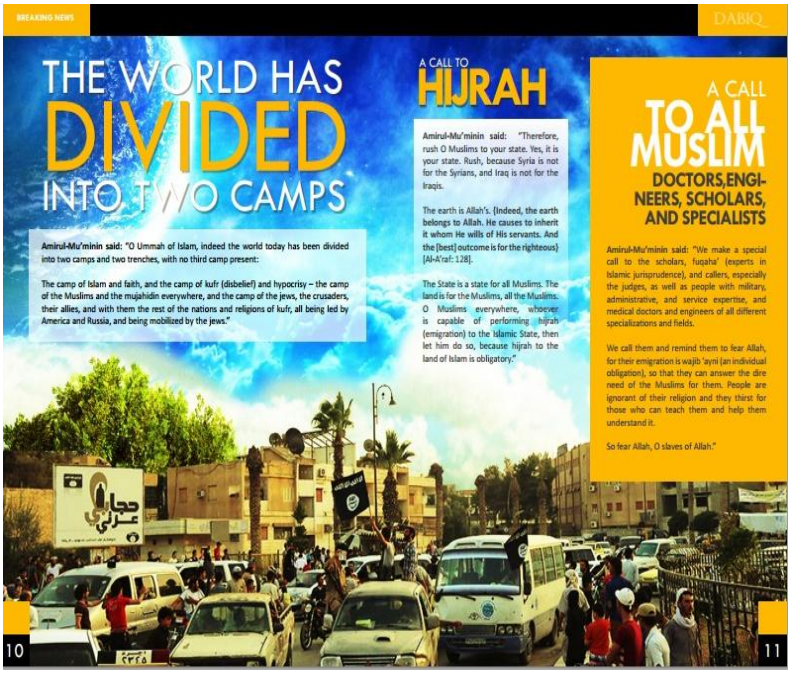
אחד הקטעים בסרט ובו טבח מרכב נוסע בהשראת משחק ה- GTA הפך להיות ויראלי. הוא צבר מיליוני צפיות ברחבי העולם, לייקים, שיתופים בפייסבוק, טוויטר, יוטיוב, וואטסאפ, דוא"ל, אתרי חדשות, אתרים מחתרתיים ופורומים של גיימרים. הסרטון "התפוצץ" לבלוגוספירה כחודש לאחר הופעתו באינטרנט.

---

[viii] החדית' הוא אוסף של הלכות, סיפורים אודות הנביא מחמד ודרך חייו, אשר מופיעים בסונה, הכוללת גם את הביוגרפיה שלו. החדית' מהווה יסוד הלכה השני רק לקוראן.

[ix] ה- Dabiq הינו המגזין הרשמי של הארגון המופק על ידי מרכז תקשורת אל-חיאת המהווה את זרוע התקשורת של הארגון. המגזין מפורסם בכמה שפות ביניהן אנגלית. המגזין נקרא על שם אזור בצפון ח'אלב שבסוריה המוזכר בחדית' כמקום בו יתרחש הקרב המכריע בין המוסלמים לצלבנים שיוביל להכרעת הנוצרים. בשימוש בשם זה ובמשמעותו בהקשר הקמת החליפות המחודשת מנסים ראשי הארגון לספק משיכה רומנטית לגיוס צעירים למאבק שיוביל להשמדת הנוצרים.

**תמונה 1: דף הבית של המגזין Dabiq**




המשחק Grand Theft Auto V ／ GTA מכר, מאז שוחרר בשנת 2013, עותקים בשווי שני מיליארד דולר, ובקרוב צפויה לצאת גרסה ל- PS4 ול-Xbox[x]. סדרת משחקי Call Of Duty היא למעשה גרסה מתקדמת ביותר של סימולטור לחימה אישי, עם מפות הניתנות לתכנון, פעולות מתוכננות עם עשרות "לוחמים" חיים ועוד. מדובר במשחקי רשת המוניים, בהם המשתתפים משחקים בתוך קהילות אונליין, אשר נפגשות לאירועים וירטואליים מבצעיים, וכן משחקים האחד מול השני באופן מזדמן. מדובר בקהילות ובפורומים המונים אלפי אנשים, אשר מעולם לא נפגשו זה עם זה. המשחקים זמינים במחשב האישי, כמו גם בקונסולות המשחק (PS, XBOX),

[x] חשוב להדגיש כי אצל רבים מבין עשרות מיליוני אנשים צעירים ומבוגרים הקונים את המשחק לא מתעורר הצורך להתחייב אלימות בעולם אמיתית.

מתאפשרת בהם רמת תקשורת גבוהה (ניהול שיחות באמצעות טקסטים, מצלמות רשת, אוזניות ומיקרופונים), המהווה כר נוח לקיום תשתית גיוס ואימון רחבת היקף וכל זאת תחת אפם של ארגוני הביטחון.

**תמונה 2: מתוך המשחק Call of Duty / Modern Warfare II**

השוואת המציאות למשחק מחשב, כמו גם הסרטים התודעתיים, מייצרים בקרב צעירי המערב את התפישה כי לקום וללכת ולהילחם בסוריה "קל כמו לצאת לחופשה לדיסנילנד" ובארגון "המדינה האסלאמית" מבינים היטב את פוטנציאל הקונוטציה הזו.

בראשית יולי השנה שחרר הארגון סרט בשם Flames of war, השונה בתכליתו מהסרטים הקודמים. הסרט, לעומת קודמיו שהוכוונו אל הקהל המוסלמי, מכוון לקהל יעד מערבי והוא מתורגם במלואו לאנגלית. הלוחם המרכזי דובר אנגלית רהוטה בדומה לג'יהדי ג'ון והסרט מעט מעודן יותר מקודמיו מבחינת כמות ועוצמת הזוועות המוצגות בו. הארגון דאג, לראשונה, לטשטש חלק מהזוועות, כיאה למסר המוכוון לקהל מערבי. קטעי הלחימה מלוטשים יותר, ומתקשרים בצורה ישירה עם סדרת משחקי ה- Call Of Duty.

**תמונה 3: מתוך הפרומו שהופץ על ידי הארגון לגרסה שלהם למשחק הפופולארי Grand Theft Auto/ Salil Al-Sawarem**

באמצע ספטמבר השנה שחרר הארגון פרומו שדימה את המשחק GTA5 בשם "Grand Theft Auto: Salil al-Sawarem". הקטעים בסרטון לקוחים מגרסת הסיפור של המשחק המקורי ומגרסת האונליין שלו. בטקסט המלווה את הסרטון הארגון מכריז שלוחמיו עושים "בשדה הקרב" בדיוק את מה שבני הנוער עושים בשחקם את המשחק באינטרנט. הסרטון מציג לוחמים ג'האדיסטים שצועקים "אללה אכבר" בזמן שהם תוקפים את ארצות הברית. לפי מחלקת המדיה של הארגון מטרת הקדימון הייתה לעודד את רוחם של הלוחמים הג'האדיסטים הפוטנציאלים, ללמד ילדים כיצד להילחם במערב וכיצד להטיל מורא בלבבות אלו המתנגדים למדינה האסלאמית.

גם אם מדובר בכלי אימון ללוחמים פוטנציאלים וגם אם מדובר בעיקר בכלי תעמולה, כפי שטוענים אחרים, הרי ברור שבכל הנוגע לתעשיית המשחקים זהו קצה הקרחון.

**תמונה 4: כרזה לסייבר ג׳האד**

התקשורת המצרית טוענת שהמשחק וקטע הווידאו נועדו "להעלות את המורל של המוג׳אהדין, להכשיר ילדים ובני נוער צעירים כדי להילחם במערב, ולזרוע טרור בלבם של אויביה של המדינה". העיתונות העולמית פרסמה ראיות לשימוש בקהילת הגיימרים והמשחקים המקוונים (בפרט COD ו-GTA) על מנת ליצור מגע, להכשיר לבבות ולפתות צעירים לרעיון הג׳האד והלחימה. התופעה הפכה מוחשית כאשר נחשף על ידי התקשורת ה"היפסטר הג׳האדיסט הראשון" - צעיר מצרי בשם אסלאם יאקן, רוצח המתהדר

בראשים ערופים. נראה כי תספורת האפרו המתולתלת שלו, המשקפיים העבים והמרובעים והמראה 'הקולי' ענו על הציפיות המערביות בדימוי 'המגניב', ועד מהרה צצו ברשת תמונותיו, ההופכות אותו לגיבור תרבות "היפסטרי" שלצעירי המערב קל להזדהות עמו.

במהלך השנתיים האחרונות, ארגונים מוסלמים סוניים קיימו באנגליה ערבי "החזרה בתשובה" לצעירים, המכונים Call of Duty: Rise of the Ummah . ערבים אלו לוו בסרטונים ובמודעות מבוססות גרפיקה הלקוחה בצורה ישירה ממשפחת סדרת המשחקים המצליחה. חלק מאותם ארגונים משמשים כיום כנציגיו הבולטים של הארגון במאבק ללגיטימציה שלו במדיה הבריטית.

**תמונה 5: הזמנה לערב החזרה בתשובה בסגנון Call of Duty**

**(ובכל זאת, בריטים - "מספר מקומות מוגבל, אנא רכשו כרטיסים מראש!")**

עוד התפרסם באנגליה, כי בחודש יוני טען אב ששני בניו הצעירים (בני 17 ו-18), פותו וגויסו ללחימה בסוריה בשורות המדינה האסלאמית, לאחר שקיבלו במתנה עותקים של המשחק הפופולארי Call Of Duty: Ghosts. בחודש אוקטובר האחרון פנה צעיר סקוטי למשטרה, לאחר שלטענתו, בעת ששיחק בגרסת האונליין של Call Of Duty: Ghosts במכשיר ה-Xbox שברשותו, פנה אליו גורם עלום וביקש ממנו לתרום כסף או להצטרף ללוחמי המדינה האסלאמית. באוסטרליה, המשטרה הפדראלית עצרה חשודים בהשתייכות לאל-קעאידה והחרימה מכשירי פלייסטיישן 3. בדוגמה אחרת, אזרח בריטי שהצטרף לקיצונים האסלאמיים התראיין לתקשורת, באומרו שהלחימה ומשימות הטרור שלו הן טובות "וכיפיות" יותר מאשר המשחק Call of Duty. בחודשים האחרונים, בעקבות חשיפות אדוארד סנודן, הודו ארגוני הביון המובילים בעולם, ביניהם ה- NSA וארגון הביון הבריטי ה- GHCQ, כי חדרו בשנים האחרונות לשרתים ולקהילות המשחקים המקוונים והם עוקבים אחר הנעשה, אחר המשתמשים וכוונותיהם. כמו כן נחשף כי הארגונים, ובראשם ה- CIA בשיתוף עם חברת טוויטר, פועלים באופן יום-יומי למחיקת חשבונות של פעילי הארגון ומנגד להפיץ באמצעות חשבונות מדומים מסרים סותרים. DARPA, מעבדת המחקר של הפנטגון, מימנה מערך של מחקרי מדיה חברתיים, הכוללים ניתוחים על פעילים פוליטיים ושיטות דיסאינפורמציה, תוך מאמץ להבין כיצד ניתן להשיג השפעה התנהגותית ("העניין הבא", re-tweeting וכו') במגוון פלטפורמות של רשתות חברתיות. לאחרונה אף הופץ ברשתות החברתיות סרט של מחלקת המדינה, המתבסס על תפיסות וכלים דומים לאלו שבסרטון Flames of war, אך מציג את האמת (הזוועות) שמאחורי מעשי הארגון. כבר בתחילת 2009 הוציא ה- HDS האמריקאי מסמך המציג את התופעה ואת הסיכון הכרוך בה,[xi] אולם נראה כי עד לאחרונה

[xi] "The Internet as A Terrorist Tool for recruitment and Radicalization of youth – white paper"

התיזה שהוצגה בו לא נלקחה ברצינות על ידי סוכנויות המודיעין והביטחון בעולם המערבי.

**גיוס חברים**

לצד מאמץ הגיוס באמצעות משחקי המחשב, מפיץ הארגון אפליקציות רשמיות הזמינות להורדה מה- Google Play. אחת האפליקציות הנקראת "שחר הבשורה המשמחת" משמשת להגדלת הפרופיל שלהם על ידי שימוש ברשתות החברתיות. אלפי משתמשים הורידו ונרשמו לאפליקציה המתוארת, המדווחת חדשות מסוריה, עיראק והעולם האסלאמי. המשתמשים מאשרים לארגון לקבל מידע רב מהמכשירים שלהם וכן הרשאה לשלוח טוויטים באמצעות החשבונות האישיים שלהם. זה מאפשר לטוויטים של הארגון להגיע למאות או יותר אלפי חשבונות, דבר הנותן תחושה שהתוכן שלהם פופולרי יותר ממה שהוא עשוי להיות במציאות.

אמצעים אלו ואחרים הובילו לתופעה שקיבלה את הכינוי "תיירות ג'האד" או "תיירות טרור" (באנגליה טבעו אף את המונח "five-star jihad"). "תיירות טרור" היא הכינוי הלא רשמי שניתן לתופעה בה גברים צעירים, משכילים, המתפקדים היטב בחברה, נוסעים למדינות מוכות מלחמה שלארצם אין הסכם הסגרה איתן, כדי להשתתף בהרפתקת לחימה לצד ארגוני מורדים וטרור ולהרוג בני אדם. לאחר מכן, התיירים יחזרו לארצם ולא יחששו מהעמדה לדין בגין מעשיהם ופשעיהם במדינות הללו. תופעת "תיירות הטרור" הולכת וגדלה ברחבי העולם. המדינות הפופולאריות ביותר כיעד ל"תיירות טרור" בימים אלו הן סוריה, אפגניסטן ועיראק. הצעיר האוסטרלי בן ה- 17, שנחשף באחד מסרטוני הארגון ביוני האחרון, שיצא להילחם בסוריה והתחייב להניף את דגל דאע"ש מעל ארמון בקינגהאם, הוא אחד הביטויים הבולטים לתופעה זו.

לטענת ה- CIA, נלחמים בעיראק ובסוריה יותר מ- 15,000 טרוריסטים זרים בלמעלה מ- 80 מדינות. לצד ג'האדי ג'ון, קיימות דוגמאות נוספות כמו ה-

Kiwi jihadi מניו-זילנד, צעירים מאוסטרליה, שעל פי העיתונות המקומית הפכה ליצואנית המובילה ללוחמי הארגון, ועוד.

אין המדובר רק בארגון המגייס פעילים ללחימה בסוריה ובעיראק באמצעים חדשניים. על פי חשדות ה- CIA כפי הנראה מדובר בתהליך ויראלי של יצירת מפגעים בודדים עצמאיים שיגבירו את הטרור במדינות המערב עצמן. לדוגמה, אזרח אמריקאי תושב בוסטון, עשה מסע הרג בו רצח ארבעה אנשים ובחקירתו התוודה שעשה זאת בתגובה לנעשה במזרח התיכון וכי זהו חלקו הקטן במאמץ הג׳האד; האחים שביצעו את הפיגוע במרתון בוסטון ונקשרו לאחר חקירה לתא של הארגון; עובד שפוטר ממפעל עיבוד מזון באוקלהומה וערף את ראשה של אחת העובדות על רקע פרסום סרטוני דאע״ש; אישה שראשה נערף בגינת ביתה בלונדון ע״י אדם שכונה "Machete man"; הסתערות של צעיר עם גרזן בניו יורק, בניסיון לפגוע בשוטרים; סדרת אירועי רצח וניסיון לרצח בקנדה, לרבות ירי בבניין הפרלמנט מחוץ לחדרו של ראש ממשלת קנדה, ששהה בבניין בזמן האירוע ועוד. לא רק שלכל האירועים הללו יש קשר מובהק בין החשודים לבין ארגון המדינה האסלאמית או לרעיונות אסלאם קיצוניים, אלא שיש להם מאפיינים ויראליים מדבקים ולכן במעשיהם שלהם – מתגייסים מפגעים חדשים.

בין המצטרפים לשורות הארגון במדינות המערב, יש צעירים רבים שנולדו במערב למשפחות מוסלמיות מהגרות, אך לצידם גל הולך וגואה של צעירים מערביים נוצרים ויהודים, המצטרפים לשורות האסלאם ומפרסמים זאת בסרטוני תעמולה בטענה שמצאו את האור. חלקם מצטרפים לשורות הלוחמים בעיראק ובסוריה, וחלקם פעילים בארצות מוצאם. ראש ה- FBI מסר כי גם לרשויות האמריקניות ידוע על שניים עשר אמריקנים שלוחמים לצד הקיצונים בסוריה. לדבריו, יותר מ-100 אמריקנים ניסו להגיע לסוריה ונעצרו בדרך, או שחזרו בינתיים לארצות הברית. הוא מסר כי כל אותם אמריקנים ששבו מסוריה לאחר לחימה לצד הטרוריסטים, נמצאים במעקב, בחקירה או שכבר נעצרו. דאגה דומה מדווחת בבריטניה, ניו-זילנד אוסטרליה ובמדינות נוספות במערב.

**היגיון ההתפשטות במרחב, מה המערב לא מבין?**

**"להבנתי, הסייבר יתגלה תוך זמן לא רב כמהפכה גדולה יותר מהמצאת אבק השריפה, שהשפעותיה יהיו משמעותיות יותר מאלו שהוביל הניסיון למצות את מימד האוויר בלחימה בתחילת המאה ה-20"**[xii], כך אמר ראש אמ"ן היוצא בתחילת השנה.

בשונה מתפישות הבוחנות את כוחו של הארגון במספר לוחמיו בעיראק ובסוריה, מספר כלי הרכב ("טנדרים") והנשק העומד לרשותם, הצליח ארגון "המדינה האסלאמית" לפתח נשק משמעותי ומסוכן פי אלפי מונים.

תוך הבנה וניצול של תופעות חברתיות והפוטנציאל הטמון בגלובליזציה הרשתית, הפעיל הארגון בצורה סימולטנית מנגנוני השפעה המוניים שונים ומגוונים, כאשר חלקם מבוססי משחקי המחשב והרשת וחלקם קונבנציונאליים יותר, מבוססי הרשתות החברתיות. המהלך הזה הוביל ליצירתו של מסע תעמולה מקוון מתוחכם ומתוזמן היטב שעומק והיקף השפעתו עשויים להיות אחד האירועים המעצבים ביותר בשנים הקרובות. ארגוני הביטחון במערב שחקרו וזיהו את התופעה לא האמינו ביכולתו של הארגון ליצור מהלך משמעותי ממשי. בדומה לאירועים בעבר - הכתובת הייתה על הקיר. במסמך היעדים הרשמי של האחים המוסלמים בצפון אמריקה משנת 1991 מופיעה תוכנית שמטרתה[xiii]:

"....grand jihad is in eliminating and destroying the Western civilization from **within**...."

גם כאן ההפנמה של פוטנציאל הנזק הבשילה מאוחר וכפתה על מנהיגי ארה"ב, העולם המערבי והערבי להימצא בנקודה אסטרטגית שלא רצו בה. הקואליציה המובלת על ידי מנהיגי המערב יצאה לפעולה קיצונית שעלותה למשלם המיסים האמריקאי, כדוגמא מייצגת, 10 מיליון דולרים ליום.

[xii] ר' אמ"ן היוצא האלוף אביב כוכבי, בנאום בכנס ה – INSS בינואר 2014.

[xiii] מסמך ששימש כראייה במשפט מלחמה בטרור כנגד התאחדות ה- HOLYLAND בשנת 2008

**הסייבר והרשתות החברתיות – מימד ההשפעה החדש**

מרחב הסייבר הינו מימד מומצא על ידי האדם, המבוסס על מחשבים (חומרה/תוכנה) ותקשורת (על מגוון סוגיה), ומייצר מידע ופעילות אנושית ענפה בו. זהו מרחב נטול תלות בגבולות גיאוגרפיים ומוסכמות משילות מודרניות. מבחינה חברתית, מרחב הסייבר מאפשר למשתמשים בו לקיים אינטראקציה במגוון דרכים: להקים ולקיים קהילות, להחליף רעיונות, לשתף מידע, לספק תמיכה חברתית, לקיים עסקים ומסחר, ליצור אמנות, לשחק במשחקים, לעסוק בדיון פוליטי וכך הלאה.

בשנים האחרונות הפך מרחב זה למרחב לחימה של ממש. לעיתים ככזה העומד בפני עצמו, ולעיתים ככזה המסייע ללחימה במרחבים המסורתיים (היבשה, האוויר והים - ויש שיוסיפו גם החלל), לעיתים כחלק מלחימה רחבה (בין היתר כמכת פתיחה לקראת לחימה) ולעיתים כמימד במערכה שבין המלחמות, לעיתים הוא מופעל על ידי מדינות ולעיתים על ידי ארגונים (טרור או אחרים). כך או כך, ברור הוא שהלחימה במרחב הקיברנטי הולכת ומתעצמת לכדי מרחב המשנה דרמטית את אופי הלחימה וסוגי האתגרים הגלומים בה.

באופן מסורתי תחום הסייבר התייחס לשלושה נדבכים בעיקר והם: CNE - ריגול, CNA - תקיפה קיברנטית ו- CND - מגננה במימד הסייבר. בשנים האחרונות הצטרף לאלו נדבך נוסף, **ה- CNI (Computer Network Influence) - השפעה באמצעות מימד הסייבר**. מדינות המנסות להתאים עצמן לעידן המתפתח עוסקות בעיקר במבנים ארגוניים שימצו באופן מיטבי את הפוטנציאל הנובע מהסינרגיה בין הנדבכים.

מדינות רבות, ומדינת ישראל ביניהן, משקיעות מאמץ, משאבים ומקיימות בשנים האחרונות תהליכים ארגוניים על מנת להיערך לעידן הסייבר. בצה"ל מחולקת האחריות על הנדבכים הללו בין אגף המודיעין לאגף התקשוב. חשוב לציין שבנדבך ההגנה פועלים במדינת ישראל מספר גופים בנוסף לצה"ל, ביניהם השב"כ (באמצעות רא"ם לשעבר – הרשות הממלכתית לאבטחת מידע), משרד המשפטים (באמצעות רמו"ט – הרשות למשפט טכנולוגיה

ומידע), משרד הביטחון (באמצעות מלמ"ב - הממונה על הביטחון במערכת הביטחון) ומשטרת ישראל.

מאז הקמתו לפני למעלה משנתיים, מוביל מטה הסייבר הלאומי את תחום הסייבר במדינת ישראל, לצד הארגונים האחרים. הצורך בשדרוג ההיערכות הלאומית בתחום הסייבר לא אחרה לבוא, ורק לאחרונה הכריז ראש הממשלה, בנימין נתניהו, על הקמת הרשות הלאומית לסייבר. נתניהו הסביר בפתח ישיבת הממשלה: "החלטתי לפתח רשות לאומית לנושא הסייבר שתסדיר ותדאג להגנת מדינת ישראל בנושא הסייבר. לא רק ההגנה על המתקנים החשובים וגופי הביטחון, אלא כיצד להגן על אזרחי ישראל מפני תקיפות. זוהי רשות חדשה, זה בעצם להקים 'חיל אוויר' נגד איומים חדשים ולא להסתמך על כך שהדבר יתבצע מתוך גופים קיימים. אנחנו בעולם חדש, מתארגנים עם כוחות חדשים. יש לזה משמעות גדולה מאוד להגנתה של מדינת ישראל"[xiv].

השפעת הרשתות החברתיות בעידן ה- Web 2.0 טרם נחקרה לעומק, ובוודאי שהשלכותיה לא מבוררות באופן מספק. יחד עם זאת השפעתן ניכרת בכל מעגלי החיים של פרטים, חברות, ארגונים ומדינות. במידה רבה ניתן לומר כי באמצעות השפעתן על הפעילות האנושית (כמו גם פוטנציאל ההשפעה בחלוקה דורית) תופעות רבות הפכו "מדבקות" (ויראליות) בהיקפים ובקצבים שטרם נראו דוגמתם. אין ספק, למשל, כי הרשתות החברתיות שיחקו תפקיד היסטורי בהפיכה במצרים. זו לא הייתה הפעם הראשונה בה רשתות חברתיות משמשות ככלי לקמפיינים עממיים וירטואליים, אך זו הייתה הפעם הראשונה בה קולו של ההמון התגבש לכלל פעולה משותפת. המחאה שהחלה בפייסבוק ובטוויטר והביאה בסופו של יום לסוף עידן מובארכ, כבר נכנסה לדפי ההיסטוריה. דף פייסבוק בשם "כולנו חאלד סעיד"[xv] נחשב לנקודת הפתיחה של המהפכה המצרית. דף זה הצליח לגייס ולאגד מאות אלפי מצרים על רקע חוסר שביעות הרצון של הצעירים במצרים, ועם רוח גבית חזקה מהמהפכה האזרחית הסוערת בתוניס. ב-25 בינואר, צלחו ההמונים את

[xiv] שלמה צזנה, "חדש: הרשות הלאומית להגנת הסייבר," ישראל היום, 21.09.2014.
http://www.israelhayom.co.il/article/220445

[xv] צעיר ששוטרים רצחו באלכסנדריה כשנה וחצי לפני תחילת המהפכה

מגבלות המרחב הווירטואלי והחלו להתקבץ בכיכר תחריר, כל זאת בליווי גל שביתות המוניות והתפרעויות ברחבי המדינה, שבסופו של דבר גרמו לנפילת משטר מובארכ.

## מה המערב עדיין לא מבין

בהופעתו בפני חברי המשנה למודיעין של וועדת חוץ ובטחון, טען ר' אמ"ן הנכנס אז, האלוף אביב כוכבי, כי "אין סכנה ליציבות השלטון במצרים" ועוד הוסיף: "אנחנו לא רואים באחים המוסלמים כוח מאורגן או מלוכד מספיק כדי לתפוס את השלטון, למרות שאם יהיו בחירות הם יקבלו 40 אחוז."[xvi] אלא שהאירועים הדרמטיים במצרים הובילו למציאות חדשה. נראה כי יש לנו קושי לתפוש את עוצמתן של התארגנויות חברתיות וירטואליות לכאורה, ועוד יותר קושי לדמיין מהפכות שבאות בעקבותיהן.

עבור מנהיגי המערב מורכב לחשוב שעריפת ראשים ופיגועי גרזן הן התוצאה של בחירה רציונלית להרוג אויבים ייעודיים בשם האסלאם. הרבה יותר קל לישון בלילה אם מניחים שמדובר רק בשני זאבים בודדים הלוקים בנפשם, במקום להבין כי מדובר בחסידים של תנועה דתית-לאומית מאורגנת, המורכבת מאלפי מאמינים אמיתיים, המוכנים להרוג ולמות בהוראתו של המנהיג הכריזמטי שלהם, בפרט כאשר הזמנות אלו יועברו באמצעות טוויטר.

חוקרים רבים עוסקים בחודשים האחרונים בשאלות: מה הניע לשינוי המהיר והדרמטי במדיניות המערב? מה הוא שגרם לנשיא ארה"ב לשנות את מדיניותו במאה ושמונים מעלות, לאחר שזו מחזירה אותו לעיראק? מה הניע את הרכבת הקואליציה של מדינות מערביות וערביות במלחמה עתירת משאבים בארגון טרור המונה כמה אלפי לוחמים? התשובה לכך נעוצה בהבנת רישותה של התופעה ומופעיה השילוחיים, המצויים כבר בתוך המערב ולא פחות מכך בפחד מפני מחזה האימים המתרחש לנגד עיננו. ההבנה היא שארגון "המדינה האסלאמית" עלול להסתבר לא כמופע הזוי בר חלוף, כי אם

[xvi] אריק בנדר, "קריאות בכנסת: 'לחקור את מחדל המודיעין,'" NRG מעריב, 31.01.2011. http://www.nrg.co.il/online/1/ART2/206/466.html

כמנגנון משוכלל ומתקדם, שמצליח בינתיים להרחיב את בסיס כוחו, ולהתפשט באופן נרחב ושיטתי גם על אדמת הדמוקרטיות הליברליות במערב. באופן פרדוקסלי, דווקא התקיפות של הקואליציה המערבית בסוריה ובעיראק כמוהן כניסיון לכיבוי מדורה בדלק. לצד ההטפה במסגדים, המהווה את התשתית לרעיון "הצדק החדש", התכנים הרשתיים המגיעים משדה הקרב בסוריה ובעיראק, המופצים ברשתות החברתיות, עשויים להעביר רבים משלב התסכול לשלב המעשה. שכן, המאבק, כך לפחות על פי גורמי ג'האד, הוא מלכתחילה על צדק כלכלי – פוליטי, וקיפוח ועל כך שכוחות מערביים פולשים, המונעים מאינטרסים כלכליים, באו לשלוט על משאביהם. הרציונליזציה הדתית של המאבק היא על הזהות האסלאמית, המופרת בכוח זה עשורים על ידי כוחות חיצוניים.

פניית הארגון למאמינים במדינות המערב לא מכוונת רק לשכבות החלשות ולשוליים סוררים. הארגון פונה בקריאה ישירה למהנדסים, רופאים ומומחים המתחברים למוסלמי שבתוכם לפנות ולסייע במאבק. כיום, משולבים במדינות המערב מוסלמים רבים בתפקידים ביטחוניים, ממשלתיים ואחרים, שהצטרפותם הרעיונית צריכה לעורר דאגה רבה בקרב ממשלות המערב. מזה כשנתיים הכינו עצמם מנהיגי הארגון לעימות חזיתי נרחב מול המערב ומדינות ערב "הכופרות". כיבוש שדות הנפט והמשך הפעלתם[xvii] מעידים כי למנהיגי הארגון ברור שלטובת המאבק הנרחב נדרש בסיס כלכלי והם מתכוננים למאבק ממושך. המאבק, אם כן, מול המעגל השלישי, המערב, מונע ראשית לכל מההכרה בצורך להסיג את השפעתו של המערב מהטריטוריה המוסלמית, ולשם כך יש להפעיל לחץ כבד, כולל באמצעי הפחדה קיצוניים, על החברות (societies) המערביות המאפשרות למנהיגיהן להמשיך במדיניות זו.

[xvii] לאחרונה התפרסמו מודעות דרושים למשרת מנהל תפעול שדות נפט בשכר 140,000 ל"ש לשנה

**"המלחמה אינה אלא המשך המדיניות באמצעים אחרים [...] החשיבות לדיכוי רוח הלחימה של היריב, אינה נופלת מהרג ממשי של חייליו [...] במלחמה ישנן דרכים רבות אל המטרה. לא בכל מקרה דרושה הכנעת האויב; השמדת כוחותיו, כיבוש מחוזותיו והחזקתם, פלישה לתוכם בלבד, פעולות המכוונות ישירות אל קשרים מדיניים ואף המתנה פסיבית לתקיפות מצד האויב – הרי כל אלה אמצעים. שניתן לנצל כל אחד מהם כדי להכניע את האויב."**

**קארל פון קלאוזביץ**

האתגרים במלחמה בארגון "המדינה האסלאמית" קשורים, ראשית לכל, להבנה שהמנגנון בנוי על תפיסת הרשתיות החברתית הגלובלית, ובפועל המדינות המערביות לא מסוגלות לפעול באופן יעיל ולמנוע המשך פעולתו. הסיבה לכך נעוצה בתפישה הליברלית הבסיסית של המדינות המערביות, שכן על מנת למנוע את התפשטות הרעיון הדאע"שי במערב יש לפעול ביד חזקה מול חירות הביטוי ברשתות ומול כל הפרת סדר על ידי מוסלמים. לכן, בראיית מנהיגי המערב, המלחמה המתנהלת ברגעים אלו מול הארגון בסוריה הינה, למעשה, מלחמה על הבית. לא רק מלחמה במובן של איום מוחשי על הריבונות המדינית (כמו פיגועי ה-11 בספטמבר) או איום מוחשי על הביטחון האישי המתערער בעקבות פיגועי ה"זאב בודד" (רצח אזרחים לא מוסלמים בעולם ובארה"ב) שכמעט בלתי ניתנים לסיכול, כי אם מלחמה על מהות אופייה של החברה המערבית הפתוחה והמדינה המערבית הדמוקרטית.

לצורך התווית כיוון פעולה מנהיגי המערב חייבים להבין את ההיגיון האופרטיבי הבסיסי המשרת את החזון של הארגון, שפיתח ושכלל התפשטות רשתית בשלושה מעגלים (עיראק, סוריה ואפגניסטן בראשון, מדינות מוסלמיות כופרות בשני, והמערב בשלישי) בדרכו למימוש "חזון אחרית הימים". ההתמודדות המערבית מוכרחה להיות סימולטנית וסינרגטית בשלושת המעגלים בהם מנסה הארגון להתפשט, אך היא אינה יכולה להתקיים בלא היגיון אסטרטגי ארוך טווח, מה שמאפיין כרגע את הגישה המערבית, ובעיקר את זה האמריקאית. האסטרטגיה צריכה להיות מסוגלת

לזהות קודם כל את הכשלים בהתנהלותו של המערב, בגישה שכונתה מאז פיגועי ה- 11 בספטמבר: המלחמה בטרור העולמי (GWOT), שהביאונו עד הלום; היא גם צריכה להצביע על פוטנציאל שיאפשר הסדרה פוליטית שתניח את דעתם של השחקנים המעורבים. אין באמתחתנו פתרון קסם ואין לנו אלא להצביע על כשל זה, שכמו שהוביל את עיראק ואפגניסטן לכאוס הנוכחי, כך צורת ההתערבות הנוכחית עלולה רק להעמיק אותו. מה שברור לעיני כל הוא, שההתנהלות האסטרטגית העכשווית של המערב הינה תגובתית ושלילית במאפייניה (ללא יעדים פוזיטיביים המגדירה יעדים לעתיד רצוי) ומינימליסטית, כלומר נועדה רק למנוע מהיריב להשיג את יעדיו.

גם ההתמודדות עם הארגון בתוך "המעגל הראשון", בעיקר מהאוויר, לא מסוגלת לגעת במקורות התופעה ובמאפייניי השפעתה על הקרקע. וכן, כמו שהורחב במאמר זה, היא אינה מתמודדת עם הרשתיות של התופעה בשלושת המעגלים ובזיקות ביניהם. העידן הדיגיטלי הביא עימו מאפיינים המשנים באופן דרמטי את אופי הלחימה, בדיוק כפי שכלי הטיס שינו באופן דרמטי את הלחימה. עלינו לפתח צורות לוחמה רלוונטיות חדשות על מנת לפתח מסוגלות להתמודד עם אתגרים מסוג זה. כמו כן, בניגוד לדרך הפעולה שנוקטות בה שותפות הקואליציה, מענה רלוונטי מחייב הבנה של התופעה מבית והתמודדות עמה בכלים מגוונים ומתקדמים. בדומה למערכת "צוק איתן" שבמסגרתה ירה החמאס אל מדינת ישראל מתוך אוכלוסייה פלסטינית, התחבא ונלחם מתוכה תוך הבנה וניצול ציני של המגבלה הישראלית המחויבת לחוקי המלחמה וטוהר הנשק, כך במערכה זו פועל ארגון "המדינה האסלאמית" באמצעות לוחמת סייבר מבוססת CNI אל ומתוך החברה האמריקאית תוך הבנה וניצול של תפישת החופש החברתי האמריקאי.

## סיכום

מאמר זה לא התיימר להציע ניתוח אידיאולוגי ומקיף של המגמה המיוצגת על ידי התפשטותו של ארגון "המדינה האסלאמית", כמו גם לא להציע פתרונות קסם שכנראה אין בנמצא. מאמר זה האיר את הפוטנציאל הגלום

במימד הסייבר, על מנת להבין ראשית לכל את התופעה, כמו גם להצביע על הפוטנציאל הגלום בו כדי להתמודד עמה. באמצעות ניתוח פעילותו של הארגון במימד הסייבר ובמיוחד בפעילות ה-CNI במסגרת הרשתות החברתיות, מודגם הפוטנציאל הגלום בהשפעה רחבה על חברות (societies) ובאמצעותן השפעה על סדר יום מדיני ועולמי. באופן מסורתי, נתפס המימד כתווך לפעילות ריגול (ריגול מסחרי, תעשייתי ועסקי), התקפה והגנה כנגד ריגול או התקפה. ארגון "המדינה האסלאמית" זיהה את הפוטנציאל הגלום בפעילות האנושית במימד זה (במיוחד בקרב צעירים עד גילאי 23) ומצליח, בתחכום, מקצועיות ותוך ניצול חופש הביטוי הדמוקרטי-המערבי, לייצר תופעה שבראיית מנהיגי וממשלות המערב נתפסת מסוכנת דיה על מנת לצאת למלחמה כוללת נגדה.

בעידן שלאחר "ויקיליקס", דאע"ש, כארגון טרור, פועל תחת חסות התפיסה הדמוקרטית ליברלית המקדשת את חופש וזכויות האדם. בראיון שהעניק בחודש מאי השנה, טען סטיוארט בייקר, יועץ בכיר ל- NSA ולשעבר עוזר השר לביטחון פנים בממשל בוש האב, כי גופי המודיעין נכנסים לעשור של קיפאון מבחינת פיתוח שיטות איסוף מידע אגרסיביות "וכך אנו נאבד יכולות מודיעיניות שאפילו לא נהיה מודעים לאובדנן - עד שנצטרך לשלוח חיילים למקום שבו הם ייפגעו בצורה שלא ציפינו".

בייקר חזה את המציאות כמעט במדויק. נראה כי הדרך בה בחרה ארה"ב להגיב, וההערכה כי זו צפויה להיות מערכה ארוכה, עלולה להסתבר כ"חרב פיפיות", שתחזק את מגמת התפשטותו של הארגון. מתקפת הקואליציה המערבית מוצגת על ידי ארגון "המדינה האסלאמית" כמתקפת הצלבנים המערביים על האומה המוסלמית, וככזו, היא מסמנת בראייתם את יריית הפתיחה בקרב אחרית הימים. מערך ההסברה של הארגון התכונן היטב לתגובה הצפויה של המערב, ומאז החלה הקואליציה לתקוף בעיראק הוא העצים ברשת את הקריאה לפיגועים כנגד הכופרים המערביים, בדגש על חיילים, שוטרים ואנשי ממסד. כך, אנו עדים בחודש האחרון לגל טרור, עצמאי לכאורה, כלפי לובשי המדים ומוסדות שלטון במדינות במערב.

התגובה המערבית המיידית לתקוף את האיום ישירות, בעיקר מהאוויר, אולי מובנת, אך היא אינה מתמודדת עם הבעיה מבית ועם ההבנה כי גורם חיצוני זר, מנסה לערער ולפגוע במרקם הרב תרבותי ובצביון החיים המערבי הסובלני. היא אף אינה מתמודדת עם המקורות והתנאים המאפשרים לתופעה זו להתעצם ולהתפשט במדינות המערב עצמן.

מנגנון גיוס התרומות וכח האדם של דאע"ש במערב לא הגיח משום מקום - הוא חבר למנגנונים קיימים ולמוסדות וארגונים סונים מוסלמים דוגמת "האחים המוסלמים" שכבר מבוססים היטב במערב. המנגנונים הללו הן למעשה תנועות שחלקן חברתיות וחלקן קהילתיות (מסגדים), אשר השתרשו כחלק מהמרקם החברתי/קהילתי הליברלי במערב ובאותה הנשימה חותרות תחתיו. דרכם ודרך עמותות שונות, דאע"ש יכל לפעול בשקט, מתחת לרדאר וללא חשש מגילוי.

בתזמון מעניין, לפני עשור בדיוק, ועדת החקירה הממלכתית לחקירת מחדלי מאורעות ה- 11 בספטמבר בארה"ב, פרסמה את מסקנותיה העיקריות: המסקנה הראשונה הייתה כי מדובר היה בכשל של הדמיון וחוסר חמור בחשיבה יצירתית אשר חלחלה למוסדות השלטון - מהנשיאים, דרך גופי הביון וכלה באחרון הפקידים. המסקנה השנייה, קשורה בהיעדרה של מדיניות מסודרת; השלישית, מתייחסת לכשל ביכולותיה של המדינה להתמודד עם איום מסוג זה, והרביעית גרסה כי ניהול האירוע לקה בכשלים רבים. יותר מעשור אחרי ומול התפתחותו הדרמטית של אותו איום, הג'האד הגלובאלי, המערב ובראשו ארה"ב מצויים אל מול אותה שוקת שבורה.

העיסוק הנרחב הקיים כיום בעולם בהקשרי הסייבר נוגע בעיקר ליכולות ריגול והתקפה שלילתית. לארגוני טרור כארגון "המדינה האסלאמית" אין כיום עניין או יכולת ממשית לפתח מערכי תקיפה ואיסוף מבוססים. אך בעוד שארגון אל-קאעדה הוציא על פי ההערכות כמיליארד דולר על מתקפות 11 בספטמבר, מצא ארגון "המדינה האסלאמית" מנגנון יעיל וזול, מבוסס סייבר, להכות במערב ולאלץ את נשיא ארה"ב לפעול בניגוד מוחלט לתפיסה שהובילה אותו טרום ובמהלך תקופת כהונתו, עד כדי התפשרות אפשרית עם תכנית הגרעין האזרחית האיראנית. ההשפעה הגלומה שבלוחמת ה-CNI,

השלכותיה, כמו גם הקושי בהתמודדות עמה מחייב השקעה במו"פ רלוונטי והתאמה מהירה של תפישות ודוקטרינות התמודדות. בהקשר הישראלי אין שום ערובה לכך שהתובנות מהמערכה של ומול ארגון "המדינה האסלאמית" לא יחלחלו לדפוסי הפעולה של חזבאללה וחמאס, כמו גם לשחקנים מאתגרים אחרים.

בתחילת 2012, במקביל להקמת המטה הקיברנטי הלאומי במשרד ראש הממשלה נטען כי האקר סעודי בשם 0xOmar גנב פרטי אשראי של עשרות אלפי ישראלים. "ישראל תוקפת והורגת פלסטינים חפים מפשע, היא מבצעת רצח עם ומפרה חוקים בינלאומיים. לכל העולם יש בעיות עם ישראל. אני רוצה לפגוע בישראל מבחינה פיננסית וחברתית", כך הסביר את מעשיו בראיון לעיתונות ההאקר הסעודי. חמאס עשה ניסיון פרימיטיבי שלא צלח לשימוש במרכיבי תודעה במערכות "עמוד ענן" ו"צוק איתן" אך אין שום ערובה לכך שתובנות הלחימה של ארגון "המדינה האסלאמית" לא יחלחלו לדפוסי הפעולה שלו או של יריבים נוספים. על רשות הסייבר המתהווה בימים אלו להבטיח ובהקדם כי מדינת ישראל ואזרחיה ערוכים להתגוננות מפני איומי סייבר מסורתיים וכאלו מתפתחים בכל אחד מהעימותים הבאים.

***"OH, East is East and West is West, and never the twain shall meet,***
***Till Earth and Sky stand presently at God's great Judgment Seat;***
***But there is neither East nor West, Border, nor Breed, nor Birth,***
***When two strong men stand face to face, tho' they come from the ends of the earth!"***

***Rudyard Kipling***

## מקורות


1) http://www.zerofox.com/whatthefoxsays/islamic-state-isis-terror-has-gone-social-infographic/#.VCR-jPmSyPb
2) http://www.ynet.co.il/articles/0,7340,L-4574916,00.html
3) http://www.forbes.com/sites/insertcoin/2014/09/20/isis-uses-gta-5-in-new-teen-recruitment-video/
4) http://www.haaretz.co.il/gallery/fashion/gentlemen/.premium-1.2409595
5) http://www.dailystar.co.uk/news/latest-news/383667/Brit-who-joined-Jihadists-speaks-on-podcast-about-ISIS-terrorism-and-Call-of-Duty
6) http://www.bbc.co.uk/newsbeat/27838978
7) http://www.businessinsider.com.au/australia-is-major-contributor-of-isis-fighters-2014-6
8) http://www.itv.com/news/2014-06-17/isiss-official-app-available-to-download-on-google-play/
9) http://www.jamestown.org/programs/tm/single/?tx_ttnews%5Btt_news%5D=42702&cHash=0efbd71af77fb92c064b9403dc8ea838#.VCV9YvmSyPY
10) http://www.ynet.co.il/articles/0,7340,L-4575106,00.html
11) http://www.frontpagemag.com/2014/mark-tapson/isis-ignites-flames-of-war/
12) https://news.vice.com/article/islamic-state-documentary-style-video-says-the-flames-of-war-have-just-begun
13) http://observers.france24.com/content/20140613-hollywood-fim-jihadist-propaganda-isis
14) http://www.dailymail.co.uk/news/article-2710478/British-brothers-fighting-Isis-Syria-groomed-extremists-using-Call-Duty-claims-father.html
15) http://www.newyorker.com/tech/elements/isis-video-game

16) http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/
17) http://news.yahoo.com/report-nsa-spying-virtual-worlds-online-games-135520383.html
18) http://edition.cnn.com/2013/12/09/tech/web/nsa-spying-video-games/
19) http://edition.cnn.com/2014/09/11/world/meast/isis-syria-iraq/index.html?hpt=hp_t1
20) http://arabcrunch.com/2014/09/twitter-collaborate-with-the-cia-in-its-propaganda-deletes-the-accounts-of-islamic-state-isis-activists-while-keeping-fake-accounts-that-claim-to-be-isis-spread-lies.html
21) http://www.globalresearch.ca/pentagon-and-cia-want-to-keep-isis-tweeting-exploiting-social-media-to-keep-the-endless-war-on-terror-alive/5391222
22) http://edition.cnn.com/2014/09/05/world/state-department-anti-isis-video/
23) https://news.siteintelgroup.com/blog/index.php/entry/285-ali-muhammad-brown-killing
24) http://www.ynet.co.il/articles/0,7340,L-4575110,00.html
25) http://www.frontpagemag.com/2014/robert-spencer/an-isis-nest-grows-in-boston/
26) http://www.telegraph.co.uk/news/uknews/crime/11075380/Woman-beheaded-in-north-London-garden.html
27) http://lacamomille.com/videopage/on/tuIEBLfiMkk.html
28) https://www.youtube.com/watch?v=8RNGc8834Zc
29) http://www.nydailynews.com/news/politics/obama-admits-u-s-underestimated-strength-rise-isis-article-1.1955804
30) http://www.nydailynews.com/new-york/nyc-crime/police-shoots-kills-man-ax-queens-article-1.1984914
31) http://time.com/3533748/canada-ottawa-shooting-parliament/

32) http://www.dailymail.co.uk/news/article-2802160/isis-s-weirdest-western-jihadi-australian-17-year-old-vows-fly-islamist-flag-buckingham-palace-calls-abu-khaled-family-call-idiot.html
33) http://www.clarionproject.org/Muslim_Brotherhood_Explanatory_Memorandum
34) http://www.slate.com/articles/news_and_politics/war_stories/2014/10/president_obama_s_campaign_against_isis_lacks_a_strategy_the_united_states.html
35) http://www.dailymail.co.uk/news/article-2816755/Wanted-experienced-oil-plant-manager-pay-140-000-p-send-CV-ISIS-Jihadists-advertising-skilled-professionals-man-failing-oil-fields-string-fatal-accidents.html
36) http://www.foxnews.com/world/2014/10/25/citizen-jihadists-isis-uses-lone-wolves-to-mount-cheap-effective-attacks-on-us/
37) http://pamelageller.com/2014/09/the-islamic-state-releases-audio-broadcast-calling-on-all-muslims-around-the-world-to-begin-murdering-non-muslims.html/
38) http://www.frontpagemag.com/2014/dawn-perlmutter/american-jihad-black-supremacy-style/

## על הכותבים

- **רס״ן עמית שיניאק**, קצין מודיעין קרבי בעברו, שירת בתפקידי תכנון אסטרטגי וכעת כראש מדור במחלקה לשיתוף פעולה צבאי באגף התכנון. בוגר האוניברסיטה העברית במחלקה למדע המדינה והמחלקה ליחסים בינ״ל, בעל תואר שני בלימודי דמוקרטיה, מדע המדינה וחינוך, ומסיים בימים אלו את עבודת הדוקטורט שלו בחוג למדע המדינה. עבד בעבר במגוון תפקידים בכנסת, באקדמיה, בסוכנות היהודית ובקרנות מחקר ופילנתרופיה.

- **אל״מ שרון אפק** משמש כמפקד קורס פיקוד ומטה ׳אפק׳. מילא שורה של תפקידים בכירים בפרקליטות הצבאית, ובהם: סגן ראש מחלקת הדין הבינלאומי, פרקליט חיל האוויר, יועץ משפטי לפיקוד מרכז ולאיו״ש וסגן הפרקליט הצבאי הראשי. בוגר תואר ראשון ותואר שני במשפטים מאוניברסיטת תל אביב ותואר שני במדעי המדינה מאוניברסיטת חיפה. בנוסף, בוגר המכללה לביטחון לאומי.

- **סרן ליאור לבד** הוא עתודאי, בוגר תואר ראשון למדע המדינה והיסטוריה של המזרח התיכון, ותואר שני בלימודי ביטחון באוני׳ תל אביב. החל את שירותו הצבאי במחלקת ההיסטוריה של צה״ל, ומשרת כעוזר מחקר במרכז דדו מזה שלוש שנים.

- **תא״ל דניאל ברן**, בוגר תואר ראשון בהנדסת חשמל מאוניברסיטת תל אביב ותואר שני בהנדסת חשמל מהטכניון. שירת במגוון תפקידי פיקוד מקצועיים בעולם ההגנה בסייבר במסגרת אגף התקשוב ומכהן כיום כמפקד לוטם – היחידה הטכנולוגית לתקשוב מבצעי באגף התקשוב.

- **מר יוסי לוי** הוא איש מדיה, בעל תואר ראשון בביולוגיה ובוגר בית הספר לקולנוע וטלוויזיה ע״ש סם שפיגל בירושלים. במאי, תסריטאי ועורך קולנוע המתמחה בעבודתו בתקשורת המונים. במהלך שירותו הצבאי שימש כלוחם ביחידות שריון בסדיר ובמילואים.

# סדרת גיליונות בין הקטבים

| | |
|---|---|
| **גיליון מס׳ 1** | **ספר** |
| **פברואר 2014** | **עיון בהתהוות האתגר בגבולות** |
| **גיליון מס׳ 2** | **שינוי והשתנות** |
| **יולי 2014** | **על גמישות צבאית במציאות מתהווה** |
| **גיליון מס׳ 3** | **סייבר** |
| **דצמבר 2014** | **אתגר והזדמנויות במרחבים חדשים** |

**בין הקטבים** הוא כתב העת של צה״ל לאמנות המערכה היוצא לאור ב**מרכז דדו לחשיבה צבאית בינתחומית**. כתב העת מבקש לתרום לפיתוח הידע בצה״ל על תופעות חדשות ומתהוות המשפיעות על סביבתנו, ועל המתחים והזיקות המגדירים את המערכת האסטרטגית ואת העיסוק האופרטיבי, באמצעות סדרת עיונים בתופעות ובמתחים אלו.

**מרכז דדו לחשיבה צבאית בינתחומית**

בסיס דיין - המכללות הצבאיות, ד.צ. 1002

**בין הקטבים** הוא כתב העת של צה"ל לאמנות המערכה היוצא לאור ב**מרכז דדו לחשיבה צבאית בינתחומית**. כתב העת מבקש לתרום לפיתוח הידע בצה"ל על תופעות חדשות ומתהוות המשפיעות על סביבתנו, ועל המתחים והזיקות המגדירים את המערכת האסטרטגית ואת העיסוק האופרטיבי, באמצעות סדרת עיונים בתופעות ובמתחים אלו.

**אמנות המערכה** מתקיימת במתח שבין האסטרטגיה והטקטיקה. כשם שהמחולל החשמלי ממצה את הפוטנציאל הטמון במתח שבין קוטבי המגנט, כך גם אמנות המערכה ממקמת עצמה בין האסטרטגיה לבין הטקטיקה במטרה למצות את הפוטנציאל הטמון במתח שביניהן, ובכך להניע יצירה של ידע חדש.

**בין הקטבים** מתייחס אפוא למקום בו ניצב המנהיג החושב והמתכנן ברמה המערכתית, בתווך שבין המעשה הצבאי לתכליתו המדינית. זהו מרחב ייחודי ומורכב של פרשנות, תיווך ויצירה, אשר במרכזם למידה ושינוי מתמידים.

•••

**גיליון מספר 3** מעמיד לדיון את התופעה המודרנית ביותר עמה מתמודד צה"ל, אשר שינתה את עולמנו לבלי היכר – הסייבר. מרחב הסייבר, שהוא יציר ידי האדם, הוא גם, אולי באופן פרדוקסאלי, מרחב שהוא במידה רבה לא-נודע. נראה כי לא ניתן להפריז בהשפעתו של מרחב הסייבר על עולמנו, ויתרה מכך – בהשפעתו הפוטנציאלית בשנים הקרבות. באמצעות סקירת דוגמאות היסטוריות, בחינת ההשפעה בהווה, והצצה אל העתיד, מציעים מאמרי גיליונו השלישי של **בין הקטבים, 'סייבר – אתגר והזדמנויות במרחבים חדשים'** זווית השקפה ייחודית על התופעה, ובכך, פותחים צוהר לדיון ולמידה מעמיקים. **עמית שיניאק** מעמיד במרכז מאמרו את ניסיונן של מדינת להחלת ריבונותן על מרחבים חדשים שנפתחו בפניהן, בדגש על המרחב הימי, כדוגמא לתהליך אפשרי שיכול לשרתן גם בהתמודדותן עם מרחב הסייבר. **שרון אפק** דן במאמרו על היבטים שונים במשפט הבינלאומי המהווים אבני דרך מרכזיות ליצירת משטר קיברנטי, אבני דרך הנדרשות לגיבוש כללי משחק מתחום המשפט הבינלאומי. כללים שיגדירו את המותר והאסור בין שחקנים בינלאומיים. בין השאר, נועדו כללים אלה לפתור את סימני השאלה ביחס לפעילות התקפית במרחב הקיברנטי. **ליאור לבד** מציע במאמרו גישה נוספת להתמודדות עם מרחב הסייבר, הנשענת על תורת המערכות המורכבות. לטענתו, מרחב הסייבר, כמערכת מורכבת, אינו ניתן לשליטה ולמשטור, אלא לכל היותר לניווט ולהשפעה. **דניאל ברן ויוסי לוי** מציעים במאמרם לקורא ניתוח מעמיק של השימוש שעושה ארגון המדינה האסלאמית (דאע"ש) במרחב הסייבר, ובכך מדגימים את מימד ההשפעה בסייבר, שלטענתם נעדר מהשיח המערבי לצד המימד ה"מוכרים" – הגנה, התקפה ומודיעין.