גיליון מס׳ 5 אוקטובר 2013

מרכז המחקר, המכללה לביטחון לאומי

ש שתונות

ההתקפה הקיברנטית - קווים משפטיים לדמותה
יישום כללי המשפט הבינלאומי על לוחמה במרחב הקיברנטי

שרון אפק

המכללה לביטחון לאומי

מרכז המחקר

עשתונות

גיליון מס׳ 5

ההתקפה הקיברנטית - קווים משפטיים לדמותה

יישום כללי המשפט הבינלאומי על לוחמה במרחב קיברנטי

שרון אפק

אוקטובר 2013, חשוון התשע״ד

שרון אפק, אלוף משנה, בוגר מחזור מ׳ של המכללה לביטחון לאומי, 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 המרכז ואיו״ש וסגן הפצ״ר. בוגר תואר ראשון ותואר שני במשפטים מאוניברסיטת תל אביב, ותואר שני במדע המדינה מאוניברסיטת חיפה.

המחבר מבקש להודות לד״ר דפנה ריצ׳מונד-ברק מהמרכז הבינתחומי בהרצליה על תרומתה הרבה בהדרכה, בהכוונה ובעצה טובה במהלך הכתיבה.

“Cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability”

Leon E. Panetta, Defence Secretary of the U.S. (Oct. 2012)

פתח דבר

חיבור 'עשתונות' זה, פרי מחקר שנערך במכללה לביטחון לאומי, הוא חלק מפיתוח הידע במב"ל אודות המרחב החדש, המסעיר קהילות ביטחון לאומי, בארץ ובעולם, המרחב הקיברנטי. מחקר זה מתמקד באחד מאזורי המבוכה והדילמות בקהילות הסייבר השונות - רלבנטיות המשפט הבינלאומי ביחס ללחימה במרחב הקיברנטי.

בגיליון רחב היקף זה נבחן, הממשק בין המרחב הקיברנטי, מרחב חדש באופן יחסי, פרי ההתפתחות הטכנולוגית של העשורים האחרונים, לבין כללי המשפט הבינלאומי, אשר התפתחו על רקע מלחמות קונבנציונליות, מסורתיות, בין צבאות של מדינות.

הכותב, אלוף משנה שרון אפק, בוגר מחזור מ' של המכללה לביטחון לאומי, עסק במספר תפקידים בכירים בפרקליטות הצבאית, בהיבטים התיאורטיים והפרקטיים של יישום כללים משפטיים על הפעילות האופרטיבית של צה"ל, הן בהקשרי עימותים נרחבים מסורתיים והן בהקשרי עימותים אסימטריים, בהם מטושטש הגבול בין הצבאי לאזרחי. מכתיבתו עולה, כי כבר כיום, יש ליישם את כללי המשפט הבינלאומי על המרחב הקיברנטי. ניתוח הדין הקיים מעלה מספר תובנות מעניינות וחשובות בעניין פעולות אסורות ומותרות במרחב הקיברנטי.

האתגר המרכזי במצב המשפטי הקיים הוא שמדינה, הנופלת קורבן להתקפה קיברנטית, שאינה גורמת נזק פיזי ישיר, אך כרוכה, למשל, בפגיעה כלכלית חמורה, אינה יכולה להגיב עליה בכוח קינטי כהגנה עצמית. אתגר זה עשוי להוביל להתפתחויות משפטיות, במספר כיוונים אפשריים. העבודה נחתמת בהמלצות למעצבי המדיניות ולמקבלי ההחלטות בתחום זה. סבורני, כי השיח בנושאים המובאים בגיליון זה עתיד להעסיק עוד רבות את קהילות הביטחון הלאומי והמשפט.

הקוראים מוזמנים להגיב.

בברכת למידה פורייה,

יוסי בידץ, אלוף

מפקד המכללות

תקציר

העבודה עוסקת בממשק בין המרחב הקיברנטי, מרחב חדש יציר אדם, פרי ההתפתחות הטכנולוגית של העשורים האחרונים, לבין כללי המשפט הבינלאומי, שהתפתחו על רקע מלחמות קונבנציונליות, מסורתיות בין צבאות של מדינות.

המרחב הקיברנטי משנה את פני האנושות. לצד יתרונותיו הרבים, אחת התופעות המטרידות, שהלכו והתפתחו בו הן התקפות קיברנטיות - פעולות באמצעות מחשבים, המיועדות לפגוע בתפקוד של מחשבים או רשת מחשבים, למטרה פוליטית או כזו הקשורה לביטחון הלאומי. מרכזיות המרחב הקיברנטי בהוויה האנושית המודרנית ופוטנציאל הנזק של ההתקפות הקיברנטיות, עוררו שיח בסוגיית המשטר המשפטי בכלל, והכללים מתחום המשפט הבינלאומי בפרט, אשר חלים כיום בתחום זה, ואשר ראוי שיחולו בעתיד.

העמדה הדומיננטית בקרב גורמים משפטיים במערב, כמו גם בממשל האמריקני, היא שיש ליישם כבר כעת את כללי המשפט הבינלאומי גם על המרחב הקיברנטי. מתוך תפיסה זו, בחרתי לנתח את המצב המשפטי הקיים ביחס לשלושה מונחי מפתח מתחום המשפט הבינלאומי. שני מונחים מתחום דיני ה-Jus ad Bellum, כלומר דינים המגבילים את זכותן של מדינות להשתמש בכוח ביחסיהן עם מדינות אחרות - 'שימוש בכוח' (פעולה שנאסרה בין מדינות מכוח מגילת האו"ם) ו'התקפה מזוינת' (פעולה אסורה, המקנה למדינה המותקפת זכות להשתמש בכוח לשם הגנה עצמית). המונח השלישי הוא מתחום דיני המלחמה, החלים במהלך סכסוך מזוין - 'התקפה' (כאשר מבוצעת 'התקפה' במהלך סכסוך מזוין, חלים עליה איסורים והגבלות, לדוגמא האיסור להתקיף מטרות אזרחיות או החובה לפעול במידתיות).

ניתוח הדין הקיים ביחס למונחים אלו מחייב זהירות בשל מספר טעמים: קיומן של מחלוקות בין המעצמות הקיברנטיות ביחס לעצם תחולת כללי המשפט הבינלאומי וביחס לתוכנם (רוסיה וסין מאתגרות

את העמדה המערבית. גישתן ממוקדת בחיזוק ריבונותן ובפיקוח על תכנים באינטרנט); הבדלי גישה וניואנסים בקרב גורמים רלבנטיים במערב; היעדר אמנות מחייבות ופסיקה של טריבונלים בינלאומיים; והיות התחום המשפטי הזה דינמי ומשתנה, מבלי שהתפתחה בו עד היום פרקטיקה משמעותית של מדינות.

חרף הסייגים האמורים, יש חשיבות וטעם רב בניתוח הדין הקיים, והדבר אכן מעלה מספר תובנות מעניינות וחשובות, שבעצם הבנתן והפנמתן יש משום חידוש:

ראשית, קיימת הסכמה רחבה, כי הדין הקיים אוסר על פעולות קיברנטיות, אשר כתוצאה מהן נגרמים באופן ישיר מוות או פציעה של אדם או נזק לרכוש. פעולות כאלו, המבוצעות בין מדינות, יהוו הפרה של האיסור על 'שימוש בכוח'; יהוו 'התקפה מזוינת', המצדיקה שימוש בכוח כהגנה עצמית מצד המדינה המותקפת; ואם הן מבוצעות במהלך סכסוך מזוין, יחולו עליהן כל ההגבלות והאיסורים הנוגעים לביצוע 'התקפה'.

שנית, מכלל ההן חשוב להצביע על הלאו. פעולות קיברנטיות, שאינן גורמות לתוצאות האמורות, אינן מהוות 'התקפה מזוינת', ולא ניתן להגיב עליהן בהגנה עצמית. במהלך סכסוך מזוין, לא ניתן לראות בהן 'התקפה' כלל. זאת, גם כאשר השפעתן המזיקה של אותן פעולות על המדינה המותקפת היא משמעותית מאד, לדוגמה במקרה של התקפות המבוצעות נגד המערכת הכלכלית והפיננסית (יצוין כי קיימות דעות, לפיהן פעולות קיברנטיות מסוימות, שאינן מתבטאות בנזק פיזי, עדיין יהוו שימוש אסור בכוח, אך הדבר שנוי במחלוקת ואינו מצוי בקונצנזוס).

שלישית, באופן חריג וייחודי, בהקשר הקיברנטי, נוצרה זהות בין פרשנות המונח המשפטי 'התקפה מזוינת' לבין פרשנות המונח המשפטי 'התקפה', הגם ששני המונחים שואבים מענפי דין נפרדים וזוכים על פי רוב, במשפט הבינלאומי, לפרשנות שונה. תיאורטית, משמעות המונח 'התקפה מזוינת', אשר בהתקיימה זכאית המדינה המותקפת לפעול בהגנה עצמית, הייתה אמורה להיות מצומצמת יותר (כלומר לחול על

פעולות חמורות יותר), מאשר זו של המונח 'התקפה' במהלך סכסוך מזוין. עם זאת, במרחב הקיברנטי, לפי הדין הקיים, משתרעים שני המונחים על אותן פעולות - הגורמות נזק פיזי ישיר לאדם או לרכוש - ועליהן בלבד. תובנה זו מבטאת את העובדה, שקביעת כללי המשחק במרחב הקיברנטי מצויה בשלב מקדמי בלבד, בו ניתן היה, עד היום, לגבש הסכמות על כללים ותובנות מצומצמים בלבד.

רביעית, ותובנה זו חשובה במיוחד בעת הזו, ניכר כי ההסדרה המשפטית של המרחב הקיברנטי מצויה בשלבי התהוות ועיצוב ראשוניים. זהו תחום דינמי, משתנה ומוכתב על ידי שיקולים אסטרטגיים רחבים, הרבה מעבר לנקודת הראייה המשפטית גרידא.

ניתוח הדין הקיים עשוי ללמד על מספר אתגרים. בראייתי, האתגר המרכזי מכולם נובע מכך שבעולם בו אנו חיים, הדין אינו יכול להסתפק במתן מענה למדינות במקרה של פגיעה פיזית בהן ותו לא. אני צופה, שמדינה אשר המערכת הכלכלית, הפיננסית וחיי השגרה השוררים בה, ייפגעו בצורה חמורה, תרצה להגיב על כך ותחוש זכאית לעשות כן. מדינות לא תוכלנה להשלים עם מצב שבו שמירה על כללי המשפט הבינלאומי בתחום הקיברנטי, תפגע ביכולתן להגן על אינטרסים קריטיים בתחום הביטחון הלאומי, בראייה רחבה של המונח.

להערכתי, האתגר המרכזי האמור עשוי להביא להתפתחות משפטית **בארבעה כיוונים מרכזיים**, כאשר ההסתברות להתרחשותו של האחרון שבהם היא הגבוהה ביותר. הכיוון הראשון הוא אימוץ פרשנות יצירתית וחדשה למונח 'התקפה מזוינת' בהקשר הקיברנטי, שתכלול במסגרת המונח גם פעולות מסוימות שאינן מובילות לנזק פיזי ישיר לאדם או לרכוש. הכיוון השני הוא הגדרת פעולות קיברנטיות, הגורמות למשל נזק כלכלי, כ'שימוש אסור בכוח', והרחבת הסעדים הנתונים למדינה במקרה זה. קידום שני הכיוונים הללו כרוך בקשיים משפטיים ואחרים של ממש.

כיוון שלישי עשוי להיות אימוצה של אמנה בינלאומית חדשה להסדרת כללי המשחק במרחב הקיברנטי. ניתן להצביע על שיקולים משכנעים

בדבר הצורך באמנה מעין זו, אך על רקע חילוקי הדעות וניגודי האינטרסים בקהילה הבינלאומית, תרחיש זה אינו מציאותי, לפחות בשנים הקרובות.

הכיוון הרביעי, עליו הצבעתי כסביר ביותר, הוא שבשנים הקרובות לא תבשיל הסדרה משפטית פורמלית של המרחב הקיברנטי, אך באופן איטי והדרגתי תתפתח פרקטיקה של מדינות בתחום. פרקטיקה זו תשפיע על הפרשנות המשפטית של הכללים ותבשיל בבוא העת למנהג בינלאומי ולכללים משפטיים מחייבים. אמנם, יתכן כי אירוע מעצב במרחב הקיברנטי, בעל משמעות עולמית בחומרתו, יוביל להאצה של ההסדרה המשפטית. אך יש לקוות כי לא כך יקרה. להערכתי, שלב העיצוב של כללי המשחק המשפטיים מצוי בחיתוליו ונכנס כעת לתקופה מכוננת.

פרק הסיום של העבודה חותם את הדיון בהמלצות למעצבי המדיניות ולמקבלי ההחלטות במרחב הקיברנטי. ההמלצות מחדדות את חשיבות המודעות לשניים: ראשית, למצב המשפטי הקיים, (אשר עיקריו מפורטים בפרק ההמלצות), על מנת שניתן יהיה לגזור את השלכותיו על הפעילות הקיברנטית המדינתית בהווה, ומכאן ולהבא. שנית, להקשר האסטרטגי בו אנו מצויים - השנים הקרובות כתקופה מכוננת, בה יעוצבו כללי המשחק והמשטר המשפטי העתידי. מדינת ישראל עומדת בפני תקופה מאתגרת ומורכבת, בה צפויים להתפתח, בה בעת, 'מירוץ חימוש קיברנטי' בהשתתפות מדינות וגופים שאינם מדינתיים, כמו גם קרב איתנים בין מזרח לבין מערב על אופי המשטר המשפטי העתידי ותכניו.

ישראל אינה שחקן שולי במרחב הקיברנטי, אלא מעצמה שעיני העולם נשואות אליה. לדבריה ולמעשיה מיוחסים משקל והשפעה. על ישראל לפעול במספר דרכים מרכזיות, ובהן:

א. מעקב צמוד אחר ההתפתחויות בזירה הבינלאומית, הבנת תמונת המצב, לימוד המגמות וגיבוש הערכת מצב להמשך.

ב. שותפות, רשמית או באמצעות מומחים, בתהליכים של יצירת 'soft law' (משטר משפטי שאינו מחייב), והשפעה על תוכנם. בנוסף, שותפות והשפעה על תהליכי יצירת משטר משפטי מחייב, ככל שיתפתחו, במוסדות מובילים כמו האו"ם.

ג. הבנה כי לפרקטיקה הישראלית, הן במעשים והן בהתבטאויות רשמיות של בכירים, עשויה להיות משמעות רבה בעיצוב הסדר העולמי החדש במרחב.

ד. פיתוח מדיניות, מנגנונים ומומחי ידע, שיתמכו בכל התהליכים האמורים.

צ'רציל, באחת מאמירותיו המפורסמות, העריך כי:

"The empires of the future are the empires of the mind"

כל מי שמבקש להחזיק בכוח ובעוצמה גם בעתיד, חייב ללמוד, להשתנות ולהתאים עצמו למציאות החדשה. כך באופן כללי, וכך בהקשר המשפטי-קיברנטי בפרט. תקוותי, כי העבודה תפתח לכך צוהר ותסייע בכך.

תוכן העניינים

מבוא

בבוקר השבעה בדצמבר 1941 התעוררו אנשי בסיס חיל הים האמריקני בפרל הארבור, הוואי, לצלילים המפתיע של למעלה מ-350 מטוסים יפניים. כמעט ארבע שנים מאוחר יותר, בשישה באוגוסט 1945, גם כן בשעות הבוקר המוקדמות, הייתה זו פצצת האטום שהוטלה על הירושימה, ששינתה את העולם. בבוקר יום שלישי, האחד עשר בספטמבר 2001, היכה הטרור העולמי בלבה של ארצות הברית, ללא אזהרה מוקדמת.

האם נתעורר באחד הבקרים לפרל הארבור קיברנטי? מזכיר ההגנה של ארצות הברית סבור שהדבר אפשרי.[1] מה שהיה מדע בדיוני, הפך למציאות. מהי תגובת המשפט הבינלאומי להתפתחות מטרידה ומרתקת זו?

ברוכים הבאים למרחב הקיברנטי

את סיפורם של הדינים, המסדירים את הלחימה בין בני אדם, ניתן לספר כמעבר בין ממדים או מרחבים. הלחימה החלה על פני היבשה, עברה אל גלי הימים, נמשכה אל המרחב האווירי, ועם ההתפתחות הטכנולוגית - חדרה אף לחלל החיצון. אין ממד, מרחב או תווך, אשר הוזנח במאמציהם של מדינות ומנהיגים להשיג עוצמה צבאית ומדינית.

לאורך ההיסטוריה, שינו ההתפתחויות הטכנולוגית את שדה הקרב ואת כללי המשחק, עיצבו את מאזן העוצמה בין השחקנים המעורבים, המליכו מלכים והורידו אחרים מכסם. כך, ניתן לתאר את ההיסטוריה הצבאית העולמית בחלוקה לתקופות, לפי סוג ההתפתחות הטכנולוגית, למשל עידן הכלים (המצאת הגלגל), עידן המכונות (כגון השימוש

[1] נאום מזכיר ההגנה האמריקני בניו יורק, אוקטובר 2012. להרחבה ראו:
http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0

בארטילריה), עידן המערכות (רדאר, מטוסים ארוכי טווח ועוד) ועידן האוטומציה (מערכות תקשורת ומחשוב מתוחכמות)[2]. את הלחימה המודרנית מרבים לתאר כלוחמת מידע, לאור המקום הנכבד שתופס בה השימוש בטכנולוגיית מחשבים[3]. במאה העשרים ואחת, מהווים המחשבים נדבך משמעותי ביותר ביכולות האסטרטגיות והכלכליות של מדינות. הם מעצימים את כוחן של מדינות, ופותחים בפניהן אופקים חדשים, אך בה בעת, מחמירה ההסתמכות על מחשבים את הפגיעות של מדינות להתקפות באמצעות מחשבים במרחב המכונה 'קיברנטי'[4].

מהו 'קיברנטי', ומהו אותו מרחב קיברנטי המתפתח לשדה לחימה מודרני?

'קיברנטיקה' אינה מונח חדש. שורשי המונח הונחו כבר בעת העתיקה, אך רק במאה העשרים הוא קנה אחיזה של ממש וזכה למשמעות בשורה ארוכה של תחומים. במקור, שואב המונח מפועל בשפה היוונית, שמשמעו 'לנתב' או 'לנווט'[5]. אפלטון עשה שימוש במונח לתאר ניווט של ספינה, ואריסטו לתיאור ניתוב של קהילה. במאה התשע עשרה, השתמש המלומד הצרפתי, אמפר (Ampere), במונח לתיאור הכוונה של ממשלה. כיום זוכה המונח להכרה רחבה (בעיקר בהטייה - 'קיברנטי' בעברית או Cyber באנגלית). מי שתרם לחדירת המונח לשיח העולמי המודרני היה אחד המדענים החשובים של המאה העשרים - הפרופסור האמריקני, נורברט ויינר. את ספרו פורץ הדרך משנת 1948 הוא כינה בתרגום חופשי: קיברנטיקה או פיקוח ותקשורת בחי ובמכונה

---

[2] Owens, 2001.

[3] להרחבה, ראו: Libicki, 1995.

[4] להרחבה: Hughes, 2009; 528-529.

[5] Geyer & Van der Zouwen, 1994. המונח תרם לשפות שונות, כמו המילים 'קברניט' בעברית ו-Government באנגלית.

Cybernetics, or Control and Communication in the Animal and the) Machine)[6].

ויינר הצביע על דמיון בסיסי בין מספר סוגי מערכות - ביולוגיות (בני אדם וחיות), מכניות (מכונות) וחברתיות (חברות אנושיות)[7]. הוא אימץ את המונח ׳קיברנטיקה׳ לתיאור הדינמיקה המתקיימת באותן מערכות. בראייתו, התהליך החשוב ביותר בכל המערכות הוא תהליך קבלת ההחלטות, או הניווט והניתוב העצמי של המערכת. כל מערכת נשלטת באמצעות העברת מידע בערוצי תקשורת, ומתקיימת בה היכולת להעביר מסר (מידע), ודרכו ליצור פעולה או תגובה. תפיסה זו, ועמה השימוש במונחים ׳קיברנטיקה׳ או ׳קיברנטי׳, אומצו במגוון רחב של תחומים, כגון רובוטיקה, מחשבים, בינה מלאכותית, ביולוגיה, סוציולוגיה, ניהול ואף מדע המדינה[8].

מהו ׳המרחב הקיברנטי׳? זהו מונח מורכב, הקשה להגדרה בפני עצמו. ניתן לתאר אותו, למשל, כמשטר היברידי ייחודי של נכסים פיזיים ווירטואליים, חומרה ותוכנה, הכולל את כל רשתות המחשבים בעולם, ובכלל זה האינטרנט, אך גם רשתות אחרות שאינן מחוברות לאינטרנט[9]. לצורך ההפשטה, ניתן להתייחס אליו ככולל את המחשבים בעולם והרשתות המקשרות אליהם וביניהם.

בלבו של המרחב הקיברנטי מצויה רשת האינטרנט (מרשתת, בעברית תקנית). האינטרנט, אסופה של רשתות המקושרות ביניהן, פותחה בשנות השישים כ-ARPANET, תוכנה צבאית שנועדה לקשר בין הרשתות של משרד ההגנה האמריקני, קבלנים שעבדו עמו ורשתות שנפרשו במספר אוניברסיטאות[10]. הרשת, שפעלה תחילה באמצעות

---

[6] Weiner, 1948.
[7] על כך הרחיב גם בספרו המאוחר יותר, Weiner, 1954 ; 26-27.
[8] Deutsch, 1963 ; 77.
[9] Maurer, 2011 ; 8.
[10] Walker, 2000 ; 1094-1095.

מספר קווי טלפון שחיברו בין מחשבים בודדים, משתרעת היום באופן גלובלי, באמצעות כל ערוצי הקשר האפשריים[11], ואליה מקושר כשליש מהאנושות.

רשת האינטרנט הביאה עמה בשורה חדשה. היא תוכננה במטרה להיות פתוחה, מינימליסטית וניטרלית[12]. לפחות מבחינה טכנולוגית, היא חסרת גבולות, חוצה גבולות וגלובלית[13]. אדם הניצב מול מסוף מחשב במדינה אחת, יכול בלחיצת כפתור לבצע פעולה שתשפיע באופן מיידי במדינה אחרת, הרחוקה ממנו אלפי מילין. הוא יכול לתרום בכך לידע, לכלכלה ולחברה באותה מדינה, אך לפעולתו עלולה להיות גם תוצאה מזיקה. לצד היתרונות העצומים של המרחב הקיברנטי, והאפשרויות הבלתי מוגבלות לשימוש בו לתכלית טובה, הוא משמש גם כר פורה לריגול, לפשיעה, ללחימה ולטרור[14].

כאשר התפתח המרחב הקיברנטי, היו שתיארו אותו כמעין 'מערב פרוע' בלתי מוסדר ונטול חוקים[15]. יתכן שהדבר תרם גם לאטרקטיביות של המרחב. עם זאת, במקביל להתפתחות הטכנולוגית, שיצרה את המרחב הקיברנטי, והפיכתו למרכזי בהוויה האנושית, התפתח, באופן טבעי, שיח בסוגיית הכללים המשפטיים שיסדירו את הפעילות בו. על רקע האופי הגלובלי וחוצה הגבולות של המרחב, ברור כי הסדרה כזו מחייבת שיתוף פעולה בינלאומי ומעורבות של שחקנים רבים. רבים מזכירים את הצורך במשטר, שימסד שיתוף פעולה בינלאומי בנושא הקיברנטי. משטר במשמעות של מכלול עקרונות ישירים ועקיפים, נורמות, חוקים ופרוצדורות לקבלת החלטות,

---

[11] Antolin-Jenkins, 2005 ; 135-136.

[12] Nye, 2010 ; 3.

[13] אם כי בפועל, פעולתה מוגבלת לעתים על ידי מדינות, חוקים לאומיים וטכנולוגיות שונות, להרחבה ראו: Maurer, 2011 ; 8.

[14] Nye, 2010 ; 16.

[15] Nye, 2010 ; 14.

שסביבם מתלכדות ציפיות של שחקנים בתחום היחסים הבינלאומיים[16].

יצירת משטר קיברנטי כרוכה אף בגיבוש כללי משחק משפטיים, מתחום המשפט הבינלאומי. בהקשר זה, אחת הסוגיות המשמעותיות ביותר, המעסיקה משפטנים בתחום המשפט הבינלאומי, היא מה הן הנורמות המסדירות כיום פעילות התקפית במרחב הקיברנטי; ולא פחות חשוב מכך - אילו נורמות ייבחרו על מנת להסדיר בעתיד פעילות כזו? כפי שיובהר כעת, עבודה זו מבקשת להתמודד עם סוגיה זו.

תכני העבודה

העבודה נעה בממשק או בציר שבין מספר עולמות. בציר הטכנולוגי-משפטי: בין העולם הטכנולוגי, הקיברנטי לבין העולם המשפטי. בציר התוך-משפטי: בין עולם המשפט הבינלאומי המסורתי, שעסק בעיקר במלחמה קונבנציונלית, לבין תפיסות משפטיות חדשות, המיועדות לתת מענה לצורות לחימה חדשות. בין המשפט הקיים לבין המשפט העתידי. בציר המשפטי-אסטרטגי: בין השיקולים המשפטיים לבין האינטרסים האסטרטגיים הרחבים. אינטרסים שהם שונים בין מערב לבין מזרח.

בכל הצירים הללו קיימים מתח, תחרות, מאבק על הגמוניה בין גורמים ושיקולים, המבקשים לעצב את כללי המשחק של העולם החדש, המצוי בשלבי התהוות. זהו שלב מכונן, בו נקבעות הנורמות. העוסקים בנושא נדרשים לאתגר משמעותי של הבנת תמונת המצב המשפטית, אפיונה, הערכה לגבי התפתחותה ועיצובה. ישראל אינה שחקן שולי במרחב הקיברנטי. נכתב עליה כי: "Israel is no stranger to cyber warfare"[17]. על מקבלי ההחלטות בהקשר הקיברנטי בישראל להכיר את מגרש

[16] Maurer, 2011; 9, המחבר מפנה להגדרתו המפורסמת של Krasner משנת 1983.
[17] Carr, 2011; 251.

המשחקים ואת הכללים הקיימים ולהשפיע על כללי המשחק של העתיד.

אציג להלן בקצרה את מבנה העבודה, תוך הבהרת ההיגיון הפנימי הטמון בו. לאחר פרק המבוא, יוקדש פרק לדיון שאינו משפטי במושג ה'התקפה' במרחב הקיברנטי. תחילה, יובהר מהי התקפה קיברנטית, מבחינה מהותית (להבדיל מהמשמעות המשפטית). בהמשך, יובא מדריך קצר בעניין סוגי התקפות קיברנטיות, ויתוארו התקפות קיברנטיות מרכזיות בזירה הגלובלית. הפרק ייחתם במבט אסטרטגי להמשך, תוך הרחבה, מהו מקור האטרקטיביות של התקפות קיברנטיות, ומהו ההקשר האסטרטגי בו מעוצבים כללי המשחק המשפטיים של המרחב הקיברנטי כעת?

הפרק השלישי יתמקד בשאלה אחת, בסיסית אך חשובה מאד: האם כללי המשפט הבינלאומי חלים במרחב הקיברנטי? זהו הפרק המשפטי הראשון, ובדומה לאלו שיבואו אחריו, הוא מורכב מניתוח כללי של עקרונות המשפט הבינלאומי הנוגעים בדבר. על מצע זה, ייבחן יישומם בהקשר הקיברנטי. גם בפרק זה יתוארו תחילה ענפי המשפט הבינלאומי הרלבנטיים: דיני ה-Jus ad Bellum המסדירים את האפשרות של מדינות לעשות שימוש בכוח; ודיני המלחמה, החלים בשעה שכבר פרץ סכסוך מזוין. בהמשך, תיבחן תחולתם של ענפי הדין האמורים על המרחב הקיברנטי.

הפרק הרביעי מוקדש לאיסור 'השימוש בכוח' במרחב הקיברנטי. איסור 'השימוש בכוח' הוא אחד מעקרונות העל בדיני ה-Jus ad Bellum והוא מעוגן במגילת האו"ם. פרשנותו הולידה לאורך השנים חילוקי דעות מרים. השאלה המרכזית, שתיבחן בפרק זה, היא אילו פעולות קיברנטיות מהוות 'שימוש בכוח'? לעניין זה תוצג העמדה הרשמית של ארצות הברית והאסכולה השלטת בכתיבה המשפטית. בסיום הפרק, יחודד האתגר בהצבעה על הדין הקיים בנושא זה.

הפרק החמישי יוקדש אף הוא למונח מפתח במשפט הבינלאומי: ׳התקפה מזוינת׳. כאשר מדינה מותקפת בדרך זו, מוקנית לה זכות ההגנה העצמית. הפרק ייפתח בניתוח המונחים בראי המשפט הבינלאומי הכללי, ויתפתח לבחינתם במרחב הקיברנטי. השאלה שתעמוד בלב הפרק היא אילו פעולות יהוו ׳התקפה מזוינת׳ קיברנטית? גם בהקשר זה, מבלי להקדים את המאוחר, ניתוח הדין הקיים הוא מאתגר ומעורר דילמות וסימני שאלה. עוד ינותחו במסגרת הפרק שתי סוגיות רבות משמעות: הגנה עצמית מקדימה במרחב הקיברנטי; ו׳התקפה מזוינת׳ במרחב הקיברנטי על ידי גורם שאינו מדינתי, למשל ארגון טרור. בשתי הסוגיות הללו היו התפתחויות משמעותיות, בהקשר של עמדת המשפט הבינלאומי, בעקבות תופעת הטרור העולמי, ששיאה התקפות הטרור של ה-11 בספטמבר. המרחב הקיברנטי עשוי להיות כר פורה להתפתחויות משפטיות נוספות.

הפרק השישי מסמן מעבר לענף דינים אחר של המשפט הבינלאומי - דיני המלחמה. בראשית הפרק יובהר מהם דינים אלו, ומהו ׳סכסוך מזוין׳, שבמהלכו הם חלים. השאלה שתיבחן בשלב זה היא האם חלים דיני המלחמה על המרחב הקיברנטי? המענה לכך אינו מובן מאליו, שכן מרבית דיני המלחמה נוסחו בתקופה, בה התקפה באמצעות מחשבים הייתה בגדר מדע בדיוני.

המשכו של הפרק יוקדש למונח החשוב ביותר במסגרת דיני המלחמה - ׳התקפה׳. כאן תוצג ותנותח שאלה נוספת: אילו פעולות קיברנטיות מהוות ׳התקפה׳ כמשמעה בדיני המלחמה?

הפרק השביעי מתיך לתוכו את התובנות, שעולות משלושת הפרקים הקודמים. הוא פותח בניתוח של הדין הקיים, בעיקרים הנוגעים לשלושת מונחי המפתח המשפטיים - ׳שימוש בכוח׳, ׳התקפה מזוינת׳ ו׳התקפה׳. הניתוח יתומצת לכדי טבלה מסכמת ולאחריה, יסוכמו התובנות המרכזיות. המשכו של הפרק בניתוח התובנה החשובה ביותר שעולה מניתוח הדין הקיים - היעדר מענה אפקטיבי להתקפה קיברנטית נגד מדינה, הגורמת לה פגיעה משמעותית, שאינה כוללת נזק

פיזי ישיר. זהו האתגר המשמעותי ביותר למשפט הבינלאומי בהקשר הקיברנטי הנוכחי.

הפרק ייחתם בתיאור ארבע מגמות והתפתחויות אפשריות להמשך, והן: אימוץ פרשנות יצירתית וחדשה למונח 'התקפה מזוינת'; הרחבת הסעדים הנתונים למדינה במקרה של 'שימוש בכוח' נגדה; גיבוש אמנה חדשה להסדרת כללי המשחק במרחב הקיברנטי; והגישה הריאליסטית - אי סדרה משפטית בטווח הקרוב והתפתחות הדרגתית של פרקטיקה של מדינות. חלופות אלה ודאי אינן מובנות בשלב המבוא, אך הן תתבררנה בהמשך. מתוך הארבע, ההתפתחות האחרונה - היעדר הסדרה, והתהוות הדרגתית ואיטית של פרקטיקה מדינתית - נראית הסבירה ביותר. זאת, אלא אם יתרחש אירוע גלובלי מעצב, מעין 'פרל הארבור' קיברנטי, שיגרום להאצת העיסוק המשפטי בנושא.

הפרק השמיני נועד לחתום במספר המלצות, לאור התובנות האמורות, בדגש על המלצות למקבלי ההחלטות בתחום הקיברנטי בישראל.

ניתוח משפטי של המרחב הקיברנטי מחייב תיאום ציפיות בין הכותב לבין קוראיו. היקף המידע, המתפרסם בנושא הסוגיות העומדות על הפרק, הוא עצום, והוא דורש תהליך ברירה קפדני. סימני השאלה עולים על סימני הקריאה. ההתפתחויות הן מהירות, והכתיבה יכולה לייצג רק נקודה בזמן. עדיין, יש לקוות שהדברים יעוררו עניין, מחשבה וצמא לידע נוסף.

התקפה במרחב הקיברנטי - משמעות, עבר, הווה ועתיד

מהי התקפה במרחב הקיברנטי?

אחד האתגרים המשמעותיים בעיסוק המשפטי במרחב הקיברנטי, עניינו שימוש במונחים. האתגר הוא כפול: ראשית, גישור על הפער שבין המונחים המקצועיים, הקיברנטיים, לבין עולם המושגים המשפטי. פער זה בולט ביחס למונח משמעותי ביותר, הקשור להסדרה המשפטית של המרחב הקיברנטי - ׳התקפה׳ (Attack)[18]. לדיון במונח יוקדש פרק משנה זה.

שנית, יצירת שפה אחידה, מובנת ועקבית, בתחום שבו טרם גובשו הסכמות ואמנות בינלאומיות הזוכות להסכמה רחבה, ולפיכך המונחים המחייבים טרם עוצבו.

עבודה זו אינה מתיימרת לחדור לנבכי העולם הטכנולוגי, ולהסביר כיצד ניתן להתקיף במרחב הקיברנטי. עם זאת, דומה כי ראוי לייחד מספר מילים, כבר בשלב מקדמי זה, להבנה המהותית מהי ׳התקפה קיברנטית׳ (Cyber-attack)? יודגש, כי אין זה דיון במשמעות המשפטית של המונח ׳התקפה׳ במסגרת המשפט הבינלאומי. לכך יוקדש דיון נרחב בהמשך. זהו ניסיון לתחום ולהבהיר, אלו פעולות טכנולוגיות הן מושא הדיון המשפטי. כלומר, המטרה היא להבין את שדה המשחק, שאת כלליו, מבקש המשפט לעצב.

התקפות קיברנטיות הפכו בשנים האחרונות לחלק מהמציאות המודרנית, אך עד היום טרם התגבשה הבנה מוסכמת ומקובלת שלהן מבחינה מהותית. הדבר אינו מפתיע, הואיל וגם למונחים משמעותיים אחרים, כמו ׳טרור׳, טרם נמצאה הגדרה מוסכמת על ידי הקהילה

[18] להרחבה ביחס לקושי שקשור לטרמינולוגיה: Schmitt, 2012.

הבינלאומית[19]. עצם הפער הזה מקשה, לא אחת, לגבש תובנות ביחס לעמדות ולגישות של שחקנים. ניתן אף להניח, כי הדבר עלול להקשות על גיבוש נורמות על ידי הקהילה הבינלאומית ועל יצירת שפה משותפת בהתמודדות עם התופעה[20].

הניסיון להגדיר עד היום את המונח 'טרור' לא צלח. בין השאר, בשל שוני באינטרסים של השחקנים בזירה הבינלאומית. ניסיון להבין מהי התקפה קיברנטית מהווה הזדמנות ראשונה, מבין מספר הזדמנויות שתהיינה בעבודה זו, להציץ אל פערי היסוד והמחלוקות האסטרטגיות, הקיימים בין המעצמות בתחום הקיברנטי. בפרט, קיימים קיטוב וחשדנות הדדית, על רקע הבדלי ערכים ותפיסות אסטרטגיות, בין ארצות הברית ומדינות מערביות לבין רוסיה וסין.

כך, בארצות הברית, המינוח המקצועי להתקפה על רשתות מחשבים הוא Computer Network Attack (CNA). משרד ההגנה של ארצות הברית הגדיר התקפות אלו, בשנת 2010, כ-

"Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and computer networks themselves"[21].

הגדרה דומה אומצה באותה שנה גם על ידי ארגון נאט"ו[22]. בהמשך, לאחר שהוקם בארצות הברית פיקוד ייעודי למרחב הקיברנטי[23],

---

[19] להרחבה בנושא: Saul, 2006. המונח 'טרור' נטבע לראשונה כבר בשלהי המאה השמונה עשרה, במהלך המהפכה הצרפתית, אך עד היום טרם נמצאה לו הגדרה מחייבת, שזכתה לקונצנזוס עולמי.

[20] ראו גם: Hathaway, 2012; 823.

[21] U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8 2010, as amended through Feb. 15, 2012, available at http://www.dtic.mil/doctrine/dod_dictionary/. קיימים שני סוגי פעילות נוספים: הגנתית שמיועדת למנוע פגיעה במידע; ו-exploitation הכולל איסוף מידע מרשתות ומחשבים זרים.

[22] NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-6)(2010), at 2-C-12

[23] הפיקוד הוקם במאי 2010, ואיחד מספר גופים, שעסקו בנושא ובכפיפות ל- Joint Services Strategic Command. זאת, מתוך הכרה בחשיבות הממד הקיברנטי כממד חמישי (בנוסף ליבשה, ים, אוויר וחלל), ובמטרה לתאם את הפעילות

פורסם בשנת 2011 לקסיקון שעניינו מבצעים קיברנטיים, ובו ההגדרה הצבאית הרשמית הראשונה של התקפה קיברנטית. לפי ההגדרה, התקפה קיברנטית היא:

"A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions".[24]

הגדרות אלו ממוקדות בשלושה רכיבים: אמצעי התקיפה - פעולה באמצעות מחשבים; גרימת הנזק; והתשתיות המותקפות - מחשבים, מידע השמור בהם ורשתות מחשבים של היריב.

העמדה של רוסיה וסין, מנגד, שמה דגש על המטרות הפסולות, בראייתן, שעלולות להיות להתקפות קיברנטיות. על עמדה זו ניתן ללמוד למשל מפעילותו של ארגון שנחאי Shanghai Cooperation Organization[25], אשר שולל במפורש, בהסכמיו ובכתביו, הפצת מידע, שנועדה להזיק למערכות חברתיות, פוליטיות וכלכליות[26]. הארגון מבקש לאסור שימוש במרחב הקיברנטי כדי לערער את היציבות הפוליטית, ומעודד סדר יום, הכולל צנזורה על רשת האינטרנט[27]. דוגמה נוספת לעמדות אלו ניתן לראות בטיוטת אמנה בנושא ביטחון

הפונקציונלית של כל הזרועות בתחום הקיברנטי. מטרתו לשמר את היכולת של ארצות הברית לפעול באופן חופשי במרחב הקיברנטי, לשם קידום האינטרסים הביטחוניים הלאומיים של ארצות הברית. ראו גם: Watts, 2011; 59. בישראל טרם הוקם פיקוד קיברנטי דומה.

[24] זהו חלקה הראשון של ההגדרה בלבד. ראוי לציין שההגדרה רחבה במובנים כמו זהות הגורם המותקף (צבא ואזרחים), משך התקיפה (קצר וארוך) ותוצאותיה (קלות וחמורות).

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

[26] להרחבה בעניין מאמצים סיניים ורוסיים לשלוט בתקשורת באינטרנט, ראו:
Tom Gjelten, Seeing the Internet as an 'Information Weapon', NPR.com(Sep.23, 2010).
available at:
http://www.npr.org/templates/story/story.php?storyId=130052701

[27] להרחבה לעניין ההשקפות המשפטיות השונות של מדינות בהקשר הקיברנטי, כמבטאות מכלולים שונים של סיכונים והזדמנויות אסטרטגיים ראו: Waxman, 2011.

מידע בינלאומי, שרוסיה הציעה לקדם בחסות האו"ם. במסגרתה מופיעה ההגדרה הבאה ל'מלחמת מידע', המדברת בעד עצמה:

"conflict between two or more States in the information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."[28].

לטעמי, הגדרות מעין אלו, המוצעות על ידי רוסיה וסין, אינן אפקטיביות לתיחום המונח 'התקפה קיברנטית', הן משום שהן פתוחות להבדלי פרשנות רחבים מדי (למשל, ביחס לשאלה, אילו פעולות חותרות תחת המערכת החברתית והפוליטית?), והן משום שלא ניתן יהיה לגבש סביבן הסכמה רחבה, שכן הן נוגדות ערכי יסוד מערביים, הנתפסים כאבן יסוד של המרחב הקיברנטי, כגון חופש הביטוי, הזכות לקבל מידע ולהחליף מידע בזמן אמת ועוד.

משכך, אבקש להציע כעת הגדרה, המבוססת על התפיסה המערבית של המונח 'התקפה קיברנטית'. איני מציע לאמץ את ההגדרות האמריקניות שהובאו לעיל כלשונן, משום שלדעתי, חסרים בהן רכיבים מסוימים, ובפרט התייחסות למטרות או לתכליות, העומדות בבסיס התקפה קיברנטית.

כהגדרה בסיסית ל'התקפות קיברנטיות', אשר ניתן להסתייע בה לצורך הבנת שדה המשחק בו יעסוק הדיון המשפטי בהמשך, אבקש להציג את ההצעה הבאה[29], לפיה:

---

[28] ראו:
http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

[29] הצעה זו מזכירה את ההצעה שמופיעה ב- Hathaway, 2012; 826-832, אך חורגת ממנה במרכיבים מסוימים ומשמעותיים. בין השאר, הגדרה זו, בניגוד להגדרת

"A cyber-attack consists of any action taken using computer or related networks or systems to undermine the functions of a computer or computer network for a political or national security purpose".

כלומר, פעולה באמצעות מחשבים או רשתות ומערכות קשורות, כדי לפגוע בתפקוד של מחשב או רשת מחשבים, למטרה פוליטית או כזו שקשורה לביטחון הלאומי.

להגדרה זו יש מספר מאפיינים, המאפשרים את תחימת הדיון. ראשית, ההגדרה משתרעת על התקפה באמצעות מחשבים ומערכות הקשורות להם, להבדיל, למשל, מתקיפה של רשת מחשבים באמצעות הפצצה קינטית. אמנם, התקפה באמצעים קינטיים עשויה לפגוע ביכולות של היריב לפעול במרחב הקיברנטי, אך אין לראות בה התקפה קיברנטית כשלעצמה[30].

שנית, הדגש בהגדרה הוא על המטרה - פגיעה בתפקוד של מחשבים ורשת מחשבים. נהוג למיין את הפגיעה בתפקוד, הנגרמת בהתקפות קיברנטיות, לשני סוגים:

Syntactic Attacks - התקפה הפוגעת במערכת ההפעלה של מחשבים וגורמת קשיי תפקוד לרשת המחשבים (לדוגמה באמצעות תולעי מחשב, וירוסים וסוסים טרויאנים)[31].

Semantic Attacks - התקפה המשמרת את מערכת ההפעלה, אך פוגעות בדיוק של המידע שהמערכת מעבדת ומגיבה אליו[32]. כתוצאה מכך, המערכת המותקפת פועלת לכאורה באופן תקין, אך בפועל תסטה מדרך הפעולה שאליה יועדה.

Hathaway, מוגבלת להתקפה באמצעים קיברנטיים (ולא כוללת תקיפת מחשבים באמצעים קינטיים), וכוללת התקפה נגד מחשבים שאינם מרושתים.

[30] לדעה שונה, לפיה ראוי לראות התקפות אלה כהתקפות קיברנטיות, ראו: Hathaway, 2012; 827.

[31] להרחבה, ראו: Antolin-Jenkins, 2005; 139. דוגמה ידועה לתקיפה כזו אירעה בבורמה, בשנת 2010, כאשר זמן קצר לפני הבחירות הדמוקרטיות במדינה, התקפת מחשבים כמעט שניטרלה את השימוש באינטרנט במדינה, ככל הנראה על מנת למנוע זרימה חופשית של מידע. ראו: Hathaway, 2012; 819.

[32] דוגמה ידועה לתקיפה כזו הייתה תקיפת וירוס Stuxnet באיראן, אשר לא התגלתה בזמן אמת, הואיל והמחשבים שהותקפו, פעלו לכאורה בצורה תקינה.

בחיי המעשה, התקפות רבות הן מעורבות, כלומר שילוב של שני סוגי ההתקפות האמורות[33].

יובהר, כי הדרישה לפגיעה בתפקוד של המחשב או רשת המחשבים, מוציאה פעולות מסוימות מכלל ההגדרה, למשל ריגול קיברנטי ואיסוף מידע קיברנטי, שכן פעולות אלו כוללות צפייה פסיבית במידע והעתקתו בלבד. כאשר לא נפגע תפקודם העכשווי או העתידי של המחשבים, מהם נשאב המידע, לא יהיה בכך משום התקפה קיברנטית[34].

שלישית, ההגדרה משקפת את האלמנט הרשתי של מחשבים ומכשירים מודרניים, המתבטא בכך שהם פועלים בערוצי תקשורת רשתיים (לאו דווקא באינטרנט, גם במערכות המכונות 'סגורות'[35]). בד בבד, ההגדרה מתייחסת גם למקרה הפחות שכיח של התקפה על מחשב בודד, אשר לכאורה אינו חלק ממערכת רשתית.

רביעית, ההגדרה מתייחסת להתקפה המיועדת למטרות פוליטיות או מתחום הביטחון הלאומי. בכך, הוצאו מגדרה פשעים קיברנטיים, כגון מרמה באינטרנט, גניבת זהויות, הפרה פיראטית של זכויות יוצרים ועוד. פשעים במרחב הקיברנטי הם תופעה חמורה, שהשלכותיה הכלכליות והחברתיות מרחיקות לכת, אך ההתמודדות עמה אינה באמצעות כללי המשפט הבינלאומי שיידונו בהמשך. עוד יודגש, כי התקפה למטרות פוליטיות וביטחוניות אינה מוגבלת למדינות בלבד, ועלולה להתבצע למשל על ידי גורמי טרור שאינם מדינתיים.

בהמשך יובהר, כי מתוך כל הפעולות במרחב הקיברנטי, העונות למאפיינים האמורים של התקפה קיברנטית, חלק קטן בלבד כפוף

---

[33] Antolin-Jenkins, 2005 ; 141.

[34] דוגמה למבצעי ריגול ידועים, שמקורם כנראה בסין, נגד גופי ממשל אמריקנים, בהם נאסף מידע רב: "Titan Rain" בשנת 2003, ו"Operation Aurora" בשנת 2010. Hathaway, 2012 ; 829.

[35] במסגרת המרחב הקיברנטי מצוי עולם שלם של מכשירים, למשל אלו השולטים במעליות, רמזורים, טלפונים ניידים, טלוויזיות, מערכות מיזוג ועוד. להרחבה: Clark & Knake, 2010 ; 70-74.

לאיסורים או להגבלות מכוח המשפט הבינלאומי הקיים. עיקר האיסורים וההגבלות הם ביחס להתקפות קיברנטיות, המסוגלות לגרום נזק פיזי ישיר. על כך ועל המשמעויות הנגזרות מכך, יורחב בהמשך.

בטרם יתוארו התקפות קיברנטיות מרכזיות, שזכו לפרסום בשנים האחרונות, יוצגו תחילה בקצרה, שלוש הדרכים המרכזיות, שבאמצעותן מבוצעות על פי רוב התקפות קיברנטיות[36]:

הראשונה, פעולות המכונות Distributed Denial of Service (DDoS, 'שלילה מבוזרת של שירותים') - הצורה הנפוצה ביותר של התקפות בשנים האחרונות[37]. כידוע, אתרי אינטרנט רבים ערוכים לכניסות רבות של משתמשים במקביל. לדוגמה, בענפי הבנקאות, התקשורת, המסחר ועוד. בסוג התקפות זה, מוחדר וירוס לעשרות אלפי מחשבים, באופן שמאפשר שימוש בהם לצרכי הגורם החודר. בהמשך, באופן מתואם, אותם botnets - אלפי מחשבים 'זומבים' ש'נחטפו' על ידי וירוסים שהוחדרו אליהם - משבשים את השרתים המותקפים, באמצעות כניסה שיטתית והמונית לאתרים מסוימים. זאת, עד לנפילת האתרים כתוצאה מהעומס שגורמות אלפי ואף עשרות אלפי הכניסות המתואמות.

אחד היתרונות בשיטה זו הוא השימוש במחשבים 'תמימים' מסביב לעולם, היוצרים, שלא מדעת, רשת של אנונימיות ביחס לזהות התוקפים, ומקשים בצורה יוצאת דופן על ייחוס ההתקפות. כיום, פועלות חברות, המציעות תמורת תשלום את יכולתן לפעול באמצעות אלפי מחשבים בו זמנית, כך שבפועל, שירותי התקפת DDoS, ניתנים לרכישה, בסכומים כספיים שאינם מרקיעי שחקים.

השנייה, שתילת מידע שגוי. זהו סוג של Semantic Attacks, במסגרתן מחדיר התוקף מידע שגוי למערכת מחשב, כאשר המחשב ממשיך

[36] להרחבה, ראו למשל: Hathaway, 2012.
[37] שם, עמ' 837.

לכאורה לפעול בצורה תקינה, גם כאשר הוא סוטה ממשימותיו[38]. לעתים, הפריצה למאגרי המידע מבוצעת באמצעות Fishing - שליחת הודעות דואר אלקטרוני מוסווית אל עובדים בארגון, המכילות קוד זדוני, באופן שמאפשר לתוקף לחדור אל מערכת המחשב של הארגון. במקרים מסוימים אף מושתלים קישורים זדוניים באתרים תמימים.

כך לדוגמה, נטען, כי ארצות הברית תכננה בשנת 1999 להזין מידע שגוי במערכות ההגנה האווירית של סרביה ולנטרל את יכולתה לפגוע במטוסי נאט"ו[39] - פעולה שלא יצאה לבסוף לפועל. סברה דומה הועלתה ביחס לישראל, לפיה פעלה בדרך זו בספטמבר 2007, כאשר שתלה מידע שגוי במערכות ההגנה האווירית של סוריה, במהלך תקיפת הכור הגרעיני שהוקם במדינה[40]. הדבר לא הוכח ואמינות הטענה מוטלת בספק.

השלישית, חדירה לרשת מחשבים וביצוע פעולות במסגרתה. פעולות משמעותיות כוללות השתלת וירוסים ו'פצצות לוגיות', בפרט במערכות מחשבים השולטות על מפעלים גדולים ותשתיות חיוניות (מערכות SCADA - Supervisory Control and Data Acquisition). תיאורטית, ניתן לפעול בדרך זו נגד מערכות רגישות, למשל בתחום תשתיות חשמל ומים.

דוגמה ידועה, המובאת בספרות המקצועית בהקשר זה, היא תקיפת וירוס Stuxnet באיראן. במהלך התקיפה נפרצה רשת מאובטחת בכור גרעיני איראני, ושובשה פעילות הצנטריפוגות, עד כדי גרימת נזק פיזי

---

[38] ראו: Libicki, 1995; 77.

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

[40] Clarke & Knake, 2010; 1-9.

משמעותי. כן מוזכרת בהקשר זה חדירה אמריקנית לרשת המחשבים של משרד ההגנה העיראקי, ערב הפלישה לעיראק[41].

התקפות קיברנטיות בזירה הגלובלית

במהלך השנים האחרונות הלכו והתרבו ההתקפות הקיברנטיות ברחבי העולם. התרחיש של מלחמה קיברנטית, שהיה בגדר תיאור אפוקליפטי של יום הדין הטכנולוגי, הפך לחלק מהמציאות, והוא בא לביטוי, מעת לעת, בראש מהדורות החדשות[42]. כותבים בנושא מצביעים על האפשרות שהתקפות קיברנטיות יגרמו להסטת רכבות ממסילותיהן, הפסקת חשמל, פיצוץ צינורות נפט וגז וקרקוע מטוסים[43]. שוררת תמימות דעים, כי בסכסוכי העתיד (ולמעשה כבר במאבקי ההווה), תשולב לחימה קיברנטית לשם פגיעה בתשתיות, במידע, בכלכלה וברוח האנשים[44]. לא בכדי, ביטחון המרחב הקיברנטי הוכתר על ידי האו״ם כאחד האתגרים המשמעותיים במאה העשרים ואחת[45].

תופעה מטרידה זו עדיין בחיתוליה. במרחב הקיברנטי טרם התרחשו אירועים מכוננים, שהשפיעו באופן דרמטי על התודעה המדינית והצבאית העולמית. ועדיין, בשנים האחרונות בוצעו מספר התקפות קיברנטיות, הממחישות את הפוטנציאל הטמון בכלים וביכולות

---

[41] הדבר שימש לשליחת דואר אלקטרוני לקצינים עיראקים, ובו הנחיות לכניעה בשלום. בדיעבד, כנראה שהדבר פעל, והיו כאלה שמילאו את ההנחיות האמורות. להרחבה: שם, עמ׳ 9-10.

[42] ראו: Banks, 2012; 157-158.

[43] Clark & Knake, 2010; 64-68.

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

[45] 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).

בדו״ח נכתב:

"Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security".

קיברנטיים לשם גרימת נזק ליריב. מאחר שהניתוח המשפטי חייב להתבסס גם על אדני המציאות, ראוי להציג בקצרה כמה מהדוגמאות הבולטות ביותר.

התקפות קיברנטיות - חבלי הלידה

חשיבותה של התקשורת בעולם המלחמה אינה חדשה. כבר לפני למעלה מאלפיים שנים, האסטרטג והפילוסוף הסיני הקדום, סון טסו (Sun Tzu), כתב על חשיבות התקשורת, והציג אותה כאחד משדות הקרב הקריטיים[46]. שנים רבות חלפו, וסין כיום היא מעצמה קיברנטית, המגלה הבנה עמוקה ביחס לאפשרויות הטמונות במרחב הקיברנטי לקידום יעדיה. סין משקיעה רבות בתחום זה, המצוי במקום גבוה בסדר העדיפויות הלאומי שלה. בסין מתפרסמים ספרים רבים בנושא אסטרטגיה צבאית במרחב הקיברנטי, לחימת מידע ולחימה אלקטרונית. בין השאר, פורסם ספר חשוב על ידי שני קצינים סיניים בכירים בשנת 1999, בשם "לחימה בלתי מוגבלת" (Unrestricted Warfare). הספר מציג מלחמות עתידיות, ככאלו שמתרחשות מעבר למרחב הצבאי המסורתי[47]. הכתיבה הסינית בנושא מעידה על הפנמה עמוקה של משקל המרחב הקיברנטי בעימותים אסטרטגיים עתידיים.

פעולה שניתן לכנותה קיברנטית, אשר נועדה לגנוב טכנולוגיה מתקדמת ממחשבים מערביים, אותרה כבר בשנת 1981, בזמן המלחמה הקרה, בפרשה מפורסמת המכונה "Farewell Dossier"[48]. ההתקפה אותרה בזמן, באמצעות שיתוף פעולה מודיעיני צרפתי-אמריקני, ואף נוצלה, לפי הטענה, לפעילות נגדית מתוחכמת[49].

---

[46] מצוטט ב-Crowell, 2012; 9.

[47] שם, עמ' 10. המקור: Qiao Liang and Wang Xiangsui, Unrestricted Warfare, 188 (1999).

[48] להרחבה, שם, עמ' 1.

[49] להרחבה: Reed Thomas C., At The Abyss, 268 (2004).

הכרה רחבה מצד הקהילה הבינלאומית בעצם הפגיעות של מערכות כלכליות וצבאיות להתקפה קיברנטית, התגבשה בסוף המילניום הקודם, כתוצאה מהחשש שעורר וירוס Y2K[50]. הבהלה הגלובלית מפני השלכות של פגיעה משמעותית במערכות מחשוב ומידע, חידדה היטב, למי שנותר ספקן, עד כמה רבה התלות המודרנית במערכות אלו ועד כמה חמורה עלולה פגיעה בהן להיות.

ההתקפה על אסטוניה

באפריל ובמאי 2007 הותקפה אסטוניה בהתקפות מסיביות על רשת המחשבים שלה[51]. ההתקפות בוצעו בתגובה לכוונת ממשלת אסטוניה להוציא אנדרטת זיכרון למלחמת העולם השנייה ממרכז עיר הבירה, טאלין, לבית קברות צבאי בפרברי העיר. בתגובה, התעוררו הפגנות אלימות של אזרחים ממוצא אתני רוסי. בהמשך בוצעו, במהלך כחודש, התקפות קיברנטיות נגד תשתיות אינטרנט ציבוריות וכלכליות, לרבות של הנשיא, ראש הממשלה, הפרלמנט, מפלגות, בנקים, התקשורת וספקי אינטרנט[52]. ההתקפות היו מסוגים שונים - Denial of service (DoS), Distributed Denial of Service (DDos), השחתת אתרי אינטרנט, הרס מידע ממוחשב ועוד, כאשר המשמעותיות שבהן היו התקפות DDoS, שהובילו לנפילת שרתים ואתרי אינטרנט.

מאז זכתה בעצמאות, השקיעה אסטוניה רבות ברשתות מחשבים והסתמכה עליהן, כך שהאינטרנט שימש כלי משמעותי בתחומים רבים במדינה. חצי מהאוכלוסייה החזיקה בגישה לרשת האינטרנט והשתמשה בה לקבלת שירותים ממשלתיים[53]; הממשלה פעלה באופן שהוגדר ׳ללא נייר׳; 95% מהפעילות הבנקאית במדינה נוהל באופן

---

[50] Antolin-Jenkins, 2005; 142.

[51] להרחבה לגבי התקיפות, ראו: Tikk, 2010; 14-33. חלק משמעותי מהתיאור העובדתי של התקיפות על אסטוניה מבוסס על מקור זה.

[52] Schmitt, 2011; 569.

[53] שם, עמ׳ 570.

דיגיטלי ו-98% משטח המדינה היה מרושת מבחינה קיברנטית[54]. על אסטוניה נאמר, כי האינטרנט במדינה חשוב כמעט כמו מים זורמים[55]. הדבר הביא לכך שהשפעת ההתקפות הייתה משמעותית. בין השאר, יכולת הפעולה האפקטיבית של שני הבנקים המרכזיים במדינה שותקה למשך מספר ימים, וחצי מסוכנויות החדשות המרכזיות נפגעו בפעולתן[56]. כן נפגעה גביית המסים, נותקו קווי החירום במדינה למשך שעה, נפגעה התקשורת הפרטית והציבורית, ובנוסף - נגרמה פגיעה באמון בכלכלת המדינה.

ההתקפות נגד אסטוניה בוצעו תוך שימוש במיליון מחשבים בערך. חלקם בשימוש ישיר ומכוון ואילו רבים אחרים שימשו כ'זומבים', שנוצלו לתכלית זו באמצעות החדרה של תוכנה מתאימה. התקפות רבות בוצעו מרוסיה, אך עקבות ההתקפות הובילו ל-177 מדינות לפחות[57], מווייטנאם ועד ארצות הברית. רוב ההתקפות בוצעו ממחשבים בעלי כתובת (IP) פרטית, אך אותרו גם מחשבים בשליטת מוסדות ממשלתיים רוסיים, אם כי לא ניתן לקבוע, האם נעשה במחשבים אלו שימוש על דעת אותם מוסדות. למעשה, לא ניתן היה לייחס אחריות להתקפות למדינה מסוימת, הגם שהחשד הכבד נפל, מטבע התפתחות האירועים, על רוסיה. לפי החשד, הפעילה רוסיה לצורך ההתקפות ארגון חסות שנקרא: Russian Business Network (RBN)[58]. לחשד תרמה העובדה שחלק מההתקפות בוצעו בצורה מאד

---

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

[55] Landler Mark & Markoff John, Digital Fears Emerge After Data Siege in Estonia, N.Y. Times, May 29, 2007, available at: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ref=estonia.

[56] Hinkle, 2012; 13.

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

[58] Chiswick Linton, Cyber Attack Casts New Light on Georgia Invasion, The First Post (Aug. 15, 2008), http://www.thefirstpost.co.uk/45135,features,cyber-attack-casts-new

מתוחכמת, דבר שהעיד על מנגנון משמעותי שעומד מאחוריהן. מכל מקום, לא היו הוכחות חזקות וחד משמעיות שממשלת רוסיה ביצעה את ההתקפות או תמרנה אותן. אסטוניה עצמה, בניתוח הסופי של האירועים, הניחה שההתקפות בוצעו על ידי קבוצות פטריוטיות של פצחנים (האקרים) רוסיים, מבלי שייחסה אותן ישירות לממשלת רוסיה עצמה[59].

כאמור, השפעת התקיפות במהלך ביצוען הייתה משמעותית. פוליטיקאים אסטוניים השוו את ההתקפות לפלישה ולפעילות צבאית קונבנציונלית. עם זאת, במבט ממרחק הזמן, הנזק שנותר מההתקפות היה מינימלי, ובעיקר כלכלי: לא אבדו חיים, חיילים לא נשלחו לגבולות ותחמושת לא נורתה. גורמי ארגון נאט״ו, שבו חברה אסטוניה, נזעקו לעסוק בנושא, והתפתח דיאלוג פוליטי בין אסטוניה ובנות בריתה לבין רוסיה. אסטוניה הגיבה בעיקר בפעולות פסיביות, למשל בהרחבת פסי התקשורת, וכן בחקירה פלילית של האירועים[60]. ההתקפות עצמן חדלו לאחר זמן מסוים. בכל משך ההתקפות, אסטוניה לא טענה לזכותה להפעלת הגנה עצמית מכוח מגילת האו״ם או חוקת נאט״ו. לאור העובדה שלא הצליחה לייחס את ההתקפות למדינה מסוימת, ממילא גם לא היה בידה לעשות כן.

בדיעבד, חשיבותן המרכזית של ההתקפות על אסטוניה הייתה בחידוש שהיה טמון בהן - קריאת השכמה, המבשרת על העידן החדש. מדינה עלולה למצוא את עצמה מתמודדת עם פעולות עוינות משמעותיות בחזית החדשה, הקיברנטית. קריאת ההשכמה נשמעה שנית, כשנה מאוחר יותר, והפעם במדינה אחרת הגובלת ברוסיה - גיאורגיה.

ההתקפה על גיאורגיה

בקיץ 2008 פרץ בין גיאורגיה לבין רוסיה סכסוך, לאחר שכוחות גיאורגים חדרו לחבל דרום אוסטיה. מבחינה משפטית, היה זה סכסוך

---

[59] Tikk, 2010; 23. light-on-georgia-invasion-

[60] שם.

מזוין בינלאומי (International Armed Conflict), כלומר סכסוך בין מדינות, שבמסגרתו חלים דיני המלחמה.[61] הסכסוך הפיזי לא היה ממושך, שכן ההתערבות הצבאית הרוסית הייתה מכרעת והגיאורגים לא יכלו להתמודד עמה.

עוד לפני החדירה הצבאית הרוסית לחבל דרום אוסטיה, בוצעו התקפות קיברנטיות רחבות היקף נגד גיאורגיה[62], לרבות תקיפות DDoS (בעיקר נגד אתרי אינטרנט ממשלתיים), שלילת שירותים (DoS) והשחתת מידע באופן קיברנטי. עם המטרות להתקפות נמנו אתרי האינטרנט של הנשיא, הפרלמנט, משרד החוץ, ההגנה והחינוך, גופי תקשורת, בנקים וגופים פרטיים (שרתים ובלוגים). בממוצע, כל התקפה נמשכה כשעתיים. התקיפות ארכו כחודש, ונמשכו גם לאחר שהסתיימה הפלישה הצבאית הרוסית והושגה הפסקת אש.

גיאורגיה אינה אסטוניה בהיבט התשתיות הקיברנטיות וחשיבות המרחב הקיברנטי לכלכלת המדינה, והדבר הפחית מחומרת הפגיעה בה. עדיין, נגרמה פגיעה בשירותים הציבוריים, בפרט ביכולת של הממשלה לתקשר עם הציבור, ובזמינות של בנקים, אשר נותקו מהרשת, כאמצעי זהירות, למשך עשרה ימים.[63] התשתיות הקיברנטיות ספגו פגיעה, אך עיקר הנזק היה תדמיתי - פגיעה בזמינות שירותי ממשלה ובנקים - ללא השפעות מרחיקות לכת לטווח הארוך. היה ברור, כי מטרות ההתקפות לא היו רק פיזיות, אלא גם ובעיקר קוגניטיביות - יצירת השפעה על האוכלוסייה בגיאורגיה.[64]

בדומה להתקפות הקיברנטיות, שבוצעו נגד אסטוניה שנה קודם לכן, לא נמצאו ראיות חד משמעיות, שמכוחן ניתן היה לייחס לממשלת

---

[61] המכונים גם - Jus in Bello, International Humanitarian Law, Laws of Armed Conflict. על כך בהמשך.

[62] Tikk, 2010; 66-90. מקור זה הוא הבסיס למרבית התיאור העובדתי שיובא בהמשך בהקשר הגיאורגי. הסכסוך פרץ לאחר שבאוגוסט 2008, כוחות גיאורגים נכנסו לדרום אוסטיה, במטרה לחדש את השליטה הגיאורגית בחבל, בו שהו אותה עת כוחות רוסיים במעמד שהוגדר על ידם כ- 'peacekeepers'.

[63] Schmitt, 2011(2), 113.

[64] Crowell, 2012; 14.

רוסיה אחריות להתקפות או מעורבות בהן. אמנם, ניתן היה לזהות כי חלק מהעקבות מובילים לרוסיה, אך לא ניתן היה לשלול את האפשרות, כי גורם כלשהו השתלט על מחשבים ברוסיה לצורך ביצוע התקפות באמצעותם. הסברה המקובלת היא שרוסיה לכל הפחות עמדה מהצד, בשעה שפצחנים (האקרים) רוסיים ביצעו את ההתקפות נגד גיאורגיה משטחה[65].

ההתקפות בגיאורגיה המחישו את האופן שבו שזורות פעולות במרחב הקיברנטי במלחמה מודרנית. חרף השפעתן המצומצמת במקרה זה, אין מקום להקל בהן ראש, על רקע התלות הגדולה של מדינות ופרטים ברשתות תקשורת ומחשבים בעידן המידע[66]. ההתקפות חשפו חולשות של מערכות קריטיות, וחידדו את ההבנה, כי לצד המערכה הצבאית, עלולה להתקיים מערכה קיברנטית משלימה. קשה להעריך, כיצד היו מגיבות לסוג זהה של התקפות, מדינות בעלות עוצמה גדולה יותר מאשר אסטוניה וגיאורגיה. יתכן שאז היו ההתקפות מוליכות לסכסוך אלים בהיקף נרחב.

התקפת Stuxnet באיראן

בשנת 2010 נפגעה התכנית הגרעינית של איראן, כתוצאה מתקיפת וירוס, המכונה Stuxnet, כנגד מערכות SCADA - (Supervisory Control and Data Acquisition) שעליהן התבססו הצנטריפוגות באחד המתקנים הגרעיניים. תולעת (Worm) שהוחדרה למערכות במתקן הגרעיני (וכנראה הופצה זמן מה קודם שנתגלתה), גרמה לצנטריפוגות להסתובב, לצאת משליטה ולהיהרס.

נהוג להתייחס לפעולה זו כאל תקדים משמעותי. זהו וירוס המחשבים הראשון, שלימד על יכולת להתקיף באופן ספציפי ולהרוס מערכות

---

[65] Hathaway, 2012 ; 838.

[66] מונח שמופיע בספרו הידוע של אלווין טופלר, הגל השלישי, המתאר מעבר מעידן תעשייתי לעידן המידע.

תעשייתיות[67]. אם עד אז, הביאו פעולות קיברנטיות לשיתוק מחשבים או לאובדן מידע, הייתה זו הפעם הראשונה, שנגרם הרס פיזי של רכוש כתוצאה מפעולה קיברנטית[68]. הדבר חידד את הפוטנציאל של המרחב הקיברנטי כאמצעי ליצירת אפקט הרס וגרימת נזק לריב. הגם שגורמים באיראן ובמדינות נוספות, ייחסו את ההתקפה לארצות הברית ולישראל[69], לא הוצגו ראיות של ממש למעורבות של מדינה מסוימת בייצור הווירוס או בהפצתו.

התקפות סיניות בארצות הברית

בשנים האחרונות הלכו והצטברו ראיות לקיומה של תכנית רחבת היקף, שבמסגרתה מבוצעות התקפות קיברנטיות בחסות ממשלת סין. בתוכנית טלוויזיה אף צולמה, בזמן אמת, התקפה קיברנטית (בשיטת DDoS), על ידי צבא סין, נגד אתר של תנועת Falun Gong בארצות הברית[70]. במקביל, בשנים האחרונות, דיווחו חברות אבטחת מחשבים בארצות הברית ש"שחקן מדינתי" (הכוונה לסין), מבצע במשך שנים התקפות קיברנטיות נגד מגוון גופי ממשל וכלכלה בארצות הברית. אחת ההתקפות הידועות, אשר בוצעה כבר בשנת 2005, כונתה "Titan Rain". היא זוהתה על ידי גורמים מערביים כפעולה שמקורה בסין ותכליתה לשאוב ולהשיג ידע אמריקני ומערבי, לרבות באמצעות פעולות שאיימו על נכסים קיברנטיים צבאיים של ארצות הברית[71].

החשיפה האחרונה והמשמעותית בנושא זה מיוחסת לחברת האבטחה Mandiant, שפרסמה בפברואר 2012 את דבר פעילותה של יחידה בצבא

---

[67] Hathaway, 2012; 819.

[68] Banks, 2013; 157-158.

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

[70] ראו: Nakashima Ellen & Wan William, China's Denials About Cyberattacks Undermined By Video Clip, Wash. Post (Aug. 24, 2011).

[71] Crowell, 2012; 16.

סין שמספרה 61398. פצחני היחידה (שכונו Comment Crew -) פרצו את מערכות המחשוב של לפחות שלוש חברות ענק אמריקניות: קוקה קולה; ענקית האבטחה הממוחשבת RSA; וחברת לוקהיד-מרטין, יצרנית מטוסי הקרב הגדולה במערב. המילה 'לפחות' במקומה, שכן לפי ההערכות, בוצעו כ-140 התקפות סיניות משמעותיות במרחב הקיברנטי נגד חברות אמריקניות גדולות, לרבות חברות המפעילות תשתיות קריטיות בתחום האנרגיה והמים[72].

יתכן כי מרבית התקיפות, המיוחסות לגורמים סיניים, מבוצעות גם מתוך אינטרסים כלכליים. אך קשה לחלוק על כך שדרך פעולה זו משרתת אינטרסי ביטחון לאומי סיניים במובנם הרחב, ועלולה להיות מנוצלת גם להתקפות בעלות אופי ביטחוני וצבאי מובהק, שמשמעותן רחבה.

מבט להמשך - האטרקטיביות של התקפות קיברנטיות והמאבק על עיצוב כללי המשחק

התקפות במרחב הקיברנטי מזכירות, בהיבטים לא מעטים, סוג אחר של התקפות, עמו נאלצה הקהילה הבינלאומית להתמודד, בעיקר מאז שנת 2001 - הטרור העולמי[73]. אין זה מפתיע שארגוני טרור מוצאים במרחב הקיברנטי כר פורה לפעילות, בין נגד גופים ממשלתיים ובין נגד גורמים מהמגזר הפרטי[74].

דרך הטרור, למרבה הצער, אומצה כדרך פעולה אטרקטיבית על ידי קבוצות ופרטים רבים, שראו בה אמצעי להגשים יעדים פוליטיים ואחרים. בשנים האחרונות מוקדשת יותר ויותר כתיבה אקדמית-משפטית לטעמים, בגינם פעילות קיברנטית התקפית צפויה אף היא

---

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

[73] Banks, 2013; 159.

[74] שם.

להיתפס כאטרקטיבית בקרב מדינות וארגונים שאינם מדינתיים. מגמה חשובה זו מחייבת תיאור קצר.

האטרקטיביות של התקפות קיברנטיות

פעולות במרחב הקיברנטי הולכות והופכות אטרקטיביות יותר כאמצעי פגיעה ביריב, בעיקר ככל שמדובר בפעולות בעצימות נמוכה (Low Intensity)[75]. לכך תורמים מספר טעמים חשובים. ראשית, יכולת ההסתרה הגבוהה של פעולות קיברנטיות, הן ביחס למקור ההתקפה ועיתויה והן ביחס להשפעותיה. בנוסף, ניתן על פי רוב לבצע פעולות קיברנטיות באופן מקוטע, כמארג של פעולות נפרדות. כך, עם התגלותן, הן נתפסות לעתים כאירועים מבודדים, שאינם קשורים האחד למשנהו[76]. הגורם המותקף מתקשה לזהות את 'התמונה הגדולה' ואת המאמץ המתואם בהתקפות נגדו.

שנית, עלותה של הטכנולוגיה הנדרשת היא נמוכה, זמינותה גבוהה ולא נדרש כוח אדם בהיקף רחב לביצוע ההתקפות הקיברנטיות. למעשה, במציאות המודרנית, גורמים פרטיים בעלי ידע רב נכונים לבצע את ההתקפות בעבור תשלום או ממניעים פטריוטיים[77]. הדבר מסייע גם למסך ולהסתיר את מעורבות הגורם היוזם מאחורי הקלעים. פעולות שנתפסות כוונדליזם או פיראטיות במרחב הקיברנטי, עשויות להיות פרי יוזמה ומעורבות מדינתית. לכך יש להוסיף את העובדה שהתקפות קיברנטיות אינן מוגבלות בשיקולי זמן ומרחק או על ידי גבולות מדיניים.

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 מנוצלת לשם פגיעה בהן. ביצוע התקפה קיברנטית

---

[75] Watts, 2011 ; 72.

[76] Lemay, 2010 ; 191.

[77] Ottis, 2010 ; 97.

קל יותר מאשר יצירת הגנה אפקטיבית מולה. 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'[78].

רביעית, התקפות קיברנטיות עשויות לאפשר פגיעה בהתפתחות הטכנולוגית, הכלכלית והחברתית של היריב. אלו תחומים שהשפעתם רבה, בפרט במציאות המודרנית. קשה לפגוע בהם באופן קונבנציונלי או קינטי, הן מבחינת יכולות והן מבחינת הלגיטימיות של הפעולה במישורים אלו. כך למשל, ליכולת להשיג באמצעים קיברנטיים יתרון טכנולוגי על היריב, עשויות להיות השלכות כלכליות וצבאיות שקשה להפריז בחשיבותן[79].

בהקשר אחרון זה, ראוי להצביע על נקודת תורפה מסוימת בחשיבה הצבאית, בפרט המערבית, המקשה על ההתמודדות עם התקפות קיברנטיות. החשיבה הצבאית-משפטית המסורתית היא דו קוטבית, דיכוטומית: מלחמה או שלום; מטרות צבאיות או אזרחיות; פעולה שמהווה 'התקפה' או שאינה כזו, ועוד. בשונה מכך, תיאורטיקנים בתחום המרחב הקיברנטי מצביעים על המרחב במסגרת זווית ראייה רחבה יותר (המקובלת למשל בסין). בראייה זו, הפעילות הצבאית היא חלק מתחרות אסטרטגית רב תחומית, המתקיימת בממדים כמו לוחמת מידע, מסחר, מטבע ומדיה[80]. מדינות וגורמים, המבקשים להילחם בממדים אלו ביריביהם, מבלי לחצות את הסף שיוביל לתגובה צבאית, מוצאים בהתקפות במרחב הקיברנטי מגרש אפקטיבי לקדם את מטרותיהם[81].

---

[78] Watts, 2011; 72-75. הגורם התוקף יבקש לפעול מתחת ל'סף התגובה' של מדינות, ולייצר לעצמו מעין חסינות קיברנטית מפני תגובה.

[79] Lemay, 2010; 190.

[80] להרחבה ספר סיני בנושא:
Qiao Liang & Wang Xiangsui, Unrestricted Warfare (1999).

[81] Watts, 2011; 74.

חמישית, כשם שהמשטר המשפטי בתחום ההתמודדות עם טרור טרם הבשיל לכדי הסדרה מלאה, כך טרם הוסדר הפן המשפטי של המרחב הקיברנטי (נקודה זו תורחב בהמשך). היעדר משטר משפטי בינלאומי אפקטיבי עלול אף הוא לעודד בחירה באמצעי של התקפות קיברנטיות, בעיקר מצד שחקנים שאינם מדינתיים.

תמונת המצב האמורה והשלכותיה אינן נסתרות מעיניהם של קובעי מדיניות, משפטנים ואקדמאים. לאחר ההתקפות הקיברנטיות על אסטוניה וגיאורגיה, היו שחזו כי הן קדימון בלבד לתופעה נרחבת של התקפות קיברנטיות, בפרט נגד מדינות מערביות. נבואה זו הגשימה עצמה באופן חלקי בלבד. התקפות קיברנטיות אינן תופעה נדירה בשנים האחרונות, אך קשה להצביע על נזק אסטרטגי שגרמו (למעט, אולי, התקפת וירוס Stuxnet באיראן, ואף על כך הדעות חלוקות).

ההקשר האסטרטגי - עיצוב כללי המשחק

בשנים האחרונות הלכה והתחדדה תשומת הלב של מדינות למרחב הקיברנטי, תוך הפנמת חשיבותו הגדולה של המרחב וחיוניותו בתחום הביטחוני, הכלכלי והחברתי-פוליטי. זהו תהליך הדרגתי, המונע על ידי מספר גורמים, כמו ההתקפות הקיברנטיות שכבר התרחשו ב'זירת הלחימה' החדשה והחשש מהתקפות עתידיות וחמורות יותר; הבנת האינטרסים הכלכליים הטמונים במרחב; והרצון של ממשלות מסוימות להגביר את הפיקוח על מידע 'מערער יציבות' ברשת האינטרנט.

לאור המגמה המתפתחת, 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 להפנות את האצבע למספר מגמות חשובות, ולו על רגל אחת. הרחבה נוספת בנושא תובא במסגרת הפרק שיעסוק בהתפתחויות

הצפויות במגרש המשפטי. בפרק משנה זה יתוארו, בקצרה בלבד, מספר התפתחויות חשובות שאירעו בשנים האחרונות: במישור המדינתי - גיבוש מדיניות בהקשר הקיברנטי; המהלכים באו"ם בתחום בקרת הנשק הקיברנטי; והחתירה ליצירת כללי משחק משפטיים.

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[82] 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"[83]. הממשל האמריקני מודע היטב לכך שההישענות המשמעותית על טכנולוגיה מודרנית ועל המרחב הקיברנטי, עלולה להיות עקב אכילס של ארצות הברית[84]. 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

---

[82] 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

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

[84] כפי שטוענים הסינים בהקשר זה. להרחבה, ראו: Krepinevich, 2009; 194.

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"[85].

ציטוט נוסף מלמד על האינטרס האמריקני בראי האיום:

"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"[86].

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[87]. 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[88].

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[89].

---

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

[86] Richard D. Clarke, שהיה אחראי לתיאום ביטחון קיברנטי בבית הלבן עד שנת 2003, כפי שצוטט ב: Maurer, 2011; 5.

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

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

[89] Maurer, 2011; 5.

בדומה לארצות הברית, גם בריטניה (הממלכה המאוחדת) התייחסה להתקפות קיברנטיות במסמך אסטרטגיית הביטחון הלאומי שלה משנת 2010, ותיארה אותן כאחד מארבעה "Tier One threats to British national Security"[90]. בשנת 2011 פרסמה בריטניה את המסמך האסטרטגי בתחום הקיברנטי[91]. ארגון נאט"ו הגדיר, בשנת 2010, את ההתקפות הקיברנטיות כאחד משלושת האיומים המרכזיים על חברות הארגון בעשור הקרוב[92]. במסמך אסטרטגי אחר של הארגון, מאותה שנה, הוצגה הכוונה להציב הגנה מרכזית ומשותפת בתחום הקיברנטי לכל חברות נאט"ו, ולחזק את המודעות לתחום בקרב חברות הארגון, את ההרתעה ואת היכולת להגיב[93].

גם למעצמות הקיברנטיות שאינן מערביות, רוסיה וסין, אינטרסים אסטרטגיים בתחום הקיברנטי[94]. רוסיה וסין מעוניינות, למשל, בחיזוק מעמדן וריבונותן במרחב האינטרנטי; בהגברת הפיקוח על תכנים ברשת האינטרנט ועוד, והן פעילות במספר פורומים בזירה הבינלאומית[95]. רוסיה שאינה מרבה בפרסומים מסוג זה, פרסמה בשנת

---

[90] HM Government, A Strong Britain in an Age of Uncertainty: The National Security Strategy 11 (2010). איומים נוספים: טרור בינלאומי; משבר צבאי בינלאומי בין מדינות ותאונה או אסון טבעי רחב היקף.

[91] HM Government, The U.K. Cyber Security Strategy: Protecting and Promoting the U.K. in a Digitized World (2011).

[92] North Atlantic Treaty Org. [NATO], NATO 2020: Assured Security: Dynamic Engagement 17 (May 17, 2010). המסמך גובש על ידי צוות מומחים בראשות מדלן אולברייט מארצות הברית.

[93] NATO, Active Defence, Modern Engagement: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation: Active Engagement, Modern Defence 16-17 (2010).

[94] להרחבה מתוך ראייה מערבית, ראו למשל: Thomas, 2009.

[95] ראו למשל: מאמרו של Sherstyuk, 2012 (עוזר מזכיר המועצה לביטחון לאומי הרוסית, בתוך פרסום של ארגון BRICS), המתייחס, בין השאר, לתפיסה הרוסית בנושא ריבונות במרחב הקיברנטי.

2011, באופן חריג, מסמך תפיסתי, המנחה את הכוחות המזוינים של המדינה ביחס לפעילות במרחב המידע[96].

בשנים שמאז נוסד האו"ם, חייבו ההתפתחויות הטכנולוגיות ומירוץ החימוש התאמות של המשפט הבינלאומי. הקהילה הבינלאומית בכלל וארגון האו"ם בפרט, נדרשו לא אחת לדון בשינויים הנדרשים בדין, וזה אכן שונה, לא תמיד בהצלחה מלאה[97]. צמיחת המרחב הקיברנטי, ההתקפות שבוצעו, הסיכונים הכרוכים בכך, התפתחותו של מעין מירוץ חימוש קיברנטי - כל אלו צפויים היו להוביל לדיונים בעלי אופי משפטי באו"ם[98]. כך גם 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[99]. בהקשר הפוליטי-צבאי, לב הדיון הוא בשאלה, כיצד טכנולוגיות וכלים במרחב הקיברנטי, עלולים לשמש למטרות שאינן מתיישבות עם שמירת היציבות והביטחון הבינלאומיים ולסכן את הביטחון של מדינות.

זירת האו"ם היא מיקרוקוסמוס, ממנה ניתן ללמוד על מירוץ החימוש, שמתרחש במרחב הקיברנטי, ועל האינטרסים השונים במסגרתו. באופן אירוני, רוסיה היא שמובילה קריאה בינלאומית לבקרת נשק במרחב

---

[96] 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

[97] להרחבה, ראו: Dinstein, 2002; 14-15.

[98] Waxman, 2011; 425. המחבר מציע ללמוד מלקחי ההיסטוריה והדיונים שנערכו בעבר בסוגיות דומות באו"ם, ובפרט מהדיונים בנושא משמעות 'שימוש בכוח' בתקופת המלחמה הקרה (למשל בסוגיה האם coercion היא בגדר שימוש בכוח).

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

הקיברנטי, ואילו ארצות הברית נתפסת כמי שחוסמת מהלך כזה[100]. מאז 1998, מניחה רוסיה הצעה בוועידה הראשונה של העצרת הכללית של האו״ם[101], שמטרתה לגבש משטר משפטי בינלאומי למניעת השימוש בטכנולוגיות מידע למטרות שפוגעות בהבטחת היציבות והביטחון הבינלאומיים[102]. מנגד, הגישה המערבית רואה בכללים המשפטיים ובאמנות הקיימות מענה אפקטיבי גם למרחב הקיברנטי, ומתמקדת בחיזוק שיתוף הפעולה בין שחקנים בינלאומיים. נציגי סין הפגינו שקט יחסי בזירת האו״ם, אם כי הצטרפו ליוזמה הרוסית החל משנת 2006. רק בשנת 2011 הסכימה ארצות הברית, לראשונה, לקדם את ההצעה, הרוסית במקורה, והייתה שותפה להחלטה של הוועידה הראשונה של האו״ם בנושא המרחב הקיברנטי[103]. ההחלטה שאומצה היא כללית ודקלרטיבית, וספק רב אם תבשיל לכדי לאמנה משפטית מחייבת[104].

במקביל, מקדמות סין ורוסיה אמנה קיברנטית אזורית, במסגרת ההסכם של ארגון שנחאי, ופועלות להרחבת סמכויות ארגון התקשורת הבינלאומי של האו״ם (ה-ITU), ברוח עמדותיהן והאינטרסים שלהן.

בעת הזו, נמצא המשטר המשפטי הבינלאומי, שיסדיר את המרחב הקיברנטי, בשלבי התהוות ראשונים (Norm Emergence, במונחי אחד המודלים המובילים, המתאר התפתחות נורמות ביחסים בינלאומיים[105]). זהו שלב של עיצוב כללי משחק משפטיים, בו גורמים שונים מנסים ליזום הצעות למשטר עתידי ולשכנע מאסה קריטית של מדינות וארגונים בינלאומיים לאמץ את הצעותיהם, בדרכים שונות.

---

[100] Clarke & Knake, 2010; 218-219.

[101] Maurer, 2011; 20. ההצעה עוסקת ב: "Developments in the field of information and telecommunications in the context of security", והופצה כבר ביום 23 בספטמבר 1998.

[102] Maurer, שם.

[103] ראה Resolution 65/41 מיום 11 בינואר 2011, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/41

[104] Maurer, 2011; 25.

[105] מודל שפותח על ידי Finnemore & Sikkink, ולא יורחב לגביו במסגרת זו.

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[106]. מסלול משפטי זה, המשולב בדיפלומטיה ציבורית ובשיח אקדמאי, מבקש לעצב גרסאות 'רכות' יותר של המשטר המשפטי העתידי, במטרה לעודד התקדמות בעיסוק בנושאים המשפטיים התלויים ועומדים, כשלב מוקדם בתהליך רב שלבי[107]. דוגמה לתהליך משמעותי ברוח זו, שנערך בחסות נאט"ו, הוא ניסוח מדריך טאלין (להלן גם - המדריך)[108], לגביו יורחב בהמשך.

מבלי להרחיב יתר על המידה, יובהר כי המשפט הבינלאומי המנהגי אינו מבוסס על מחוקק אחד והוא אף אינו מצוי בקובץ חוקים אחד, אלא הוא מתפתח באופן דינמי, בהתבסס על מקורות שונים. בהכללה, נודעים למשפט הבינלאומי שלושה מקורות: המנהג, אמנות בינלאומיות וכללים משפטיים בסיסיים אוניברסליים (כמקורות משניים ניתן לציין גם החלטות שיפוטיות ומשנת מלומדים)[109]. המנהג נוצר כאשר מדינות, באמצעות נציגיהן, פועלות בדרך מסוימת (State Practice), לאורך זמן, בצורה עקבית ומתוך תחושה של מחויבות משפטית לפעול כך (Opinio Juris)[110]. ראוי לייחס חשיבות גדולה לפרקטיקה העתידית של מדינות (הן להתנהגות, במעשים ובהצהרות, והן למחויבות המשפטית שבבסיסה), אשר עשויה להשליך בצורה משמעותית על עיצוב כללי המשחק המשפטיים העתידיים במרחב הקיברנטי[111].

---

[106] להרחבה: Boyle, 1999; 901-902.

[107] Maurer, 2011; 14.

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

[109] סייבל, 2010; 51-67.

[110] Shaw, 2008; 70. המחבר מצטט גם את סעיף 38(1) לחוקת בית הדין הבינלאומי.

[111] ראו גם Boyle, 1999; 904.

האם כללי המשפט הבינלאומי חלים במרחב הקיברנטי?

עבודה זו מתמקדת בכללי המשפט הבינלאומי, החלים בהקשר של סכסוכים מזוינים, במסגרתה, יוצגו מספר עקרונות מרכזיים, המעוגנים בכללים אלו, ותיבחן ישימותם במרחב הקיברנטי.

כדי לאפשר זאת, נדרשים שני פרקים קצרים בפתח הדברים. הראשון, מבהיר מה הם ענפי הדינים שבהם תעסוק העבודה; השני, עוסק בשאלה המשלימה, האם ענפי דינים אלו חלים בכלל ביחס למרחב הקיברנטי?

דיני המשפט הבינלאומי החלים בעניין סכסוכים מזוינים

כללי המשפט הבינלאומי, החלים בעניין סכסוכים מזוינים, כוללים שני גופים נפרדים של דינים: ה-Jus ad Bellum וה- Jus in Bello[112].

דיני ה-Jus ad Bellum - המשפט הבינלאומי המודרני מטיל מגבלות על זכותן של מדינות להשתמש בכוח צבאי ביחסיהן עם מדינות אחרות, במסגרת מערכת כללים, המכונה Jus ad Bellum[113]. דינים אלו, בהכללה, עוסקים בשאלה: מתי מדינות, במסגרת מדיניותן הלאומית, רשאיות לעשות שימוש בכוח?

דינים אלו כוללים, בין השאר, את איסור השימוש בכוח בין מדינות ואת חריגיו. מטרתם לשמור על יחסי שלום בקרב קהילת העמים, באמצעות קביעת קריטריונים נוקשים למצבים, בהם מדינות יכולות לנקוט ביניהן צעדים כוחניים.

דיני ה-Jus in Bello, הם הדינים החלים בעת סכסוך מזוין. הם מכונים גם ׳דיני המלחמה׳ (Laws of War), המונח בו ייעשה שימוש בהמשך, וכן ׳דיני הסכסוך המזוין׳ (Law of Armed Conflict). האו״ם וארגון הצלב

[112] Schmitt, 2012; 284.
[113] סייבל, 2010; 499.

האדום הבינלאומי מבכרים את המונח 'משפט הומניטרי בינלאומי' (International Humanitarian Law). תחת כל כותרת, אלו דינים החלים במצב של סכסוך מזוין, בין אם עצם קיומו של הסכסוך המזוין היה מלכתחילה חוקי או בלתי חוקי על פי המשפט הבינלאומי[114].

דינים אלו עוסקים בשאלה, כיצד הצבא וגורמים חמושים אחרים רשאים לעשות שימוש בכוח במהלך סכסוך מזוין. מטרתם לצמצם את הפגיעה באנשים וברכוש, בדגש על כזו שאינה נחוצה על מנת להשיג את המטרות הצבאיות הלגיטימיות או שהיא מוגזמת ביחס למטרות אלו. זאת, בעיקר באמצעות הצבת איסורים והגבלות על ביצוע 'התקפות' (Attacks).

מכנה משותף לשני ענפי הדינים הוא המשקל המרכזי, שראוי לייחס למונח 'התקפה' (מונח המכונה לעתים, בספרות המשפטית, "Term of Art"[115]), הגם שמונח זה מופיע בהם בהקשרים שונים. על כך יורחב בהמשך.

המרחב הקיברנטי והמשפט הבינלאומי - ביחד או לחוד?

בטרם אדון באופן שבו מיושמים כללי המשפט הבינלאומי במרחב הקיברנטי, נדרש דיון מקדמי בשאלה: האם הכללים המקובלים והקיימים מסדירים בכלל מרחב זה? המענה לשאלה זו אינו חד משמעי. קיימות גישות שונות, המבטאות שיקולים משפטיים 'טהורים', לצד שיקולים רחבים יותר - אסטרטגיים ואידיאולוגיים.

מדוע המענה אינו חד משמעי? הדבר נובע, בראש ובראשונה, מאחר שאותן אמנות בינלאומיות, המהוות את עמוד השדרה של כללי המשפט הבינלאומי, נוסחו בעידן שבו המרחב הקיברנטי היה בגדר מדע עתידי[116]. האמנות אינן מתייחסות, באופן ישיר וייעודי, לפעולות

[114] שם, 521.
[115] Schmitt, 2012.
[116] מדריך טאלין, 3.

במרחב זה. יתר על כן, קשה מאד להצביע על פרקטיקה של מדינות, ממנה ניתן לגזור את הכללים המנחים מדינות בהתמודדותן עם מרחב זה, מאחר שפרקטיקה כזו לא קיימת[117]. לאור האמור, נדרשות צניעות וספקנות ביחס לכל יומרה להציג, ברמה גבוהה של ודאות, את המצב המשפטי הקיים במרחב הקיברנטי.

בפרק הקודם צוין בקצרה שבמרחב הקיברנטי מתנהל מאבק בין מעצמתי, רווי אינטרסים והקשרים, במסגרתו מנסות המעצמות לעצב את כללי המשחק ואת דפוסי הפעולה. גם בשאלה שלפנינו, האם המשפט הבינלאומי חל על המרחב הקיברנטי? המענה עשוי להשתנות, בהתאם למקום מגוריו של המשיב - בייג׳ינג, מוסקבה או וושינגטון.

קל יותר להתחקות אחר עמדות משפטיות מערביות מאשר אלו של סין ורוסיה. עם זאת, נראה כי ניתן לתאר את העמדה הסינית כמתנגדת לגישה (המערבית) בדבר תחולת כללי המשפט הבינלאומי במרחב הקיברנטי[118]. אשר לגישה הרוסית, דומה שזו יותר מורכבת - הרוסים מכירים בכללי המשפט הבינלאומי הקיימים כנקודת מוצא לדיון במרחב הקיברנטי, אך מציגים להם פרשנות החורגת מפרשנותם המקובלת במערב, לצד דרישה להכללת עקרונות משפטיים נוספים[119].

במערב, המוביל את העיסוק המשפטי, אין תמימות דעים. ניתן להצביע על קשת של דעות, החל מאמירות, לפיהן יש להחיל את כללי המשפט הבינלאומי באופן מלא על כל סוגי השימוש בכוח, לרבות במרחב הקיברנטי; דרך דעות, לפיהן ההחלה מחייבת שינויי תפיסה

---

[117] מדריך טאלין, 5.

[118] כעולה מדו״ח משרד ההגנה האמריקני לקונגרס אודות ההתפתחויות בתחום הקיברנטי בסין (Military and Security Developments involving the People Republic of China). ראו:
http://www.defense.gov/pubs/pdfs/2012_CMPR_Final.pdf.

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

משמעותיים; וכלה באמירות, כי הדין הקיים אינו חל על פעולות קיברנטיות, בהיעדר קביעה מפורשת במסגרתו בעניין זה[120].

דומה, עם זאת, כי העמדות הדומיננטיות בקרב גורמים רשמיים בממשלת ארצות הברית, כמו גם בקרב חוקרים ומלומדים העוסקים בתחום בארצות הברית, היא שיש ליישם את כללי המשפט הבינלאומי גם על המרחב הקיברנטי[121]. העמדה האמריקנית הרשמית 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"[122].

דברים דומים נאמרו בנאום דוקטרינרי, שנשא היועץ המשפטי של מחלקת המדינה בארצות הברית, ביום 18 בספטמבר 2012[123].

מנסחי מדריך טאלין התנגדו אף הם לאפיון המרחב הקיברנטי, כמרחב מנותק, בו חלים כללים שונים מאלו המוכרים[124]. בראייתם, המבוססת, בין השאר, על פסק הדין של בית הדין הבינלאומי בהאג

---

[120] מדריך טאלין, 3. במדריך מצוטטת, בין השאר, עמדת ארגון הצלב האדום הבינלאומי, לפיה הדינים חלים במרחב הקיברנטי.

[121] מדריך טאלין, 5. לדעה מעניינת, לפיה המשפט הבינלאומי ההומניטרי צריך להתפתח כדי להסדיר את התחום הקיברנטי, ואף לעודד פעילות התקפית קיברנטית כתחליף למלחמה קונבנציונלית, ראו: Kelsey, 2008.

[122] 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.pdf

[123] Koh Honhgu Harold, 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. (להלן - נאום Koh).

[124] Schmitt, 2012(2); 17.

בנושא חוקיות השימוש בנשק גרעיני[125], העובדה שבמרחב הקיברנטי נעשה שימוש במחשבים, להבדיל מכלי נשק קונבנציונליים, אינה מאיינת את התחולה של עקרונות יסוד, כמו איסור השימוש בכוח[126].

לצד הקביעה העקרונית, המקובלת בארצות הברית ובמדינות מערביות, כי יש להחיל את כללי המשפט הבינלאומי במרחב הקיברנטי, קיימות דעות שונות בעניין מידת ההתאמה של הכללים למרחב זה והקלות שבה ניתן ליישמם[127]. העמדה האמריקנית הרשמית היא שנדרשת עבודה משפטית, במטרה לקבוע כיצד הכללים חלים ואילו הבנות נדרשות כדי להשלים אותם[128]. לעמדה זו מצטרפים אנשי משפט ומדיניות, הקוראים לחידוד הבהירות לגבי האופן שבו יש ליישם את כללי הדין הבינלאומי על התקפות בתחום הקיברנטי[129]. מלומדים רבים הולכים מעבר לכך, וטוענים כי קיים הכרח בבחינה משמעותית של כללי המשפט הבינלאומי לאור ההתפתחויות במרחב הקיברנטי, ואף נדרש פיתוח דין חדש בהקשר הקיברנטי[130].

גם המאמינים ההדוקים ביותר בישימותם הרחבה של כללי המשפט הבינלאומי הקיימים, יסכימו לקביעה שיישומם במרחב הקיברנטי הוא מאתגר, בלשון המעטה[131]. המרחב הקיברנטי חותר תחת פרדיגמות מסורתיות של המשפט הבינלאומי. כך למשל, פעולה של מדינה, שאינה מתבטאת בהפעלת כוח פיזי ואין לה תוצאות פיזיות ישירות, עלולה

---

[125] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 77 (להלן - פרשת חוקיות הנשק הגרעיני).

[126] Schmitt, 2012(2); 14.

[127] דוגמאות לגישות שונות: Watts, 2010; 425, קובע שדיני המלחמה מכסים כל שימוש בכוח, יהיה האמצעי אשר יהיה. Schmitt, 2002; 195, טוען שדיני המלחמה נותרים בתוקף, אם כי עליהם להתמודד עם אמצעים חדשים בעולם הקיברנטי, וקיימות עוד גישות רבות אחרות.

[128] 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.pdf.

[129] לדוגמה: Lewis, 2010; 16.

[130] לדוגמה: Hollis, 2007; 1027-1028.

[131] Hathaway, 2012; 840.

להיות הרת אסון לביטחון הלאומי של מדינה אחרת. היכולת לזהות התקפה בזמן אמת או לייחס אותה לגורם התוקף - מוגבלת מאד. הפרדות מסורתיות: בין מדינות; בין תשתית צבאית לבין תשתית אזרחית; בין התקפה לבין הגנה - אינן בהכרח תקפות.

המשפט הבינלאומי התמודד עם הרחבת הלחימה לממדים נוספים (ים, אוויר וחלל), ועם התפתחות תופעת הטרור העולמי, תוך התמודדות עם סוגיות הקשורות ליישום הכללים הקיימים. דומה, כי המרחב הקיברנטי, על מאפייניו הייחודיים והאפשרויות הגלומות בו, מעורר אף אתגרים משמעותיים ביותר בהקשר זה.

חוסר הבהירות במצב המשפטי הקיים, מטריד לפחות חלק מקהילת האומות. הגידול במספר ההתקפות הקיברנטיות והיעדר הסכמה בינלאומית בדבר הסדרת הנושא באופן מחייב, עלולים לתרום לתרחיש שבו מדינה תבחר להגיב להתקפה קיברנטית משמעותית בהפעלת אמצעים קונבנציונליים-קינטיים, דבר שעלול להסלים לסכסוך מזוין. כך למשל, בשנת 2011 פרסמה ארצות הברית הצהרה, המצביעה על אפשרות זו[132].

ההנחה, המקובלת לפחות במערב, כי כללי המשפט הבינלאומי חלים על המרחב הקיברנטי, משמעה, בין השאר, כי על הגורמים שמקבלים את ההחלטות ברמה המדינתית ביחס לפעולות קיברנטיות, ובפרט ביחס לפעולות התקפיות, להכיר את הכללים המשפטיים הרלבנטיים ואת

---

[132] בהתאם לדו"ח משרד ההגנה האמריקני משנת 2011, ארצות הברית שומרת את הזכות להגיב להתקפות קיברנטיות, בשימוש בכל האמצעים הקיימים - דיפלומטיים, קיברנטיים, צבאיים וכלכליים. ראו:

Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011.

דוגמה נוספת היא מסמך מדיניות שפורסם ביוני 2013 על ידי ה-Guardian, ובו הנחיות נשיא ארצות הברית, אובמה, להגדיר יעדים להתקפות קיברנטיות מחוץ לארצות הברית. הנוסח המלא מופיע ב:

http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

השלכות ישימותם[133]. עבודה זו מיועדת לפתוח צוהר, בהקשרים מסוימים, הן לכללים הקיימים (lex lata), והן לכללים שצפויים להתפתח או שרצוי שיתפתחו (lex ferenda).

[133] ראו לעניין חשיבות חידוד המטריה המשפטית למקבלי ההחלטות: Joyner, 2001; 863-864.

איסור השימוש בכוח במרחב הקיברנטי

פרק זה מוקדש לאחד הנדבכים החשובים של דיני ה-Jus ad Bellum, והוא איסור השימוש בכוח. תחילה, ייסקר האיסור באופן כללי במשפט הבינלאומי, ובהמשך, ינותח האופן בו מיושם העיקרון במסגרת המרחב הקיברנטי.

איסור השימוש בכוח - כללי

לאורך ההיסטוריה האנושית נתפסה המלחמה, למרבה הצער, כבחירה לגיטימית של מדינה או חברה באשר לדרך שבה היא מקדמת את האינטרסים שלה. המלחמה נתפסה כהמשך המדיניות, באמצעים אחרים, לא רק בתקופתו של קלאוזוביץ', שכתב את הגותו בתחילת המאה ה-19, אלא גם בראשית המאה העשרים. כך, בשנת 1907, נכתב בספר מרכזי, שהתייחס למצב המשפטי באותה עת:

"For the redress of wrongs or the prosecution of claims, states may appeal to force either by way of war or by certain measures."[134].

משנת 1899 החלה הקהילה הבינלאומית בניסיונות להגביל את השימוש בכוח לצורך פתרון סכסוכים בינלאומיים. עם אבני הדרך המרכזיות, שניתן לציין בהקשר זה, נמנית אמנת פריס משנת 1928 (הידועה גם כהסכם קלוג-בריאן), אשר אסרה על המדינות שחתמו עליה לצאת למלחמה כחלק ממדיניות חוץ רשמית. אבן דרך חשובה נוספת הונחה על ידי הטריבונל הצבאי בנירנברג, שפסק בדבר אי חוקיות היציאה למלחמה כאמצעי לניהול מדיניות על ידי ממשלת גרמניה הנאצית, תוך הגדרת מלחמה זו כפשע במישור הבינלאומי, הגורר אחריות אישית[135].

---

[134] מתוך: J. Westlake, International Law, Part II, War (1907), 1.

[135] להרחבה, ראו למשל: סייבל, 2010; 500.

סעיף 2(4) למגילת האו"ם - איסור השימוש בכוח

ההוראה המרכזית, המעגנת את עיקרון איסור השימוש בכוח, היא הוראת סעיף 2(4) למגילת האו"ם (להלן גם - 'המגילה'). הוראה זו נחשבת, כפי שקבע בית הדין הבינלאומי בהאג, אחד מאדני היסוד של מגילת האו"ם[136], ולפיה, 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".

מקובל לראות בהוראת סעיף 2(4) כמבטאת משפט בינלאומי מנהגי[137] (בקצרה, משפט בינלאומי מנהגי הוא "General practice accepted as law"; כדי שיתפתח משפט כזה, על מדינות לנהוג לפי פרקטיקה מסוימת, מתוך הבנה שהדבר מבטא מחויבות משפטית רחבה). המשמעות היא שההוראה מחייבת גם מדינות שאינן חברות באו"ם. עם זאת, קיים סימן שאלה ביחס לתחולת איסור השימוש בכוח על גופים שאינם מדינתיים (פרטים, קבוצות מאורגנות וארגוני טרור)[138].

אחד החידושים המשמעותיים בהוראת סעיף 2(4) היה הוספת איסור האיום בכוח[139]. האיסור חל אך ורק על פעולות, מפורשות או עקיפות, שהן קומוניקטיביות באופיין, כלומר, מהותו באפקט הכופה או המאיים ביחס למדינה אחרת. על מנת להמחיש זאת, יובהר שהאיסור אינו חל על פעולות שאמנם יש בהן פוטנציאל סיכון למדינה אחרת, אך אינן קומוניקטיביות באופיין, לדוגמה, הצטיידות במערכת נשק התקפית. גם אם אותה מערכת עלולה בעתיד לשמש לתקיפה, כל עוד

---

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

[137] ראו: Military and Paramilitary Activities (Nicaragua v. U.S.), 1986 I.C.J. 14, 98-101 (June 27) (להלן - פרשת ניקרגואה).

[138] אלא אם ניתן לייחס את מעשי אותם גורמים למדינה, בהתאם לכללים הרלבנטיים. במקרה כזה, הפרת הכלל תהיה מצד המדינה ולא מצד אותם גורמים. מדריך טאלין, 46.

[139] איסור שחל כמובן רק בנסיבות בהן השימוש בכוח, שלגביו נעשה האיום, אסור בפני עצמו. זאת כמפורט בחוות דעתו של בית הדין הבינלאומי בפרשת חוקיות הנשק הגרעיני.

המדינה המצטיידת בה אינה נוקטת לשון איומים, אין בכך איום בשימוש בכוח מצדה[140].

עוד יצוין, כי לצד איסור השימוש בכוח, התפתח במשפט הבינלאומי עיקרון נוסף שעניינו אי התערבות (Non intervention). לפיו, נאסר על מדינה להתערב בענייניה הפנימיים של מדינה אחרת[141]. כלומר, כאשר פעולה מסוימת נמצאת מתחת לרף השימוש בכוח, אך עדיין מהווה התערבות אסורה בענייני מדינה אחרת, היא פסולה. מבלי להרחיב, ההיקף והפרשנות המדויקים של העיקרון נתונים בוויכוח. בפסק הדין של בית הדין הבינלאומי בהאג בפרשת ניקרגואה נפסק, כי התערבות אסורה היא בנושא, בו המדינה שבעניינה התערבו, רשאית, לפי עיקרון הריבונות של מדינות, להחליט באופן חופשי, כמו למשל בעניין השיטה הפוליטית, הכלכלית, החברתית והתרבותית ועיצוב מדיניות החוץ שלה[142].

לכאורה, האיסור על שימוש בכוח הוא ברור וחד. בפועל, כל אחת מהמילים המרכיבות אותו, ופרשנותו הכוללת, עמדו במרכזם של ויכוחים ערים וזכו לכתיבה אקדמית ענפה[143]. בין השאר, נדונה פעמים רבות שאלת יסוד מהותית: מהו היקף האיסור? או במילים אחרות - מהו 'שימוש בכוח'?

'שימוש בכוח' - מהו?

הוראת המגילה נוקטת מינוח כללי - 'שימוש בכוח' (Use of force). הדגש בנוסח ההוראה הוא על מכשיר הכפייה (Instrument of Coercion) בו נעשה שימוש - כוח (Force). הבחירה הניסוחית הזו אינה מובנת מאליה,

---

[140] שם, para. 47-48

[141] הסעיף הרלבנטי במגילת האו"ם, לצד סעיף 2(4), הוא סעיף 2(7). הכלל קיבל מעמד של משפט בינלאומי מנהגי לפי פסיקת בית הדין הבינלאומי בפרשת ניקרגואה, 202.

[142] שם, 205. באותו מקרה, נפסק שאספקת כספים למורדים נגד מדינה מסוימת אינה 'שימוש בכוח' נגד המדינה, אך מהווה התערבות אסורה בענייניה.

[143] להרחבה: Waxman, 2011; 427.

מפני שפעמים רבות, ההיבט החשוב בראיית מדינות, אינו המכשיר בו פועלים נגדן, אלא התוצאות שמהן הן סובלות[144].

אין מחלוקת שהאיסור חל על פעולות שהן התקפות צבאיות או בגדר אלימות מזוינת (Armed Violence), המתבטאות בתוצאות פיזיות-קינטיות[145]. שיגור פגזים לארץ אויב, למשל, הוא ׳שימוש בכוח׳.

האם האיסור מוגבל אך ורק לפעולות צבאיות, שיש להן תוצאה פיזית? נקודת המוצא הפרשנית להתמודדות עם סוגיה כזו, חייבת להיות לשון המגילה[146]. הקושי הוא, שכאמור, לשון המגילה כללית ואינה חד משמעית. מצד אחד, בחינה של מכלול הניסוחים במגילה והיסטוריית המשא ומתן שהביאה לניסוחה, מלמדת על רצון של המנסחים למנוע שימוש בכוח פיזי, שנתפס בדרגת חומרה שונה משאר האמצעים שמדינה עשויה להפעיל[147]. מצד שני, עצם בחירת מנסחי המגילה במונח 'Force' ולא למשל 'Armed Force', עשויה ללמד כי המונח ׳כוח׳ משתרע על קשת רחבה של פעולות, ולא רק על הפעלת כוח צבאי מזוין גרידא.

מבלי להקדים את המאוחר, ניסוח מגילת האו״ם כולל מדרג של פעולות אסורות מצד מדינה. המדרג כולל רף נוסף, מעבר ל׳שימוש בכוח׳, והוא ׳התקפה מזוינת׳ (Armed Attack). רק כאשר מדינה מבצעת ׳התקפה מזוינת׳ נגד מדינה אחרת, רשאית המדינה המותקפת להגיב בהגנה עצמית, לרבות בשימוש בכוח. בפרשת ניקרגואה[148] הובהר שלא כל ׳שימוש בכוח׳ מהווה ׳התקפה מזוינת׳, אלא הצורות החמורות

---

[144] ראו: Schmitt, 2011 ; 573.

[145] ראו: Comm. On Offensive Info. Warfare, Nat'l Research Council, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattacks Capabilities (2009), 253.
(להלן - דו״ח NRC). הוועדה קבעה כי הדין המקובל מדגיש מוות ופציעה של אנשים ונזק לרכוש כקריטריון להגדרת ׳שימוש בכוח׳.

[146] Vienna Convention on the Law of Treaties, art. 31(1)-(2), May 23, 1969, 1155 U.N.T.S 331, 340.

[147] ראו: Waxman, 2011 ; 428.

[148] ראו: Military and Paramilitary Activities (Nicaragua v. U.S.), 1986 I.C.J. 14, 98-101 (June 27).

ביותר של 'שימוש בכוח' בלבד, מגיעות לכדי 'התקפה מזוינת'. המסקנה, אם כך, היא שהמונח 'שימוש בכוח' כולל ספקטרום רחב של פעולות, לאו דווקא 'מזוינות' (Armed).

ואכן, בית הדין הבינלאומי בהאג קבע, בפרשת ניקרגואה, כי 'שימוש בכוח' נגד מדינה אחרת יכול להיעשות גם שלא בדרך של פעולה צבאית-פיזית, בעלת תוצאות קינטיות. באותו מקרה, בית הדין הבינלאומי התייחס לחימוש ואימון של לוחמי גרילה, שפעלו נגד ניקרגואה, כ'שימוש בכוח' נגד המדינה[149].

בד בבד, העמדה הפרשנית הדומיננטית התנגדה לראייה של פעולות, המהוות לחץ כלכלי או פוליטי על מדינה כ'שימוש בכוח' נגדה[150]. ארצות הברית ובנות בריתה הובילו עמדה זו לאורך השנים, בין השאר על בסיס הטענה, כי כוונת מנסחי המגילה הייתה לאסור על שימוש בכוח צבאי[151]. מנגד, עמדו מדינות מתפתחות, בפרט בתמיכת הגוש הסובייטי במהלך המלחמה הקרה, אשר טענו שהמונח 'כוח' כולל כל סוג של לחץ, לרבות כפייה פוליטית וכלכלית, המסכנת את האוטונומיה של המדינה שנגדה מופעל הכוח. עמדה זו לא זכתה להסכמה רחבה ואינה משקפת את המצב המשפטי הקיים[152].

לסיכום נקודה זו, שהוצגה בתמצית בלבד, על מנת שפעולה תהיה בגדר 'שימוש בכוח', היא חייבת לעמוד בסף חומרה מסוים. אמנם, אין היא חייבת לגרום נזק פיזי ברמה של תקיפה קינטית, אך עליה להיות מעבר ללחץ כלכלי או פוליטי גרידא. כעת, ניתן לבחון את הדברים ביחס למרחב הקיברנטי.

---

[149] הכוונה לחימוש ואימון לוחמי גרילה (הקונטראס) על ידי ארצות הברית. להבדיל, מימון לוחמי הגרילה לא נתפס כשימוש בכוח. להרחבה ראו פרשת ניקרגואה.

[150] ראו: Schmitt, 2011 ; 574.

[151] Waxman, 2011 ; 427. להרחבה, ראו גם Farer, 1985.

[152] בין השאר, מאחר שקשה מאד להפריד בין כפייה בלתי חוקית לבין לחץ חוקי, שהוא חלק בלתי נפרד מהדיפלומטיה והמדיניות המודרנית. להרחבה: Waxman, 2011 ; 429.

איסור השימוש בכוח במרחב הקיברנטי

רקע לדיון

כאשר איסור השימוש בכוח עוגן במסגרת מגילת האו״ם, בשנת 1945, מנסחי המגילה ראו לנגד עיניהם את זוועות מלחמת העולם השנייה. הם לא חזו עולם עתידי, בו מחשבים הם נשק בידי מדינות. כשבעים שנים מאוחר יותר, העולם שאנו מכירים הוא אחר. הדבר מציב אתגר משמעותי ביישום הוראת סעיף 2(4) למגילת האו״ם על פעולות במרחב הקיברנטי[153].

השאלה הראשונה בהקשר זה (המהווה הקשר פרטני של הדיון הרחב בתחולת כללי המשפט הבינלאומי על המרחב הקיברנטי), היא האם עצם האיסור על שימוש בכוח, שנברא מתוך מחשבה על הפעלת נשק קונבנציונלי-קינטי, חל גם על שימוש ב׳נשק׳ המחשבים ורשתות התקשורת?

מבלי להרחיב, הדעה המקובלת, לפחות במערב, היא חיובית. בית הדין הבינלאומי בהאג כבר פסק ביחס לסעיף 2(4) למגילת האו״ם, כי זה חל על כל שימוש בכוח, בלי קשר לשאלה באיזה נשק נעשה שימוש[154]. מנסחי מדריך טאלין סבורים שאמירה זו משקפת את כללי המשפט הבינלאומי המנהגי, כך שהאיסור חל גם על שימוש בכוח, המבוצע באמצעות מחשבים[155]. הדבר בא לביטוי בניסוחו של כלל 10 במדריך טאלין, הקובע כי פעולה קיברנטית, שמהווה איום או שימוש בכוח - אינה חוקית[156].

בפרק המשנה הקודם אוזכר, כי את איסור השימוש בכוח משלים עיקרון אי ההתערבות בענייניה של מדינה אחרת. עבודה זו אינה מתמקדת בעיקרון זה, ולכן תובא בעניינו התייחסות קצרה בלבד. בתמצית, ברור שלא כל הפרעה למדינה מסוימת במרחב הקיברנטי,

---

[153] Schmitt, 2011; 572.

[154] פרשת חוקיות הנשק הגרעיני, פסקה 39.

[155] מדריך טאלין, 42.

[156] שם.

באמצעות שימוש במחשבים, היא התערבות אסורה. התערבות, בהכללה, היא פעולה שכוללת אלמנט של כפייה[157]. פעולות של ריגול ואיסוף נתונים ממחשבים במדינה זרה אינן בגדר התערבות אסורה, מאחר שיש בהן מרכיב של חדירה לרשת מחשבים זרה ולא של כפייה או לחץ על אותה מדינה. באילו נסיבות עשויה פעילות קיברנטית, שאינה עולה כדי שימוש בכוח, לכלול מרכיב של כפייה על מדינה אחרת? דוגמאות אפשריות עשויות להיות ביצוע מניפולציה, באמצעות מחשבים, בתוצאות של בחירות או בדעת קהל ערב בחירות, וכן פגיעה בקמפיין הפוליטי האינטרנטי של מפלגה מסוימת[158]. יודגש, עם זאת, שלא כל התערבות פוליטית בערוצים קיברנטיים או אחרים (למשל כלכליים), משמעה כפייה אסורה והפרת עיקרון אי ההתערבות.

טרם הדיון באיסור השימוש בכוח, ייוחדו מספר מילים לאיסור האיום בכוח, בהקשר הקיברנטי. בהכללה, האיסור הוא על איום, המועבר בכל דרך שהיא (למשל בתקשורת הגלויה, ולאו דווקא באינטרנט) לבצע פעולה קיברנטית, המהווה שימוש בכוח[159].

יש לעמוד על שני דגשים ביחס לאיסור זה. ראשית, האיסור חל אך ורק על פעולות קומוניקטיביות. לפיכך, איום בהתקפה קיברנטית הרסנית נגד תשתיות של מדינה אחרת, עומד בניגוד לאיסור. מנגד, החדרה חשאית של תוכנות זדוניות או וירוסים למערכת המחשבים של מדינה אחרת, אשר אינה גורמת נזק מיידי, אך עלולה להיות מנוצלת להתקפה קיברנטית בעתיד, אינה בגדר איום בשימוש בכוח. זהו גם המצב כאשר מדינה מצטיידת ביכולות קיברנטיות התקפיות, מבלי שהיא מאיימת בשימוש בהן[160]. האיסור יופר רק כאשר תהיה למשל הכרזה פומבית

[157] פרשת ניקרגואה, פסקה 205.
[158] מדריך טאלין, 45.
[159] האיסור קיבל ביטוי למשל בכלל 12 למדריך טאלין.
[160] מדריך טאלין, 53.

בדבר היכולות, וניצול ההכרזה לשם כפייה על המדינה שעלולה להיות מותקפת[161].

שנית, איום בפעולה שהיא מותרת כשלעצמה, למשל בשימוש לגיטימי בכוח - אינו אסור. כך למשל, ׳איום׳ של מדינה, כי תגן על עצמה בכוח, לרבות בכוח קיברנטי, כאשר תותקף - אינו אסור[162].

כעת ייבחן הנושא שבליבת הפרק: אילו פעולות קיברנטיות מהוות שימוש בכוח?

אילו פעולות קיברנטיות מהוות ׳שימוש בכוח׳ - מסגרת השאלה

הקושי לפרש את הוראת סעיף 2(4) ולהגדיר מהו ׳שימוש בכוח׳, לאור הניסוח הכללי והתמציתי של ההוראה, מתעצם בהקשר הקיברנטי. כך למשל, קשה להסתמך על דברי הפרשנות למגילה, אשר נכתבו בעידן נטול מרחב קיברנטי.

כפי שכבר נכתב, קיימת הבנה מה אינו מהווה ׳שימוש בכוח׳ - פעולות שהן בגדר כפייה כלכלית, פסיכולוגית או פוליטית גרידא. מכאן, שכאשר מבוצעת פעולה קיברנטית, השקולה להפעלת כפייה כזו - לא יראו בה ׳שימוש בכוח׳[163]. דוגמה לפעולות שאינן ׳שימוש בכוח׳ - פעולות קיברנטיות, המשפיעות במישור הפסיכולוגי, במטרה להחליש את אמון הציבור בממשלה או בכלכלה; הפצה של מידע הפוגע באינטרסים פוליטיים של המשטר ועוד.

הבנה נוספת היא ש׳שימוש בכוח׳ אינו חייב להיות בכוח צבאי, שהשפעתו פיזית-קינטית. הבנה זו חשובה במיוחד במרחב הקיברנטי, הואיל ופעולות קיברנטיות אינן כוחניות מטבען (Non forceful). אם כך, אילו פעולות קיברנטיות הן משמעותיות דיין, כדי להיחשב ׳שימוש בכוח׳? לשם הכרעה בעניין זה יוצגו מספר גישות מרכזיות לנושא.

---

[161] Schmitt, 2011; 572.

[162] מדריך טאלין, 53.

[163] מדריך טאלין, 46.

גישת ממשלת ארצות הברית

בשנים האחרונות הובילה ארצות הברית את הכתיבה בנושא השימוש בכוח במרחב הקיברנטי, ואף הרבתה לספק אינדיקציות ביחס למדיניותה. אמנם, ארצות הברית טרם פרסמה עמדה רשמית וכוללת בנושא פרשנות סעיף 2(4) בהקשר הקיברנטי[164], אך ניתן לגבש הבנה טובה של עמדת הממשל.

עמדת ארצות הברית, כפי שהתגבשה עם הזמן, היא שהתקפות קיברנטיות עשויות להוות 'שימוש בכוח', כאשר יש להן מאפיינים ותוצאות, המזכירים התקפות צבאיות או הפעלת כוח קינטי[165]. כבר בשנת 2009 נכתב בדו"ח של מועצת מחקר לאומית אמריקנית, כי התקפה קיברנטית עשויה להיכלל בגדר ה-Jus ad Bellum כאשר התוצאה שלה מקבילה להתקפה צבאית[166]. ביטוי מוחשי לקו מחשבה זה הופיע למשל בדברים שנשאה מזכירת המדינה של ארצות הברית, הילארי קלינטון, בשנת 2010. בהתייחסה לכוונה של ארצות הברית להגן על הביטחון הקיברנטי, עשתה הדוברת שימוש במונחים מהעולם הצבאי, שעיקרם מענה לשימוש בכוח ואף הגנה עצמית[167]. הד לגישה זו ניתן למצוא גם בדברי הגנרל קית' אלכסנדר, מפקד הפיקוד הקיברנטי האמריקני, בשימוע שנערך לו בוועדת הסנאט[168].

---

[164] Waxman, 2011; 431.

[165] שם. המחבר מפנה, בין השאר, למסקנות דו"ח NRC ולמאמרו של Schmitt, 1999.

[166] דו"ח NRC, 33-34.

[167] Hillary Rodham Clinton, U.S. Sec'y of State, Remarks at the Newseum in Washington , D.C. (Jan. 21, 2010), available at: http://www.state.gov/secretary/rm/2010/01/135519.htm.

[168] כדבריו:

"If the President determines a cyber event does meet the threshold of a use of force / armed attack, he may determine that the activity is of such scope, duration or intensity that it warrants exercising our right to self-defense and / or the initiation of hostilities as an appropriate response".

Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S.

בראייה רחבה יותר, הגישה האמריקנית לפרשנות 'שימוש בכוח', היא Effects (or consequences)-based[169]. כלומר, אם התוצאות של פעולה קיברנטית תהיינה מקבילות לתוצאות של 'שימוש בכוח', שאינו קיברנטי, בעולם הצבאי 'הרגיל' - יראו בה שימוש בכוח[170].

סקירה סדורה של הגישה האמריקנית הוגשה בספטמבר 2012, בנאום דוקטרינרי שנשא היועץ המשפטי של מחלקת המדינה. גם מדבריו עלה, כי התוצאות הפיזיות של הפעולה הקיברנטית הן המפתח להגדרתה כ'שימוש בכוח'. לגישתו, פעולות קיברנטיות שמובילות לתוצאה של מוות, פציעה או הרס רכוש משמעותי, ייתפסו ככל הנראה כשימוש בכוח[171]. כך למשל, כאשר התוצאות הפיזיות של התקפה קיברנטית תהיינה שקולות לתוצאות של הטלת פצצה או ירי טיל. הדובר אף הציע שורה של גורמים או אמות מידה, אותם ראוי לשקול בהחלטה הפרטנית, האם התקפה קיברנטית מסוימת מהווה 'שימוש בכוח' - כמו ההקשר של האירוע, השחקן שביצע את הפעולה, המטרה והכוונה מאחורי הפעולה[172]. כדוגמאות לפעולות קיברנטיות שיהוו שימוש בכוח, הוצגו על ידו תרחישים של גרימת התכה במתקן גרעיני, פריצה של סכר באזור מיושב או נטרול של בקרת תעופה.

ניתוח ההתבטאויות הרשמיות האמריקניות מלמד על חשש מפני פעילות נגד ארצות הברית במרחב הקיברנטי, והבנה כי קשה להישען במרחב זה על צורות מסורתיות של הרתעה צבאית קונבנציונלית[173]. הממשל האמריקני מודע לכך שבהיעדר הסכמה בינלאומית על משמעות המונח 'שימוש בכוח' בהקשר הקיברנטי, קיים חוסר ודאות

Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), available at: http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander.%2004-15-10.pdf (להלן - שימוע אלכסנדר).

[169] וכפי שיוצג בהמשך, גישה זו חלה גם לגבי 'התקפה מזוינת'.

[170] ובאופן משלים - מה שאינו מקביל ל'שימוש בכוח' בעולם המסורתי, כמו ריגול, אינו אסור. להרחבה בעניין פעולות ריגול, ראו: Smith, 2007; 544.

[171] נאום Koh, 4.

[172] שם.

[173] Waxman, 2011; 434.

באשר לאופן בו מדינות יפרשו את האיסור עליו. בשימוע שנערך למפקד הפיקוד הקיברנטי בארצות הברית, הגנרל אלכסנדר, נאמר על ידו:

"There is no international consensus of the precise definition of a use of force, in or out of cyberspace. Consequently individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force" [174].

אחת הדרכים להתמודד עם החשש הזה היא המאמץ לעצב כללי משחק משפטיים, בתקווה שיתפתחו למשטר משפטי מחייב בעתיד. לכך הוקדש מדריך טאלין, שגישתו תיסקר כעת.

אסכולת שמיט ומדריך טאלין

מעצב דעה מרכזי בסוגית 'השימוש בכוח' במרחב הקיברנטי הוא שמיט, אשר התייחס לנושא במאמר משפיע כבר בשנת 1999. הוא סבר שלשימוש בכוח לא חייבות להיות תוצאות פיזיות, והציע לבחון האם התקפה קיברנטית מהווה 'שימוש בכוח' על בסיס שורה של אמות מידה, המאפיינות באופן היסטורי שימוש בכוח צבאי [175]. גישה זו זכתה לאורך השנים לתמיכה בכתיבה מצד מלומדים נוספים [176].

שמיט היה הרוח החיה מאחורי קבוצת המומחים, שניסחה את מדריך טאלין. התהליך שהביא לניסוח המדריך הובל על ידי גוף הפועל בחסות 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

[174] שימוע אלכסנדר. מעניין לציין, כי אלכסנדר אמר, במקביל, כי קיימים דין, מדיניות וסמכות מספקים כדי לנהל את הפעילות הקיברנטית.

[175] Schmitt, 1999.

[176] כדוגמה מני רבות: Clark & Knake, 2010.

בנושא הדין החל על לוחמה קיברנטית[177]. עם קבוצת המומחים נמנו משפטנים בעלי ניסיון פרקטי רב, אקדמאים ומומחים טכניים[178]. התהליך שהחל בשנת 2009, הבשיל בקיץ 2012, אז הושלם המדריך ופורסם, תחילה באופן מקוון, ובמארס 2013 גם בדפוס[179].

הכללים, המופיעים במדריך, נוסחו על בסיס של קונצנזוס בקרב המומחים, ככאלו שמבטאים לדעתם את המשפט בינלאומי 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. המדריך כולל חלק פרשני (commentary), המבהיר את התפיסה שבבסיס הכללים המוצעים ומשקף את מנעד הדעות של המומחים, לרבות כאלו שלא באו לביטוי בניסוח הסופי.

לא במפתיע, במדריך טאלין אומצה גישת שמיט לעניין הגדרת ׳שימוש בכוח׳. כך, בהתאם למדריך:

״A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of use of force״[180].

בהתאם למנסחי המדריך (ובדומה לגישת הממשל האמריקני), כאשר פעולה קיברנטית גורמת למוות או לפציעה של אנשים או להרס רכוש,

---

[177] 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.

[178] לא היה ישראלי בקרב המומחים. מכל מקום, משתתפים רבים החזיקו ברקע ביטחוני ובניסיון פרקטי ביישום עקרונות משפטיים על תרחישים מבצעיים וביטחוניים.

[179] Tallinn Manual on The International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.

[180] כלל 11 במדריך טאלין. המונח ״scale and effect״ לקוח מתוך פרשת ניקרגואה, הגם שבאותו פסק דין נעשה בו שימוש בהקשר של ׳התקפה מזוינת׳, ולא של ׳שימוש בכוח׳.

היא תהווה שימוש בכוח, למעט במקרים שהפגיעה טריוויאלית ומינורית בלבד[181].

בנוסף, לגישתם, פעולות קיברנטיות מסוימות שאין להן תוצאות פיזיות ישירות, ואינן כרוכות כלל בהפעלת כוח צבאי, יהוו בכל זאת 'שימוש בכוח'. מתי כך יהיה? אין במדריך טאלין מענה חד משמעי. במדריך אומצה גישה, המתיימרת לספק כלים לצורך הניבוי, מהו הסיכוי שפעולה קיברנטית מסוימת תיתפס על ידי מדינות העולם כ'שימוש בכוח'[182]. הוצעו שמונה קריטריונים, המתייחסים הן לרמת הנזק, שנגרם כתוצאה מהפעולה, והן למאפיינים איכותיים, והם:

א. *חומרת הפעולה* מבחינת השלכות תוצאותיה על אינטרסים לאומיים חיוניים. ככל שהתוצאות חמורות מבחינת היקף, משך ותחולה - רב הסיכוי שהפעולה תוכר כ'שימוש בכוח'. בפרט, כאשר נגרמים נזק לרכוש, פציעה או מוות, קיים סיכוי גבוה מאד שהפעולה תיחשב שימוש בכוח. זהו המשמעותי ביותר מבין כלל הקריטריונים.

ב. *מיידיות* התממשות התוצאות. ככל שתוצאות הפעולה מיידיות יותר, תגבר הנטייה לראות בה 'שימוש בכוח'.

ג. *ישירות* - ככל שהקשר הסיבתי בין הפעולה לתוצאה חזק יותר, הנטייה תהיה להכיר בה כ'שימוש בכוח'.

ד. *חודרניות* - מידת החדירה למרחב הקיברנטי. ככל שהחדירה מכוונת יותר נגד גורמים ממשלתיים, בפרט אלו המוגנים בצורה חזקה באופן יחסי, תגבר הנטייה לראות בה 'שימוש בכוח'.

ה. *מדידות האפקטים* - ככל שתוצאות הפעולה ניתנות יותר לכימות ולזיהוי, הנטייה תגבר לראות בה 'שימוש בכוח'.

ו. *אופי צבאי* - ככל שקיים קשר בין הפעילות הקיברנטית לבין מבצעים צבאיים, גדל הסיכוי שיראו בה 'שימוש בכוח'.

---

[181] סייג שאומץ אף הוא מתוך פסק הדין בפרשת ניקרגואה.

[182] מדריך טאלין, 48.

ז. *מעורבות מדינתית* - ככל שקיים קשר ברור וקרוב יותר בין מדינה מסוימת לבין פעולות קיברנטיות שבוצעו, גדל הסיכוי שיראו בהן 'שימוש בכוח'.

ח. *הנחת הלגיטימיות* - במשפט הבינלאומי קיימת הנחה, כי מה שלא נאסר במפורש - מותר. כך לדוגמה ריגול, תעמולה (פרופגנדה), לחימה כלכלית או לחימה פסיכולוגית, לא נאסרו בפני עצמם. ככל שאין איסור קונקרטי על פעולה מסוימת במרחב הקיברנטי, קטנה הנטייה לראות בה 'שימוש בכוח'.

מנסחי המדריך הכירו בכך שהדרך בה מדינות יתייחסו לפעולות קיברנטיות, מושפעת מגורמים רבים, כמו הסביבה הפוליטית-מדינית, זהות השחקנים, עברם בתחום הקיברנטי ועוד היבטים שאינם באים לביטוי בהכרח בקריטריונים.[183]

כדוגמה לפעולה שמהווה 'שימוש בכוח', הגם שאינה מביאה לנזק פיזי ישיר, הוצג במדריך תרחיש, בו מדינה אחת מציידת קבוצה מאורגנת בתוכנות זדוניות, שישמשו את הקבוצה כדי לתקוף במרחב הקיברנטי מדינה אחרת. בראי פסק הדין בפרשת ניקרגואה, והקריטריונים האמורים, זהו בגדר 'שימוש בכוח'. מנגד, מתן מקלט בלבד לאותה קבוצה, אינו מהווה לגישת מנסחי המדריך 'שימוש בכוח'. הקריטריונים מתאימים לכאורה גם לבחינה של מקרים, בהם התקפות קיברנטיות פוגעות בצורה חמורה במערכות מידע ממוחשב, עליהן נשענות תשתיות לאומיות, תוך גרימת פגיעה כלכלית, גם ללא גרימת נזק פיזי ישיר.[184]

שמיט מבקש להצביע על זהות כמעט מלאה בין עמדת הממשל האמריקני לבין גישת מדריך טאלין.[185] נראה כי הגישות אכן זהות

---

[183] מדריך טאלין,51-52. לעניין הלוגיקה בהצעה, ראו גם: Antolin-Jenkins, 2005; 171.

[184] להרחבה ראו גם: דו"ח NRC, 253-254. מהדו"ח עולה כי פעולות קיברנטיות שיפגעו באופן משמעותי בפונקציות של תשתיות קריטיות, ניתן להתייחס אליהן בצורה היגיונית כשימוש בכוח, בין אם הן גורמות נזק פיזי ישיר ובין אם לאו.

[185] ראו: Schmitt, 2012 (2). המאמר כולו עוסק בניסיון ליישב בין הדברים.

ביחס למקרים בהם פעולה קיברנטית גורמת לנזק פיזי ישיר, לאדם או לרכוש, ורואות בכך 'שימוש בכוח'. אשר למקרים שאינם כרוכים בנזק פיזי ישיר, אותם מציע מדריך טאלין לבחון לפי שורה של קריטריונים, ספק רב בשלב זה, האם ארצות הברית הרשמית אכן תראה בהם 'שימוש בכוח'[186].

מהו הדין הקיים ביחס ל'שימוש בכוח' במרחב הקיברנטי?

מדריך טאלין הוא הניסיון המשמעותי ביותר, עד כה, להציג הבנה סובייקטיבית של מומחי משפט בינלאומיים ביחס לדין הקיים[187] (באופן כללי ובהקשר של איסור השימוש בכוח במרחב הקיברנטי). דומה, עם זאת, כי עדיין קשה להצביע על 'דין קיים' בהקשר זה, במידה ראויה של וודאות.

ראשית, אין פרקטיקה של מדינות, שעשויה לספק קווים מנחים לגבי הבנתן את הדין. עד היום, אין מדינה שבחרה לייחס, באופן רשמי ומבוסס, פעולה של 'שימוש בכוח' נגדה מצד מדינה אחרת. כפי שכבר צוין, המשפט הבינלאומי המנהגי מתבסס מתוך מספר מקורות, כאשר אחד החשובים שבהם הוא המנהג, ובכללו הפרקטיקה של מדינות וההנמקה המשפטית שבבסיסה. לפרקטיקה זו אמור להיות משקל משמעותי בעיצוב דמותו המשפטית של איסור השימוש בכוח במרחב הקיברנטי[188].

שנית, העמדה האמריקנית-מערבית אינה אחידה. הממשל האמריקני עצמו הולך על חבל דק בין אינטרסים שונים, דבר המקשה עליו לעצב משטר משפטי בהובלתו. כך, יש גורמים אמריקנים הממוקדים בראייה

---

[186] נאום Koh אינו חד משמעי בנקודה זו, ומתייחס באופן ברור כ'שימוש בכוח' רק למקרים של גרימת נזק פיזי ישיר.

[187] במבוא למדריך טאלין עצמו, ציינו מנסחי המדריך כי במצב הקיים, קשה לקבוע באופן מוחלט כי קיימות נורמות של משפט בינלאומי מנהגי בתחום הקיברנטי. המנסחים אינם טוענים שקביעות המדריך משקפות את המשפט הבינלאומי הקיים באופן שאינו מעורר מחלוקת, אלא מבקשים לשקף את הקונצנזוס, ששרר בקרב המומחים לגבי הדין הקיים, להבדיל מהדין הרצוי. ראו מדריך טאלין, 5-6.

[188] ראו גם מדריך טאלין, 42.

התקפית ומבקשים לשמר כלים קיברנטיים התקפיים, ואילו אחרים מדגישים את הפן ההגנתי. הראשונים, אינם ממהרים להגדיר פעולה קיברנטית כ'שימוש בכוח', ואילו האחרונים מבכרים להוריד את דרישות הסף לכך[189].

בנוסף, קו דק מפריד בין הרצון למנוע השפעות הרסניות של התקפות קיברנטיות, בפרט נגד תשתיות קריטיות במערב, לבין חשש משינוי רדיקלי בפרשנות מגילת האו"ם[190]. לאורך השנים, עמדו ארצות הברית ובנות בריתה כחומה בצורה נגד פרשנות מרחיבה של סעיף 2(4) למגילה. שעה שחברות הגוש הסובייטי טענו כי המערב מפעיל עליהן כוח באמצעים כלכליים ופוליטיים, והדבר מהווה איסור שימוש בכוח לפי מבחן התוצאה (Effect), התעקשה ארצות הברית כי המבחן הוא המכשיר (Instrument) בו נעשה השימוש בכוח[191]. ההתפתחויות במרחב הקיברנטי מעוררות מבוכה ודילמה במערב, והן עשויות לשנות את כללי המשחק. לאור הסיכונים הקיברנטיים, יתכן שמדינות מערביות יתמכו כעת בפרשנות רחבה לסעיף 2(4) למגילה, כך שזו תשתרע מעבר להפעלת כוח צבאי, ברוח מדריך טאלין[192]. הצהרות פומביות של גורמים רשמיים אמריקנים כבר מצביעות על מגמה של מעבר לפרשנות שהיא "Effects-based" בהקשר של 'שימוש בכוח' קיברנטי[193]. עם זאת, יקשה לאבחן ולהסביר, מדוע סנקציות כלכליות, מצויות מחוץ לאיסור השימוש בכוח, ואילו פעולות קיברנטיות שגורמות נזק כלכלי גרידא, הן

---

[189] Waxman, 2011; 436.

[190] שם.

[191] להרחבה: Banks, 2013.

[192] ראו לדוגמה גישתו של Sharp, 1999; 129-133. שארפ ביקש להציג גישה אלטרנטיבית לזו של שמיט, אם כי ההבדל אינו חד. בכתיבתו בשנת 1999, הציג הצעה שמבוססת על ספקטרום ליניארי של פעולות, שנעות בין פעולות בעת שלום, איומים על השלום, איום בכוח ושימוש בכוח. עם זאת, נראה שלא הצביע על קו ברור, המייחד 'שימוש בכוח', לפחות במצבים בהם לא נגרם נזק פיזי עקב הפעולה.

[193] Waxman, 2011; 436-437.

אסורות[194]. המתחים הפנימיים הללו, מקשים על גיבוש עמדה ברורה ואחידה ביחס לדין הקיים.

שלישית, אין לשכוח, כי לצד העמדה המערבית, קיימות גישות מתחרות בעיקר מצד רוסיה וסין. מבלי לשוב ולהרחיב, מדינות אלו תובעות לכלול במסגרת האיסורים במרחב הקיברנטי, גם כלי ואמצעי השפעה, הנתפסים כמקורות איום פוטנציאליים על האידיאולוגיה והמשטר שלהן, ולחזק את יכולתן להפעיל בקרה ושליטה במרחב. מדינות (ובהקשר הקיברנטי - מעצמות) אלו רחוקות מהגישה המערבית, והשיח עמן עשוי להזכיר את הוויכוח בימי המאבק הבין גושי, ביחס למשמעות סעיף 2(4) למגילת האו"ם.

[194] ראו למשל: Antolin-Jenkins, 2005; 135.

'התקפה מזוינת' והגנה עצמית במרחב הקיברנטי

זכות ההגנה העצמית במרחב הקיברנטי

הפרק הקודם הוקדש לאיסור השימוש בכוח והאיום בו. לאיסור זה, המעוגן בהוראת סעיף 2(4) למגילת האו"ם, שני חריגים בלבד במגילה: שימוש בכוח בהתאם להחלטת מועצת הביטחון של האו"ם, שהתקבלה מכוח פרק VII למגילה, ופעולות הננקטות בהגנה עצמית.

החריג הראשון, שלא ייסקר בהרחבה, קשור לסמכותה של מועצת הביטחון של האו"ם, לפי סעיף 39 למגילת האו"ם, לזהות "איום על השלום, הפרת השלום או אקט של תוקפנות". במקרים אלו, המועצה יכולה להמליץ או להחליט על צעדים להשבה או לשמירת השלום והביטחון הבינלאומיים. לפי סעיפים 41 ו-42 למגילה, בהתאמה, מועצת הביטחון רשאית לנקוט צעדים שאינם כרוכים בהפעלת כוח צבאי, וכן להסמיך גורמים לנקוט צעדים שכרוכים בהפעלת כוח באוויר, בים או ביבשה. קשה להצביע על מבחנים מדויקים לגבי הנסיבות, בהן תפעיל מועצת הביטחון את סמכותה. המועצה היא גוף פוליטי, המקבל החלטות פוליטיות, וקשה מאד לגבש במסגרתו קונצנזוס של חמש החברות הקבועות לפעולה מעין זו[195]. מאחר שסוגיית הפעלת סמכותה של מועצת הביטחון חורגת מעבודה זו ומעוררת היבטים לבר-משפטיים רבים, המיקוד יהיה בחריג השני לאיסור השימוש בכוח - זכות ההגנה העצמית.

זכות ההגנה העצמית מפני 'התקפה מזוינת'

זכותן של מדינות להשתמש בכוח לשם הגנה עצמית היא זכות יסוד במשפט הבינלאומי המנהגי[196]. היא מעוגנת בסעיף 51 למגילת האו"ם, ומקנה זכות להגנה עצמית, אינדיבידואלית או קולקטיבית, כאשר

---

[195] Hathaway, 2012; 844.

[196] דינשטיין מתאר זכות זו בהרחבה בספרו:
Dinstein Yoram, War, Agression & Self-Defence (4th ed. 2005).

מבוצעת 'התקפה מזוינת' (armed attack) נגד מדינה החברה באו"ם, כל עוד לא נקטה מועצת הביטחון אמצעים החיוניים לשמירת השלום והביטחון הבינלאומיים. בלשון הסעיף:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security".

סעיף 51 למגילת האו"ם לא התיימר ליצור זכות חדשה, אלא ביקש להכיר בזכותן הטבעית (Inherent right) של מדינות להגנה עצמית[197]. בפועל, זכות ההגנה העצמית היא האמצעי המרכזי, באמצעותו מדינות מבטיחות את ביטחונן. ייחודה של זכות ההגנה העצמית, בכך שהיא מאפשרת למדינה שימוש בכוח צבאי, בלי שהדבר מותנה בהחלטה של מועצת הביטחון. לא אחת, מתעוררים ויכוחים עזים בין מדינות ובקרב הקהילה הבינלאומית לגבי הפעלת הזכות, ומוטל ספק בטענה של מדינה, כי היא פועלת משיקולי הגנה עצמית בלבד[198].

סעיף 51 מתייחס לשימוש בהגנה עצמית, כאשר מתרחשת נגד מדינה 'התקפה מזוינת'. בהתאם, כאשר נבחנת טענה של מדינה כי פעלה בהגנה עצמית, שאלת המפתח תהיה: האם אכן מתרחשת 'התקפה מזוינת' נגדה? רק בהתקיים תנאי זה, רשאית מדינה להגיב בכוח. בנסיבות אחרות, הדבר אסור. נקודה זו משמעותית מאד - לא כל שימוש בכוח נגד מדינה מגיע לכדי 'התקפה מזוינת'. אם מדינה נפגעת

[197] Schmitt, 2012; 285.
[198] Hathaway, 2012; 844.

כתוצאה משימוש בלתי חוקי בכוח נגדה, שאינו מגיע לסף של ׳התקפה מזוינת׳, אין היא יכולה להגיב בכוח.[199]

הדיכוטומיה בהוראות מגילת האו״ם, שעיקרה היכולת להגיב בכוח ל׳התקפה מזוינת׳ בלבד, אינה מקרית. היא נובעת מהתפיסה הכללית של מגילת האו״ם, המיועדת למנוע שימוש בכוח בין מדינות. בפרט מבקשת הקהילה הבינלאומית למנוע שימוש חד צדדי בכוח מצד מדינה מסוימת, להבדיל מפעולה שנתמכת על ידי הקהילה הבינלאומית כולה. רק כאשר מדינה נפלה קורבן ל׳התקפה מזוינת׳, וזהו החריג, מוקנית לה זכות התגובה, לרבות במרחב הקיברנטי, ללא תלות בהחלטת מועצת הביטחון של האו״ם.

אם כך, חלק בלבד מהפעולות שמהוות שימוש בכוח, מגיעות לרמת חומרה של ׳התקפה מזוינת׳. בפסק הדין בפרשת ניקרגואה, קבע בית הדין הבינלאומי בהאג, כי יש צעדים שהם בגדר ׳שימוש בכוח׳, אך אינם מגיעים לכלל ׳התקפה מזוינת׳. בראייתו, ׳התקפה מזוינת׳ היא בגדר "the most grave forms of the use of force"[200]. במילים אחרות, התקפה מזוינת היא: "A subset of violent acts within a broader grouping of acts that qualify as uses of force".[201]

מהו קו פרשת המים, המפריד בין שימוש בכוח ׳רגיל׳ לבין שימוש בכוח המהווה ׳התקפה מזוינת׳? לכאורה המונח "Armed" (מזוינת), הוא המפריד. בדומה ל׳שימוש בכוח׳, גם ׳התקפה מזוינת׳ היא מונח המכונה Instrument-based (או Act-based); המונח גובש מתוך מחשבה על התקפות צבאיות-קינטיות. בראיית הקהילה הבינלאומית, רק כאשר מדינה נופלת קורבן להתקפות מסוג זה, תישמר זכותה להגיב בכוח בהגנה עצמית.[202]

---

[199] Watts, 2011; 67.

[200] פרשת ניקרגואה, 191 ו-210.

[201] Watts, 2011; 65.

[202] Schmitt, 2012; 287.

אמנם, לפי פסיקת בית הדין הבינלאומי בהאג, סוג האמצעי בו נעשה שימוש נגד מדינה אינו מהותי לעניין עצם זכותה להגנה העצמית[203]. עם זאת, פרשנות מילולית של המונח 'מזוינת', מצביעה לכאורה על אמצעי צבאי, אשר סביר שתוצאתו תהיה פגיעה באנשים או ברכוש. בעוד המונח 'שימוש בכוח' פורש כמשתרע גם על פעולות שאינן קינטיות-צבאיות, המונח 'מזוינת' מאפשר יצירתיות פחותה בפרשנותו.

בית הדין הבינלאומי בהאג, בפרשת ניקרגואה, הוסיף וקבע, כי 'התקפה מזוינת' היא כזו שיש לה "Scale and Effects"[204]. באותו מקרה, נפסק כי סיוע בנשק ובלוגיסטיקה למורדים אינו מהווה 'התקפה מזוינת' ואינו מבסס את הזכות להגנה עצמית (אף שהוא עשוי להוות 'שימוש בכוח'). בית הדין, עם זאת, נמנע מלהגדיר קריטריונים ברורים לעניין משמעות הדרישה.

ראוי להדגיש, כי הגנה עצמית כפופה לשני תנאים משפטיים מרכזיים, הנחשבים חלק מהמשפט הבינלאומי המנהגי - צורך (Necessity) ומידתיות (Proportionality)[205]. תנאים אלו, ששורשיהם כבר באמצע המאה התשע עשרה, קנו אחיזה ונחשבים חלק מהמשפט הבינלאומי המנהגי.

'צורך' - משמעו היעדר חלופות אפקטיביות אחרות, שאינן כרוכות בהפעלת כוח, אשר יביאו להסרת האיום או הסכנה. אמצעים חלופיים שאינם כוחניים, עשויים להיות למשל סנקציות כלכליות, מהלכים דיפלומטיים או אכיפת החוק[206].

גם כאשר קיים צורך, הפעלת הכוח נדרשת להיות מידתית. אסורה הפעלת כוח, כאשר היקפו והאינטנסיביות שלו מופרזים ביחס לסיכון

---

[203] פרשת חוקיות הנשק הגרעיני, 39.

[204] פרשת ניקרגואה, 195.

[205] דרישות שמקורן בפרשה הידועה של האוניה Caroline משנת 1837. על העקרונות חזר בית הדין בהאג בשורה של פסקי דין מפורסמים, והם אף מופיעים במשפטי נירנברג. ראו מדריך טאלין, 61.

[206] מדריך טאלין, 62.

הנשקף למדינה.[207] יודגש, כי אין צורך שפעולת ההגנה העצמית תיעשה באמצעות הפעלת סוג כוח זהה לזה שמולו היא מתגוננת. כך, למשל, ניתן להגיב על תקיפה קינטית באמצעות פעולה קיברנטית ולהפך. הדגש הוא על עצם היכולת של מדינה להגן על עצמה.

זכות ההגנה העצמית במרחב הקיברנטי

החריג הראשון לאיסור השימוש בכוח הוא הפעלת סמכותה של מועצת הביטחון של האו״ם, לפי סעיף 39 למגילת האו״ם, על בסיס קביעה שנוצר ״איום על השלום, הפרת השלום או אקט של תוקפנות״. החלטה כזו, באופן תיאורטי, עשויה להתקבל גם במענה להתקפה במרחב הקיברנטי, ובמסגרת מימושה, עשויה המועצה להנחות על נקיטת צעדים במרחב זה.

בחיי המעשה, הואיל והחלטות מועצת הביטחון מחייבות קונצנזוס של חמש החברות הקבועות, ובהן רוסיה וסין - שתי שחקניות רבות עוצמה במרחב הקיברנטי, החוששות מהגבלת יכולתן ומייצגות אינטרסים שונים משל מדינות המערב - ספק של ממש, האם מועצת הביטחון תהיה גוף אפקטיבי בהקשר הקיברנטי, בוודאי בשנים הקרובות. בהקשרים פחות שנויים במחלוקת, מועצת הביטחון משרכת רגליה טרם תפעיל סמכויות אלו. ההססנות הצפויה ביחס לפעולה במרחב הקיברנטי היא בגדר קל וחומר, בהיותו עדיין שדה בלתי חרוש, עמוס בסימני שאלה ביחס לכללי המשחק ולמפות האינטרסים האסטרטגיים. יהיה זה מרחיק לכת לצפות להסכמה פוליטית רחבה בין חברות מועצת הביטחון בהקשרים קיברנטיים.[208]

לאור האמור, ימוקד פרק זה בזכות ההגנה העצמית בתגובה להתקפה מזוינת במרחב הקיברנטי.

---

[207] Sloane, 2009; 108-109, מציין שעיקרון המידתיות מצוי בזיקה הדוקה לעיקרון הצורך. במסגרתם בוחנים, האם ניתן יהיה להשיג את אותה תוצאה של הפעולה הצבאית, באמצעות דיפלומטיה או אמצעי בלתי כוחני אחר, באותו מחיר או אף במחיר מעט יותר גבוה.

[208] Schmitt, 2011; 586.

מהי 'התקפה מזוינת' במרחב הקיברנטי? גישת שמיט ומדריך טאלין

מימוש זכות ההגנה עצמית והפעלת כוח במסגרתה, מתאפשרים אך ורק כתגובה להתקפה שהיא 'מזוינת'. האם פעולה קיברנטית עשויה להוות 'התקפה מזוינת', ולהצדיק את מימוש זכות ההגנה העצמית?

לכאורה, התשובה האינסטינקטיבית היא שלילית. 'התקפה מזוינת' נתפסת, כפשוטו, ככזו הכוללת שחרור של כוח קינטי, הגורם באופן ישיר (או מכוון לגרום) לתוצאות הרסניות[209]. התקפה קיברנטית אינה כוחנית. על פניו - זהו הדין הקיים[210].

תוצאה זו, לפיה מדינה עלולה להיות קורבן להתקפה משמעותית מאד באמצעים קיברנטיים, אך לא תוכל לנקוט הגנה עצמית בתגובה, היא בעייתית, בלשון המעטה. כאשר מדינות מותקפות בצורה חמורה, ואינן יכולות להגיב בכוח, הדבר אינו מתיישב עם תכלית מגילת האו"ם. היצמדות לפורמליזם משפטי, לניסוח שאינו מביא בחשבון את ההתפתחויות הטכנולוגיות, עלולה להוביל לתוצאות אבסורדיות[211]. בפועל, מדינות אינן מתכוונות לשבת באפס מעשה נוכח פגיעה קשה בהן. היועץ המשפטי של מחלקת המדינה האמריקנית כבר הצהיר, כי ארצות הברית תממש את זכותה להגנה עצמית, במקרה שתותקף באמצעים קיברנטיים, אם הפעילות נגדה תגיע לכדי 'התקפה מזוינת'[212].

בשנים האחרונות, בשלה בקרב כותבים ומעצבי דעה בתחום המשפטי-קיברנטי במערב, ובעיקר בארצות הברית, התובנה כי התקפה קיברנטית עשויה להיות 'התקפה מזוינת', במונחי מגילת האו"ם. בהקשר זה, הוצגו דעות שונות[213], כאשר המקובלת מתוכן היא זו

---

[209] Schmitt, 2012; 287.

[210] Schmitt, 2011; 588.

[211] Schmii, 2012; 287.

[212] נאום Koh, 4.

[213] Hathaway, 2012; 845-848. המחברים מתארים בהרחבה את הגישות, המכונות: Instrument-based, target-based and effects-based. מקוצר היריעה, לא יובא תיאורן.

שניתן לכנותה Effects-based. כלומר גישה הבוחנת ומסווגת פעולות לאור חומרת התוצאות שלהן, ולאו דווקא לאור האמצעי בו נעשה שימוש (נשק מזוין)[214].

שמיט למשל מדגיש, כי לפי פסיקת בית הדין הבינלאומי, סוג האמצעי בו נעשה שימוש אינו מהותי לעניין זכות ההגנה העצמית[215]. משכך, העובדה, שהתקפה מבוצעת באמצעות מחשבים, אינה מונעת ממנה להיות 'מזוינת'. לגישתו, ניתוח מגילת האו"ם ופרשנותה המקובלת, מכוון למספר עקרונות: לא כל 'שימוש בכוח' הוא 'התקפה מזוינת'; פרשנות המונח 'התקפה מזוינת' חייבת להיות צרה, במטרה לצמצם שימוש חד צדדי בכוח על ידי מדינות; והפרשנות חייבת להתמודד עם מאפייני המונח 'מזוינת', המופיע לרוב בהקשר צבאי[216]. הדרך, שמצא שמיט ליישם את העקרונות, היא בקביעה שפעולה קיברנטית עשויה להיות 'התקפה מזוינת', אם תוצאותיה הצפויות תהיינה אנלוגיות לאלו של 'תקיפה מזוינת קינטית' - כלומר גרימת מוות או פציעה לאנשים ופגיעה ברכוש[217].

גישת שמיט אומצה במדריך טאלין, ובאה לביטוי במסגרתו בכלל מספר 13. בקרב מחברי המדריך היה קונצנזוס, כי פעולות קיברנטיות עלולות להיות כה חמורות, עד שיהיה מוצדק להגדירן כ'התקפה מזוינת'. הם הוסיפו, כי לא כל שימוש בכוח יהווה 'התקפה מזוינת'. נדרשים 'Scale and Effects', על מנת ש'שימוש בכוח' יגיע לכדי 'התקפה מזוינת'[218].

בהקשר אחרון זה, יש להצביע על פער מהותי בין הגישה של מנסחי מדריך טאלין לבין העמדה של גורמים רשמיים אמריקנים. עמדת ארצות הברית היא לכאורה שניתן לפעול בהגנה עצמית אל מול 'שימוש

---

[214] בולט בגישה שמיט, אך אינו יחיד בה. ראו למשל Kanuck, 1996; 282.

[215] פרשת חוקיות הנשק הגרעיני, פסקה 39. ולראייה, מדינות רבות ראו בהתקפות כימיות וביולוגיות 'התקפה מזוינת', גם אם אין להן אופי קינטי.

[216] Schmitt, 2012; 288.

[217] שם.

[218] מונח שלקוח מפסק הדין בפרשת ניקרגואה, פסקה 195.

בכוח' קיברנטי, ואין רף מסוים של היקף וחומרה, בו השימוש בכוח נדרש לעמוד, כתנאי מוקדם למימוש ההגנה העצמית[219].

מהכלל אל הפרט - אילו פעולות יהוו 'התקפה מזוינת' קיברנטית?

בקרב כותבים וגורמים רשמיים במערב קיימת רמה גבוהה של הסכמה, כי כאשר לפעולה קיברנטית תהיינה תוצאות פיזיות משמעותיות - הרג אנשים, פציעות חמורות, נזק משמעותי לרכוש - יראו בהן משום 'התקפה מזוינת'. לצורך הדוגמה, כך יהיה כאשר פעולה קיברנטית תביא להסטת רכבת מפסי המסילה או לפריצת סכר מים באזור מיושב. מה באשר לפגיעה ברכוש שהוא מידע? הפרשנות המקובלת היא שאיסוף מידע קיברנטי, גניבת מידע ואפילו השמדת מידע או שינויו, אינם 'התקפה מזוינת' בפני עצמם[220]. החריג לכך עשוי להיות רק במקרה שבו נפגע מידע, המיועד להיהפך באופן מיידי לחפצים מוחשיים, כגון מידע בנקאי ששקול לכסף מזומן. במקרה כזה, הפגיעה במידע עשויה להיחשב פגיעה ברכוש[221].

הסוגיה המורכבת ביותר, לגביה לא קיים קונצנזוס, עניינה מצבים בהם נגרמת למדינה מסוימת, כתוצאה מהתקפה קיברנטית, פגיעה קשה ומשמעותית, שאינה מתבטאת בנזק פיזי לאדם או לרכוש. יש הסבורים, כי התקפה כזו אינה יכולה בהגדרה להיות 'מזוינת'. אחרים, סבורים שלא אופי התוצאות (פגיעה גופנית או הרס) צריך להיות המבחן הקובע, אלא ההיקף של האפקט הנגרם, כך שבמקרים חמורים תהיה זו 'התקפה מזוינת'[222].

ניתן להדגים את הדילמה באמצעות תרחיש של התקפה קיברנטית על הבורסה בניו יורק, שתגרום לה להתרסק, בשל פגיעה באמינות המידע

---

[219] נאום Koh, 7.

[220] אחרת המשמעות תהיה שכמעט כל הפעולות במרחב הקיברנטי תהיינה 'התקפה מזוינת' - פרשנות בלתי סבירה, על פניה. ראו: Schmitt, 2011; 589.

[221] שם.

[222] מדריך טאלין, 56.

ובתשתית המחשבים. יהיו כאלה שיסברו שזהו נזק כלכלי גרידא, שאין לפעולה מאפיינים של פגיעה פיזית, ולכן אינה ׳התקפה מזוינת׳. אחרים יסברו שהתוצאות הקטסטרופליות של הפעולה, מצדיקות תיוג שלה כ׳התקפה מזוינת׳[223]. בראיית האחרונים, אי הכרה בפעולה בעלת השלכות כלכליות הרסניות כ׳התקפה מזוינת׳, חותרת תחת זכות ההגנה העצמית של מדינות ואינה מתיישבת עם תכלית מגילת האו״ם.

מנסחי מדריך טאלין בחרו לשקף את היעדר הקונצנזוס ביחס להתקפה קיברנטית, שאינה גורמת נזק פיזי ישיר, ולא הכריעו בין הגישות. הדבר מעיד, כי לפחות בראיית הדין הקיים, להבדיל מהדין הרצוי, לא ניתן לסווג פעולות חמורות כאלו כ׳התקפה מזוינת׳.

בראיית מנסחי מדריך טאלין, קיים, כאמור, משקל מכריע לתוצאות של הפעולה הקיברנטית, לצורך ההכרעה, האם תהווה ׳התקפה מזוינת׳. בראייתם, יש להביא בחשבון כל תוצאה של הפעולה, שניתנת לצפייה באופן סביר[224]. לדוגמה, כאשר מותקף מתקן לטיהור מים, יש להביא בחשבון חולי ומוות שייגרמו עקב זיהום המים שייווצר.

יש המצביעים על נקודת תורפה בגישה זו - הקושי המהותי לצפות מראש, מתי להתקפה קיברנטית תהיינה תוצאות של פגיעה באנשים או ברכוש; וזאת, בשל האופי הבלתי ישיר של השפעותיה[225]. לדוגמה, קשה לחזות מראש האם התקפה קיברנטית על בורסה לניירות ערך תביא לפגיעה משמעותית ברכוש, והאם התקפה קיברנטית על מערכת בקרה אווירית תביא בפועל לפגיעה בחיי אדם[226]. אכן, מבחינה

---

[223] שם.

[224] לדעה זו שותפים גם אחרים. למשל: Silver, 2002; 90-91. סילבר הציג בהקשר זה עמדה ששמה, בדומה למדריך טאלין, את מירב המשקל על הנזק הצפוי ועל יכולת הצפייה שלו. לדבריו התקפה קיברנטית מצדיקה הגנה עצמית:

״only if its foreseeable consequences is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion״.

[225] Hathaway, 2012; 847.

[226] שם, 847-848: המחברים מציינים שאף הפרמטרים ששמיט הציע לעניין ׳שימוש בכוח׳, והצביע עליהם כפוטנציאל לעניין זיהוי ׳התקפה חמושה׳, מותירים מרחב

עובדתית, קיים קושי לצפות תוצאות אפשריות של פגיעה בתשתיות מחשוב. עם זאת, סבורני שאין מנוס מהסתמכות על יכולת הצפייה הסבירה בעת ביצוע הפעולה. שהרי, גם ביחס להתקפה קינטית, עלולות, לא אחת, להיגרם תוצאות שקשה לצפות אותן מראש.

שאלה אחרת ביחס למקרה בו מדינה ספגה פגיעה המאפיינת 'התקפה מזוינת', היא: האם יש חשיבות ליסוד הנפשי ('כוונה') מצד הגורם התוקף? לדוגמה, מדינה שביקשה לבצע פעולת ריגול בלבד במדינה אחרת, אך שלא במתכוון, גרמה נזק משמעותי מאד לתשתית הקיברנטית באותה מדינה. רוב המומחים, שניסחו את מדריך טאלין, סברו שלעניין מימוש זכות ההגנה העצמית, הכוונה של התוקף אינה רלבנטית, וההכרעה תהיה לאור היקף ואפקט הפעולה שגרם[227]. לעניות דעתי, ומבלי להרחיב, גישה זו נכונה אולי במישור המשפטי-תיאורטי, אך בחיי המעשה, תגובה של מדינה למעשה של מדינה אחרת מושפעת משיקולים רבים, ובהם הכוונות שמיוחסות למדינה שפעלה[228]. מכאן, שלכוונת התוקף עשויה בהחלט להיות משמעות.

בהקשר דומה, אחד המאפיינים של פעילות במרחב הקיברנטי, הוא האפשרות שפעולה המכוונת נגד מדינה מסוימת, תגלוש בהשפעותיה למדינה שלישית (Bleed-over effects), שלא במתכוון. במקרה כזה, אם תוצאות הפעולה במדינה השלישית יגיעו לכלל 'התקפה מזוינת', אותה מדינה שלישית תהיה זכאית להפעיל כוח נגד הגורם התוקף על בסיס

שיקול דעת רחב מדי, ולא מסייעים בהכרח לניתוח אפקטיבי. לעניות דעתי, קושי זה אכן קיים, והוא עלול להביא, גם אם ייושמו הפרמטרים, לפרשנויות שונות של גורמים שונים.

[227] מדריך טאלין, 57.

[228] לדוגמה, ישראל פעלה תחילה באופן מתון בתגובה לירי משטח סוריה לתחום מדינת ישראל, מתוך סברה שכוונות מבצעי הירי היו לפעול נגד מורדים סוריים ולא נגד גורמים ישראליים. להרחבה ראו: "לראשונה ממלחמת יום כיפור: צה"ל ירה לעבר סוריה בתגובה לירי לרמת הגולן", כהן גילי ואשכנזי אלי, הארץ, 11 בנובמבר 2012, פורסם ב:
http://www.haaretz.co.il/news/politics/1.1861642

הגנה עצמית. כוונתה המקורית של המדינה, שביצעה את ההתקפה, אינה משנה אף לעניין זה[229].

לבסוף, ומבלי להרחיב בדבר, 'התקפה מזוינת', לרבות במרחב הקיברנטי, אינה חייבת להתבצע נגד שטח המדינה, אלא יכולה להיות, למשל, נגד אנשי ממשל או מתקן ממשלתי (שגרירות או בסיס צבאי) מחוץ למדינה. כזו תהיה, לשם הדוגמה, התקפה קיברנטית המיועדת לפגוע בראש מדינה בהיותו מחוץ לארצו. ההכרעה, האם מדובר בפעולה נגד מדינה, במקרים שבהם מתעורר ספק, נגזרת בדרך כלל ממספר שיקולים, כגון היקף הנזק, האם הרכוש שנפגע ממשלתי או ציבורי, האם ההתקפה מונעת משיקולים פוליטיים וכיוצא באלה[230].

דרישות הצורך והמידתיות

דרישות הצורך והמידתיות, המגדירות את גבולות ההגנה העצמית, חלות גם במרחב הקיברנטי. הן באות לביטוי, למשל, בכלל 14 במדריך טאלין, לפיו, 'שימוש בכוח', המערב פעילות קיברנטית, חייב להיות נחוץ ומידתי[231]. הדרישות באו לידי ביטוי גם בעמדת ארצות הברית, במסמך אסטרטגי שפורסם בשנת 2011[232]. הגם שנראה כי יש הסכמה רחבה ביחס לתקפותן של הדרישות, הלכה למעשה, יישומן צפוי לעורר דילמות לא מעטות.

המשמעות של דרישת הצורך, בתמצית, היא היעדר חלופות פעולה שאינן בגדר שימוש בכוח. בהקשר הקיברנטי, כאשר מנגנוני ההגנה הפאסיביים (Passive Defense) של הרשת המותקפת, כמו מנגנוני חומת אש (firewalls), מספיקים כדי להדוף את ההתקפה, אין הצדקה לכאורה לשימוש בכוח התקפי נוסף[233]. באופן דומה, אם פעולות קיברנטיות,

---

[229] שם. ראו גם: Schmitt, 2011; 590. ראוי לציין כמובן כי עדיין תחולנה כל ההגבלות, הרלבנטיות לעניין הגנה עצמית (צורך, מידתיות ועוד).

[230] מדריך טאלין, 60.

[231] מדריך טאלין, 62.

[232] The White House, International Strategy for Cyberspace 5 (May, 2011).

[233] מדריך טאלין, 62.

שאינן מגיעים לכדי 'שימוש בכוח', מספיקות כדי להדוף את ההתקפה או למנוע אותה, אין לעשות שימוש בכוח - קינטי או קיברנטי. עוד יודגש, כי הצורך נבחן תמיד בראיית המדינה שנפלה קורבן להתקפה הקיברנטית ועל בסיס המידע שברשותה. על ההכרעה לגבי קיומו להיות סבירה בנסיבות העניין[234].

דרישת המידתיות עוסקת בשאלה, בכמה כוח ניתן להגיב, קיברנטי וקינטי? הדרישה מגבילה את היקף, תחולת, משך ואינטנסיביות התגובה ההגנתית, למה שנדרש כדי להפסיק את ההתקפה, ולא מעבר לכך[235]. יובהר, כי המידתיות אין משמעותה שעל התגובה להיות בסוג כוח זהה לזה בו נעשה שימוש ב'התקפה המזוינת'. ההגבלה היא להיקף הנדרש לאיון ההתקפה, להפסקתה, והדבר תלוי כמובן בהקשר ובנסיבות.

בהקשר הקיברנטי, מדינות רבות עושות שימוש בהגנה אקטיבית (Active Defense), אשר פוגעת, במקרה של התקפה, ברשתות המתקיפות ומשתקת את מקור ההתקפה. זוהי מעין התקפה קיברנטית נגדית, המבוצעת נגד המערכת של האויב, פוגעת ומנטרלת אותה בטרם תגרום נזק נוסף או תיזום התקפות נוספות בעתיד[236]. מערכת כזו יכולה לפעול באופן אוטומטי או בהפעלה ידנית[237]. ארצות הברית, למשל, הצהירה בגלוי שהיא מפעילה 'הגנה אקטיבית קיברנטית'[238]. גורמים אמריקנים הצביעו על יתרון במערכת כזו - פעולתה המיועדת לשיתוק ההתקפה, מבטיחה, כביכול, את עמידתה בדרישת המידתיות[239].

---

[234] שם.

[235] מדריך טאלין, 62-63.

[236] הגנה אקטיבית משמעה: "electronic countermeasures designed to strike attacking computer systems and shut down cyber-attack midstream". ראו: Carr, 2011, 46.

[237] להרחבה, ראו: Hinkle, 2012, 19-20.

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

[239] Hinkle, 2012, 20.

השימוש ב׳הגנה אקטיבית קיברנטית׳ אינו נטול בעיות, וזאת ניתן להדגים בהקשר של ההתקפה על אסטוניה. מערכת הגנה אקטיבית אסטונית עשויה הייתה להגיב בהתקפות DDoS הדדיות נגד המחשבים שפעלו מול אסטוניה, ובכלל זה נגד רשתות מחשב רוסיות. הקושי הוא שהתקפה נגדית כזו נגד תשתית קיברנטית של מדינה כמו רוסיה, עלולה לגרום נזק רחב מאד, שהיקפו בלתי צפוי[240]. חוסר המידתיות הפוטנציאלי של התגובה עלול לנבוע מכך שמדינה בעלת תשתית קיברנטית מצומצמת, פועלת מול מעצמת ענק. במקרה כזה, קיים סיכוי שעצם התגובה האסטונית תתפרש כ׳התקפה מזוינת׳, ותוביל לתגובה צבאית רוסית. זו בגדר דוגמה לאתגר היישום של עיקרון המידתיות במרחב רגיש זה.

לבסוף, צוין כי דרישת המידתיות אינה מגבילה את סוג הכוח המופעל בהגנה עצמית לאותו סוג כוח, באמצעותו בוצעה ההתקפה. כך, כאשר מבוצעת נגד מדינה התקפה במרחב הקיברנטי, והיא נטולת כלים קיברנטיים להפסיקה, אין היא ממצה בכך את דרכי הפעולה הפרושות בפניה. ביכולתה, למשל, להפעיל אמצעים קינטיים במסגרת ההגנה העצמית, במטרה לכפות על התוקף להפסיק את ההתקפה במרחב הקיברנטי, כל עוד הללו עומדים בדרישות המידתיות והצורך.

׳הדין הקיים׳ ביחס להגדרת ׳התקפה מזוינת׳ במרחב הקיברנטי - סיכום קצר

הצבעה על הדין הקיים ביחס להגדרת ׳התקפה מזוינת׳ במרחב הקיברנטי, המאפשרת הגנה עצמית על דרך של ׳שימוש בכוח׳, מעלה אתגרים דומים מאד לאלו שהוצגו ביחס לאיתור הדין הקיים בנושא ׳שימוש בכוח׳.

ראשית, הכתיבה בעניין ׳התקפה מזוינת׳ קיברנטית היא תיאורטית, הואיל ובראי הפרקטיקה של מדינות, אין עוד מקרה בו מדינה טענה

[240] שם. לדוגמה שיתוק שירותי החירום ברוסיה לשעה, כפי שאירע באסטוניה, עלול להתבטא בקורבנות רבים.

שנפלה קורבן להתקפה כזו. המומחים שניסחו את מדריך טאלין, סברו למשל, כי ההתקפות על אסטוניה וגיאורגיה לא הגיעו לכדי 'התקפה מזוינת'. מרבית המומחים סברו כי ההתקפה באמצעות וירוס Stuxnet, שבוצעה נגד צנטריפוגות בכור באיראן בשנת 2010, הגיעה לכאורה לכדי 'התקפה מזוינת' (אלא אם הייתה לה הצדקה בפני עצמה כהגנה עצמית מקדימה).[241] בהיעדר פרקטיקה של מדינות, קשה להצביע על פרשנות מסוימת כמשקפת את המשפט הקיים בתחום הקיברנטי. יש גם לזכור, כי טרם פסק בנושא טריבונל בינלאומי.

שנית, אכן האסכולה שמוביל שמיט, הבאה לביטוי בניסוח מדריך טאלין, מייצגת פרשנות דומיננטית של הדין הקיים, והיא אומצה על ידי רבים.[242] עם זאת, בהקשר של 'התקפה מזוינת', קיימת מחלוקת בין מנסחי המדריך, ביחס לפעולות קיברנטיות שאינן גורמות נזק פיזי לאדם או לרכוש, האם לראות בהן 'התקפה מזוינת'. בנוסף, גישת ממשלת ארצות הברית אינה מכירה בדרישה, המופיעה במדריך טאלין, כי לפעולה הקיברנטית יהיו 'Scale and Effect' כתנאי להיותה 'התקפה מזוינת'. עיקרו של דבר, ניתן להצביע על קונצנזוס מערבי רק ביחס לכך שפעולות קיברנטיות עשויות להוות 'התקפה מזוינת', כאשר הן צפויות לגרום נזק פיזי לאדם או לרכוש. נוסחה כזו מאזנת בין היכולת של מדינה להגיב לאותן התקפות קיברנטיות, שהן אנלוגיות להתקפות קינטיות חמורות, לבין הרצון למנוע שימוש תכוף מדי באמצעים כוחניים, שלא יתיישב עם רציונל מגילת האו"ם.[243] האיזון הזה מבטא את התפיסה הרווחת, לפחות במערב.

שלישית, מבלי לחזור על דברים שכבר נכתבו, הגישה האמריקנית או המערבית רחוקה מאד מתפיסתן של המעצמות הקיברנטיות במזרח, סין ורוסיה. הללו מונחות על ידי סדר עדיפויות שונה וראייה אסטרטגית אחרת, ואינן צפויות להביע הסכמה לזווית הראייה

---

[241] מדריך טאלין, 58.

[242] ראו למשל Jensen, 2002, המציע ניתוח דומה ביחס לראיית 'התקפה מזוינת'.

[243] Hathaway, 2012 ; 848.

המערבית. הבדלי הגישות האסטרטגיים הללו עשויים (או עלולים) להוביל לעיכוב ביצירת משפט בינלאומי מנהגי בתחום הקיברנטי, ולהשפיע על תוכנו, אשר לא ישקף בהכרח את ההשקפה המערבית.

ההגנה הטובה היא ההתקפה?

הגנה עצמית מקדימה במרחב הקיברנטי

העיקרון של הגנה עצמית מקדימה (Preemptive or Anticipatory Self-Defence) משמעותו שמדינה אינה חייבת להמתין בחיבוק ידיים להתקפת האויב, שעה שברור, כי היא אכן עומדת להיות מותקפת בכוח מזוין. עיקרון זה נולד עוד בטרם נוסחה מגילת האו״ם[244].

סעיף 51 למגילת האו״ם מתייחס, כלשונו, למצבים בהם כבר בוצעה ׳התקפה מזוינת׳ נגד מדינה, ולכאורה אינו מאפשר הגנה עצמית טרם ביצוע ההתקפה. עם זאת, הפרשנות המקובלת היא שמדינה יכולה להגן על עצמה, שעה שההתקפה נגדה היא Imminent[245], באופן לגיטימי כהגנה עצמית מקדימה. אמנם, לאורך השנים היו דעות, שסייגו את החוקיות של הגנה עצמית מקדימה[246], אך הן פחות מקובלות.

מדינת ישראל ׳תרמה׳ לא מעט לעיסוק הקהילה הבינלאומית בסוגיית ההגנה המקדימה. כך, במלחמת ששת הימים הייתה ישראל הראשונה שהפעילה כוח (הגם שטענה כי היא פועלת מתוך הגנה עצמית ׳רגילה׳, ולא מקדימה, בתגובה לאירועים קודמים שאיימו על ביטחון ישראל). באותו מקרה, נמנעה הקהילה המשפטית הבינלאומית מגינוי פעילותה של ישראל. בשנת 1981, בעקבות הפצצת הכור הגרעיני בעיראק על ידי

---

[244] סייבל, 2010 ; 508 (לעניין זה מצוטט Bowett).

[245] הגדרת הדרישה נוסחה כבר במאה ה-19 על ידי מזכיר המדינה האמריקני, Webster, בפרשת Caroline. ההגדרה אוזכרה פעמים רבות מאז, לדוגמה במשפטי נירנברג. International Military Tribunal (Nuremberg), Judgment and Sentences, Oct. 1, 1946 reprinted in 41 Am. J. Int'l L. 172, 205 (1947).

[246] לדוגמה, דעה שזו מותרת רק כשההתקפה כבר יצאה לדרכה אך טרם הגיעה ליעדה. להרחבה: Dinstein, 2011 ; 203-204.

ישראל, התקיים דיון במועצת הביטחון בשאלת הזכות להגנה עצמית מקדימה[247].

לאחר התקפות הטרור מיום 11 בספטמבר 2001, התעורר מחדש הדיון בנושא, בהובלת ארצות הברית, שפתחה במבצע צבאי רחב היקף למיגור הטרור באפגניסטן. ארצות הברית הצדיקה את המבצע בהגנה עצמית מקדימה - הצורך להרתיע מפני ביצוע התקפות טרור חוזרות[248]. בריטניה הציגה עמדה דומה והצטרפה למבצע[249]. במישור המשפטי, ניתן לומר שארצות הברית אימצה תפיסה חדשה, לפיה, ככל שהסכנה מפעולות האויב גדולה יותר, כך מתחזקים הצורך בנקיטת צעדים מקדימים והלגיטימיות שלהם, גם אם קיים חוסר ודאות לגבי העיתוי והמיקום המדויקים של התקפת האויב[250]. גישה זו אינה חותרת, בראייה האמריקנית, תחת הכלל המשפטי שמגדיר הגנה עצמית מקדימה, אלא ניתן לראות בה, לפחות לתפיסתם, יישום עדכני למציאות הלחימה המודרנית בטרור, בה ארגוני טרור פועלים באופן בלתי צפוי, בלי שקיים מידע מוקדם בדבר מקום ועיתוי פעילותם[251].

תופעת הטרור הבינלאומי, כמו גם התפתחויות טכנולוגיות, לרבות השימוש בכלי נשק ארוכי טווח ויכולות השמדה המונית, משנות את כללי המשחק ומחדדות את מורכבות סוגיית ההגנה העצמית המקדימה. מרחק גיאוגרפי, גבולות מדיניים, זמני היערכות, מידע מודיעיני מקדים - כל אלו קיבלו משמעות חדשה, שעיקרה צמצום חלון ההזדמנויות, הפתוח בפני מדינות לפעול על מנת לסכל התקפה משמעותית נגדן. המרחב הקיברנטי מעצים מגמה זו.

---

[247] סייבל, 2010 ; 509.

[248] להרחבה ראו O'connell, 2002. הכותבת מותחת ביקורת על הצדקה זו.

[249] ראו: Gray, 2003 ; 603-605.

[250] The White House, The National Security Strategy of the United States of America 15 (2002).

[251] ועדיין, תפיסה מרחיבה זו שנויה במחלוקת, ראו למשל: Dinniss, 2012 ; 91-93.

כאמור, הגנה עצמית מקדימה עוררה מחלוקות ודיון ער לאורך השנים [252]. כשם שהתקפות הטרור שינו את תפיסת ארצות הברית והקהילה הבינלאומית ביחס להגנה עצמית מקדימה, המרחב הקיברנטי מציב אף הוא אתגרים ביחס לתפיסות הקיימות. בדומה להתקפות טרור, גם במרחב הקיברנטי מבוצעות התקפות ללא הודעה מוקדמת וללא סימנים מעידים שהאיום קרוב. הזמן החולף בין שיגור ההתקפה לבין תוצאותיה עלול להיות קצר מאד, ומספר הנפגעים מהשלכות ההתקפה, עלול להיות רב מאד. בדומה למאבק בטרור, גם בהקשר הקיברנטי, נראה, כי שאלת המפתח היא: כיצד להבטיח את יכולתה של מדינה להגן על עצמה, בכלים המשפטיים הקיימים? [253].

העמדה האמריקנית הרשמית [254], כמו גם עמדת מנסחי מדריך טאלין, מכירה באפשרות של הגנה עצמית מקדימה במרחב הקיברנטי. העיקרון בא לביטוי, למשל, בכלל מספר 15 במדריך טאלין, לפיו: הזכות לשימוש בכוח כהגנה עצמית חלה אם התקפה קיברנטית מתרחשת או שהיא מיידית (Imminent). הדבר כפוף לדרישת המיידיות (Immediacy) [255].

שמיט ומרבית המומחים, שניסחו את מדריך טאלין, מיישבים בין התפיסה המסורתית של הגנה עצמית מקדימה לבין מציאות הלחימה המודרנית, באמצעות הקביעה שניתן לנקוט הגנה עצמית מקדימה, כאשר התוקף נחוש בבירור לבצע התקפה מזוינת, והמדינה המותקפת תאבד את ההזדמנות להגן על עצמה באופן אפקטיבי, אם לא תפעל מיד [256]. זהו מבחן דומה למבחן שאומץ בהקשרים אחרים, הבוחן מתי עומד להיסגר חלון ההזדמנויות לפעול נגד האיום (הסטנדרט - Last

---

[252] להרחבה: Gill, 2007.

[253] Schmitt, 2011; 593.

[254] נאום Koh, 4.

[255] מדריך טאלין, 63. דרישה זו נועדה להפריד בין פעולה של הגנה עצמית לבין פעולת תגמול, retaliation, והיא מתייחסת לפרק הזמן שלאחר ההתקפה המזוינת, בו מדינה יכולה עדיין להגיב בכוח. נדרשת סמיכות זמנים, בהתחשב בנתונים כמו משך הזמן הנדרש לזהות את התוקף ולהכין את התגובה.

[256] ראו: Schmitt, 2008; 16-19.

feasible window of opportunity)[257]. כלומר, המבחן אינו בהכרח סמיכות הזמנים בין ההגנה המקדימה לבין ההתקפה הצפויה, אלא עד מתי תוכל מדינה להגן על עצמה באפקטיביות מפני ההתקפה הצפויה[258].

כאשר נבחנת הגנה עצמית מקדימה במרחב הקיברנטי, חשוב להבחין בין צעדים מכינים (Preparatory Actions) לבין כאלה שמהווים שלב תחילתי של 'התקפה מזוינת'[259]. נקיטת צעדים, המקנים יכולת למדינה לבצע תקיפה עתידית במרחב הקיברנטי נגד מדינה אחרת, אינה מספיקה כדי להצדיק הגנה עצמית מולה. נניח שמדינה מחדירה תוכנה זדונית למערכת המחשבים של מדינה אחרת, אותה ניתן יהיה להפעיל מרחוק, למשל לצורך תקיפה קיברנטית עתידית. האם הדבר מאפשר הגנה מקדימה כתגובה? התשובה היא שלילית, שכן דרישת המיידיות אינה מתקיימת. רק כאשר ליכולת מצטרפות כוונות - החלטה לבצע 'התקפה מזוינת' באמצעות הפעלת אותה תוכנה זדונית, אז מתקיימת דרישת המיידיות, וניתן לשקול הגנה מקדימה. מאחר שיכולות תקיפה קיברנטיות הן זמינות וקלות להשגה, הצבעה על כוונות היריב לתקוף היא הדרישה המשמעותית כתנאי מקדים לפני פעולות הגנה מקדימה[260].

למעשה, ניתן לתאר את המבחן המשפטי כצורך בהתקיימות שלושה תנאים: מסקנה סבירה, שאכן צפויה התקפה קיברנטית; התוצאות הצפויות של ההתקפה מקבילות לאלו הנגרמות על ידי 'התקפה מזוינת' קינטית; והצורך בפעולה מיידית כדי להתגונן, לפני שייסגר חלון ההזדמנויות לפעולה[261].

---

[257] ראו: Schmitt, 2010; 166.
[258] מדריך טאלין, 64.
[259] שם, 65.
[260] Schmitt, 2012 (2); 24.
[261] Schmitt, 2011; 593.

במישור הפרקטי, היכולת להעריך שהתקפה קיברנטית היא מיידית, ולפעול בהגנה מקדימה, היא, בלשון המעטה, מאתגרת מאד[262]. לעתים, למשל, קשה מאד לזהות את כוונת הפעולה. כך לדוגמה, חדירה למערכת המחשבים של מערך הגנה אווירית, עשויה להיות הכנה לשיתוק המערכת לקראת תקיפה צבאית או איסוף מודיעין ותו לא. באופן דומה, קשה להעריך את התוצאות, שינבעו מפעולה קיברנטית (בפרט במעגלים שאינם ישירים[263]) והאם הן מקבילות ל׳התקפה מזוינת׳, ואף קשה לקבוע את לוחות הזמנים בהם יוותר ׳חלון ההזדמנויות׳ פתוח. לבסוף, קשה מאד לייחס, באופן מבוסס, פעולה קיברנטית לגורם מסוים (Attribution).

קשיים אלו מחדדים את השאלה, מהי רמת הוודאות הנדרשת ממדינה כתנאי לביצוע צעדי הגנה עצמית מקדימה? ככלל, כאשר מדינה מכריזה שהיא פועלת מתוך הגנה עצמית, נטל ההוכחה הוא עליה[264]. על המדינה להציג ראיות, הן ביחס להגנה עצמית, לאחר שהיא הותקפה (ביחס למקור ואופי ההתקפה), וקל וחומר במקרה של הגנה עצמית מקדימה (ביחס ליכולת וכוונות היריב וביחס לחלון ההזדמנויות שעמד להיסגר)[265].

ביחס להצגת ראיות לגבי זהות הגורם התוקף, הציע שמיט נוסחה, לפיה המידע בדבר זהות התוקף יהיה ׳Clear and Compelling׳[266]. זהו מעין מדד ראייתי, שניתן לתארו כמצוי בין הרמה הראייתית, הנדרשת במשפט פלילי, לבין זו הנדרשת בהליך אזרחי. מבלי להיכנס לניתוח מבחן זה, נראה כי קשה להצביע על סטנדרט ראייתי חד משמעי. במשפט הבינלאומי המנהגי הקיים[267].

---

[262] ראו: Jensen, 2002; 223-239.

[263] להרחבה: Elliot, 2009; 21, 24.

[264] Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 189 (Nov. 6). להלן: פרשת אסדות הנפט.

[265] Schmit, 2011; 596.

[266] שם, 594-595.

[267] שם, 594.

'התקפה מזוינת' במרחב הקיברנטי על ידי גורם שאינו מדינתי

הגנה עצמית מול ארגון טרור

הדיון עד כה הוקדש ל'התקפה מזוינת', המבוצעת בידי מדינה אחת נגד מדינה אחרת. ואכן, העמדה המסורתית של מומחי המשפט בינלאומי הייתה, כי סעיף 51 למגילת האו"ם, המעגן את זכות ההגנה העצמית בתגובה ל'התקפה מזוינת', חל אך ורק על יחסים בין מדינות[268]. פעולות אלימות נגד מדינות מצד גורמים שאינם מדינתיים (בהנחה שלא ניתן לייחס אותן למדינה מסוימת), כמו קבוצות מזוינות וארגוני טרור, נותרו, לפי תפיסה זו, במסגרת הפרדיגמה של המשפט הפלילי ומחוץ למשטר המשפטי של מגילת האו"ם.

השינוי המשמעותי בתפיסה הוא תוצאה של אירועים טרגיים - התקפות הטרור שבוצעו על ידי אל קאעדה ביום ה-11 בספטמבר 2001, אשר המחישו את עוצמתם הקטלנית של ארגוני הטרור הבינלאומיים. ארגונים שפיתחו עוצמה ויכולת להפעיל כוח הרסני, שבעבר היו שמורות למדינות בלבד. התקפות הטרור התקבלו בקהילה הבינלאומית כ'התקפה מזוינת', המאפשרת להגיב עליה בשימוש בכוח. החלטות רבות ברוח זו אומצו על ידי מועצת הביטחון של האו"ם, לרבות שתי החלטות שהתקבלו בקונצנזוס ימים ספורים לאחר ההתקפות[269]. ארצות הברית, נאט"ו, מדינות וארגונים רבים נקטו גישה זו[270]. הן מועצת הביטחון של האו"ם והן נאט"ו השתמשו במונחי הגנה עצמית, השאובים ממגילת האו"ם, לתיאור ההתמודדות עם התקפות הטרור[271]. אף לא מדינה אחת התנגדה לכך. כפי שציין היועץ המשפטי

---

[268] ראו למשל: Brownlie, 2008; 57-58.

[269] ראו: S.C. Res. 1373, U.N. DOC. S/RES/1373 (Sept. 28, 2001); S.C. Res. 1368, U.N. DOC. S/RES/1368 (Sept. 11, 2001).

[270] להרחבה והפניות: Schmitt, 2011; 600. יש לציין שנאט"ו הפעיל את סעיף 5 לחוקתו, שמשמעותו שבוצעה התקפה נגד כל חברות הארגון.

[271] Watts, 2011; 65.

של משרד החוץ האמריקני, לא התעורר כל קושי לבסס את הטענה בדבר הזכות להשתמש בכוח כהגנה עצמית נגד אל קאעדה[272].

היחס להתקפות הטרור של אל קאעדה כ׳התקפה מזוינת׳ לא היה מקרה חריג וחד פעמי בהיסטוריה של המאבק בטרור. גם מלחמת לבנון השנייה, אליה יצאה ישראל בשנת 2006, כתגובה לטרור מצד ארגון החיזבאללה, התקבלה במידה רבה על ידי הקהילה הבינלאומית כהגנה עצמית לגיטימית נגד ׳התקפה מזוינת׳ מצד שחקן שאינו מדינתי[273]. אף תורכיה מעלה, באופן עקבי את זכותה לפעול בהגנה עצמית נגד קבוצות טרור כורדיות, הפועלות לטענתה משטח צפון עיראק. לבסוף, מועצת הביטחון של האו״ם התירה, בשנת 2008, שימוש בכוח נגד פיראטים, אשר נמלטו באופן קבוע לשטחה הריבוני של סומליה[274].

יש לציין, שפרשנות רחבה זו אינה מנותקת מלשון מגילת האו״ם. בניגוד לסעיף 2(4) למגילת האו״ם, המתייחס במפורש לשימוש בכוח מצד מדינות, סעיף 51 שעניינו הגנה עצמית, אינו כולל קביעה דומה ביחס ל׳התקפה מזוינת׳ (מהנוסח ברור למדי, שהגנה עצמית עצמה מסורה רק למדינות).

דווקא בית הדין הבינלאומי בהאג מיאן להשלים עם שינוי התפיסה, בשני מקרים שהובאו בפניו, בעניין גדר הביטחון שהקימה ישראל[275] ובעניין קונגו[276]. בית הדין נמנע מלהביע הסכמה לרעיון ש׳התקפה מזוינת׳ עשויה להתבצע מצד גורם שאינו מדינתי ולאפשר הגנה עצמית במקרה כזה. לדוגמה, ביחס לטענה של ישראל, כי גדר הביטחון הוקמה בהתאם לזכות ההגנה העצמית בסעיף 51 למגילת האו״ם, קבע בית

---

[272] שם.

[273] להרחבה: Schmitt, 2008 (2).

[274] סייבל, 2010; 506.

[275] Legal Consequences of the Construction of the wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9) (להלן - פרשת החומה).

[276] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, 160 (Dec. 19). גם במקרה זה בית הדין התעלם מניתוח הסוגיה המתבקשת של עצם הפעלת זכות ההגנה העצמית נגד שחקן שאינו מדינתי. פסק הדין נתקל בביקורת על החמצת ההזדמנות לחדד נושא חשוב זה.

הדין, בדעת הרוב, כי לסעיף 51 אין רלבנטיות ביחסים עם גורם שאינו מדינתי, כמו הרשות הפלסטינית[277]. בית הדין הבינלאומי לא נימק באופן מהותי את קביעתו, והתעלם מדברי המיעוט של השופט היגינס, לפיהם לשון סעיף 51 אינה מוגבלת למדינות[278]. בית הדין אף התעלם מפרקטיקה של מדינות, שהצביעה על פרשנות הפוכה[279], ומכך שמועצת הביטחון כבר הכירה ב'התקפה מזוינת' מצד גורמי טרור. חוות הדעת של בית הדין נתקלה בביקורת רבה בקרב הקהילה המשפטית הבינלאומית ונותרה שנויה במחלוקת, בלשון המעטה[280].

הססנות בית הדין הבינלאומי מובנת לאור החשש מההשלכות של שינוי התפיסה, ומניצול הפרשנות המרחיבה לרעה על ידי מדינות. מדינות עלולות להשתמש באמצעים צבאיים מרחיקי לכת נגד גופים שאינם מדינתיים, תוך העדפת כלים מתחום ההגנה העצמית על פני כלים מתחום אכיפת החוק. עם זאת, ממול עומדת עמדה חזקה למדי של מדינות, ובראשן ארצות הברית[281], הדורשות להכיר בצורך של מדינות להתגונן בפני הטרור העולמי בכלים אפקטיביים, ותובעת בהתאם את מימוש זכות ההגנה עצמית לשם כך[282].

כתוצאה מכך, נוצר פער הולך ומתרחב בין לשון מגילת האו"ם וכוונת מנסחיה, לצד פסיקת בית הדין הבינלאומי, לבין הפרקטיקה של מדינות והחלטות מועצת הביטחון של האו"ם וארגון נאט"ו[283]. הכף נוטה לטובתם של האחרונים. עם הזמן, מתייצבת פרשנות משפטית, הנותנת הד לפרקטיקה של מדינות ומכירה באפשרות של הגנה עצמית נגד גופים שאינם מדינתיים. זאת, מתוך הבנה שעל המשפט הבינלאומי

---

[277] פרשת החומה, 139.

[278] שם, 33 (דעתו הנפרדת של השופט היגינס).

[279] ראו: Gray, 2008; 136.

[280] לדוגמה מני רבות: Pomerance, 2005.

[281] ראו למשל: Banks, 2013; 173.

[282] ראו לדוגמה: Paust, 2010; 238-239. לדבריו, רוב הכותבים מסכימים שהתקפה מזוינת על ידי גורם שאינו מדינתי נגד מדינה, יכולה להפעיל את זכות ההגנה העצמית, גם אם חלק מהכוח התגובתי מופעל במדינה זרה.

[283] Watts, 2011; 66.

לאפשר למדינות, הנופלות קורבן להתקפה, להגן על עצמן. למגמה זו משמעויות גם לעניין המשטר המשפטי במרחב הקיברנטי.

'התקפה מזוינת' במרחב הקיברנטי על ידי גורם שאינו מדינתי

בשנים האחרונות הולך וגובר החשש מהאפשרות, שארגוני טרור בינלאומיים וגופים שאינם מדינתיים ינצלו את המרחב הקיברנטי להתקפה על מדינות. חשש זה כבר הובע בצורה מפורשת על ידי ממשלת ארצות הברית ועל ידי ארגון נאט"ו[284]. כך לדוגמה, במחשב של ארגון אל קאעדה שנתפס, נמצאו תכניות של סכרים (מטרה אטרקטיבית להתקפה קיברנטית) ותכניות מחשב הדרושות לניתוח של אותם סכרים ודרכי פעולה לפגיעה בהם[285].

ההססנות, שהפגין בית הדין הבינלאומי בעניין הגנה עצמית מול גורם שאינו מדינתי בהקשר של הטרור העולמי, רלבנטית בהחלט גם בתחום הקיברנטי. במרחב הקיברנטי פועלים גורמים רבים מאד, שאינם מדינתיים, ומתן אפשרות למדינות לפעול נגדם בכלים של הגנה עצמית, עשויה להיות מאד משמעותית לעניין היקף השימוש בכוח בזירה העולמית[286].

התפיסה המערבית, המובלת על ידי ארצות הברית, מכירה בזכותן של מדינות לפעול בהגנה עצמית, נגד גורם שאינו מדינתי, גם במרחב הקיברנטי[287]. בדומה לכך, רוב מנסחי מדריך טאלין סברו שהפרקטיקה של מדינות, לאחר התקפות הטרור של ה-11 בספטמבר 2001, מבססת את הזכות להגנה עצמית בעקבות 'התקפה מזוינת' של גורם שאינו מדינתי, כמו ארגון טרור או קבוצת מורדים. זכות זו יכולה להתממש, למשל, בעקבות פעולה קיברנטית מזוינת, שמבצע ארגון טרור או אף תאגיד פרטי, הממוקם במדינה אחת, נגד מדינה אחרת,

---

[284] ראו: Scmitt, 2011; 600.

[285] ראו: Clay, 2003; 11-13.

[286] Schmitt, 2011; 601.

[287] Schmitt, 2012 (2); 24.

המגיעה לכדי 'התקפה מזוינת'[288]. עוד סברו מרבית מנסחי המדריך, כי תנאי למימוש זכות ההגנה העצמית הוא שההתקפה בוצעה על ידי קבוצה מאורגנת, להבדיל מבודדים, וכאמור, גרמה לתוצאות השקולות לאלו של 'התקפה מזוינת' קינטית[289].

ההרחבה של זכות ההגנה העצמית במרחב הקיברנטי גם ביחס לגורם שאינו מדינתי, עלולה לכאורה להוביל לשימוש נרחב בכוח. ארגוני טרור, למשל, יכולים לרכוש בקלות יחסית יכולות וכלים קיברנטיים, ומוטיבציה לפגוע במדינות - אינה חסרה. בראייתי, מבחינה משפטית, ההרחבה היא במקומה, שכן עלול בהחלט להתפתח תרחיש, שבו מדינה תידרש לשימוש בכוח כתגובה לפעולה קיברנטית של ארגון טרור. עם זאת, נכון להיום, החסם העיקרי בפני התפתחות כזו הוא בדרישה שההתקפה הקיברנטית תוביל לתוצאה של גרימת נזק פיזי לאדם או לרכוש, כתנאי להגדרתה כ'התקפה מזוינת'. גרימת תוצאות כאלה בדרך קיברנטית אינה פשוטה, לפחות במצב הטכנולוגי הנוכחי[290].

[288] מדריך טאלין, 58.
[289] מדריך טאלין, 59-60.
[290] Schmitt, 2011 ; 602.

דיני המלחמה במרחב הקיברנטי

דיני המלחמה ותחולתם במרחב הקיברנטי

רקע - דיני המלחמה ו'סכסוך מזוין'

דיני המלחמה (Laws of War - או בשמותיהם הנוספים: Jus in Bello, Laws of Armed Conflict, International Humanitarian Law) הוא הענף המשפטי החל בעת סכסוך מזוין. דינים אלו מסדירים את התנהגות הצדדים במהלך סכסוך מזוין, ללא קשר לשאלה, האם עצם קיום הסכסוך הוא חוקי לפי המשפט הבינלאומי.

לדיני המלחמה שורשים היסטוריים. כך למשל, רעיונות האבירות בימי הביניים באירופה, שסיפקו ריסון מסוים בפני אכזריות הקרב. במאה ה-17, נכתב לראשונה קוד משפטי סדור בנושא מלחמה ושלום על ידי Hugo Grotius. התפתחות הדין המודרני החלה במלחמת האזרחים האמריקנית[291], בין השאר בעקבות הכניסה למערכה של כלי נשק חדשים וקטלניים - ספינות חמושות, צוללות, מוקשים יבשתיים, מכונות ירייה, קליעים מתפוצצים ועוד[292]. למעשה, במלחמה זו שידר לראשונה מפקד צבא הצפון, הנשיא אברהם לינקולן, פקודות למפקדיו בשטח באמצעות הטלגרף. הכנסת אמצעי תקשורת ארוכי טווח לשדה הקרב היא, במובנים מסוימים, לידתה של ההתפתחות הקיברנטית-צבאית, בה עוסקת עבודה זו[293].

במהלך מלחמת האזרחים, בשנת 1864, נוסח Lieber Code, אליו נוהגים להתייחס כקודיפיקציה הראשונה של דיני המלחמה. הנשיא אברהם לינקולן אימץ את הקוד והפיץ אותו כפקודה כללית מספר 100 לצבא האיחוד בזמן המלחמה[294]. בשנת 1863 נוסד ארגון הצלב האדום הבינלאומי ושנה לאחר מכן, בשנת 1864, נוסחה אמנת ז'נבה בדבר טיפול בפצועים. בהמשך, לאורך יתר המאה ה-19 והמאה העשרים,

---

[291] Hughes, 2009; 2-3.

[292] שם.

[293] שם, 6.

[294] Antolin-Jenkins, 2005; 147.

נוסחו האמנות המרכזיות בתחום דיני המלחמה, בעקבות זוועות המלחמות, היקף הקורבנות וההתפתחויות הטכנולוגיות. בין השאר, נוסחו כללי האג משנת 1899 ו-1907; לאחר מלחמת העולם השנייה, בשנת 1949, נערכו מספר אמנות לקובץ הנקרא אמנות ז'נבה; בשנת 1954 נוסחה אמנת האג בדבר הגנה על נכסי תרבות; ובשנת 1977 נוסחו שני פרוטוקולים נוספים לאמנות ז'נבה. הראשון עניינו הגנה על קורבנות בסכסוכים בינלאומיים; והשני מתייחס לכללים הומניטריים (מתחום דיני המלחמה), אשר יחולו גם על סכסוכים שאינם בינלאומיים, כגון מלחמת אזרחים.

דיני המלחמה הם תחום דינמי ומתפתח. עליהם להגיב למציאות, המשתנה בשדה הקרב המודרני בקצב מהיר. כך היה בראשית המאה העשרים ואחת, לנוכח התפתחות תופעת הטרור הבינלאומי והשינוי בכללי המשחק, שנבע מפעילותם של ארגוני הטרור. כך תהיה ההתמודדות של דיני המלחמה עם ההתפתחויות במרחב הקיברנטי. על דיני המלחמה להתאים עצמם למלחמות של המחר, אשר עשויות להתנהל בלחיצת כפתור. התמודדות זו מצויה בחיתוליה. טרם ניתן לגבש תמונה ברורה של הכיוונים, אליהם צועד המשפט הבינלאומי בעולם הקיברנטי[295]. מטרת העבודה, בהקשר זה, היא לפזר מעט את הערפל.

דיני המלחמה חלים בהתקיים **סכסוך מזוין** (Armed Conflict). מכאן, נובעת חשיבותו של המונח 'סכסוך מזוין' כ-Legal Term of Art[296], כלומר מונח מפתח, המהווה שער כניסה למכלול שלם של כללים - דיני המלחמה. בהיעדרו, אין תחולה לדיני המלחמה, אלא חלים כללים אחרים, למשל מתחום הדין הפנימי ודיני זכויות האדם.

המונח 'סכסוך מזוין' קנה אחיזה במסגרת הנוסח של אמנות ז'נבה משנת 1949, ובכך החליף למעשה מונח בו נעשה שימוש בעבר -

[295] Hughes, 2009; 5.

[296] Schmitt, 2012; 285.

'מלחמה'. המשפט הבינלאומי אינו מגדיר במדויק מהו סכסוך מזוין. תחת זאת, הוא נוקב בשני סוגי הסכסוכים האפשריים: סכסוך מזוין בינלאומי וסכסוך מזוין שאינו בינלאומי[297].

סוגיית סיווגם של סכסוכים מזוינים היא מהמורכבות, שבהן עוסק המשפט הבינלאומי, וחלו בה התפתחויות רבות בעשורים האחרונים, בעיקר לאור תופעת הטרור העולמי, המונע על ידי שחקנים רבי עוצמה, שאינם בהכרח מדינתיים[298]. בארצות הברית ובישראל הנושא נדון בהרחבה בפסיקת בית המשפט העליון, תוך שאומצו כיוונים משפטיים שונים[299]. הקושי להתאים סכסוכים חדשים לאבחנות המסורתיות, אף הוליד קריאות לא מעטות ליצירת קטגוריה חדשה של סכסוך מזוין, לדוגמה "Transnational armed conflict"[300], שלא התקבלו על ידי הקהילה הבינלאומית. מטעמי קוצר היריעה, לא ניתן יהיה לעסוק בעבודה זו בהרחבה בסיווג של סכסוכים. אך פטור בלא כלום - אי אפשר, ועל כן יוצג אזכור תמציתי של סוגי הסכסוכים המזוינים בלבד.

סכסוך מזוין בינלאומי, ההתייחסות המקובלת אליו והמשקפת משפט בינלאומי מנהגי, מעוגנת בסעיף 2 המשותף לאמנות ז'נבה משנת 1949. זו כוללת שני אלמנטים עובדתיים מרכזיים - סכסוך בין מדינות (מרכיב ה-International) ופעולות איבה המגיעות לכדי סכסוך מזוין (מרכיב ה-Armed)[301].

הרכיב הבינלאומי מחייב שהפעולות שהובילו לסכסוך, תבוצענה על ידי מדינות או באמצעות פעילות של קבוצה מאורגנת או פרטים, הניתנת

---

[297] להרחבה בעניין סוגי סכסוכים, ראו Detter, 2000 ; 38-61.

[298] Schmitt, 2012(3) ; 246.

[299] שם (השוואה בין פסק הדין בעניין 'הסיכול הממוקד' בישראל ופסק הדין בעניין חמדאן בארצות הברית).

[300] ראו למשל: Corn Geoffrey, *Hamden, Lebanon and the Regulation of Armed Conflict*, 40 Vanderbilt Transnat'l L.J. (2006) 295. בנושא כתיבה ענפה נוספת, שלא זה המקום לפרטה.

[301] מדריך טאלין, 79.

לייחוס למדינה[302]. לעניין רכיב ה-Armed, נדרש שיתקיימו פעולות איבה (Hostilities) בין הצדדים לסכסוך.

סכסוך מזוין שאינו בינלאומי הוגדר במסגרת סעיף 3 המשותף לאמנות ז'נבה, המשקף משפט בינלאומי מנהגי. ההגדרה על דרך השלילה: סכסוך מזוין, שאינו בעל אופי בינלאומי, המתרחש בשטח של אחת המדינות שהן צד לאמנה[303]. למעשה, מדובר בסכסוך בין מדינה לבין קבוצה מזוינת מאורגנת או בין שתי קבוצות כאלו.

כדי שיתקיים סכסוך מזוין שאינו בינלאומי, נדרשת לפי הפסיקה (Case Law) אלימות ממושכת (Protracted Armed Violence) בין קבוצות מזוינות מאורגנות (Organized Armed Groups) בתוך מדינה. למעשה, אלו שני תנאים מצטברים: אינטנסיביות פעולות האיבה ומעורבות של קבוצות מזוינות מאורגנות[304].

האם דיני המלחמה חלים במרחב הקיברנטי?

כאשר נבחנים דיני המלחמה ביחס למרחב הקיברנטי, מתעוררת מיד שאלה מקדמית: האם מנסחי הדינים כיוונו לכך? שהרי, הללו נוסחו בצלן של מלחמות קונבנציונליות, בהן המחשב עשה, לכל היותר, את צעדיו הראשונים. העולם הקיברנטי לא היה חלק ממחשבתם של המושכים בעט כתיבת הדינים. לא בכדי אין בדיני המלחמה הקיימים, כללים קונקרטיים, המתייחסים בצורה מפורשת לפעילות קיברנטית.

---

[302] קיימת גם דעה, שבאה לביטוי בפסק הדין של בית המשפט העליון בישראל בנושא 'הסיכול הממוקד', לפיה יתכן סכסוך מזוין בינלאומי גם מול קבוצה מאורגנת, הפועלת באופן בינלאומי (חוצה גבולות), אף אם פעולותיה אינן ניתנות לייחוס למדינה מסוימת. דעה זו פחות מקובלת בקהילה הבינלאומית ולא יורחב לגביה. ראו: בג"ץ 769/02 הוועד הציבורי נגד עינויים בישראל נ' ממשלת ישראל, פ"ד נז (6) 285.

[303] מבלי להרחיב, הדעה המקובלת כיום היא שאין חובה שהסכסוך המזוין הבינלאומי יתקיים כולו בשטחה של מדינה אחת, ראו למשל: Hamdan v. Rumsfeld, 548 U.S. 557, 630-631 (2006). היעדר הגבלה זו חשוב במיוחד בהקשר הקיברנטי, שכן פעולות קיברנטיות אינן מוגבלות על ידי גבולות גיאוגרפיים.

[304] ראו למשל: Prosecutor v. Milosevic, Case No. IT-02-54-T, Decision on Motion for Judgement of Acquittal (Intl. Crim. Trib. For the Former Yugoslavia, June 16, 2004) para. 16 - 17.

כפי שגם עלה בפרקים קודמים, הדעה המקובלת בקרב כותבים במערב, ובארצות הברית בפרט, היא שדיני המלחמה חלים בזמן סכסוך מזוין גם על המרחב הקיברנטי[305], כפי שיחולו בכל מרחב וממד אחר ועל כל פעילות לחימה אחרת. זאת, הן במהלך סכסוך מזוין בינלאומי והן במהלך סכסוך מזוין שאינו בינלאומי. הדבר בא לביטוי גם בנוסח של מדריך טאלין, במסגרת כלל 20[306], וכן בעמדות ממשלת ארצות הברית[307].

בדומה להקשרים אחרים, גם בהקשר של יישום דיני המלחמה על המרחב הקיברנטי, העמדות של סין ורוסיה רחוקות מאלו המערביות. הגישה המערבית מכפיפה את המרחב הקיברנטי לדיני המלחמה, שעיקרם הצורך למנוע או לצמצם פגיעה פיזית באזרחים וגרימת נזק מיותר. לא קל להתחקות אחר הגישות של רוסיה וסין, בהקשר המשפטי, אך ניכר כי הן ממוקדות באינטרסים אחרים, למשל מניעת החשיפה של אזרחים למידע שמסכן, בראייתן, את הביטחון הלאומי ואת יציבות המשטר. רוסיה למשל, מוכנה להכיר בתחולת כללי המשפט הבינלאומי במרחב הקיברנטי, אך רואה הפצת מידע מזיק ולוחמה פסיכולוגית כפעולות לחימה וככלי נשק[308].

מעבר לפוליטיקה הבין מעצמתית, ראוי להכיר בכך שיישום דיני המלחמה על התקפות קיברנטיות היא מלאכה מורכבת, המלווה בקשיים פרקטיים של ממש, החל מעצם זיהוי ההתקפה: מי עומד מאחוריה, מה מטרתה ומה השפעתה; דרך ביצוע התקפות נגד ויישום עקרונות יסוד כמו אבחנה ומידתיות; וכלה במניעת גלישה של הסכסוך

---

[305] Schmitt, 2011 (2); 115.

[306] מדיך טאלין, 75.

[307] Schmitt, 2012 (2); 25.

[308] כך למשל, כפי שכבר צוין בפרק השני בעבודה, הדברים עולים מטיוטת אמנה שהציעה רוסיה בשנת 2011 בנושא ביטחון מידע בינלאומי, ובפרט מהגדרת ׳מלחמת מידע׳ בטיוטה.

למדינות שלישיות ולהפעלת כוח קינטית. מכל מקום, לפי הגישה המערבית, אין בקשיים אלו כדי לאיין את עצם התחולה של הדינים[309].

התקפות קיברנטיות במהלך סכסוך מזוין

דיני המלחמה חלים בהתקיים סכסוך מזוין, לרבות על פעולות קיברנטיות המבוצעות במהלך סכסוך מזוין. כך לדוגמה, יש המצביעים על כך שההתקפות הקיברנטיות, שבוצעו נגד גיאורגיה, היוו למעשה חלק (ולמעשה השלב הראשון) בסכסוך מזוין כולל שפרץ בין גיאורגיה לבין רוסיה[310]. סוגיית תחולת דיני המלחמה במקרה זה לא התחדדה, ולו משום שגיאורגיה לא הוכיחה את עמידת רוסיה מאחורי ההתקפות הקיברנטיות ולא טענה בתוקף למעורבות זו.

שאלה המתעוררת בהקשר זה היא, מהו סוג הקשר הנדרש בין הפעולות הקיברנטיות לבין הסכסוך המזוין? במילים אחרות, האם מספיקה לעניין זה סמיכות זמנים בין הסכסוך המזוין לבין ההתקפות או חפיפה בזמנים, אלא נדרש קשר נוסף ביניהם?

מנסחי מדריך טאלין היו חלוקים בדעותיהם בנושא. חלקם סבר, כי דיני הסכסוך המזוין יחולו על כל פעולה קיברנטית של צד אחד לסכסוך מזוין נגד צד אחר. אחרים סברו, כי דיני המלחמה יחולו אך ורק על פעולה קיברנטית שבוצעה על ידי צד אחד לסכסוך נגד הצד האחר, כתמיכה במאמץ המלחמתי[311]. את ההבדל בין הדעות ניתן להמחיש באמצעות הדוגמה הבאה: במהלך סכסוך מזוין, משרד המסחר של מדינה אחת יוזם התקפה קיברנטית נגד חברות פרטיות במדינה

---

[309] עוד יובהר, מבלי לפרט, כי כאשר דיני המלחמה אינם חלים, המשמעות אינה שההתקפות הקיברנטיות מתבצעות בוואקום משפטי, אלא קיימים עקרונות יסוד משפטיים, שעודם חלים, ובפרט Martens Clause. להרחבה ראו מדריך טאלין, עמ' 77-78.

[310] מדריך טאלין, 75-76.

[311] מדריך טאלין, 76.

האחרת, במטרה להשיג סודות בעלי ערך כלכלי. לפי הדעה הראשונה יחולו במצב זה דיני המלחמה. לפי הדעה השנייה, הדינים לא יחולו[312].

משמעות ה'התקפה' במהלך סכסוך מזוין

מושג ה'התקפה' (Attack) הוא מרכזי מאד בדיני המלחמה. התקפה היא 'שער הכניסה' למכלול רחב של הגבלות ואיסורים משפטיים, אשר חלים אך ורק כאשר היא מתקיימת. כך למשל, חל איסור על 'התקפה' המכוונת נגד מטרות אזרחיות[313], ועל 'התקפה' לעמוד בדרישת המידתיות[314]. 'התקפה' היא 'שומר הסף' - סף הכניסה לחלק משמעותי מעולמות התוכן, המסדירים את המותר והאסור במסגרת סכסוך מזוין[315].

כבר בפתח הדברים חשוב להדגיש, כי המונח 'התקפה' אינו זהה למונח אחר, שנדון קודם לכן בהקשר אחר (הקשר של דיני ה-Jus ad Bellum) - 'התקפה מזוינת'.

כאשר מבקשים להבין את משמעות המונח 'התקפה' בדיני המלחמה, ניתן להסתייע בסעיף 49 לפרוטוקול הראשון של אמנות ז'נבה (להלן - הפרוטוקול). בסעיף מוגדרת 'התקפה' כ- "Acts of violence against the adversary…". הגדרה זו מניחה את עיקר הכובד על פעולה שהיא 'אלימה'. פעולות שאינן אלימות, למשל לוחמה פסיכולוגית (פיזור כרוזים, שידור לאוכלוסיית האויב או פגיעה בשידורים במדינת האויב), לוחמה כלכלית וריגול, אינן בגדר 'התקפות'[316]. זאת, גם אם הפעולות הללו, למשל סנקציות כלכליות, גורמות נזק עצום למדינה נגדה הן

---

[312] שם.

[313] סעיף 52 לפרוטוקול הראשון של אמנות ז'נבה.

[314] כלל המידתיות (פרופורציונליות) קובע כי פגיעה אגבית באזרחים או במטרות אזרחיות לא תיחשב להפרת דיני המלחמה, כל עוד הפגיעה באזרחים או במטרה אזרחית היא ביחס סביר (מידתי) לתועלת הצבאית שבהתקפת המטרה הצבאית. סעיף 51(5) לפרוטוקול הראשון של אמנות ז'נבה.

[315] Schmitt, 2012 ; 285.

[316] שם, 289.

ננקטות.[317] דגש על כך ש'התקפה' היא פעולה צבאית בעלת רכיב של אלימות, מעוגן גם בפרשנות הרשמית של ארגון הצלב האדום לפרוטוקול.[318]

מתי פעולות הן 'אלימות'? בניגוד אולי לפרשנות האינטואיטיבית, אין הכרח שפעולות 'אלימות' תהיינה בעלות אפקט קינטי בדרך פעולתן. כך לדוגמה, השימוש בנשק כימי או ביולוגי אינו מחייב בהכרח הפעלה בדרך קינטית, אך קיימת הסכמה שהפעלת נשק כזה נגד מדינה, בכל צורה, תהיה 'התקפה'.[319]

לאור הכתיבה המשפטית, ביסוד ההוראות שמתייחסות ל'התקפה' עמד הרצון למנוע תוצאות אלימות מסוימות, שהקהילה הבינלאומית מיאנה להשלים עמן.[320] סעיפי הפרוטוקול מנוסחים אמנם באופן שהוא Act-based (מניעת התקפה אלימה, או המבוצעת באלימות), אך הם בעצם Consequence-based (מיועדים למנוע תוצאה אלימה של פגיעה באדם וברכוש[321]). במילים אחרות, כאשר לפעולה יש תוצאות 'אלימות', הרסניות, היא תיחשב 'התקפה'. מסקנה זו נתמכת בניסוחם של סעיפים רבים בפרוטוקול ובדברי הפרשנות הרשמיים לו מטעם ארגון הצלב האדום הבינלאומי.[322]

על רקע כללי זה, תיבחן כעת השאלה: באילו נסיבות, במהלך סכסוך מזוין, עשויה פעולה קיברנטית להיחשב 'התקפה', ולפיכך, להיות כפופה לאיסורים והגבלות רבים מתחום דיני המלחמה?

---

[317] Waxman, 2011; 422.

[318] ICRC, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, para. 1875

[319] ראו: Prosecutor v. Tadic, Case No. It-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia (ICTY), 2 October 1995, para. 120, 124.

[320] Schmitt, 2012; 290.

[321] שם.

[322] מדריך טאלין, 107. מנסחי המדריך ציינו גם את עיקרון ה-de minimis, כלומר נזק מזערי אינו מצדיק התייחסות לפעולה כ'התקפה'.

'התקפה' קיברנטית - במובן דיני המלחמה

כאמור, 'התקפה' כמשמעותה בדיני המלחמה, מחייבת מרכיב 'אלים' בתוצאה של הפעולה. מכאן, שהמונח אינו כולל פעולות כמו לחימה פסיכולוגית, לחימה כלכלית או ריגול, אף כשהללו מבוצעות באמצעים קיברנטיים או גורמות נזק כבד שאינו 'אלים'[323].

התקפות קיברנטיות אינן אלימות בדרך ביצוען, במובן של שחרור כוח קינטי, אך הן עלולות לגרום לתוצאה אלימה - מוות או פציעה של אנשים ונזק או הרס של רכוש[324]. כך לדוגמה, פעולה קיברנטית, שמטרתה לשבש פעילות של מערכת בקרה אווירית או לפרוץ סכר, שאוגר מים רבים בסביבה אזרחית. אין סיבה היגיונית להבחין בין התקפה קינטית על סכר לבין התקפה קיברנטית, אשר תגרום תוצאה זהה. בוודאי שמבחינת המדינה המותקפת, התוצאה חמורה מאד בשני המקרים.

בקרב כותבים משפטיים, בעיקר מארצות הברית, קיימת הסכמה רחבה למדי, שבאה לביטוי גם בכלל 30 במדריך טאלין, ולפיה - פעולות קיברנטיות, הגנתיות או התקפיות, שצפויות לגרום, באופן סביר, לפציעה[325] או מוות של אנשים או לנזק או הרס של רכוש, הן בגדר 'התקפות'. לעניין עצם ההגדרה כ'התקפה', אין זה משנה אם הפגיעה תיגרם לאזרחים או ללוחמים, לרכוש אזרחי או צבאי[326].

מה באשר למקרה, בו התוצאות של פעולה קיברנטית הן פחותות מפגיעה באנשים וברכוש? לא קיים בקרב הכותבים המשפטיים קונצנזוס, כי ניתן להתייחס למקרה כזה כ'התקפה'. כדי להבהיר את הדברים, יוצגו מספר תרחישים רלבנטיים.

---

[323] New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949, 289 (Bothe M. , Partsch K.J. & Solf W.A. eds., 1982).

[324] Schmitt, 2012(2); 26.

[325] לפי תפיסה זו, פציעה כוללת גם חולי ופגיעה בריאותית, שעלולים להיגרם מהשלכות פעולה קיברנטית, לדוגמה במקרה של תקיפת מתקן לטיהור מים במטרה לזהם מי שתייה או תקיפה שנועדה לגרום הרעבה.

[326] Schmitt, 2011(2); 120.

במקרים מסוימים, התקפה קיברנטית עשויה לפגוע בתפקוד של מערכת, אשר מבוססת על מחשבים, ולגרום לה נזק.[327] מרבית מנסחי מדריך טאלין, הציעו מבחן, שלפיו, פגיעה בתפקוד של מערכת, אשר השבתה לפעולה מחייבת החלפה של רכיבים פיזיים, היא בגדר 'התקפה'.[328] אחדים ממנסחי המדריך התנגדו לפרשנות זו ולא ראו בה 'התקפה'. חילוקי דעות דומים התגלו ביחס למקרה בו תיקון המערכת מחייב התקנה מחדש של מערכת ההפעלה[329], וכן ביחס למקרה, בו תיקון המערכת שנפגעה, מחייב הזנה מחדש של מידע (שאינו מערכת ההפעלה).

יש לציין כי ארגון הצלב האדום הבינלאומי הביע עמדה, לפיה כאשר התקפה קיברנטית משתקת את פעילות המערכת המותקפת, אף כאשר תיקון המערכת כרוך בהזנת מידע בלבד, יש לראות בכך גרימת נזק לרכוש, ולהתייחס לפעולה כאל 'התקפה' כמובנה בדיני המלחמה.[330] בעמדה זו יש היגיון רב בראייה כלכלית, שכן פגיעה אף במידע בלבד, עלולה להיות יקרה ומשמעותית מאד לגורם הנפגע. עם זאת, העמדה איננה משקפת קונצנזוס ביחס למשמעות המונח 'התקפה' בדין הקיים. עד כה הוצגו תרחישים בהם, לכל הפחות, נפגע רכוש מסוים. מה באשר להתקפה קיברנטית, שאינה מתבטאת בנזק ישיר לאדם או לרכוש, אך נושאת עמה תוצאות רחבות היקף, בעלות משמעות כבדה? למשל, חסימת כל תשדורת הדואר האלקטרוני במדינה או מניעת מתן שירותים על ידי תשתיות מחשב ציבוריות ופרטיות, שאינה כרוכה בפגיעה פיזית קבועה באותן תשתיות? הדעה המקובלת היא שפעולות

---

[327] דוגמה שהקהילה הבינלאומית מרבה לאזכר בהקשר זה היא הפגיעה של וירוס Stuxnet בצנטריפוגות במתקן גרעיני באיראן.

[328] מדריך טאלין, 128-129.

[329] שם.

[330] ראו: International Committee of the Red Cross, 31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report 31c/11/5/1/2, oct. 2011. (להלן - ועידת הצלב האדום). הגישה של הצלב האדום משקפת רף משפטי נמוך מאד, באופן יחסי.

קיברנטיות אלו אינן בגדר 'התקפה'[331]. לקביעה זו משמעות רבה, מאחר שבמהלך סכסוך מזוין, עלול צד לסכסוך לבצע פעולות קיברנטיות רחבות היקף כאלו, אשר יגרמו חוסר נוחות, פגיעה בסדר הציבורי, בכלכלה ובאמון בה, בתקשורת ובשירותים הממלכתיים. זאת בוודאי כאשר לא ייוחס לו עקב כך ביצוע 'התקפה'. נכון להיום, זהו המצב המשפטי החל[332]. כדי להמחיש את הדברים, הפעולות הקיברנטיות נגד גיאורגיה, גם בהנחה שחלו במהלך סכסוך מזוין עם רוסיה, לא היו, ככל הנראה, בגדר 'התקפות', שכן הן לא גרמו כלל לפגיעה ישירה בבני אדם או נזק לרכוש.

תוצאה זו יוצרת תחושת אי נוחות, שכן מדינות שיפלו קורבן לפעולות קיברנטיות, שאינן מתבטאות בנזק ישיר לאדם ולרכוש, עלולות שלא להשלים עמן ולראות בהן 'תקיפה' במהלך סכסוך מזוין. כך למשל, ישראל התמודדה עם התקפות קיברנטיות רחבות היקף במהלך מבצע "עופרת יצוקה" שהתנהל ברצועת עזה בדצמבר 2008 - ינואר 2009[333], ועם התקפות בהיקף רחב אף יותר במהלך מבצע "עמוד ענן", שהתנהל ברצועת עזה בשלהי שנת 2012[334].

פעולות קיברנטיות במהלך סכסוך מזוין עשויות להביא בפני עצמן, למשל, לתגובה קינטית נגד מטרות צבאיות ולוחמים של היריב[335]. אף הצלב האדום הציג סימני שאלה לגבי הדרך בה יתמודדו בפועל מדינות בעתיד עם פגיעות כאלה במרחב הקיברנטי[336].

---

[331] מדריך טאלין, 109.

[332] Schmitt, 2012; 292.

[333] להרחבה, ראו למשל Carr, 2011; 19. שם צוין שלפי הערכות, בתקופה זו נערכו כ-10,000 פעולות קיברנטיות נגד אתרי אינטרנט ישראליים ואחרים. רוב ההתקפות היו פשוטות ונועדו להשחית אתרי אינטרנט. רוב התוקפים היו ככל הנראה מהרשות הפלסטינית, מרוקו, אלג'יריה, ערב הסעודית וטורקיה, וניתן היה להצביע גם על קשרים לאיראן ולארגון החיזבאללה.

[334] ראו למשל פרסום בעניין מיליוני ההתקפות הקיברנטיות נגד אתרי אינטרנט ממשלתיים בזמן המבצע:
http://www.haaretz.co.il/captain/net/1.1867635

[335] Schmitt, 2011 (2); 131.

[336] ועידת הצלב האדום (ראו לעיל).

למען שלמות התמונה, ראוי להזכיר עמדה, שבאה לביטוי במסמך של הצלב האדום משנת 2011, אשר הופץ בוועידה של הארגון[337]. בראיית הארגון, גם כאשר פעולות קיברנטיות אינן מגיעות לכלל 'התקפה', אין לכוון אותן נגד מטרות אזרחיות, אלא ניתן לכוונן נגד מטרות צבאיות בלבד. כפי ששמיט מציין, עמדה זו לוקה בהיבט המשפטי, שכן הכלל, שעניינו אבחנה בין מטרות צבאיות לבין מטרות אזרחיות, חל רק כאשר מתרחשת 'התקפה'. בהיעדר 'התקפה' מלכתחילה, האבחנה שעליה מצביע הצלב האדום אינה רלבנטית[338].

סוגייה מעניינת מתעוררת במקרה בו, למשל, תוכנה זדונית (Malware) מוחדרת לרשת המחשבים של מדינה מסוימת, אולם הפעלתה מושהית ומותנית בהפעלה עתידית. מה דין פעולה כזו, בהנחה שהתוצאות הצפויות של ההפעלה הן גרימת נזק המאפיין 'התקפה'? לפי דעת רוב מנסחי מדריך טאלין, ניתן לראות במקרה כזה 'התקפה', בדומה למצב שבו מונח מוקש יבשתי שטרם התפוצץ בשטח מדינה אחרת. במקרה כזה בוצעה 'התקפה' בראי דיני המלחמה, הגם שהתוכנה לא הופעלה[339]. בדרך דומה, התקפה קיברנטית שיורטה בזמן (למשל באמצעות אנטי וירוס) ולא גרמה נזק בפועל - עודנה בגדר 'התקפה'. לבסוף, פעולה שלא זוהתה על ידי הגורם המותקף (תרחיש סביר בתחום הקיברנטי) - עדיין תיחשב 'התקפה', אם היא עונה למאפיינים הנדרשים[340].

תובנה חשובה ומעניינת (ויש שיאמרו - מפתיעה) היא שהניתוח המשפטי של המונח 'התקפה' בהקשר של דיני המלחמה, מוליד, פחות או יותר, ניתוח זהה לזה שהוצג בהקשר של דיני ה-Jus ad Bellum, ביחס למונח 'התקפה מזוינת'. בשני המקרים, בסופו של יום, הדין הקיים רואה בגדר המונחים רק את הפעולות הקיברנטיות, הגורמות באופן

---

[337] שם.

[338] Schmitt, 2012 ; 292-293.

[339] מדריך טאלין, 110.

[340] שם.

ישיר למוות או לפציעה או נזק לרכוש. אמנם, מאחר שהמונחים מופיעים בהקשרים משפטיים שונים, עשויים להיות ביניהם ניואנסים מסוימים[341], אך במהות, הניתוח דומה מאד. התוצאה היא שבהקשר הקיברנטי מתקיימת תופעה משפטית ייחודית, שאינה קיימת בהקשרים אחרים, בהם נבחן יישום כללי המשפט הבינלאומי על פעולות מלחמתיות או צבאיות. התופעה היא, ששני מונחי סף משפטיים מרכזיים, מעולמות תוכן שונים - ׳התקפה מזוינת׳ המקימה זכות להגדרה עצמית, ו׳התקפה׳ המבוצעת במהלך סכסוך מזוין ועליה חלים כללים מסוימים - מתלכדים למשמעות זהה. שני המונחים, בהתאם להבנת הדין הקיים, משתרעים על סוג פעילות אחד: התקפה קיברנטית, הגורמת באופן ישיר לפגיעה באדם או לנזק לרכוש, ותו לא. יתכן כי תופעה זו לא תימשך זמן רב, ובעתיד, עם השתכללות הדיון המשפטי במרחב הקיברנטי, תתפתחנה פרשנויות ותובנות שונות לכל אחד מהמינוחים, גם ביחס ליישומם במרחב זה.

[341] ראו גם: Schmitt, 2012; 291.

'שימוש בכוח', 'התקפה מזוינת' ו'התקפה': הדין הקיים ומשמעותו, אתגרים וכיוונים להמשך

הדין הקיים - עיקרים

במסגרת הפרקים הקודמים נסקר, בין השאר, המצב המשפטי ביחס לשלושה מונחי מפתח מתחום המשפט הבינלאומי, בהקשר הקיברנטי. שניים מהמונחים הם מתוך עולם דיני ה-Jus ad Bellum, כלומר הדינים המגבילים את זכותן של מדינות להשתמש בכוח צבאי ביחסיהן עם מדינות אחרות - 'שימוש בכוח' ו'התקפה מזוינת'. המונח השלישי לקוח מתחום דיני המלחמה - 'התקפה'.

בפרק זה ירוכזו העיקרים, העולים מניתוח הדין הקיים, כלומר מהמפגש בין כללי המשפט הבינלאומי לבין המרחב הקיברנטי, בנקודת הזמן הזו, בכל הקשור לפרשנות מונחי המפתח האמורים.

מבלי לחזור על הדברים, ראוי לשוב ולהבהיר, כי הצגת הדין הקיים מחייבת זהירות כפולה ומכופלת, בשל מספר טעמים כבדי משקל: **ראשית**, קיומה של מחלוקת בין מעצמתית בשאלות היסוד: האם כללי המשפט הבינלאומי בכלל חלים במרחב הקיברנטי? ובהנחה שהם חלים - מה תוכנם המהותי? משכך, ההתייחסות לדין הקיים תהיה אך ורק במשקפי הכתיבה המערבית בכלל, וארצות הברית בפרט. **שנית**, גם במערב קיימים מבוכה מסוימת ואינטרסים סותרים, כך שאין תמימות דעים ביחס לדין הקיים. ניכרים הבדלי גישה וניואנסים, למשל, בין עמדות ממשלת ארצות הברית לבין אסכולת שמיט ומנסחי מדריך טאלין. **שלישית**, בהיעדר אמנות מחייבות ופסיקה של טריבונלים בינלאומיים, הדין הקיים קשה לזיהוי. **רביעית**, התחום הקיברנטי מתפתח, דינמי, מצוי בראשית דרכו, ואין בו פרקטיקה של מדינות, המסתייעת בהבנת הדין הקיים.

עם כל הסייגים האמורים, יש חשיבות בהצגת המצב הקיים. לא רק מפני שניתן לשקף כך מציאות משפטית קיימת ושיח משפטי ער, בעת

הזו, אלא גם על מנת לפתוח צוהר לחשיבה בדבר כיווני התפתחות עתידיים, אשר ניתן להעריך שבוא יבואו.

טבלת הדין הקיים ביחס לפעולות קיברנטיות [342] -

סקירה תמציתית

	׳שימוש בכוח׳ Jus ad Bellum	׳התקפה מזוינת׳ Jus ad Bellum	׳התקפה׳ Jus in Bello
המקור	סעיף 2(4) למגילת האו״ם	סעיף 51 למגילת האו״ם	סעיף 49 לפרוטוקול ה-I
פעולות שיש לגביהן הסכמה	פעולה שתוצאותיה מזכירות ׳שימוש בכוח׳ צבאי: מוות, פציעה או נזק לרכוש	פעולה שיש לה תוצאות פיזיות - מוות, פציעה חמורה, נזק משמעותי לרכוש (לרבות מידע בנקאי המומר לכסף)	פעולה שצפויה לגרום באופן סביר למוות, פציעה או נזק לרכוש
פעולות שיש לגביהן מחלוקת	פעולה שאינה גורמת נזק פיזי, אך מדינות עשויות לראות בה ׳שימוש בכוח׳; ההכרעה לפי רשימת קריטריונים (אין על כך קונצנזוס מלא, אך הגישה מקובלת מאד)	פעולה שיש לה השלכות משמעותיות וקשות, אך שאינן מתבטאות בנזק פיזי	פעולה הפוגעת בתפקוד של מערכת, המחייבת החלפה של רכיבים פיזיים, התקנה מחדש של מערכת הפעלה או הזנה מחדש של מידע

[342] בהמשך לניתוח שהובא בעמוד הקודם, ניתן להסתייע בטבלה שלעיל, כדי לפשט את הדברים, ככל הניתן, גם במחיר של הכללות והצגה שלדית ומתומצתת של רעיונות מורכבים.

	'שימוש בכוח' **Jus ad Bellum**	**'התקפה מזוינת'** **Jus ad Bellum**	**'התקפה'** **Jus in Bello**
פעולות שאינן כלולות בגדר המונח	כל השאר, לרבות כפייה כלכלית, פסיכולוגית ופוליטית	כל השאר, לרבות כפייה כלכלית, פסיכולוגית ופוליטית	פעולות משמעותיות שאינן מתבטאות בנזק פיזי (כמו חסימת תקשורת, מניעת שירותים) וכל השאר
המשמעות שנובעת מכך שפעולה קיברנטית היא בגדר המונח	לא ניתן להגיב בשימוש נגדי בכוח; מותרות תגובות לא כוחניות כצעדים דיפלומטיים ו'אמצעי נגד' מוגבלים בהיקף	מותר להגיב בהגנה עצמית, הכוללת שימוש בכוח	חלים על הפעולה כל האיסורים וההגבלות מתחום דיני המלחמה

מניתוח הדין הקיים, ובפרט הסוגיות שלגביהן ניתן להצביע על קונצנזוס רחב יחסית, ניתן להצביע על מספר תובנות מרכזיות, ובהן:

ראשית, עיקר הקונצנזוס בדין הקיים הוא על האיסור ביחס לפעולות קיברנטיות, אשר כתוצאה מהן נגרם נזק פיזי, בדמות מוות או פציעה של אנשים או נזק לרכוש. מצבים כאלה יהוו, ככלל, למעט אולי בנסיבות טריוויאליות, ׳שימוש בכוח׳, ׳התקפה מזוינת׳ ו׳התקפה׳.

שנית, מכלל ההן חשוב להצביע על הלאו. במשקפי הקונצנזוס הקיים, פעולות קיברנטיות שאינן מתבטאות בנזק פיזי, כאמור, אינן בגדר ׳התקפה מזוינת׳ או ׳התקפה׳ (לגבי ׳שימוש בכוח׳, הדעה מקובלת, אם כי לא בהסכמה מלאה, היא שפעולות מסוימות, שאינן מובילות לנזק פיזי, עדיין עשויות להוות ׳שימוש בכוח׳).

בהתאם, לא ניתן להגיב לפעולות קיברנטיות, שאינן גורמות לנזק פיזי, באמצעים כוחניים (בהיעדר סכסוך מזוין). כאשר מתנהל סכסוך מזוין, לא חלים עליהן האיסורים וההגבלות הרלבנטיים ל׳התקפה׳ בתחום דיני המלחמה. זאת, גם כאשר מדובר בפעולות שהשפעתן המזיקה, למשל במישור הכלכלי, עשויה להיות משמעותית ביותר.

כפי שיובהר בהמשך, תובנה זו אולי משקפת את הדין הקיים, אך לעניות דעתי אין היא צפויה לשקף את הפרקטיקה שמדינות תאמצנה במדיניות התגובה שלהן.

שלישית, הטבלה מאפשרת להצביע על קווי התיחום בין ׳שימוש בכוח׳ לבין ׳התקפה מזוינת׳. בהתאם לפסיקה ולספרות המשפטית הכללית, הבדל מרכזי בין שני המונחים הוא בכך שבתוך הספקטרום של ׳שימוש בכוח׳, רק המקרים, שבהם התוצאות הפיזיות הן החמורות ביותר, ועומדות בדרישה של ״Scale and Effect״, יהוו ׳התקפה מזוינת׳. מנסחי מדריך טאלין תמכו באבחנה זו גם במרחב הקיברנטי. עם זאת, קשה, נכון להיום, להצביע באופן חד וברור על אבחנה כזו, שכן לפחות חלק מההתבטאויות של גורמים רשמיים אמריקנים, מצביע על כך שכל גרימת נזק פיזי באמצעים קיברנטיים, תצדיק בראייתם הגנה

עצמית[343]. כלומר, גם אם בתיאוריה המשפטית אמור להיות הבדל בין המצבים, ספק רב האם בחיי המעשה ארצות הברית מכירה בו.

ההבדל, שנותר בין 'שימוש בכוח' לבין 'התקפה מזוינת', נוגע למצבים שבהם כתוצאה מהתקפה קיברנטית לא ייגרם נזק פיזי כלל. קיימת הסכמה רחבה למדי, גם אם לא בקונצנזוס מלא, כי גם פעולות מסוימות, שאינן מתבטאות בנזק פיזי, ייתפסו על ידי מדינות כ'שימוש בכוח' וראוי לראות בהן 'שימוש בכוח' (לדוגמה, מדינה המציידת קבוצת פצחנים מאורגנת בתוכנות זדוניות, על מנת שתפעל נגד מדינה אחרת במרחב הקיברנטי). בכך, המונח 'שימוש בכוח' עודנו רחב מהמונח 'התקפה מזוינת'.

רביעית, ניתן להתרשם כי בפועל, קיים דמיון רב, בהקשר הקיברנטי, בין המונח 'התקפה מזוינת' לבין המונח 'התקפה' בדיני המלחמה, לפחות בראי הקונצנזוס הקיים. זאת, הגם שמונחים אלו שאובים מהקשרים שונים ומענפי דין אחרים. ביחס לתכולת שני המונחים, קיימת כיום הסכמה יחסית רחבה רק ביחס לפעולות קיברנטיות, הגורמות פגיעה פיזית לאדם או נזק לרכוש. תיאורטית, המונח 'התקפה מזוינת' היה אמור להשתרע על פעולות מצומצמות יותר (וחמורות יותר) מאשר המונח 'התקפה' בדיני המלחמה, אך כאמור, במצב הקיים בין המונחים דמיון רב מאד. תובנה זו אולי מפתיעה, אך נראה שהיא מבטאת את העובדה שקביעת כללי המשחק במרחב הקיברנטי מצויה בשלב מקדמי בלבד, בו גובשו הסכמות בהיבטים מצומצמים ותו לא[344].

הדבר קשור לתובנה **החמישית**, ואולי החשובה מכולן. ההסדרה המשפטית של המרחב הקיברנטי היא בשלבי התהוות ועיצוב. משכך, ראוי להתייחס לנושא כדינמי, משתנה ומוכתב על ידי שיקולים אסטרטגיים רחבים, הרבה מעבר לתחום המשפטי. מונחים רבים טרם

[343] נאום koh, 7. להרחבה ראו הדיון בפרק 5 שעניינו 'התקפה מזוינת' במרחב הקיברנטי.

[344] לעניין הדמיון בין המונחים, ראו גם: Schmitt, 2012 ; 291.

חודדו בהקשר הקיברנטי, ולא ברור האם משמעותם במרחב הקיברנטי תהיה זהה לפרשנות המוכרת כיום בהקשרי לחימה אחרים. כך לדוגמה, צפוי דיון רחב במשמעות המשפטית של פגיעה בריבונות המדינתית במרחב הקיברנטי[345]; ובשאלה המשפטית, כיצד להתייחס להתקפה קיברנטית במהלך סכסוך מזוין מצד שחקנים שאינם מדינתיים, כגון תאגידי ענק[346]. יתכן כי בעולם המחר, פעולות הצבועות כיום בגווני אפור, ייאסרו או יותרו בצורה מפורשת. כדי להעריך את המגמות הצפויות, יוקדש פרק המשנה הבא לאתגר המרכזי העולה מהמצב הקיים.

האתגר המרכזי - פגיעה קיברנטית משמעותית, שאינה כרוכה בנזק פיזי

עיצוב משטר משפטי בינלאומי למרחב הקיברנטי מעורר אתגרים רבים, שחלקם נפרשו במסגרת פרקי עבודה זו. מבין שלל האתגרים, ימוקד הדיון כעת באתגר מרכזי אחד.

המסגרת הנורמטיבית הקיימת של כללי המשפט הבינלאומי, מבוססת על תפיסה מסורתית של עולם המלחמה. לאורך ההיסטוריה, שיבשו מדינות את הסדר העולמי באמצעות פגיעה בבני אדם וגרימת נזק לרכוש. הנורמות שאומצו בתגובה על ידי הקהילה הבינלאומית, נועדו למנוע תוצאות שנתפסו, בעת שהכללים נוסחו, כהרסניות ליציבות העולמית ולביטחון המדינות[347].

ההתפתחות הקיברנטית מאתגרת את הגישה המסורתית מן היסוד. במרחב הקיברנטי, ניתן ליצור השפעות, אשר יערערו את היציבות של מדינות מהיסוד, באמצעות פעולות שאינן קינטיות, ואם לחדד את הדברים - באמצעות הקשה על לוח המקשים של מקלדת מחשב או

---

[345] דוגמה לדיון בנושא מצויה במסגרת כלל מספר 1 במדריך טאלין, 15.

[346] לדיון מעניין בנושא ראו: Rosenzweig, 2013.הכותב מתמקד בסוגיית הפעלת אמצעי הגנה אקטיבית על ידי גורמים מהמגזר הפרטי.

[347] Schmitt, 2011 ; 603.

מסך מגע. כלים ויכולות קיברנטיים, שאיש בעבר לא חשב לאסור, עלולים לגרום תוצאות, שייתפסו כ-Casus Belli. במילים כלליות יותר, המרחב הקיברנטי מנתק את החפיפה בין המשטר המשפטי הקיים לבין התוצאות שהוא מבקש ונועד למנוע. אין זה דבר של מה בכך.

בסופו של יום, המשטר המשפטי הבינלאומי נוסח על ידי מדינות, כדי למנוע מהן תוצאות מסוימות. הוא אמור לאפשר למדינות להגן על עצמן, נוכח תוצאות שנתפסות כחמורות מאד בראייתן[348]. בעולם המודרני, הדין אינו יכול לספק למדינות מענה לפגיעה פיזית ותו לא. מדינה שבה האזרחים לא יוכלו לגלוש באינטרנט, האמון במערכת הבנקאית ייפגע, הבורסה תהיה משותקת, או שירותי הממשלה הממוחשבים לא יתפקדו, תראה זאת בחומרה רבה, והיא תחוש פגיעה ודאגה, שאינן נופלות מאלו הנגרמות כתוצאה מפעולה קינטית-צבאית; היא תראה צורך להגיב ותחוש הצדקה לכך. המשפט יצטרך לתת מענה גם לסוג הפעולות הקיברנטיות הללו.[349] גם אם הדין ימלא פיו מים, הפרקטיקה של המדינות תכתיב כללי משחק חדשים.

במצב המשפטי הקיים, פעולה שאינה הרסנית ואינה גורמת נזק פיזי, אינה בגדר 'התקפה מזוינת', גם אם טלטלה את הכלכלה ופגעה בסדר הציבורי. אם פעולה כזו מבוצעת במהלך סכסוך מזוין, היא לא תיחשב 'התקפה' בראי דיני המלחמה, חרף תוצאותיה. זהו הדין המצוי, אך דומה שאין לראות בו דין מספק או רצוי.

סימנים לקושי בהשלמה עם המצב המשפטי הקיים כבר התגלו, ולא רק בכתיבה האקדמית. לדוגמה, בדו"ח של האקדמיה הלאומית האמריקנית למדע, הוצגה 'התקפה מזוינת' באמצעות דוגמאות של התקפה קיברנטית על הבורסה לניירות ערך, המשבשת את פעילותה לאורך זמן, ושל התקפות על מערכות שליטה של תשתיות לאומיות[350].

---

[348] Schmitt, 2012; 287.

[349] שם, 288-289.

[350] דו"ח NRC, 354-355.

ספק רב אם פעולות אלו נחשבות 'התקפה מזוינת' בהתאם למצב המשפטי הקיים. ניתן להעריך שכך מדינות יראו אותן בפועל.
מדינות עלולות לחוש מוגבלות על ידי המשפט הקיים, ונטולות מענה אפקטיבי לאיומים עליהן[351]. שמירה על כללי המשפט הבינלאומי עלולה לעמוד בניגוד לאינטרסים שלהן בתחום הביטחון הלאומי. בהקשרים אחרים, הקהילה הבינלאומית ביקשה בעשורים האחרונים להגיע לאיזון בין העקרונות המשפטיים התיאורטיים לבין המציאות של הלחימה המודרנית, בתהליך שהבשיל להתפתחויות חשובות. כך, לדוגמה בלבד, העיסוק הבינלאומי בפרשנות המונח 'אזרחים הנוטלים חלק ישיר בפעולות איבה' בדיני המלחמה, שאף הוביל לגיבוש מדריך פרשני על ידי ארגון הצלב האדום הבינלאומי[352].
ככל שהטכנולוגיה תתקדם, וירבו התקפות קיברנטיות, מדינות תידרשנה בתדירות גבוהה לקבל החלטות, האם להגיב באמצעות שימוש בכוח[353]. מדינות שיחלקו על הדין הקיים ופרשנותו הנוכחית במרחב הקיברנטי, עשויות להחליט על שימוש בכוח, לפי שיקולים פרטניים, שאינם מבטאים הסכמה בינלאומית רחבה. בראייה פסימית, הדבר עלול להוביל לסביבה ביטחונית כאוטית ולשימוש בכוח, קיברנטי וקינטי, ללא שליטה. בוודאי שמגמה זו עומדת בניגוד לרציונל שבבסיס מגילת האו"ם. מקבלי ההחלטות, כמו גם הקהילה המשפטית והאקדמית, אינם יכולים להישאר אדישים להתפתחות זו.
בפרק הבא יוצגו מספר מגמות אפשריות בהסדרה המשפטית העתידית של הפער המתואר לעיל, המיועדת להתמודד עם אתגר משמעותי זה.

---

[351] ראו גם: Watts, 2011; 76.
[352] להרחבה, המדריך, שפורסם בשנת 2009 לאחר עבודה רבה של מומחים בנושא, מצוי ב: http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf
[353] Watts, 2011; 78.

עתיד שכולו טוב? מגמות והתפתחויות אפשריות להמשך

ניתוח כלל המגמות וההתפתחויות בהסדרה המשפטית של המרחב הקיברנטי עשוי להשתרע על פני ספרים רבים. ניתן לומר, כי זהו שדה בלתי חרוש, אשר עיבודו צפוי להעסיק את הקהילה המשפטית במשך שנים רבות.

פרק משנה זה יוקדש להתפתחויות אפשריות ביחס לאתגר המרכזי שהוצג קודם לכן. עניינו המתח בין שניים: מצד אחד, היכולת לפגוע באמצעים קיברנטיים בצורה משמעותית במדינה מסוימת, גם ללא גרימת נזק פיזי. מצד שני, המצב המשפטי הקיים, בו כל עוד הפעילות הקיברנטית אינה גורמת נזק פיזי ישיר, אין היא מהווה 'התקפה מזוינת' ולא ניתן להגיב עליה בהגנה עצמית, תוך שימוש בכוח. כאמור, זהו מתח שמדינות יתקשו מאד להשלים עמו.

ניתן להצביע ולהעלות על הדעת כיווני התפתחות רבים, שתכליתם להתמודד עם מתח זה ולגשר על הפער שיצר אותו. כמה מהם יוצגו להלן, בתמצית, על יתרונותיהם והקשיים הצפויים במימושם.

פרשנות יצירתית וחדשה ל'התקפה מזוינת'

נכון להיום, הקונצנזוס הקיים ביחס להגדרת 'התקפה מזוינת' נקשר רק לפעולות, המובילות באופן ישיר לנזק פיזי לאדם או לרכוש. במילים אחרות, נדרש שתוצאות הפעולה תהיינה 'מזוינות' או 'אלימות'. חלק מהכותבים, ובראשם שמיט, מעלים את האפשרות כי בבוא העת תתפתח תפיסה חדשה לגבי 'התקפה מזוינת', במסגרתה ייבחנו לא רק סוג האמצעי שבו מבוצעת הפעולה (או למעשה סוג התוצאה שלה), אלא גם ההשפעה הכוללת שלה[354]. לפי הצעתו, הדגש עדיין יהיה על מבחן התוצאה - כלומר מה הן השפעות הפעולה הקיברנטית. התוצאות ייבחנו לא רק באופן דיכוטומי, בראי טבען (אלימות - 'התקפה מזוינת';

[354] שמיט מתאר מבחן איכותני וכמותני. ראו: Schmitt, 2011; 605.

לא אלימות - אינן 'התקפה מזוינת'), אלא בראי רחב של השפעתן הכוללת.

למעשה, מהות ההצעה היא לבחון את קיומה של 'התקפה מזוינת', באמצעות מבחן דומה לזה שהוצע על ידי מנסחי מדריך טאלין ביחס לסיווג פעולות קיברנטיות כ'שימוש בכוח'[355]. הפעולה הקיברנטית תיבחן בראי רשימה של קריטריונים (חומרת התוצאה, מיידיות, חודרניות, ישירות ועוד), המבקשים לנבא, עד כמה צפוי שמדינות תתייחסנה אליה כאל 'התקפה מזוינת'[356]. מבחן זה יאפשר, במקרים מסוימים, להתייחס גם אל פעולות קיברנטיות שלא גרמו נזק פיזי, אך השפעתן לרעה הייתה משמעותית מאד, כאל 'התקפה מזוינת' במרחב הקיברנטי. מדינות תהיינה רשאיות להגיב להתקפה כזו בהגנה עצמית, הכוללת 'שימוש בכוח'.

שמיט מכיר בכך שהקריטריונים המוצעים הם גמישים ומותירים מרחב שיקול דעת רחב ביישומם. עדיין, יש בכך שיפור לעומת המצב הקיים, שכן המשפט הבינלאומי אינו מספק כיום מענה כלשהו לאתגר זה[357], ולכאורה - איש הישר בעיניו יעשה. להערכתו, אם ייעשה שימוש בקריטריונים ותאומץ פרשנות יצירתית ל'התקפה מזוינת', עשויה להתפתח פרקטיקה עתידית של מדינות, על בסיס השימוש בקריטריונים, שתעצב את הפרשנות של סעיף 51 למגילת האו"ם בצורה ראויה[358].

הצעה זו מצביעה על הצורך באימוץ פרשנות חדשה למונח 'התקפה מזוינת', שאינה מוגבלת לפעולות המובילות לנזק פיזי לאדם או לרכוש. פרשנות זו עשויה לעשות שימוש ברשימת קריטריונים, כאשר ההנחה היא שתתפתח פרקטיקה עתידית, אשר תעצב בבוא העת את הפרשנות המחייבת של סעיף 51 למגילת האו"ם בהקשר הקיברנטי.

---

[355] הצעה שנוסחה כבר לפני שנים רבות, ראו: Schmitt, 1999.

[356] רשימת הקריטריונים מפורטת בפרק הרביעי, שבמרכזו בירור המונח 'שימוש בכוח'.

[357] Schmitt, 2012; 287.

[358] Schmitt, 2011; 588.

להצעה מספר יתרונות. הבולט בהם הוא שהיא מבקשת להסתמך על המשטר המשפטי הקיים במגילת האו״ם ולהציע לו פרשנות עדכנית. אין צורך באימוץ אמנות חדשות או ביצירת יש מאין, תהליכים שנמשכים זמן רב ומותנים במפגש אינטרסים בינלאומי, שסיכויו קלושים. יתרון נוסף הוא בכך שההצעה מביאה בחשבון את המורכבות של העולם הקיברנטי, ומציעה שורה של קריטריונים לסיווג פעולות קיברנטיות, להבדיל מהסתמכות על מבחן קשיח ודיכוטומי אחד. הדבר עשוי לאפשר קבלה של ההצעה על ידי שחקנים רבים יותר ופיתוח הדרגתי ובלתי כופה של הדין, בזיקה לפרקטיקה שתתפתח מצד מדינות.

יתרונותיה של ההצעה הם גם חסרונותיה. הניסיון להתבסס על המשטר המשפטי של מגילת האו״ם, מאלץ להתמודד עם לשון המגילה. סעיף 51 למגילה מגדיר במפורש ׳מזוינת׳ ביחס להתקפה, וקשה ליישב ניסוח זה עם פעולה שאינה גורמת נזק פיזי. יתר על כן, למגילה פרשנות צרה שנחצבה לאורך השנים, בהובלת ארצות הברית[359]. פרשנות שאינה מכירה, למשל, בכפייה כלכלית משום ׳שימוש בכוח׳ (קל וחומר ׳התקפה מזוינת׳). זאת, גם אם תוצאותיה, מבחינת המדינה הנפגעת, הן מרחיקות לכת. נדרשת יצירתיות משפטית יוצאת דופן להסביר, כיצד פגיעה כלכלית חמורה באמצעי קיברנטי מהווה ׳התקפה מזוינת׳, ואילו כאשר היא מבוצעת בדרך של כפייה כלכלית (כמו באמצעות אמברגו, הגבלות ייבוא, פיקוח על ייצוא וצעדים אחרים) - אין בכך פסול[360].

הפרשנות הרחבה עלולה גם לעמוד בניגוד לרציונל של מגילת האו״ם, המבקש לצמצם את היכולת של מדינות להפעיל כוח על בסיס שיקול דעתן ובאופן חד צדדי. כאשר למדינות מוקנית הזכות לפעול, על בסיס רשימת קריטריונים גמישה, הדבר עלול להיות מתכון לשימוש מופרז

[359] להרחבה, דברים שנכתבו לגבי הגישה האמריקנית כבר בשנות השישים: Brownlie, 1963 ; 362.

[360] להרחבה: Antolin-Jenkins, 2005 ; 173.

בכוח ולחוסר וודאות שיאיימו על הסדר העולמי, ובכך טמון סיכון של ממש.

הרחבת הסעדים הנתונים למדינה במקרה של ׳שימוש בכוח׳ נגדה

ערוץ שני של התפתחות עשוי לכלול שני רכיבים: הגדרת פעולות קיברנטיות, המסבות נזק משמעותי שאינו פיזי, כ׳שימוש בכוח׳; ובד בבד, הרחבת הסעדים, המוקנים למדינה שנפגעת משימוש אסור בכוח במרחב הקיברנטי.

המגמה של הכרה בפעולות קיברנטיות, שאינן גורמות נזק פיזי, כ-׳שימוש בכוח׳ נדונה כבר בהרחבה. כך למשל, מרבית מנסחי מדריך טאלין תומכים בכך, בהתאם לרשימת קריטריונים שנקבעה לתכלית זו[361].

הבנת המהלך המשלים מחייבת מספר מילות הקדמה. בהתאם לכללי המשפט הבינלאומי, כאשר מדינה נפגעת מ׳שימוש בכוח׳, שאינו מגיע לכדי ׳התקפה מזוינת׳, אין היא יכולה לפעול בהגנה עצמית ולהגיב באופן כוחני. הסעדים המוקנים למדינה במצב כזה הם מצומצמים, וכוללים, בין השאר, אפשרויות של פיצוי[362] וצעדים דיפלומטיים. בנוסף, המדינה הנפגעת רשאית לנקוט ׳אמצעי נגד׳ (Countermeasures). נהרות של דיו נשפכו בנושא אמצעי נגד. לצרכי דיון זה, תספיק האמירה כי מדובר באמצעים, המיועדים להפסיק את הפגיעה ולהחזיר את המצב לקדמותו[363]; אין הם כוללים שימוש בכוח (כלומר, אין מרכיב של הדדיות - גם מדינה שנפגעה משימוש אסור בכוח, אינה

---

[361] מדריך טאלין, 48-51.

[362] ראו: Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the Int'l Law Comm'n, 53d Sess., Apr. 23-June 1, July 2-Aug. 10, 2001, UN DOC. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001), art. 34-37. (להלן - דו״ח הוועדה).

[363] שם, 324. להרחבה, ראו גם: Hathaway, 2012; 857. שם צוין שבעבר, נעשה שימוש במונח reprisals שמשמעותו מעט שונה, אך כיום ׳אמצעי נגד׳ הוא המונח הרלבנטי.

יכולה להגיב בכוח[364]; והם כפופים לדרישות כמו צורך ומידתיות, המחלישות את האפקטיביות שלהם, בפרט במרחב הקיברנטי[365]. האפשרות של נקיטת אמצעי נגד בהקשר הקיברנטי, מעוגנת למשל בכלל 9 במדריך טאלין.

הרעיון, שעומד על הפרק, הוא הרחבת היקפם של אמצעי הנגד, כך שיספקו למדינה שנפגעה סעד משמעותי ומוחשי יותר מאשר בהתאם למצב המשפטי הקיים. בהקשר זה מוזכרת חוות דעתו של השופט סימה (Simma) בפרשת אסדות הנפט. השופט סבר, כי יש לאפשר למדינה שנפגעה משימוש אסור בכוח מעין הגנה עצמית מרוככת (Defensive military action short of full-scale-self-defence), אשר תכלול שימוש בכוח, שיהיה מוגבל מבחינת היקפו ועוצמתו[366]. מאחר שפעולות קיברנטיות רבות עשויות להיות 'שימוש בכוח', אך אינן בגדר 'התקפה מזוינת', ההצעה הזו תאפשר למדינות הנפגעות מהן להגיב בצורה פעילה, מבלי להיתפס כמפרות את הכללים המשפטיים[367].

ההצעה לאפשר למדינות להגיב לשימוש קיברנטי בכוח באמצעי נגד 'מוגברים', לרבות בשימוש מוגבל בכוח, קוסמת על פניה. יתרונותיה ברורים - היא שומרת על המשטר המשפטי של מגילת האו"ם ואינה מחייבת יצירת דין חדש; והיא יצירתית בנושא שטרם עוצב באופן משכנע וברור - 'אמצעי הנגד'[368]. במישור המהותי, ההצעה עונה לצורך אמיתי - הלחץ להגיב, בו תהיה נתונה מדינה, אשר נפלה קורבן לשימוש בכוח קיברנטי.

מנגד, ראוי להבהיר, כי גישתו של השופט Simma אינה מקובלת כחלק מהמשפט הקיים. הגמישות שבה אינה מתיישבת עם נוסח הדין, כלומר עם המבחנים הדיכוטומיים והנוקשים שאומצו במגילת האו"ם, ואין

---

[364] דו"ח הוועדה, סעיף 50(1)(a).

[365] להרחבה, ראו מדריך טאלין, 36-41. ראו גם: Hinkle, 2012; 18.

[366] פרשת אסדות הנפט, 12 (דעת השופט Simma).

[367] להרחבה: Hinkle, 2012.

[368] שם. להבדיל ממונח כמו 'שימוש בכוח', שנושא עמו מטען כבד ואין רצון לסטות מפרשנותו, 'אמצעי נגד' מונח פחות טעון, וניתן לכאורה לחתור לפרשנות חדשה לגביו.

לה גם תימוכין בפרשנות הנהוגה[369]. יותר מכך - אין היא מתיישבת עם הרציונל שבבסיס המשטר הקיים במגילה: צמצום השימוש בכוח באופן חד צדדי על ידי מדינות, והימנעות מהרחבתו.

מעבר לכך, ומבלי להרחיב, ההצעות שהועלו בנושא, מעבר לרעיון הבסיסי של חיזוק ׳אמצעי הנגד׳, הן כלליות ואינן מפותחות. קשה להבין מהן למשל, אילו ׳אמצעי נגד׳ יהוו מענה לשימוש קיברנטי בכוח. נראה, כי הנושא מחייב פיתוח והעמקה, ואינו בשל לשינוי, לפחות בעת הזו[370]. קשה להכחיש את הפוטנציאל שיש להעמקת העיסוק המשפטי בעולם ׳אמצעי הנגד׳, אך פוטנציאל זה טרם מומש. ההצעות הכלליות בנושא הן בגדר הזמנה לגבש מודלים קונקרטיים. בשלב הנוכחי, פתיחת פתח להרחבת השימוש בכוח, ולו באופן מוגבל במסגרת ׳אמצעי נגד׳, כרוכה בסיכונים משפטיים רבים מדי.

אמנה חדשה להסדרת כללי המשחק במרחב הקיברנטי

כיוון התפתחות נוסף, שקנה לו אחיזה בקרב רבים[371], הוא יצירת אמנה בינלאומית חדשה, שתגדיר את כללי המשחק המשפטיים במרחב הקיברנטי, בדרך שונה מהמשטר המשפטי המעוגן במגילת האו״ם ובכללי המשפט הבינלאומי המקובלים.

המצדדים בכיוון זה, תומכים את משנתם במספר טעמים מרכזיים. **ראשית**, הקושי במשטר המשפטי הקיים, שנותן מענה, נכון להיום, רק לפעילות קיברנטית אלימה, ואינו עוסק במכלול שלם של פעולות קיברנטיות מטרידות ביותר, שאינן גורמות נזק פיזי. **שנית**, המשטר המשפטי הקיים הוא דיכוטומי, מבוסס על אבחנה בין מצבים (למשל סכסוך מזוין או היעדרו) ועל דרישות סף (שימוש בכוח, התקפה מזוינת וכיוצא באלה). מנגד, האיומים המודרניים, ובראשם טרור ופעילות

---

[369] Watts, 2011; 68-69.

[370] ראו: Hinkle, 2012; 21.

[371] לדוגמה, ראו התייחסות לנושא: Hathaway, 2012; Waxman, 2011; Banks, 2013.

קיברנטית, מצויים תמיד על רצף - מהטרדה ועד תוצאות קטסטרופליות. לכן, נדרש משטר משפטי חדש, שיספק מענה גמיש ומגוון יותר לכל ספקטרום הפעילות[372]. **שלישית**, ניסיון מאולץ ומלאכותי להסדיר את המרחב הקיברנטי, באמצעות המשטר המשפטי הקיים, עלול לפגוע במבנה האינטגרטיבי והעדין של הכללים הקיימים[373]. הורדת הרף, כלומר הכרה רחבה מדי בפעולות קיברנטיות כ'שימוש בכוח' או כ'התקפה מזוינת', עלולה להוביל להסלמת סכסוכים ולהחמיר את הסיכון שפעולות קיברנטיות יובילו לסכסוך צבאי[374]. **רביעית**, ההתמודדות עם המרחב הקיברנטי, שאינו יודע גבולות, מחייבת מנגנונים משמעותיים של תיאום ושיתוף פעולה בינלאומי, שאינם מצויים בהכרח בדין הקיים. במילים אחרות, הבעיה היא גלובלית וכזה חייב להיות גם הפתרון. בהקשר זה, קובע מסמך האסטרטגיה של משרד ההגנה האמריקני:

"No single state or organization can maintain effective cyber defences on its own".[375]

חלק מהכותבים, מצביע על הדמיון בין האתגר המשפטי, שהציב הטרור העולמי, לבין האתגר שמציב המרחב הקיברנטי[376]. בעקבות תופעת הטרור העולמי, היו תמורות במשפט הבינלאומי, למשל הרחבת זכות ההגנה העצמית של מדינות ביחס להתקפה שמבוצעת על ידי ארגונים שאינם מדינתיים[377]. תמורות, ואף משמעותיות יותר, עשויות להתרחש על רקע העולם הקיברנטי. שינוי פרדיגמטי, עשוי להתפתח ביחס למונחי מפתח כמו 'התקפה מזוינת', 'שימוש בכוח' ו'התקפה', תוך אימוץ פרשנות שונה מזו של מגילת האו"ם. שינוי כזה קשה לקדם

---

[372] Banks, 2013 ; 162-163.

[373] שם.

[374] Libicki, 2009 ; 69-70.

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

[376] Banks, 2013.

[377] בעקבות תופעת הטרור העולמי היו התפתחויות משפטיות נוספות, כמו הפרשנות האמריקנית החדשה למבחן המיידיות בהקשרי הגנה עצמית (סגירת חלון ההזדמנויות). כאמור, פרשנות עדכנית זו רלבנטית בהחלט גם למרחב הקיברנטי.

במסגרת הדין הקיים, ויתכן כי תידרש לו אכסניה משפטית נפרדת וחדשה.

במובנים מסוימים, הסיכוי שיתפתח דין חדש בהקשר הקיברנטי, גדול יותר מאשר בהקשר המאבק בטרור. בניגוד לטרור, שהיכה בעיקר מדינות מסוימות (והמאבק בו זוהה בעיקר עם ארצות הברית), כמעט כל מדינה היא קורבן פוטנציאלי להתקפות קיברנטיות, ומכאן הפוטנציאל להשגת מכנה משותף. בנוסף, המרחב הקיברנטי נתפס כשונה מאד משדה המלחמה המוכר, והקושי ליישם בו את המשפט הקיים בולט וכמעט אינטואיטיבי[378].

השיקולים בזכות אמנה בינלאומית חדשה נשמעים משכנעים, אך ניתן לצפות כי יוזמות לכך ינחתו במהרה על קרקע המציאות. הגעה להסכמה בינלאומית צפויה להיות מאתגרת ומורכבת, בלשון המעטה. מבלי להרחיב, הקושי המרכזי הוא בהבדלי ההשקפה, הערכים והאינטרסים האסטרטגיים בין ארצות הברית ודמוקרטיות מערביות אחרות לבין מעצמות קיברנטיות כמו רוסיה וסין. במערב, אינטרס ראשון במעלה הוא מניעת התקפות קיברנטיות על תשתיות חיוניות. במזרח, רוסיה וסין רואות התקפות קיברנטיות בצורה רחבה, וכוללות בהן הבעת עמדות פוליטיות והפצת מידע, המסכן את היציבות והמשטר. יוזמות בזירה הדיפלומטית המקודמות על ידן, מבטאות תפיסה זו ומחדדות את הקושי בהגעה להבנות בינלאומיות.

על רקע זה, וקשיים נוספים שיפורטו בפרק המשנה הבא, דומה כי מכנה משותף רחב בין המעצמות לא יושג בטווח הקרוב[379]. איני צופה הסדרה פורמלית ואוניברסלית של מרחב הסייבר בשנים הקרובות. להערכתי, הדבר ייארך זמן רב וייגזר, בראש ובראשונה, ממדיניות שתתפתח באמצעות פרקטיקה של מדינות, באופן הדרגתי.

---

[378] ראו גם: Banks, 2013.

[379] Hathaway, 2012; 882.

הגישה הריאליסטית - אי הסדרה והתפתחות הדרגתית של פרקטיקה

הגישה המפוכחת או הריאליסטית ביותר ביחס להתפתחות הצפויה של המשטר המשפטי, לפחות בשנים הקרובות, אינה משפטית טהורה, אלא מבוססת על ניתוח של ההקשר האסטרטגי, בו מתנהל מרחב זה. גישה זו מבקשת לבחון, בראייה רחבה, את יחסי הגומלין והדינמיקה בין המשפט לבין תמונת המצב האסטרטגית. זאת, מאחר שבחיי המעשה, בוודאי ביחס למשפט הבינלאומי, האסטרטגיה מעצבת את המשפט והמשפט מעצב את האסטרטגיה[380].

מלומדים, החוקרים את המרחב הקיברנטי, מצביעים על שורה ארוכה של אתגרים, שיקשו מאד על השגת הסכמה בינלאומית רחבה, בוודאי בדמות אמנה בינלאומית חדשה, אך גם על עצם גיבוש הסכמה רחבה ביחס לפרשנות הדין הקיים בהקשר הקיברנטי[381].

האתגרים נובעים, בראש ובראשונה, ממאפיינים שונים, בעיקר טכנולוגיים[382], של המרחב הקיברנטי. כך, הקושי לזהות מקור של התקפה ולייחס אותה לגורם כלשהו[383]; כמו גם היות המרחב חוצה גבולות, והקושי לקיים חקירות מחוץ לגבולות המדינה[384]; דרך הפעלת גורמים שאינם מדינתיים, תוך מיסוך וטשטוש של הגורם היוזם, בדומה, ל-Proxy Warfare בזמן המלחמה הקרה; וכלה, למשל, בקושי לקבוע את הקשר הסיבתי (להגדיר מהו הנזק שנגרם עקב התקפה קיברנטית מסוימת). לדוגמה, כאשר מותקפת מערכת בנקאות או בורסה במדינה מסוימת, אילו השלכות, שייגרמו כתוצאה מכך ולאורך כמה זמן, עדיין ייחשבו נזק כתוצאה מההתקפה[385]?

---

[380] להרחבה: Waxman, 2011; 425.

[381] למשל: Waxman, 2011.

[382] Banks, 2013; 195-196, לעניין הניסיון של המשפט לרדוף אחר ההתפתחויות הטכנולוגיות.

[383] Hollis, 2007; 1031-1032.

[384] ראו: Greenberg, 1998; 23.

[385] Waxman, 2011; 445-446.

לכך מצטרפת הסביבה האסטרטגית המורכבת. כותבים כמו וקסמן, מצביעים על כך שלאורך השנים התנהל מאבק על פרשנות מגילת האו"ם. הפרשנות שנבחרה, ביטאה את הכוח היחסי של המעצמות בהיבטי עוצמה ומשאבים עולמיים. במילים אחרות: למעצמה החזקה - ארצות הברית - הייתה אפשרות לכפות את רצונה ביחס לפרשנות הסעיפים.[386] תופעה זו, שבה התפתחות המשפט הבינלאומי מוכתבת על ידי מדינות חזקות, אינה חדשה ומקובלת כחלק ממאפייניו של תחום משפטי זה.[387] ואכן, הפרשנות שאומצה למגילת האו"ם במהלך המלחמה הקרה הייתה נוחה לארצות הברית. האיסור על שימוש בכוח קונבנציונלי איפשר לארצות הברית להתבסס, ובו בזמן להפעיל את שריריה הכלכליים והדיפלומטיים כדי ללחוץ על מדינות קטנות יותר.[388]

במרחב הקיברנטי, לעומת זאת, חלוקת הכוח והעוצמה שונה מזו הכלכלית-צבאית. למעשה, המגמות אינן לטובת מעצמה כמו ארצות הברית.[389] לארצות הברית יש אמנם עוצמה רבה במרחב הקיברנטי, אך הכוח הוא גם חולשה. כפי שצוין במסמך האסטרטגיה הלאומית של ממשל הנשיא אובמה משנת 2010, הטכנולוגיות שמעצימות את ארצות הברית, מעצימות גם את מי שרוצים להרוס אותה ולפגוע בה:

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority ... Our daily lives and public safety depend on power and electric grids, but

---

[386] Waxman, 2010; 450.

[387] להרחבה: Shaw, 2008; 79-80. ובדברי המחבר:
"This follows from the nature of the international system where all may participate but the views of those with greater power carry greater weight."

[388] שם, 449.

[389] שם, 450-451.

potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale״ .[390]

לארצות הברית אינטרסים בתחום הקיברנטי, הקשורים לפרשנות המשפט הבינלאומי. למשל, היא מעוניינת לאסור פגיעה פיזית באמצעות התקפה קיברנטית; היא מבקשת למנוע התדרדרות של פעילות קיברנטית לסכסוך צבאי, אך להמשיך ולאפשר איסוף מידע קיברנטי, תחום בו היא חזקה.[391] מדינות אחרות פועלות בהקשר של פרשנות הדין ויצירת דין חדש, תחת מערכת שונה של הנחות אסטרטגיות לגבי העתיד. מדינות קטנות רואות במרחב הקיברנטי פוטנציאל לשינוי מאזן הכוח, ואינן מעוניינות בהכרח לחדד את ההגדרות המשפטיות ולהצר את צעדיהן. מדינות רבות חשות בנוח במצב של חוסר בהירות קיברנטי.[392] סין רואה במרחב הקיברנטי כלי מאזן ומשווה כוח מול היתרון הקונבנציונלי האמריקני, ולא תרצה לאמץ משטר משפטי שיגביל את יכולותיה. רוסיה וסין מבקשות לכונן משטר, שיגבה את יכולתן לפקח על תכנים ולהגן על ערכיהן במרחב הקיברנטי.

המאפיינים הטכנולוגיים והסביבה האסטרטגית אינם עומדים להשתנות בקרוב. חוקרים, שבחנו את הניסיון הדיפלומטי שנצבר במלחמה הקרה והדיונים סביב פרשנות מגילת האו״ם, מצביעים על כך שהגעה לקונצנזוס צפויה להיות איטית וקשה. להערכתם, לא תהיה הסדרה כתוצאה ממאמץ דיפלומטי אחד, אלא זו תתפתח באופן לא

---

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

קושי נוסף הוא שלמעצמה דמוקרטית כמו ארצות הברית, קושי לכפות סטנדרטים פנימיים נוקשים על גורמים פרטיים בתחום ההגנה הקיברנטית.

[391] Waxman, 2011; 452.

[392] Schmitt, 2011; 604.

מרוכז, תוך השפעות של שחקנים רבים - מדינות, מוסדות בינלאומיים, גופים בעלי עניין, אקדמיה ועוד[393].

הגעה למשטר משפטי מוסכם היא אפשרית, אלא שבאופן ריאליסטי, ההתהוות של השיח המשפטי, התפתחות פרקטיקה של מדינות, חילופי העמדות (במונחי Reisman), צפויים לארוך זמן רב. התרחיש הסביר הוא שלפחות בשנים הקרובות, המשטר המשפטי יהיה בלתי צפוי[394]. לאט ובאופן הדרגתי, תלך ותתפתח פרקטיקה של מדינות בתגובה לאתגרים קיברנטיים. זו תשפיע לאורך זמן על הפרשנות המשפטית של האמנות הקיימות, ואולי בבוא היום, תבשיל גם להסדרה חדשה, במסגרת אמנה ייעודית.

ההתפתחויות האפשריות

ניתן להצביע על כיווני התפתחות רבים ביחס להסדרה המשפטית של המרחב הקיברנטי, וקשה לצפות ולהעריך מה יילד יום. מבין החלופות הרבות, הוצגו לעיל ארבעה כיוונים מובילים: פרשנות יצירתית וחדשה למונח ׳התקפה מזוינת׳; הרחבת הסעדים הנתונים למדינה במקרה של ׳שימוש בכוח׳ נגדה; אימוץ אמנה חדשה להסדרת כללי המשחק במרחב הקיברנטי; והגישה הריאליסטית - אי הסדרה והתפתחות הדרגתית של פרקטיקה בנושא.

מתוך הכיוונים האמורים, נראה כי ההסתברות להתרחשותו של האחרון היא הגבוהה ביותר. זאת, לאור האתגרים והקשיים בהם צפויה להיתקל הסדרה בשאר הכיוונים, ובהיות תרחיש זה, במידה רבה, מעין ברירת מחדל בסביבה אסטרטגית מורכבת. תהליכי התהוות המשפט הבינלאומי הם, על פי רוב, מורכבים וממושכים. קיים פער בין האידיאולוגיה והכוונות הטובות של מדינות מעל השולחן, לבין הציניות האסטרטגית והריאליזם שמתחתיו.

---

[393] לתיאור התהליך המורכב הזה: Reisman, 2003; 83.

[394] ראו גם: Waxman, 2011; 458-459.

יתכן, עם זאת, כי אירוע מעצב בעל משמעות עולמית של ממש, מעין 'פרל הארבור' או 'פיגועי התאומים' במרחב הקיברנטי, יטרוף את קלפי המשחק ויוביל להאצה בהסדרת הנושא, בין בדרך אמנה חדשה ובין באימוץ פרשנות חדשה לכללי המשפט הקיימים. עבודה זו נפתחה בציטוט של מזכיר ההגנה האמריקני, ליאון פנאטה, אשר התריע בדיוק מפני אירוע טראומטי כזה.

ספק אם התקפות הטרור של ה-11 בספטמבר 2001 יצרו עולם משפטי חדש בתחום המאבק בטרור העולמי, אך בוודאי שהיו בגדר זרז ותרמו להאצת העיסוק המשפטי, תוך יצירת תובנות משפטיות חדשות ומשמעותיות. יש לקוות כי 'פרל הארבור' קיברנטי לא יתרחש, אך אם אסון בסדר גודל כזה יקרה - ניתן לצפות גם קפיצת מדרגה בעיסוק המשפטי.

סיכום ותובנות עיקריות

המרחב הקיברנטי בכלל, ורשת האינטרנט בפרט, נולדו מתוך מחשבה על מרחב דמוקרטי, פתוח, נייטרלי ויצירתי[395]. העולם הקיברנטי אינו מזוהה, בוודאי באופן אינטואיטיבי, עם הגבלות משפטיות ועם משטר משפטי, בוודאי לא בהקשר של שימוש בכוח בין מדינות ודיני מלחמה. ואולם, המרחב הקיברנטי אינו מתנהל בריק משפטי. כפי שאמר בשנת 2012 היועץ המשפטי של מחלקת המדינה בארצות הברית:

"Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint"[396].

עבודה זו מיועדת לפתוח צוהר לחלק מאותם כללים וריסונים, החלים על מדינות בפעולתן במרחב.

ההמלצות המרכזיות, החותמות עבודה זו, קשורות למודעות של מעצבי המדיניות ומקבלי ההחלטות במרחב הקיברנטי, ובפרט הגורמים האמונים על פעילות התקפית והגנתית, לכללים המשפטיים החלים במרחב. ועדת וינוגרד, שבדקה את אירועי מלחמת לבנון השנייה, המליצה כי נושאי דיני הלחימה יוטמעו בדרג המקצועי והמדיני, ויוצגו כחלק מעבודת המטה בנוגע להחלטות רלבנטיות, וכי בדיקתן של תכניות והנחיות מבצעיות, מבחינת התאמתן למשפט הבינלאומי, יהיה שלב מקדים מחייב לפני אישורן[397]. המלצה זו, שלא כאן המקום להרחיב בטעמים שביסודה, יפה גם ביחס למרחב הקיברנטי. בפרט חשובה המודעות בשני אלה: **ראשית**, הבנת המצב המשפטי הקיים, על מנת שניתן יהיה לגזור את השלכותיו על הפעילות הקיברנטית בהווה; **שנית**, הבנת ההקשר האסטרטגי - השנים הקרובות כתקופה מכוננת, בה עתידים להתעצב כללי המשחק והמשטר המשפטי העתידי. ההבנה

---

[395] ראו: Nye, 2010; 3.

[396] נאום Koh.

[397] דו"ח הוועדה לבדיקת אירועי המערכה בלבנון 2006, ועדת וינוגרד, דין וחשבון סופי, ינואר 2008, 493.

עשויה לאפשר גיבוש מדיניות ישראלית משפיעה ואפקטיבית, ככל האפשר, בתקופה חשובה זו.

אשר למצב המשפטי הקיים, מעצבי המדיניות ומקבלי ההחלטות, בישראל (ובעולם), צריכים להיות מודעים, בין השאר, לתובנות הבאות:

א. המשפט הבינלאומי החל על סכסוכים מזוינים (הן דיני ה- Jus ad Bellum, המסדירים שימוש בכוח בין מדינות, והן דיני המלחמה, המסדירים הפעלת כוח במהלך סכסוך מזוין) חלים במרחב הקיברנטי.

ב. פעולה קיברנטית, שיש לה תוצאות פיזיות (מוות, פציעה ונזק משמעותי לרכוש) עלולה להיתפס כ'התקפה מזוינת', ולהצדיק שימוש נגדי בכוח במסגרת הגנה עצמית (על פי סעיף 51 למגילת האו"ם).

ג. פעולה שאלו תוצאותיה בין מדינות עלולה להביא לפריצתו של 'סכסוך מזוין', בו ניתן לפעול גם באמצעים קינטיים, מעולם המלחמה 'הרגיל', ולא רק בכלים קיברנטיים.

ד. כאשר פעולה קיברנטית, הצפויה לגרום מוות, פציעה או נזק לרכוש, ננקטת במהלך 'סכסוך מזוין' קיים, היא עלולה להיחשב 'התקפה' (כמובנה בסעיף 49 לפרוטוקול הראשון של אמנות ז'נבה). ככזו, יחולו עליה כלל האיסורים וההגבלות מתחום דיני המלחמה (למשל האיסור לפעול נגד מטרות אזרחיות, החובה לפעול במידתיות וכיוצא באלו).

ה. איום בפעולה קיברנטית, שצפויה לגרום נזק פיזי, מצד מדינה שיש בידה יכולות קיברנטיות לממש את האיום, עלול להוות 'איום אסור בכוח', העומד בניגוד למגילת האו"ם.

ו. פעולות קיברנטיות, שאינן גורמות לנזק פיזי, אך פוגעות באופן משמעותי במדינה שנגדה הן מבוצעות, עלולות להפר את איסור 'השימוש בכוח' בין מדינות. גם אם הדבר אינו מקנה למדינה

הנפגעת זכות להגנה עצמית, יש לכך משמעויות (שלא יפורטו במסגרת זו).

ז. פעולות קיברנטיות, שהן בגדר לוחמה כלכלית, פסיכולוגית או פוליטית גרידא, אינן מהוות שימוש אסור בכוח. גם ריגול ואיסוף מידע קיברנטיים אינם בניגוד לאיסור זה (לפעולות אלו כמובן השלכות בהקשרים אחרים).

ח. למדינה זכות להגנה עצמית מקדימה, כאשר מדינה אחרת נחושה לבצע נגדה התקפה קיברנטית שתגרום נזק פיזי, והמדינה המותקפת תאבד את ההזדמנות להגן על עצמה באופן אפקטיבי אם לא תפעל מיד.

ט. הגנה עצמית במרחב הקיברנטי רלבנטית גם לנוכח ׳התקפה מזוינת׳, הכרוכה בנזק פיזי, מצד גורם שאינו מדינתי.

רשימה זו אינה כוללנית ואינה ממצה, אלא מיועדת להמחיש תובנות יסודיות, אשר חשוב שתהיינה (בליווי ייעוץ משפטי מתאים וקונקרטי) בידיעת הגורמים האמונים על המרחב הקיברנטי מטעם כל מדינה.

לגבי ההקשר האסטרטגי, על מעצבי המדיניות ומקבלי ההחלטות להבין, כי השנים הקרובות תהיינה שלב מכונן ביצירת כללי משחק ועיצוב המשטר העתידי. זהו שלב מאתגר ומורכב, בו צפויים להתפתח, מצד אחד, מירוץ חימוש קיברנטי, כאשר מדינות וגופים שאינם מדינתיים, יבקשו להעצים את יכולותיהם הקיברנטיות ואת הכלים שברשותם, בהתקפה ובהגנה. מצד שני, צפוי להתחולל קרב איתנים בין מזרח לבין מערב, בו ינסו המעצמות לעצב את המשטר המתפתח, כך שישרת את האינטרסים האסטרטגיים שלהן, בראייה רחבה.

תהליך זה צפוי לארוך זמן ממושך, וישולבו במהלכו ניסיונות לגבש ׳soft law׳ - משטר משפטי שאינו מחייב, אך מיועד להשפיע על הפרקטיקה של מדינות ועל המשטר המשפטי העתידי. ניסוח מדריך טאלין מדגים מאמץ משמעותי ורחב יריעה ברוח זו. עם זאת, הסיכוי

שתיכרת אמנה משפטית מחייבת בהקשר זה, בשנים הקרובות, אינו רב.

ישראל אינה שחקן שולי במרחב הקיברנטי. לדבריה ולמעשיה מיוחסים משקל והשפעה. נראה כי עליה לפעול במספר דרכים מרכזיות:

א. מעקב צמוד אחר ההתפתחויות בזירה הבינלאומית, הבנת תמונת המצב, לימוד המגמות וגיבוש הערכת מצב להמשך.

ב. שותפות, רשמית או באמצעות מומחים, בתהליכי יצירת 'soft law', והשפעה על תוכנם. בנוסף, שותפות והשפעה על תהליכי יצירת משטר משפטי מחייב, ככל שיתפתחו, במוסדות מובילים כמו האו"ם.

ג. הבנה, כי לפרקטיקה הישראלית, הן במעשים והן בהתבטאויות רשמיות של בכירים, עשויה להיות משמעות בעיצוב הסדר העולמי החדש במרחב.

ד. פיתוח מדיניות, מנגנונים ומומחי ידע, שיתמכו בכל התהליכים האמורים.

אחת מאמרותיו הידועות של וינסטון צ'רציל הייתה:

"The empires of the future are the empires of the mind".

כל מי שמבקש להחזיק בכוח ובעוצמה גם בעתיד, חייב ללמוד, להשתנות ולהתאים את עצמו למציאות החדשה. כך באופן כללי, וכך בהקשר המשפטי-קיברנטי בפרט. תקוותי כי העבודה תסייע בכך.

ביבליוגרפיה

סייבל רובי (2010), **משפט בינלאומי**, ירושלים: האוניברסיטה העברית, מהדורה שנייה.

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

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

Boyle Alan E., *Some Reflections on the Relationship of Treaties and Soft Law*, The International and Comparative Law Quarterly 48.4 (1999), 901.

Brownlie Ian, International Law and The Use of Force by States (1963).

Brownlie Ian, Principles of Public International Law (7th ed. 2008).

Carr Jeffrey, Inside Cyber Warfare (2nd ed., 2011).

Clarke Richard A. & Knake Robert K., Cyber War: The Next Threat to National Security and What to Do About It (2010).

Clay Wilson, Cong. Research Serv., RL32114, Computer Attack And Cyber Terrorism: Vulnerabilities and Policy Issues for Congress (2003).

Crowell Richard M., War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare (2012).

Detter Ingrid, The Law of war, (2nd ed.,2000).

Dinniss Heather H., Cyber Warfare and the Laws of War (2012).

Dinstein Yoram, *Computer Network Attacks and Self-Defense*, 76 Int'l L. Stud. 99 (2002).

Dinstein Yoram, War, Aggression and Self Defence (5th ed. 2011).

Elliot David, *Weighing the Case for a Convention To Limit Cyberwarfare*, Arms Control Today (Nov. 2009).

Farer Tom J., *Political and Economic Coercion in Contemporary International Law*, 79 Am. J. Int'l L. 405 (1985).

Geyer Felix & Van der Zouwen Johnnes, *Norbert Wiener and the Social Sciences*, Kybernetes, Vol. 23 ,6, 46 - 61 (1994).

Gill Terry D., *The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy*, in International Law and Armed Conflict: Exploring the Faultlines 113 (Michael N. Schmitt & Jelene Pejic eds., 2007).

Gray Christine, *The Use of Force and International Legal Order*, in International Law (Malcolm Evans ed. 2003).

Gray Christine, International Law and the Use of Force (3rd ed. 2008).

Greenberg Lawrence T., Goodman Seymour E. & Soo Hoo Kevin J., Information Warfare and International Law (1998).

Hathaway Oona A., 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.

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

Hollis Duncan B., *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023 (2007).

Hughes Rex, *Towards a Global Regime for Cyber Warfare*, in The virtual battlefield: perspectives on cyber-warfare 106 (Christian Czosseck and Kenneth Geers, eds., 2009).

Jensen Eric T., *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence*, 38 Stan. J. Int'l L. 207 (2002).

Joyner Christopher C. & Lotrionte Catherine, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 Eur. J. Int'l L. 825 (2001).

Kanuck Sean P., *Information Warfare: New Challenges for Public International Law*, 37 Harv. Int'l L. J. 272 (1996).

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

Krepinevich Andrew F., 7 Deadly Scenarios: A military Futurist Explores War in the 21st Century (2009).

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

Lewis James A., *Multilateral Agreement to Constrain Cyberconflict,* Arms Control Today (June 2010).

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

Libicki Martin C., Cyberdeterrence and Cyberwar (2009).

Maurer Tim, *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).

Nye Joseph S., *Cyber Power*, Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010).

O'connell Mary E., *The Myth of Preemptive Self-Defence,* American Society of International Law Task Force On Terrorism Paper Series.
Available at: http://www.asil.org/taskforce/oconnell.pdf.

Ottis Rain, *From Pitchforks to Laptops: Volunteers* in Conference on Cyber Conflict, Proceedings 2010, 97 (Czosseck Christian & Podins Karlis eds., 2010).

Owens William, Lifting the Fog of War (2001).

Paust Jordan J., *Self-Defense Targeting of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan,* 19 J. Transnat'l L. & Pol'y 237 (2010).

Pomerance Michla, *The ICJ's Advisory jurisdiction and the Crumbling Wall Between the Political and the Judicial*, 99 (1) Am. J. of Int'l L. 26 (2005).

Reisman Michael W., *Assessing Claims To Revise the Laws of War*, 97 AM. J. INT'L L. 82 (2003).

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

Rosenzweig Paul, *International Law and Private Actor Active Cyber Defensive Measures* (May 27, 2013). Stanford Journal of International Law, Vol. 47, Forthcoming. Available at: http://ssrn.com/abstract=2270673 or http://dx.doi.org/10.2139/ssrn.2270673

Schmitt Michael N., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

Schmitt Michael N., *Wired Warfare: Computer Network Attack and the Jus in Bello,* in Computer Network Attack and International Law 187 (Michael N. Schmitt & Brian T. O'donnell eds., 2002).

Schmitt Michael N., *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework,* 56 Naval L. Rev. 1 (2008).

Schmitt Michael N., *"Change Direction" 2006: Israeli Operations in Lebanon and the International Law of Self-defense,* 29 Mich. J. Int'l L. 127 (2008). (Schmitt 2008(2)).

Schmitt Michael N., *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, in National Research Council of the National Academies, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (2010).

Schmitt Michael N., *Cyber Operations and the Jus Ad Bellum Revisited*, Villanova Law Review, Vol. 56, 569 (2011).

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

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

Schmitt Michael N, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 Harv. Int'l L. J. Online 13 (2012). (Schmitt, 2012(2)). Available at: http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.

Schmitt, Michael N., *Classification of Cyber Conflict*, 17 Journal of Conflict and Security Law 245 (2012). (Schmitt, 2012(3)).

Sharp Walter G. SR., CyberSpace and the Use of Force (1999).

Shaw Malcolm N., International Law (6th. ed., 2008).

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

Silver Daniel B., *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, in Computer Network Attack and International Law 73 (Michael N. Schmitt & Brian T. O'donnell eds., 2002).

Sloane Robert D., *The Cost of Conflation: Preserving the Dualism of Jus Ad Bellum and Jus in Bello in the Contemporary Law of War*, 34 YALE J. INT'L L. 47 (2009).

Smith Jeffrey H., *State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543 (2007).

Tallinn Manual on The International Law Applicable to Cyber Warfare (2013).

Thomas Timothy L., *Nation-state Cyber Strategies: Examples from China and Russia*, in Cyberpower and National Security 465 (Kramer Franklin D., Starr Stuart H. & Wentz Larry K. eds. 2009).

Tikk Eneken, Kaska Kadri & Vihul Liis, International Cyber Incidents: Legal Consideration (2010).

Walker George K., *Information Warfare and Neutrality*, 33 Vand. J. Transnat'l L. 1079 (2000).

Watt Sean, *Combatant Status and Computer Network Attack*, 50 VA. J. Int'l L. 391 (2010).

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

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

Weiner Norbert, Cybernetics, or Control and Communication in the Animal and the Machine (1948).

Weiner Norbert , The Human Use of Human Beings - Cybernetics and Society (1954).

עשתונות - במה למחשבות ורעיונות

עורכת: סגן אלוף נאוה גרוסמן-אלוני

מרכז המחקר של המכללה לביטחון לאומי
ראש המרכז: פרופ׳ ארנון סופר

מרכז המחקר של המכללה לביטחון לאומי שואף לעסוק בחקר תופעות מתהוות בהקשרי הביטחון הלאומי, מפתח ידע אקטואלי להוראה במכללה ומשתתף בניסיון לנסח תפיסת ביטחון רשמית ועדכנית למדינת ישראל, בהובלת המטה לביטחון לאומי. חצר המכללות מבקשת לשמש אכסניא ובית מדרש, אשר בו יתפתח ידע חדש ורלבנטי עבור גופי הביטחון הלאומי, מכללות צה״ל וגופי מחקר עמיתים, בארץ ובחוץ לארץ, ובהשתתפותם. המרכז שם לו למטרה לממש את הייעוד המחקרי של המכללה לביטחון לאומי, תוך ניצול יתרונו היחסי בתחום הביטחון הלאומי כמקום מפגש בין-ארגוני ולאור ניסיונם המעשי של התלמידים, הבא לידי ביטוי במחקר.

השנה מתמקד מרכז המחקר בנושאים הבאים:
הופעת אזורי ׳הספר הפרוע׳ המתפתחים לאורך גבולותיה של מדינת ישראל (סיני, רמת הגולן, ירדן וכדומה);
ממד הסייבר כמרחב חדש בהקשרי הביטחון הלאומי;
איראן ב׳יום שאחרי׳;
תשתיות לאומיות ועורף צבאי;
בחינה אופרטיבית של תפיסת ההכרעה וההרתעה של צה״ל
תפישת הביטחון של מדינת ישראל

מפקד המכללות: אלוף יוסי בידץ

המדריך הראשי: אלוף משנה איציק כהן

סגל המדריכים: אלוף משנה אורן גוטר, מר זאב בוקר, ניצב משנה גדעון מור, ד״ר רדא מנצור, תת ניצב יעקב מבורך

חברי מרכז המחקר: פרופ׳ ארנון סופר, ד״ר פיני יחזקאלי, ד״ר דימה אדמסקי ד״ר עפרה גרייצר, ד״ר אודי ערן, אלוף משנה (במיל׳) גור ליש

עמיתי מחקר: אלוף משנה יורם כנפו, אלוף משנה דרור שלום, עו״ד רם רביב

מרכז המחקר של המכללה לביטחון לאומי

מחנה דיין, גלילות, ד״צ 02624, צה״ל

טל׳: 03-7607335, דוא״ל: navag@indc.org.il

הודפס בבית הדפוס של המכללות הצבאיות

צבא ההגנה לישראל, המכללה לביטחון לאומי

ראו אור בסדרה:

צפרי-אודיז מירב (2013), **השלכות התגרענותה של איראן על 'הסדר הגרעיני העולמי** (גיליון 4)

אורטל ערן, תמיר ידעי (2013), **'פרדיגמת סבבי ההרתעה' - דפוס אסטרטגי ודוקטרינה במבוי סתום** (גיליון 3)

אורטל ערן (2013), **חדשנות פרדיגמטית בצה"ל? על למידה בהקשרי בניין הכוח, הפעלתו ומה שביניהם** (גיליון 2)

אורטל ערן (2013), **על העברת מלחמות האש לשטח האויב ועל הכרעה פרדיגמטית** (גיליון 1)

עשתונות* - במה למחשבות ורעיונות היא סדרה עתית הרואה אור במסגרת מרכז המחקר של המכללה לביטחון לאומי. הדברים המובאים בה נועדו להביא לקהילת הביטחון הלאומי, מחשבות, תפיסות ורעיונות רעננים וחדשניים בנושאים הרלבנטיים לה. הקוראים מוזמנים להרהר ולערער אחר הדברים. אנו חותרים לשיח מאתגר, פתוח וביקורתי, מתוך אמונה ששיח כזה יחדד את עשתונותינו - לבל נאבדם.

***במקרה של אובדן, נא לפנות לגורמים המוסמכים.**

עֶשְׁתּוֹן ז' (מן עשת; מצוי בספרות בעיקר בריבוי) עֶשְׁתּוֹנוֹת, עֶשְׁתּוֹנִים - מחשבות, רעיונות. "כי רבים עשתוני בני אדם" (בן-סירא ג כב); "ורחקו מאד מחשבות איש מעזוז עשתונותיו" (אברהם אבן-עזרא, א 192); "עיניו מפליגות בחלומות וברעיונות עשתונות שונים" (הזז, צל, 120); "אבדו עשתונותיו" (שאול מתהילים קמו ד): נבוך, התבלבל.

(מילון אבן-שושן)

מרכז המחקר, המכללה לביטחון לאומי