המרכז הבינתחומי הרצליה

מדיניות התגובה למתקפת טרור סייבר

אסף נקש

המחקר זכה במקום הראשון במסגרת תחרות מלגות קרן רגוניס לשנת 2016-2017
לעידוד עבודות מחקר התחום הלוחמה בטרור והגנת המולדת
המלגות הוענקו לזכרו של רס״ן איל רגוניס ז״ל לאור פועלו בתחום העשייה הצבאית והאזרחית

הקדמה

החוקר אסף נקש, בן 25 מרמת גן. אסף בוגר קורס קציני מודיעין בהצטיינות ובעל הכשרה מקצועית במגוון קורסים בתחום אבטחת המידע והסייבר. במסגרת הכשרותיו, אסף בוגר קורס 'האקרים אתיים' Certified "Ethical Hacking בהסמכה בינלאומית מאת EC-Council וכמו כן, בוגר קורס מודיעין סייבר ביחידת 8200 באמ"ן. אסף נקש בן 25 מרמת-גן שרת בעת כתיבת המחקר במחלקת מבצעים בחטיבת ההגנה בסייבר במקביל ללימודיו האקדמאיים כסטודנט, מצטיין דיקן, בשנה ב' לתואר LL.B במשפטים במרכז הבינתחומי הרצליה. אסף זכה במלגת לשכת עורכי הדין לשנת תשע"ו בגין הצטיינותו הלימודית בשילוב תרומה חברתית ענפה.

המחקר עוסק באיום טרור מסוג סייבר, אשר נמצא בליבת עיסוקם של גורמי ההגנה והביטחון במדינת ישראל ובעולם כולו. בהתבסס על מגמות עולמיות בתחום הטרור והסייבר, מתגבשת הנחה לפיה ארגוני הטרור עתידים לעשות שימוש במרחב הסייבר לשם השגת יעדים אסטרטגיים. ההבנה כי טרור סייבר עתיד להיות מרכיב בארגז הכלים של ארגוני הטרור, מאתגרת את גורמי ההגנה במניעת מתקפות אלו וסיכולן. בתוך כך, עולים אתגרים משפטיים וטכניים לאיתור מוקד התקיפה וזהות התוקף, ואלו משפיעים על בחירת מדיניות התגובה. במסגרת המחקר, נותחו חמישה מקרי בוחן והתקיימו שבע פגישות מחקריות עם בכירים במערכת הביטחון ומוקדי ידע בתחום הגנה בסייבר, המשפט והטרור. מחקר זה 'צופה פני עתיד' בדבר האיום הפוטנציאלי של התממשות איום טרור הסייבר. ולפיכך, מהווה אבן יסוד בתחום מדיניות התגובה למתקפות אלו.

המחקר זכה במקום הראשון במסגרת תחרות מלגות קרן רגוניס לשנת 2016-2017 ע"ש רס"ן איל רגוניס ז"ל. לאור זאת, בחר מכון ICT בנושא טרור-סייבר כנושא המרכזי בערב חלוקת המלגות. במעמד זה, לקחו חלק משפחתו של אייל רגוניס ז"ל, משה (בוגי) יעלון חבר קרוב של המשפחה, ד"ר אביתר מתניה - ראש מטה הסייבר הלאומי במשרד רה"מ, פרופ' בועז גנור -מנכ"ל ומייסד המכון למחקר טרור ודיקן ביה"ס לממשל במרכז הבינתחומי, ד"ר עמיחי מגן, ד"ר דימה אדמסקי וד"ר דרור הראל.

תוכן עניינים

<u>פרק א'</u>

1. הגדרת המונח 'טרור-סייבר':

המונח טרור הוכר תחילה בראשית שנות השישים של המאה העשרים. מאז ועד היום ישנו קושי רב במציאת הגדרה כוללת ומוסכמת למונח 'טרור'. פרופ' בועז גנור[1] מגדיר טרור כסוג של מאבק אלים אשר במסגרתו נעשה שימוש מכוון באלימות כלפי אזרחים, לשם השגת מטרות פוליטיות (לאומית, חברתית-כלכלית, אידאולוגית, ודתית). הגדרתו מתבססת על שלושה נדבכים המגדירים פעולה כפעולת טרור: מהות הפעולה, המטרה שעומדת בבסיסה ויעד הפגיעה של הטרור. הצעה זאת יכולה להוות מענה ללקונה הקיימת בחקיקה ובאמנות הבינלאומיות במטרה לפתח כלי עזר בסיסי למאבק בינלאומי משותף. הטרור עושה שימוש בזריעת חרדה ופחד בקרב הציבור, זאת במטרה להשפיע על יכולת השלטונות לשמור ביעילות על הסדר הציבורי ובתקווה אף לחולל שינוי חברתי-פוליטי. בהקשר זה יצוין, כי **ישנה מחלוקת מהותית בנוגע להגדרת המונח טרור. מחד, סין ורוסיה המתייחסות לטרור כפעילות לטובת שמירה על זכויות האדם בתוך המדינה ומאידך, מדינות המערב ובהם ישראל מתייחסת לטרור כפעולה לאומנית כנגד אוכלוסייה אזרחית**. יצוין, כי הבחנה מהותית זו בנוגע להגדרת המונח טרור אינה מוסדרת באופן מיטבי בחוק הישראלי. בתוך כך, הועלתה **הצעת חוק המאבק בטרור[2]-** הצעה המהווה ניסיון להסדיר את החקיקה הישראלית הפנימית ולסייע בהתאמת האמצעים שבידי הרשויות להתמודדות עם איומי הטרור המתחדשים. החוק נועד לאזן בין האינטרסים הביטחוניים לבין השמירה על עקרונות היסוד של השיטה הליברלית-דמוקרטית וזכויות האדם הנהוגות במדינה.

על אף הרושם כי סייבר הינו מונח בין ימינו, את תחילת דרכו עשה בעת העתיקה. במקור שאוב המונח מפועל בשפה היוונית שמשעמו לנתב או לנווט. כיום מופיע בעיקר בהטיה בעברית 'קיברנטי' ובאנגלית CYBER. המרחב הקיברנטי הוא מרחב מורכב להגדרה אך ניתן להתייחס אליו כאל מרחב הכולל את כלל המחשבים בעולם והרשתות המקושרות אליהם וביניהם. המרחב הקיברנטי הוא מרחב מטאפורי (cyber space) והוא מרחב של מחשבים ורשתות בהם נאגרים נתונים אלקטרוניים, המאפשר תקשורת אינטראקטיבית ללא תלות במיקום גאוגרפי של המשתמשים בו. בלבו של המרחב הקיברנטי מצויה רשת האינטרנט אליה מקושרים כשליש מהאנושות. התלות של האנושות ברשת האינטרנט הולכת וגוברת ובתוך כך גם החשיפה לאיומים. **מרחב האינטרנט מאפשר בלחיצת כפתור לבצע פעולה העשויה להשפיע באופן מידי על מדינה אחרת**, יכולת זו הינה חיובית כל עוד שימושה הן למטרות טובות כמו לדוגמא העברת מידע והנגשתו למשתמש אחר ברחבי העולם.

הגדרת טרור סייבר - ההגדרה הראשונה המשמעותית למונח טרור סייבר שייכת לדנינג[3]: (Denning, 2000) - תקיפות לא חוקיות ואיומים על תקיפות נגד מחשבים, רשתות ומידע השמור בתוכם במטרה להשיג מטרות פוליטיות או חברתיות על ידי הפחדה או הפעלת לחצים אחרים. נוסף על כך, כדי שתקיפה תיחשב לסייבר-טרור, עליה לכלול אלימות המופנית כלפי אנשים או רכוש, או לפחות לגרום די נזק לזרוע פחד.

[1] http://ictlib.cet.ac.il/pages/item.asp?item=16561
[2] http://knesset.gov.il/committees/heb/material/data/H07-10-2015_14-42-37_.pdf
[3] http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

לאור האמור לעיל, טרור-סייבר הינו שילוב המציב בפני החברה המודרנית איום טרור חדש (Cyberterrorism). ההבדל בין סוגי הטרור טמון באמצעים בהם עושים שימוש, בעוד בטרור קונבנציונלי נעשה שימוש באמצעים פיזיים מוחשיים (חומר נפץ, פיגועים, חטיפת מטוס וכדומה) הרי בסייבר-טרור האמצעי לביצוע הפעולה הוא האינטרנט- רשתות המחשב המקשרות בין מחשבים. החברה מודרנית תלויה כמעט לחלוטין במערכות המחשוב לצורך המשך חיים תקין ומסודר, ולפיכך האיום בחדירה לאחת ממערכות אלו, דוגמת חדירה למערכת החשמל ושיבושה, מהווה איום מהותי על אזרחים רבים. כמו כן, לטרור מסוג סייבר יתרונות נוספים ביחס לטרור במרחב הפיזי כדוגמת האנונימיות שבתקיפת סייבר, היעדר סיכון חיי אדם, היכולת לבצע פעילות לאורך זמן מבלי להיתפס, היכולת להגיב במקרים חריגים באופן מידי, מקסום אפקט ההשפעה וצמצום פערי הכוחות עם מדינות מודרניות חזקות המבוססות מערכות ממוחשבות. לא מן הנמנע, כי ארגוני הטרור הממקדים פעילותם בפיגועי תופת במרחב הקינטי, עשויים בתוך זמן הקרוב להסב משאביהם למתקפת טרור בסייבר[4]. יצוין, כי תרחישים בקנה מידה זה לא אירעו עד כה אך כלל **מומחי הסייבר סבורים כי שאלת התממשות האיום אינה השאלה העומדת במוקד הנושא, אלא שאלת מועד ואופן התממשות האיום**.

הגדרות נוספות לטרור מסוג סייבר ניתנו ע"י [5] **US State Department** - משרד החוץ האמריקאי[6], **CSIS**- המרכז ללימודים אסטרטגים ובינלאומיים[7], **FBI**[8] - Federal Bureau of Investigation: לשכת החקירות הפדרלית, **FEMA**[9] - הסוכנות הפדרלית לניהול מצבי חירום של ארצות הברית, **OSCE**[10] - Organization for Security and Co-operation in Europe, **קבוצת העובדה של האו"ם** במאבק כנגד שימוש הטרור באינטרנט [11], **ITU**[12] - סוכנות מיוחדת של האו"ם לטכנולוגיות מידע ותקשורת, **EC**[13] **ומועצת אירופה**[14] - ארגון בינלאומי הפועל למען שיתוף פעולה בין מדינות אירופה.

הפוטנציאל הטמון בסייבר-טרור מעורר שאלה מהותית בדבר יכולת ארגוני הטרור לבצע תקיפה מסוג זה. יש הטוענים כי בשלב זה, למרבית הטרוריסטים בעלי המוטיבציה לביצוע פעולות טרור בסייבר אין יכולת לעשות כך. אולם, טענה זו איננה עומדת בקנה אחד עם התפתחות הטכנולוגיה, היקף המידע הזמין במרחב האינטרנט והתרבותם של האקרים (פצחנים בעברית) אשר מעמידים למכירה את יכולתם הטכנולוגית ברשת האפלה- Dark Net. לא מן הנמנע, כי בעתיד ארגוני הטרור יפנימו את פוטנציאל הנזק הטמון בהעסקת פושעי סייבר כבסיס לפעילות טרור בסייבר ויסבו את משאביהם לתחום זה.

---

[4] http://michal.harel.org.il/cmc.htm
[5] Adv. Deborah Housen-Couriel, The envolving law on Cyber Dilemmas in International Law and Israeli law, 2013.
[6] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 15 August 2005, p. I-4: "Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves."
[7] CSIS has defined it as "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population." (James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, 2002, p.1).
[8] FBI- "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, ICTWPS March 2013 [13]/28. in furtherance of political or social objectives." As cited in S. Gordon and R. Ford, Cyberterrorism?, Symantec White Paper, p.4 (no date).
[9] Referenced in ENISA Threat Landscape, 8.1.2013 (https://www.fas.org/sgp/crs/terror/RL32114.pdf).
[10] Brussels Ministerial Declaration of 7 December 2006, Decision No. 7/06, "Countering the Use of the Internet for Terrorist Purposes", at #9 (http://www.osce.org/mc/23078). http://www.osce.org/cio/126475
[11] UNODC, supra note 12
[12] See the ITU's 2010 Toolkit for Cybercrime Legislation , and its analysis below.
[13] http://www.cleanitproject.eu/about-the-project/
[14] Council of Europe, "Cyberterrorism – the use of the internet for terrorist purposes", 2008

העתיד לבוא

כיום, מדינות מפותחות, ובתוכן ישראל, מבינות כי אלמלא השקעת משאבים בהגנה מפני מתקפות סייבר, האיום עלול להתממש. בניגוד להבנה ההיסטורית שלנו לגבי קרבות פייסים, במרחב הקיברנטי היתרון תמיד עומד לצד התוקף בשל האופי הא-סימטרי של ההתקפה. כתוצאה מכך, **פוטנציאל הפגיעה של ארגוני הטרור באמצעות מרחב הסייבר עשויה להוביל לתוצאות זהות לטרור הקונבנציונלי ואף לתוצאות חמורות ממנו.**

2. השינויים המרכזיים בגופי הסייבר במדינת ישראל

בשנת 2011 ראש ממשלת ישראל, בנימין נתניהו, החליט להקים מטה סייבר לאומי, נוכח פוטנציאל האיום הטמון בסייבר, אשר החל לפעול בשנת 2012. במסגרת תפקיד המטה, נקבע כי יגבש אסטרטגיה מדינתית להגנה בסייבר, מתן המלצות למדיניות קיברנטית ויישומן בפועל. בהמשך לכך, ב - 14 בספטמבר 2014, הוחלט על הקמת **רשות לאומית להגנה** אופרטיבית בסייבר. הרשות עתידה לקבל אחריות וסמכות הנדרשות להגנת המרחב האזרחי מפני איומי סייבר. כמו כן, במסגרת החלטת הקמת הרשות, נקבע[15] כי תנהל את פעולות ההגנה כדי לתת מענה מקיף נגד תקיפות סייבר לרבות טיפול באיומים ואירועים בזמן אמת. הרשות תפעיל מרכז לסיוע בהתמודדות עם איומים CERT[16] הלאומי, במטרה לחזק את חוסנם של כלל הארגונים והמגזרים במשק. **CERT-IL** [17]הינו מרכז לאומי שנועד לחזק את החוסן של המשק הישראלי בסייבר באמצעות מתן סיוע ראשוני וטיפול באיומי סייבר וכן ריכוז מידע רלוונטי מכלל הגופים בישראל ובעולם. מתפקידיו המרכזיים של המרכז- טיפול באירועי סייבר, טיפול בחולשות, בפוגענים, התמודדות ומניעה של איומי סייבר, פיתוח ידע להתגוננות מפני האיום ותפיץ את תובנותיה לקהל היעד הרלוונטי לתקיפה. בנוסף, כחלק מתפקידה לבצע הסברה , העלאת מודעות מדינתית ופיתוח קשרים עם גופים מקבילים בעולם.

בנוסף לשינוי הארגוני המשמעותי אותה מובילה ממשלת ישראל, ניתן להשליך על חשיבות הנושא מתוך התבטאויותיו של בנימין נתניהו, ראש הממשלה (23.06.15): "לפני כמה שנים הצבתי יעד לדאוג לכך שישראל תהיה אחת המדינות המובילות בעולם בתחום של ביטחון סייבר. תפקידי כראש ממשלה הוא להבטיח שהיא תישאר כך[18]".

זרוע סייבר בצה"ל- באחרונה (15.6.15) החליט הרמטכ"ל רב-אלוף[19] ,גדי איזנקוט, כי לאור האתגרים המשמעותיים איתם מתמודד צה"ל בממד הסייבר, נדרשת הקמת זרוע סייבר אשר תוביל את הפעילות המבצעית במימד זה. רא"ל אייזנקוט ציין כי הקמת הזרוע הינה בעלת חשיבות עליונה להתאמת צה"ל לשינויים בזירת הלחימה ומהווה נדבך נוסף בדינמיות של צה"ל. לדבריו, מימד הסייבר הופך משמעותי מיום ליום והקמת הזרוע תאפשר לפעול הן הגנתית והן התקפית בצורה טובה יותר בזירות אלו. יצוין, כי בעוד ארה"ב מפעילה פיקוד סייבר[20], החלטתו של רא"ל אייזנקוט הינה כי בצה"ל הסייבר איננו פיקוד לחימה אלא מרחב לחימה נוסף בדומה לזרוע יבשה, אוויר וים. בשלב הראשון בצה"ל, הוחלט על הקמת חטיבת ההגנה

[15] http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber150215.aspx
[16] CERT – Community Emergency response team.
[17] https://cert.gov.il/About2/mission/Pages/mission.aspx
[18] http://gpo.gov.il/NewsRoom/GPOnews/Pages/pm230615q.aspx
[19] http://www.idf.il/1133-22318-he/Dover.aspx
[20] http://www.arcyber.army.mil/org-uscc.html

בסייבר[21] באגף התקשוב. בראש החטיבה יעמוד תא״ל [22] שיהיה אחראי על מאמצי ההגנה בסייבר אשר מפקדו יהיה בשלב זה ר׳ אגף התקשוב. כחלק מתפקידיה של החטיבה יושקעו מאמצים באיסוף מודיעיני מוכוון הגנה, כמו גם בכוח אדם מותאם ויכולות טכנולוגיות לחיזוק יכולות ההגנה בסייבר. כמו כן, החטיבה תהיה אחראית על תיאום אופרטיבי בשעת פעילות.

לאור התבטאויותיו של בנימין נתניהו, ראש ממשלת ישראל, החלטותיו בנוגע להקמת רשות נוספת להגנה בסייבר ולאור השינויים בתחום הגנה בסייבר בצה״ל נראה כי **מדינת ישראל שואפת להוביל בתחום הקיברנטי הבינלאומי**. בתוך כך, עליונותה של ישראל במרחב הקיברנטי עשויה להשפיע על יכולותיה ההגנתיות, ההתקפיות ובסיוע במאמץ הבינלאומיים בתחום ההגנה בסייבר.

<u>פרק ב׳ - בחינת הקשיים בסייבר - הדינים המשפטיים והפערים הטכניים</u>

הקדמה : בחינת הדינים המשפטיים

פרק זה מתייחס לדילמות המשפטיות בדבר יישום הדינים הבינלאומיים הפומביים למרחב הסייבר וכן לדינים הפנימיים הנוגעים לסייבר בישראל. הניתוח כולל את הדין הפנימי בישראל ואת הדין הבינלאומי-פומבי אשר עסק באיום הקינטי, ללא התייחסות מפורשת לאיום הקיברנטי שטרם היה באופק.

1. דיני המשפט הבינלאומי-פומבי במרחב הקיברנטי

במדינות המערב, המובילות בעיסוק בדיני המשפט הבינלאומיים, אין דעה נחרצת בדבר תחולת המשפט הבינלאומי על המרחב הקיברנטי. בבחינת העמדה הדומיננטית בקרב גורמים רשמיים של **ארה״ב**, נראה כי מבחינתם **יש ליישם את כללי המשפט הבינלאומי על המרחב הקיברנטי**. על העמדה האמריקאית הרשמית ניתן ללמוד ממסמך האסטרטגיה הבינלאומית למרחב הקיברנטי שפורסם בשת 2011-

"[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 behavior - in times of peace and conflict - also apply in cyberspace"

בראייתם, המבוססת על פסיקת בית הדין הבינלאומי בהאג בסוגיית חוקיות השימוש בנשק גרעיני, ההבדל המהותי בין שימוש בנשק קונבנציונאלי לעומת השימוש במחשבים לא מבטל את תחולתם של עקרונות היסוד כמו איסור השימוש בכוח. לצד קביעה עקרונית זו, ישנן דעות שונות בנוגע לאופן יישומן של הכללים הבינלאומיים במרחב הקיברנטי. העמדה האמריקאית הרשמית היא שנדרשת עבודה משפטית מעמיקה, במטרה לקבוע כיצד הכללים חלים וכיצד יש ליישמן. שותפים לעמדה זו, אנשי משפט ומדינות רבות קוראים ליצירת בהירות בכל הנוגע ליישום כללי הדין הבינלאומי במרחב הקיברנטי. בטענתם, מתבססים על העובדה כי המרחב הקיברנטי התקדם במהירות רבה בעוד הדינים הבינלאומיים לא עברו שינויים בהתאם. המרחב הקיברנטי מאתגר את הקביעות המסורתיות של המשפט הבינלאומי. בתוך כך, ההפרדה בין תשתיות צבאיות

[21] http://www.tikshuv.idf.il/901-8536-he/tikshuv.aspx#.Vtx4LPl97IU
[22] http://news.walla.co.il/item/2911579

לתשתיות אזרחיות, בין הגנה להתקפה אשר נקבעו בבחינת הפעולות הקינטי, לא ניתנות להקבלה באופן מלא לפעולות במרחב הקיברנטי. אולם, למשפט הבינלאומי ניסיון עבר עם הרחבת הלחימה לממדים נוספים כדוגמת אוויר, חלל וים לאור התפתחות הטרור העולמי, ובהתאם לכך, קיימת גישה לפיה ניתן להרחיב את הדינים למרחב לחימה נוסף- מרחב הסייבר.

נוכח האמור לעיל, היעדר הסכמה בינלאומית בדבר יישום המשפט הבינלאומי על המרחב הקיברנטי מוביל את יחסי המדינות בתחום זה למצב נפיץ בו כל מדינה תפרש את החוק בהתאם לצרכיה ותפעל בהתאם לשאיפותיה ומטרותיה המדיניות. היעדר בהירות במצב המשפטי הקיים, עלול להוביל לתרחיש בו מדינה תבחר להגיב להתקפה קיברנטית משמעותית באמצעות הפעלת אמצעים קינטיים, דבר שעשוי להוות עילה לפתיחה במערכה מזוינת. דוגמא לכך ניתן לייחס לדו"ח משרד ההגנה האמריקאי משנת 2011 בו נכתב כי ארה"ב שומרת לעצמה את הזכות להגיב להתקפות קיברנטיות, בשימוש כל האמצעים הקיימים דיפלומטיים, קיברנטיים, צבאיים וכלכליים[23].

תחולת הדינים הבינלאומיים בעת סכסוכים מזוינים במרחב הקיברנטי

כללי המשפט הבינלאומי החלים בעניין סכסוכי מזוינים כוללים שני גופים נפרדים של דינים: Jus ad Bellum ו- Jus in Bello.

- **דיני Jus ad Bellum** - המשפט הבינלאומי מגביל את זכות המדינות להשתמש בכוח צבאי אל מול מדינות אחרות, מסגרת הכללים זו מכונה Jus ad Bellum. דינים אלו בין היתר, עוסקים באיסור שימוש בכוח בין מדינות ובחריגים לכך. תכלית כללים אלו הינה שמירה על יחסי שלום וקביעת רף משפטי גבוה לנקיטת אמצעים צבאיים כצעד כוחני.
- **דיני Jus in Bello** - דינים אלו חלים בעת סכסוך, מכונים גם 'דיני מלחמה' (Law of War) ובשם נוסף דיני הסכסוך המזוין (Law of Armed Conflict). במחקרי זה אעשה שימוש במונח דיני מלחמה על מנת לתאר סוג זה של דינים. האו"ם וארגון הצלב האדום מתייחסים למונח המשפטי 'משפט הומניטרי בינלאומי' (International Humanitarian Law) על מנת לבחון את השאלה המרכזית בעימותים מזוינים- האם הסכסוך מלכתחילה הינו חוקי או בלתי חוקי על-פי המשפט הבינלאומי. תכלית דינים אלו לצמצם פגיעה בגוף וברכוש בדגש על פגיעה שאיננה נחוצה לצורך השגת המטרה הצבאית. תכלית זו מושגת באמצעות הצבת איסורים והגבלות על ביצוע מתקפות.

[23] 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

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

מגילת האו"ם חלה על מדינות האומות המאוחדות והיא המסמך המכונן של ארגון האומות המאוחדות, אשר מהווה חוקה לארגון. המגילה נחתמה ב-26 ביוני 1945 בוועידת האומות המאוחדות בנושא ארגון בינלאומי, אשר התקיימה בסן פרנסיסקו, ארצות הברית, על ידי 50 מתוך 51 המדינות שהיו חברות בארגון באותה העת (המדינה ה-51, פולין, לא נכחה בוועידה אך חתמה על המגילה מאוחר יותר), ונכנסה לתוקף ב-24 באוקטובר 1945, לאחר אישור חמשת החברות הקבועות במועצת הביטחון של האו"ם ויתר המדינות החתומות.

הצורך בהגבלת השימוש בכוח נובע מהבנה לפיה בעבר מדינות ראו בכך דרך לגיטימית לקידום אינטרסים ולאור זאת נדרש איסור על השימוש בכוח כחלק ממגילת האו"ם. ההוראה המרכזית, המעגנת את עיקרון האיסור השימוש בכוח היא הוראת סעיף 2(4) למגילה: "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". ניתן לייחס להוראה זו תחולה על מדינות שאינן חברות באו"ם מתוך תפיסת ההוראה כמבטאת משפט בינלאומי מנהגי "General practice accepted as law". החידוש בא לידי ביטוי בהוספת איסור האיום בכוח לצד איסור השימוש בכוח. בתוך כך, אמירה שאינה מהווה איום באופן מובהק, ככל הנראה לא תכנס תחת הגדרת האיום בהתאם ללשון המגילה.

הוראת המגילה נוקטת מינוח כללי בהתייחסותה לשימוש בכוח 'Use of force'. האיסור חל על שימוש בכוח כחלק התקפות צבאיות או על פעולה הנכנסת תחת הגדרת אלימות מזוינת (Armed violence) שאינה התקפה צבאית. הסעיף עושה שימוש במונח force ולא ב armed force ובכך מרחיב את המונח שימוש בכוח לפעולות נוספות האסורות על מדינה מלבד שימוש בכוח פיזי. כתוצאה מפרשנות מרחיבה זו ניתן להניח כי בדומה לפעולה קינטית, שימוש בכוח באמצעים קיברנטיים נדרש לעמוד ברף חומרה בעל פוטנציאל השפעה מוכח. לפיכך, לא כל פעולה באמצעות שימוש במחשבים מהווה התערבות אסורה. התערבות טומנת בחובה כפייה ולפיכך פעולת ריגול שקטה שאינה מפריעה למדינה לעבודתה השוטפת עשויה להיתפס כפעולה שאינה עונה להגדרת השימוש בכוח. יודגש, כי פרשנות מבוססת על לשון הסעיף ואין בה כדי לחזות את יישום הסעיף על מתקפת סייבר עתידית.

בבחינת האיום בכוח במימד הקיברנטי נראה כי נדרש איום על פעולה קומוניקטיבית. בתוך כך, איום בהתקפה קיברנטית לפגיעה בתשתיות קריטיות של מדינה זרה סותר ככל הנראה את איסור השימוש בכוח. בהקשר זה יצוין, כי פעולת ריגול אשר כוללת איום לפגיעה עשויה לעמוד בניגוד לאיסור. יודגש, כי ישנם מקרים בהם מנהיגים בוחרים ל'איים' בתגובה למתקפת סייבר על מדינתם כדוגמת נשיא ארה"ב, ברק אובמה, כנגד מתקפת הסייבר על חברת Sony האמריקאית[24]. איום מסוג זה לא נתפס כשימוש אסור בכוח הסותר את הסעיף הקבוע במגילת האו"ם.

[24] ראו הרחבה בפרק ג' מקרי בוחן – בחינת מדיניות ארה"ב כנגד מתקפת הסייבר על חברת סוני האמריקאית.

מדריך טאלין [25] -

המדריך נכתב בידי 20 מומחי משפט שעבדו בשיתוף פעולה עם המועצה הבינלאומית של הצלב האדום ועם פיקוד הסייבר האמריקאי. המומחים הוזמנו על ידי מרכז הגנת הסייבר המשותף בטאלין, בירת אסטוניה ומכאן שמו. המדריך הינו תוצר הועדה CCDCE[26] אשר התכנסה לטובת יצירת מסמך משפטי בדבר החלת הדין על לוחמה קיברנטית. תהליך כתיבת המסמך החל בשנת 2009 אך זה יצא לאור רק בשנת 2013. מסמך זה הינו הניסיון הראשון לקבוע כיצד יש ליישם את החוק הבינלאומי על מתקפות סייבר. עם זאת יודגש, כי המדריך מסייע למשפטנים בהתמודדות עם הכלת הדין הבינלאומי הקיים למרחב הסייבר אך אינו מהווה מסמך רשמי ומחייב מטעם נאט"ו.

המומחים מציינים במבוא כי במצב הקיים, קשה לקבוע באופן מוחלט כי קיימות נורמות של משפט בינלאומי מנהגי בתחום הקיברנטי. המומחים אינם טוענים שקביעת המדריך משקפות את המשפט הבינלאומי הקיים באופן שאינו מעורר מחלוקות, אלא משקפים באמצעות המדריך את הקונצנזוס בקרב המומחים באותה העת. המדריך קובע, כי ניתן לפתוח במלחמה קונבנציונלית בשל מתקפה על מערכות מחשב[27]. כמו כן, כתבו המומחים כי האקרים כדוגמת 'אנונימוס'[28] המשתתפים במתקפות מקוונות יכולים להיות מטרה חוקית במהלך מלחמה, למרות שהם אזרחים. נוסף על כך, נקבע במדריך כי **פעולה קיברנטית הגורמת למוות, פציעה של אנשים או פגיעה ברכוש מהווה שימוש בכוח,** באם הפגיעה היא לא מינורית[29]. בתוך כך, במדריך נקבעו שמונה קריטריונים אשר מהווים הצעה לבסיס בחינת הפעולה כשימוש בכוח:

א. **חומרת הפעולה** בבחינת השלכותיה על אינטרסים לאומיים חיוניים.

ב. **מידיות הפעולה**- במסגרת כך נבחנת מידתיות התממשות התוצאה מהפעולה. ככל שהתוצאות קרובות יותר לפעולה כך נוח יותר לראות בפעולה כשימוש בכוח.

ג. **ישירות**- ישנו הכרח במציאת קשר סיבתי בין הפעולה לבין התוצאות ללא קשר זה ישנו קושי לשייך את הפעולה לתוצאה ולהכיר בה כשימוש בכוח.

ד. **חודרניות**- בהיבט זה נדרשת בחינת עומק החדירה למרחב הקיברנטי. פעילות חדרנית הכוללת עקיפת מנגנוני אבטחה והגנה תיחשב כשימוש בכוח.

ה. **כימות התוצאה**- פעולה אשר תוצאתה ניתנת לכימות, עשויה לסייע בהכרת כפעולה הכוללת שימוש בכוח.

ו. **אופי צבאי לפעולה** - האם קיים קשר בין הפעילות הקיברנטית לבין מבצעים צבאיים.

---

[25] Tallinn Manual on The International Law Applicable to Cyber Warfare (2013).
http://issuu.com/nato_ccd_coe/docs/tallinnmanual/37?e=5903855/1802381
[26] NATO- Cooperative Cyber Defense Centre for excellence ; ccdcoe.org/index.html
[27] http://www.haaretz.co.il/captain/net/1.1971006
[28] http://tech.walla.co.il/item/2844066
[29] סעיף 11 במדריך טאלין "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 "

ז. **מעורבות מדינתית**- ככל שניתן לשייך תקיפה קיברנטית למדינה מסוימת כך יגדלו הסיכויים להכיר בפעילת כשימוש בכוח. יצוין, כי אחת מיתרונות התקיפה בסייבר היא חשאיות לפיכך קיים קושי במציאת מקור התקיפה הקיברנטית.

ח. **הנחה נורמטיבית**- נוכח העובדה כי מדובר בדינים בינלאומיים וקשת הפעולות במרחב הקיברנטי רחבה מכדי לנבא את כלל הפעולות הפוטנציאליות מראש. לאור זאת, **חזקה על פעולה קיברנטית כפעולה שאינה מהווה שימוש בכוח** כל עוד אין איסור מפורש בחוק.

התקפה מזוינת והגנה עצמית במרחב הקיברנטי

לאיסור בשימוש בכוח המעוגן בסעיף 2(4) במגילת האו״ם שני חריגים: שימוש בכוח בהתאם להחלטת מועצת הביטחון של האו״ם ופעולה הננקטת כחלק מהגנה עצמית אשר אינה מצריכה אישור מקדים מהמועצה. יצוין, כי המועצה תתיר שימוש בכוח במידה ומדובר ב״איום על השלום, הפרת השלום או אקט של תוקפנות״ לשון סעיף 39 למגילה. כמו כן, החלטה מסוג זו צריכה להתקבל בקונצנזוס של חמש חברות קבועות ובהן סין ורוסיה ומכאן הקושי בקבלת החלטה אפקטיבית ואקטיבית מצד מועצת הביטחון של האו״ם בזמן מתקפה קיברנטית.

זכות ההגנה העצמית

סעיף 51 במגילה האו״ם[30]מקנה זכות טבעית להגנה עצמית, אינדיבידואלית או קולקטיבית כנגד ׳התקפה מזוינת׳ נגד מדינה החברה באו״ם. ייחודה של זכות זו היא הקניית רשות למדינות להשתמש בכוח מבלי לחכות להחלטה רשמית ממועצת הביטחון. השימוש בזכות להגנה עצמית הינו כתגובה ל׳התקפה מזוינת׳ ולצורכי הגנה מפני המקפה. מדינה אשר תעשה שימוש בכוח ותטען להגנה עצמית שלא ב מסגרת ׳התקפה מזוינת׳ מרחיבה את ההגדרה. **הגנה עצמית כפופה לשני תנאים משפטיים מרכזיים הצורך והמידתיות**[31]. השימוש בזכות להגנה עצמית יתאפשר בתנאי שאין חלופה אפקטיבית אחרת להסרת האיום שאינה כרוכה בהפעלת כוח. כמו כן, בהתקיים צורך להגנה עצמית, הפעולה נדרשת להיות מידתית ביחס למתקפה בהיקפה ובאופן מידתי לאיום או הסכנה הנשקפת מהמתקפה למדינה. סלואן[32] טוען כי שתי הדרישות הצורך והמידתיות מצויות בזיקה הדוקה האחת לשנייה.

ניתן להניח, כי בעתיד יועצים משפטיים ימליצו למקבלי ההחלטות לפעול באמצעות חריג ההגנה העצמית המאפשר שימוש בכוח. באם טענות אלו יענו על דרישות הצורך והמידתית תנאי הסעיף יתקבלו הן ויאפשרו בכך למדינות להגיב למתקפות קיברנטיות מבלי לקבל אישור לכך ממועצת הביטחון.

---

[30] "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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-defense 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"

[31] Necessity and Proportionality. כלל מספר 14 במדריך טאלין

[32] 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).

'התקפה מזוינת' במרחב הקיברנטי אינה שונה מההגדרה להתקפה קינטית. בתוך כך, ניתן להיעזר בקביעת המומחים במדריך טאלין כפעולה קיברנטית הגורמת למוות, פציעה של אנשים או פגיעה ברכוש מהווה שימוש בכוח[33]. בתוך כך, התקפות קיברנטיות אשר ניתן לכמת את תוצאותיהם בדומה להתקפות קינטיות יקלו על הקביעה כי מדובר בהתקפה מזוינת. בתוך כך, מתקפות קיברנטיות בעלות תוצאות פיזיות משמעותיות כדוגמת הרג אזרחים עשויים להיחשב התקפה מזוינת. עם זאת, פעולות קיברנטיות כדוגמת ריגול יתקשו להיכנס תחת הגדרת התקפה מזוינת. בהקשר זה יצוין, כי מנסחי מדריך סטאלין, בחרו לשקף את היעדר הקונצנזוס ביחס להתקפה קיברנטית שאינה גורמת נזק פיזי ישיר ולא הכריעו בסוגיה.

הגנה עצמית מקדימה במרחב הקיברנטי

הגנה עצמית מקדימה, Preemptive or Anticipatory self -Defense, הינה פעולה לצורך הגנה עצמית בטרם הופעת המתקפה המזוינת. סעיף 51 למגילת האו"ם מתייחס למצבים בהם בוצעה 'התקפה מזוינת' נגד מדינה ולפיכך בהתאם לכך הסעיף לא מתייחס להגנה עצמית כפעולה מקדימה להתקפה המזוינת. המבחן המשפטי ב**הצדקת פעילות להגנה עצמית מקדימה** מחייב עמידה ב**שלושה תנאים**: מסקנה סבירה שאכן תתקיים מתקפה קיברנטית, התוצאות הצפויות של ההתקפה מקבילות לתוצאות הנגרמות מ'התקפה מזוינת' קינטית והצורך בפעולה מידית כדי להתגונן. יצוין, כי דרישה משולשת זו מעמידה בספק הצדקה מדינתית לפעולה מסוג זה לאור ייחודו של המרחב הקיברנטי המקשה על הצבעה על התוקף. יתר על כן, היכולת לפעול באופן מידי למול איום שאינו ניתן לצפייה מקשה אף הוא על הצדקת תגובה מסוג זה.

אפשרות להגנה עצמית מקדימה במרחב הקיברנטי באה לידי ביטוי בסעיף 15 במדריך טאלין לפיו: "הזכות לשימוש בכוח כהגנה עצמית חלה אם התקפה קיברנטית מתרחשת או שהיא מידית, הדבר כפוף לדרישת המידיות". בתוך כך, יודגש כי קיים הבדל מהותי בין צעדים מכינים לבין צעדים המהווים תחילתו של 'התקפה מזוינת'. בהקשר זה יוזכר, כי בתגובה למתקפת הטרור בתאריך 11/9/2001 פתחה ארה"ב במבצע צבאי למיגור הטרור באפגניסטן. ארה"ב טענה כי פעולתה מהווה 'הגנה עצמית מקדימה' לאור הצורך להרתיע מפני ביצוע התקפות טרור חוזרות[34]. גישה מרחיבה זו מתמקדת בגודל האיום והסכנה מפניו ומתעלמת מהודאות הנדרשת בנוגע לעיתוי ומיקום המתקפה המזוינת הצפויה. המצדדים בגישה זו טוענים, כי הטרור המודרני מתאפיין בכך שאינו צפוי ויכול להתרחש בכל מקום ובכל עיתוי ולכן ישנו הכרח לממש את הזכות להגנה עצמית מקדימה.

זכות ההגנה עצמית מול ארגון טרור (שאינו מדינתי)

סעיף 51 במגילת האו"ם מתייחס לזכות להגנה עצמית בתגובה ל'התקפה מזוינת' במסגרת היחסים בין מדינות. בתוך כך, פעולות אלימות נגד מדינות מצד גורמים שאינם מדינתיים, כמו ארגוני טרור וקבוצות מזוינות, נותרו בחינת לשון הסעיף כפשוטו, מחוץ למשטר המשפטי הבינלאומי הגלום במגילת האו"ם. לצד הגישה המצמצמת המפרשת את הסעיף כפשוטו וככזה החל על מדינות בלבד, ישנה גישה המרחיבה את הסעיף גם למערכת היחסים בין מדינה לארגון טרור. בתוך כך, התקפות הטרור שביצעו גורמי אל-קאעידה בשנת

[33] סעיף 11 במדריך טאלין

[34] https://www.asil.org/insights/volume/14/issue/37/international-law-drones

2001 נתפסו ע"י ארה"ב והקהילה הבינלאומית כ'התקפה מזוינת'[35] וסייעו לארה"ב להצדיק את התגובה[36] תוך שימוש במונחי 'הגנה עצמית' אשר עד כה יוחסו רק למערכת היחסים בין מדינות. בהקשר זה יצוין, כי ישראל טענה לזכותה להגנה עצמית בבניית גדר ביטחון. בית הדין בפרשת הגדר קבע, כי יש לפרש את סעיף 51 במגילת האו"ם בצמצום באופן שאינו חל על יחסים בין מדינה לבין גורם שאינו מדינתי כדוגמת הרשות הפלסטינית[37]. לאור זאת, ישנה גישה הטוענת כי בעימות בין מדינות לארגוני טרור, אין הדין הבינלאומי מגביל את המדינות בהתמודדות עם איומי הטרור בשונה מעימותים בין מדינות. לא מן הנמנע כי, גישת ארה"ב בנוגע לזכותן של מדינות לפעול בהגנה עצמית נגד גורם שאינו מדינתי במרחב הקינטי תקפה גם למרחב הקיברנטי. בהקשר זה יוזכר, כי רוב מנסחי מדריך טאלין סברו כי פרקטיקת מדינות, כדוגמת טענות ארה"ב לאחר התקפות הטרור ב 11/9/2001, מבססת את הזכות להגנה עצמית נוכח 'מתקפה מזוינת' גם כנגד גורמים שאינם מדינתיים. לדעתם, מימוש הזכות מצריך מתקפה בהיקף משמעותי, מתקפה מאורגנת ולא ספוראדית ומתקפה אשר תוצאותיה שקולה לתוצאות 'מתקפה מזוינת קינטית'[38]. הרחבת הסעיף למערכת היחסים בין מדינות לארגוני טרור עשוי להרחיב את השימוש בכוח מצד מדינות שכן יתכן וירתיע ארגוני טרור מביצוע מתקפות טרור. עם זאת, הרחבה זו עומדת בסתירה לכוונה המקורית של מנסחי המגילה להגביל את השימוש בכוח ולאפשר במקרים חריגים זכות להגנה עצמית ועל כן מבוססת על פרקטיקת מדינות בלבד.

2. דיני המלחמה במרחב הקיברנטי

דיני המלחמה Laws of War או בשמם הנוסף Jus in bello, International Humanitarian Law, הוא הענף המשפטי החל בעת סכסוך מזוין. דינים אלו מסדירים את התנהגות הצדדים במהלך סכסוך מזוין, מבלי להידרש לשאלה המקדמית, האם העימות עומד בדינים הבינלאומיים. דיני המלחמה הינם דינים דינמיים המתפתחים ומשתנים בהתאם בשדה הקרב. הלחימה במרחב הקיברנטי מתעצבת אף היא ולכן, ניתן להניח כי התמודדות דיני המלחמה במרחב הקיברנטי מצויה בתהליך אשר עשוי להתפתח ולהשתנות. דיני המלחמה חלים בהתקיים סכסוך מזוין (Armed Conflict) ולפיכך ישנה חשיבות מכרעת לקביעה כי העימות הינו 'סכסוך מזוין'. המונח 'סכסוך מזוין' קנה אחיזה במסגרת הנוסח של אמנות ז'נבה בשנת 1949 ובכך החליף מונח מסורתי ידוע, 'מלחמה'. ניתן לזהות שני סוגי סכסוכים מזויינים מרכזיים: סכסוך מזוין בינלאומי וסכסוך מזוין שאינו בינלאומי[39].

סכסוך מזוין בינלאומי נקבע בסעיף 2 לאמנת ז'נבה משנת 1949. הסכסוך כולל שתי דרישות עובדתיות מרכזיות: האחת, סכסוך סין מדינות והשנייה פעולת איבה העולה לכדי פעולה מזוינת[40].

סכסוך מזוין שאינו בינלאומי הוגדר בסעיף 3 לאמנות ז'נבה על דרך השלילה: סכסוך שאינו בעל אופי בינלאומי המתרחש בשטחה מדינה שהיא צד לאמנה. דרישת השטח מקשה על הגדרת סכסוך מזוין שאינו

35 S.C. Res. 1373, U.N. DOC. S/RES/1373 (Sept. 28, 2001);
36 Watts, 2011
37 http://weblaw.haifa.ac.il/he/Journals/lawatch1/lawatchF/2004c_wall.htm

[38] מדריך טאלין עמודים 59-60

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

[40] מדריך טאלין עמוד 79

בינלאומי במרחב הקיברנטי לאור הקושי בתיחום המתקפה ועמידה על מקור התקיפה. לאור זאת, יתכן כי בעת מתקפה קיברנטית עתידית הדין הבינלאומי עשוי להגמיש את דרישת השטח בעת מתקפה קיברנטית.

תוקפם של דיני המלחמה במרחב הקיברנטי

בדומה למנסחי מגילת האו״ם אשר הושפעו ממלחמות קינטיות, דיני המלחמה נוסחו גם הם בצל מלחמות קינטיות מבלי להתייחס מפורשות למרחב הקיברנטי. הדעה המקובלת במערב כמתואר בסעיפים הקודמים, היא שניתן להחיל את דיני המלחמה בזמן סכסוך מזוין גם על המרחב הקיברנטי כפי שמחילים את יתר הכללים והדינים הבינלאומיים על כל מרחב ומימד אחר[41]. יישום דיני המלחמה למרחב הקיברנטי מעלה קשיים כדוגמת הגדרת מערכה קיברנטית כסכסוך מזוין ובאופן שבו ניתן להצדיק מתקפות נגד מערכה קיברנטית במסגרת הסכסוך המזוין. יצוין, כי עד כה לא התקיימה מערכה קיברנטית העולה לכדי סכסוך מזוין כהגדרת דיני המלחמה באמנת ג׳נבה. בבחינת התקפה קיברנטית במהלך סכסוך מזוין ישנן שתי גישות בהתאם למנסחי מדריך טאלין. מחד, מחילים את דיני המלחמה על כל פעולה של צד אחד לסכסוך מזוין נגד צד אחד. ומאידך, מחילים את דיני המלחמה רק על התקפות קיברנטיות שבוצעו ע״י צד אחד לסכסוך כנגד הצד האחר כחלק מהמאמץ המלחמתי[42]. דיני המלחמה מחייבים מרכיב ׳אלים׳ במסגרת תוצאת הפעולה, ולפיכך פעולת ריגול במרחב הקיברנטי הגם שהיא חלק מהמערכה לא תוכר ככל הנראה כ׳התקפה מזוינת׳. עם זאת, התקפה קיברנטית אשר תוצאותיה מכילים מרכיב אלים, כדוגמת פגיעה בהספקת החשמל לבית חולים, עשוי לשמש כ׳התקפה קיברנטית׳ כחלק מסכסוך מזוין. יוזכר, כי כלל 30 במדריך טאלין קבע, כי פעולות קיברנטיות, הגנתיות או התקפיות, שצפויות לגרום באופן סביר, לפציעה או מוות של אנשים או לנזק או הרס של רכוש הן בגדר ׳התקפות׳. הדרישה המופיעה בכלל מספר 30 עשויה להקשות על מדינות להגדיר התקפות קיברנטיות כ׳התקפות מזוינות׳ נוכח העובדה כי שאלת תוצאת התקיפה איננה ידועה לרוב ולעיתים פעילות ריגול אשר עשויה להיתפס כפעולה שאינה מזוינת עשויה לשמש לאיסוף מודיעין לפעילות מזוינת.

3. הדין הפנימי בישראל

חוק המחשבים תשנ״ה 1995 [43] - החוק מצומצם ומתייחס בעיקר לפעולות מחשב המוכרות כעבירה פלילית. בחוק הגדרות בסיסיות כגון: חומר מחשב, מחשב, מידע , פלט ותוכנה. כמו כן, החוק מגדיר מהו שיבוש שנעשה על ידי מחשב ומגדיר איסור על פעולה אסורה בתוכנה.

חוק שירות הביטחון הכללי התשס״ב 2002 [44] **-** החוק מגדיר את גבולות פעולת שירות הביטחון הכללי. מתוקף החוק, שירות הביטחון הכללי מוגדר כסמכות טיפול לפעולות טרור במדינה. לאור זאת, ישנה חשיבות בהגדרת פעולה כפעולת טרור לשם יישום הסכמות הקבועה בחוק. במקרים בהם ארגוני הטרור לוקחים אחריות באופן רשמי על הפעילות, הודעה זו מאפשרת לשב״כ לפעול באמצעים המוקנים בחוק. בשירות הביטחון הכללי בדומה ליתר גופי המודיעין והביטחון קיים יחידה משפטית אשר תפקידה לוודא כי השב״כ פועל בהתאם לסמכותו ובכפוף לחוק.

[41] http://www.harvardilj.org/2012/12/online-articlesonline_54_schmitt/.

[42] מדריך טאלין 76

[43] http://www.nevo.co.il/law_html/Law01/214_001.htm

[44] http://www.shabak.gov.il/about/yoamash/pages/law.aspx

החוק להסדרת הביטחון בגופים ציבוריים התשנ"ח 1998[45] **-** החוק מגדיר מה כוללת אבטחה מערכות ממוחשבות חיוניות ומגדיר את משרדי הממשלה והגופים הציבוריים אשר כפופים לחוק. שירות הביטחון הכללי עד לאחרונה היה אחראי מתוקף החוק על אבטחת המערכות הממוחשבות החיוניות בגופים אלו. עם הקמת הרשות הלאומית להגנה בסייבר, בוצעו מספר שינויים בחוק אשר עיקרם העברת האחריות על הביטחון בגופים ציבוריים המופיעים בחוק, משירות הביטחון הכללי לרשות הלאומית להגנה בסייבר. החוק מעיד באופן רשמי על דאגתה מפני האיום הקיברנטי של מדינת ישראל והרצון לצמצם איום זה.

הצעת 'חוק המאבק בטרור' התשע"ה 2015 [46]**-** הצעת החוק מהווה ניסיון להסדיר את החקיקה הישראלית הפנימית ולסייע בהתאמת האמצעים שבידי הרשויות להתמודדות עם איומי הטרור המתחדשים. כמו כן, החוק נועד לאזן באופן מיטבי בין האינטרסים הביטחוניים שבפניהם ניצבת המדינה, לבין שמירה על עקרונות היסוד של השיטה הדמוקרטית המכירה בזכויות אדם כזכויות יסוד. יצוין, כי החוק טרם אושר וגופים רבים בהם המכון למדיניות נגד טרור ICT הביעו עמדתם ופרסמו המלצות לתוכנו של החוק הרצוי[47].

כתיבת חוק רשות - בימים אלו מתגבשת המדיניות הרצויה ברשות הלאומית להגנה בסייבר במשרד רה"מ המוגדרת 'צופה פי עתיד', המדיניות באה לידי ביטוי בעבודה על כתיבת חוק המגדיר את הגבולות המשפטיים לטיפול באירועי הגנה בסייבר. החוק בדומה לחוק שירות הביטחון הכללי, עתיד לשמש את הרשות הלאומית להגנה בסייבר הן לסמכויות טיפול באירועי הגנה והן באופן הטיפול תוך התייחסות לפגיעה המותרת בזכויות האזרחים. הצעת החוק אשר נכתבת ברשות הלאומית ומובלת ע"י יועמ"ש הרשות, עו"ד עמית אשכנזי תועבר ל'ועדת חוקה' ועתידה להסדיר את הפעילות ההגנתית בסייבר בתוך שטח המדינה. חוק רשות זה הינו נדבך נוסף בהסדרת ומיצוב ההגנה הלאומית במרחב הקיברנטי כחלק מהשינויים במדינת ישראל[48].

4. תמצית הפערים הטכניים במרחב הקיברנטי

במסגרת ניתוח התגובה המדינתית למתקפות קיברנטיות עולה הצורך בתיאור פערים טכניים אשר אינם באים לידי ביטוי במתקפות קינטיות מוכרות. בתקיפה קינטית, מקור התקיפה והיקף התקיפה לרוב ידועים דבר אשר מסייע למנהיגים בקבלת ההחלטות. במרחב הקיברנטי ישנו קושי רב בזיהוי מקור התקיפה, איתור סימנים מעידים למתקפה ובזיהוי מגמות וגלי טרור. בתוך כך, שונה המרחב הקיברנטי ממרחבים אחרים אשר בהם ניתן לזהות את התקיפה ולעיתים אף להתמגן מפניה. במרחב הקיברנטי תפקיד המגן מאתגר, היכולת להגן על מערכות ממוחשבות באופן שוטף הינה מורכבת. לתוקף באמצעות המרחב הקיברנטי נדרש פער אבטחתי אחת על מנת להשיג את מטרותיו. גופי המודיעים והביטחון מורגלים בסיכול פיגועי טרור כדוגמת מפגע עם מטען נפץ נוכח סדר הפעולות הנדרש מצד המפגעים למימוש פיגוע מסוג זה. לעומת זאת, המרחב הקינטי מאפשר למפגעים לפעול באופן אנונימי, לעשות שימוש **במטבע וירטואלי**[49] **(כדוגמת Bitcoin)** על מנת לטשטש את עקבותיו ולהקשות על המגן באיתור התוקף. יתרה מכך, גורמי תקיפה מבעלי יכולת גבוה רוכשים

[45] http://www.dinimveod.co.il/hashavimcmsfiles/Pdf/sh1685.pdf
[46] http://knesset.gov.il/committees/heb/material/data/H07-10-2015_14-42-37_.pdf
[47] https://www.ict.org.il/Article/1634/Position-Paper-Counter-Terrorism
[48] ראו הרחבה בפרק א'
[49] http://www.isa.gov.il/GeneralResearch/179/Documents/%D7%9E%D7%98%D7%91%D7%A2%D7%95%D7%AA%20%D7%93%D7%99%D7%92%D7%99%D7%98%D7%9C%D7%99%D7%99%D7%9D%209.pdf

מספר שרתים ברחבי העולם ומבצעים את המתקפה באמצעות שרשרת שרתים אשר מאתגרת את גופי ההגנה במעקב המחשב ממנו נשלחות הפקודות למתקפה ומייצרת 'תשתית בידול' בין התוקף ליעד. במסגרת הפערים הטכניים עולים קשיים ביחס המשפטי לשרת בשרשרת התקיפה אשר נפרץ על ידי התוקף וממנו נשלחות פקודות זדוניות ליעד. בהתאם לעקרון האחריות הטריטוריאלית סמכות השיפוט ניתנת למדינה בה השרת מאוחסן. המרחב הקיברנטי מאתגר עקרון זה, ישנו קושי להגדיר מיקום פיזי למידע ולפיכך המשפט הבינלאומי לעיתים מתקשה ביישום הדין הבינלאומי על המרחב הקיברנטי. לפי שעה, הדרך המובילה לפתרון שאלת הסכמות המשפטית נפתרת בעזרת שיתוף פעולה בין מדינות להן מוקנת הסמכות מכוח עקרון האחריות הטריטוריאלית. גופי ההגנה המדינתיים פועלים במתח תמידי בין הסרת האיום כחלק מהאינטרס הציבורי לבין הפגיעה בזכות לפרטיות ובזכות לקניין של האזרחים. קשיים אלו ואחרים מחייבים את המגן לשינוי דרכי החשיבה והתגובה מהמתקפות המוכרות במרחב הקינטי. בהתאם לכך, מדינת ישראל עיגנה בחקיקה מערכות ממוחשבות חיוניות בנכסים קריטיים עליהם ההגנה מחייבת טיפול מידי בהסרת האיום[50].

המידע הטכני בדבר המתקפה הקיברנטית מהותי למקבלי ההחלטות בדבר בחירת תגובה הולמת. מקבלי ההחלטות אשר עד כה מיקדו את החלטותיהם על מידע מדויק בדבר מתווה התקיפה הקינטית והיקפה עשויים להתמודד עם מתקפות קיברנטיות אשר רב הנסתר על הגלוי באשר לזהות התוקפים. לפיכך, ישנה חשיבות רבה לגופי ההגנה והמודיעין לשפר את יכולתם באיתור מוקדי התקיפה, יעד התקיפה והיקפה על מנת לאפשר למקבלי ההחלטות מידע מספק לבחירת מדיניות תגובה הולמת.

<u>פרק ג' מקרי בוחן</u>

1. <u>מתקפת סייבר על אסטוניה 2007</u>

בחודשים אפריל ומאי בשנת 2007 הותקפה אסטוניה במתקפה קיברנטית[51]. ההתקפות נמשכו כחודש ימים והתמקדו בתשתיות האינטרנט באסטוניה אשר כללו השחתת אתרי אינטרנט, הרס מידע ממוחשב ומניעת שירות מאתרים רבים. לאור ההכרה בעצמאות אסטוניה, השקיעה הממשלה משאבים רבים ברשתות מחשבים והאינטרנט הפך משמעותי בחיי היום יום של אזרחיה. הממשלה פעלה באופן שהוגדר 'ללא נייר' ולפיכך הפגיעה הכלכלית באסטוניה הייתה משמעותית. במסגרת החקירה הטכנית אחר מקור התקיפה נמצאו כמיליון מחשבים מ 177 מדינות אשר לקחו חלק במתקפה מבלי שידעו על כך. מתקפה זו מתאפשרת באמצעות החדרת תוכנה זדונית למחשב אשר מאפשרת לתוקף לשלוח פקודה מהמחשב המודבק ליעד התקיפה. בהקשר אפשרי לכך יצוין, כי ממשלת אסטוניה התכוונה להוציא אנדרטת זיכרון ממלחמת העולם השנייה ממרכז בירתה, טאלין, לבית קברות צבאי בפרברי העיר. אזרחים ממוצא אתני רוסי מחו על כך והתפתחו הפגנות אלימות באזור למניעת המעבר. קשר נסיבתי זה הקשה על יחוס המתקפה לרוסיה ומלבד זאת לא נמצאו ראיות נוספות אשר קשרו את ממשלת רוסיה או אזרחים רוסים למתקפה.

[50] החוק להסדרת הביטחון בגופים ציבוריים 1998

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

<u>מדיניות התגובה האסטונית</u> כללה פעולות פאסיביות כדוגמת הרחבת פסי התקשורת לטובת מזעור הנזק מהמתקפה וכן בחקירה פלילית של האירוע. בזמן המתקפה אסטוניה לא טענה בזמן זה לזכותה להגנה עצמית מכוח מגילת האו״ם או חוקת נאט״ו. העובדה כי אסטוניה לא יכלה להצביע על מקור התקיפה הקשה עליה לטעון לזכותה להגנה עצמית. האירוע מעיד על הקושי ההגנתי של מדינה בהתמודדות עם מתקפה קיברנטית בלתי מזוהה.

2. <u>תקיפה הסייבר על גיאורגיה 2008</u>

כוחות גיאורגים חדרו לחבל דרום אוסטיה בקיץ 2008 דבר אשר הוביל לסכסוך בין רוסיה לגאורגיה. מבחינה משפטית, היה זה סכסוך מזוין בינלאומי בין שתי מדינות עליו חלים דיני המלחמה [52]. הסכסוך לא נמשך זמן רב , התערבות צבאית של רוסיה הכריעה את הגאורגים. טרם החדירה הצבאית הרוסית לחבל דרום אוסטיה, בוצעו התקפות קיברנטיות[53]רחבות היקף נגד גיאורגיה. המתקפות כללו מניעת שירות מאתרי ממשלתיים והשחתת מידע באמצעות פגיעה במערכות מחשוב ואחסון נתונים. המתקפה ארכה כחודש ימים ובממוצע של שעתיים ביום. בהקשר זה יצוין, כי בניגוד לאסטוניה אשר עיקר פעילות הממשלה התבססה על מערכות מחשוב, חשיבות התשתיות הממוחשבות בגיאורגיה פחותה מאשר באסטוניה. המתקפה אמנם פגעה בשירותים הציבוריים, ביכולת הממשלה לתקשר עם הציבור ובזמינות הבנקים אשר נותקו מהרשת למשך עשרה ימים אך אין בכך פגיעה משמעותית לתפקוד המדינה. במסגרת החקירה הטכנית לא נמצאו ראיות הקושרת את התקיפה לממשלת רוסיה באופן רשמי. החקירה מצאה מספר מחשבים רוסים אשר לקחו חלק במתקפה אך לא היה בכך די בכדי להאשים את רוסיה במתקפה.

<u>מדיניות התגובה הגיאורגית</u> לא נראתה בשטח הן במרחב הקינטי והן במרחב הקיברנטי. הגיאורגים הוכרעו אל מול היריב הרוסי החזק והתקשו למנוע את המתקפות. בשל ההשפעה המועטה על תפקוד המדינה, עיקר השפעתה של המתקפה הקיברנטית הינה תודעתית. באם אכן תקיפה זו הינה תקיפה בהובלת ממשלת רוסיה, זוהי הפעם הראשונה בהיסטוריה בה מדינה עושה שימוש במרחב הקיברנטי כחלק ממערכה קינטית. גאורגיה לא הגיבה למתקפות אלו אך מדיניות זו בה בחרו הגאורגים נובעת ככל הנראה מפערי היכולות בין המדינות ולא מקבלת החלטה של מנהיגיה להימנע מתגובה.

3. <u>תקיפת האקרים איראנים את הבנקים האמריקאים 2013</u>

המערכת הפיננסית בארה״ב חוותה (החל מספטמבר 2012) **מתקפה קיברנטית**[54]. מטרת המתקפה מניעת גישה לשירותים בנקאיים מקוונים. בינואר 2013 פורסם לראשונה כי איראן[55] עומדת מאחורי מתקפת מניעת השירות חסרת התקדים[56]. ראש מנהל המודיעין האמריקאי DNI[57] דאז, התייחס בוועידת המודיעין של הסנאט בהקשר ליכולות הסייבר ההתקפיות האיראניות נגד ארה״ב וטען כי הן השתפרו בעומקן ובמורכבותן באופן דרמטי.

---

[52] ראו הרחבה בנושא דיני מלחמה בפרק ב׳

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

[54] http://www.israeldefense.co.il

[55] http://www.calcalist.co.il/internet/articles/0,7340,L-3592648,00.html

[56] http://news.walla.co.il/item/2605254

[57] http://www.dni.gov/index.php

המערכת הבנקאית בארצות הברית מחויבת למסירת מידע זמין ואמין לציבור ועל כן פגיעה במערכת הבנקאות פגעה בכלכלת ארה״ב ובאמון האזרחים במערכת. ברקע לכך יוזכר, כי איראן איימה מספר פעמים שאם ייתקפו מתקני הגרעין שלה, היא תגיב בהפצצת הבסיסים האמריקאים במפרץ ומתקפת טילים על ישראל. איראן האשימה את ישראל וארה״ב בהתקפת סייבר על מתקני הגרעין שלה ולא מימשה את איומיה יתכן לאור הקושי בשיוך התקיפה באופן ודאי לישראל ו/או לארה״ב[58]. עם זאת, איראן לא נטלה אחריות למתקפה הקיברנטית על ארה״ב. **<u>מדיניות התגובה האמריקאית</u>** לא כללה תגובה אקטיבית גלויה כלפי איראן למרות החשדות כלפיה. ארה״ב לא פרסמה התייחסות פומבית בנוגע למתקפה הקיברנטית דבר אשר מעיד על בחירה במדיניות הכחשה. כמו כן, יתכן וגופי המודיעין והביטחון החזיקו במידע אודות התוקפים אשר הושג באמצעות אמצעים טכנולוגיים ומודיעיניים ולצורך שמירה על מקורותיהם בחרו שלא לעשות שימוש במידע ולהימנע מחשיפתו. היעדר תגובה פומבית אמריקאית מקשה על ניתוח מדיניותה בדבר מתקפה קיברנטית נגדה.

4. <u>מתקפה קיברנטית על ישראל במהלך מבצע 'צוק איתן' - 2014</u>

במהלך מבצע 'צוק איתן' (8.7.2014-26.8.2014) ישראל ביצעה מערכה ברצועת עזה לצורך צמצום איום המנהרות על שטח מדינת ישראל. במקביל למערכה הקינטית, מרחב האינטרנט הישראלי חווה מתקפה קיברנטית מסוג מניעת שירות. התקיפה התמקדה בשיבוש רשתות המערכת הביטחונית והמערכת הפיננסית בישראל. קצין בכיר בצה״ל ייחס את התקיפה לגורמים איראניים[59]. לטענתו, המתקפות הגיעו לשיאן ב-25 ביולי 2014, יום שישי האחרון בחודש הרמדאן, המצוין באיראן כ״יום ירושלים״, יום התנגדות לישראל ולציונות. המתקפה נחסמה במאמץ משולב של גורמי צה״ל ושב״כ, אשר היו ערוכים מבחינה הגנתית לסכל את המתקפה ולמזער את השפעותיה על מרחב האינטרנט הישראלי. גבי סיבוני[60] התייחס לתקיפה וטען כי ״בישראל טרם סוכמה תפיסת ההכנה הכוללת וטרם נקבע הגורם המוביל את ההגנה מול מתקפות רחבות כאלה. במרחב הסייבר של ישראל פועלים מגוון גופים בהם: צה״ל, השב״כ, המוסד, חברות וספקי תקשורת, בנק ישראל ובנקים מסחריים, משרדי ממשלה, משטרת ישראל, חברות אבטחה אזרחיות וגופים נוספים עוסקים בנושא. היעדר הסדרה של סמכויות במאמץ ההגנתי והסיכולי, עלולה לייצר חורים ״בכיפת הברזל״ הדיגיטאלית המגנה על ישראל ולאפשר לגורמים עוינים לפגוע בישראל״. מבחינה טכנית[61] המתקפה נחשבה לאחת ממתקפות הקיברנטיות הנרחבות ביותר על מרחב האינטרנט הישראלי. המתקפה התרכזה בחברות תקשורת ובספקי אינטרנט במטרה לגרום לרשתות ישראליות לקרוס מעומס יתר, תוך ניסיון להציף את רשת האינטרנט בבקשות שאין ביכולתן להכיל.

<u>בבחינת מדיניות התגובה הישראלית</u> - ישראל, באמצעות צה״ל והשב״כ, נקטה גישה פרו אקטיבית להכלת האירוע ויישמה אסטרטגיית הגנה הכללה הפעלת יכולות תפעוליות מתקדמות, אשר הצליחה לספק הגנה וביטחון. צה״ל והשב״כ הצליחו לסכל ניסיונות לפגוע ברשתות ממשלתיות ובתשתיות חיוניות. אחת משיטות ההגנה התבטאה בחסימת כתובות אינטרנט זרות למשך שעתיים. ישראל אשר ניהלה מערכה קינטית ברצועת

[58] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[59] http://heb.inss.org.il/index.aspx?id=4354&articleid=7583
[60] חוקר בכיר העומד בראש תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי INSS
[61] http://www.dentech.org/articles/article_9_2015_f.pdf

עזה בחרה שלא להגיב למתקפה הקיברנטית אשר יוחסה לאיראן אלא הסתפקה בהכלת האירוע והסרת האיום.

היעדר התגובה למתקפה הקיברנטית מקשה על ניתוח המדיניות הישראלית העתידית בנוגע למתקפות קיברנטיות. במתקפה לא נגרם נזק מהותי לאזרחי מדינת ישראל ולחייהם והאירוע הוכל בהצלחה על ידי גופי ההגנה. לא מן הנמנע, כי בנסיבות אחרות ישראל תבחר במדיניות תגובה שונה מהכלה והתאוששות.

5. <u>תקיפה צפון קוריאה את חברת SONY האמריקאית 2014</u>

חברת SONY הפיקה סרט בשם 'ראיון סוף' העוסק בהתנקשות במנהיג קוריאה הצפונית, קים ג'ונג און. ביוני 2015 פרסמה ממשלת צפון קוריאה כי הסרט מהווה 'הכרזת מלחמה מצד הממשל האמריקאי'[62]. בעקבות ההתעלמות האמריקאית מכך, הגישה צפון קוריאה מחאה רשמית לאו"ם והצביעה על הממשל האמריקאי כמי שאחראי על הכפשת מנהיג של מדינה ריבונית. נוסף על כך, דרשו למנוע את הפצת הסרט ואיימו בתגובה 'חסרת רחמים'. האמריקאים לא לקחו איומים אלו ברצינות ועיקר דאגת חברת SONY התמקדו בהשפעת הפרסומים על היקף המכירות הצפוי. כחודש לפני פרסום הסרט, חברת SONY חוותה תקיפה אלימה בסייבר. במחשבי החברה פורסמה הודעה אנונימית לפיה "ראו הוזהרתם השתלטנו על כל מערך הנתונים שלכם דרך האינטרנט ואנחנו מחזיקים בידינו את כל סודות החברה. זאת רק ההתחלה". מיד לאחר מכן, הודלפו לרשת מסמכים סודיים של הנהלת החברה בהם פירוט שכר כוכבי הקולנוע, פרטיהם האישיים ותכתובות מייל אישיות של מנהלי האולפנים. בשלב זה, חברת SONY, שירותי הביון האמריקאים, והמטה ללוחמת סייבר לא הצליחו להצביע על האשמים במתקפה. ממשלת צפון קוראיה הכחישה מעורבות בתקיפה אך המשיכה לדרוש את גניזת הסרט. לאחר מכן, התוקפים הטילו את האיום המהותי ביותר "זכרו את 11 בספטמבר 2001 אנו ממליצים לכם להתרחק מהמקומות (שבהם יוקרן הסרט) בזמן שזה יקרה". סת' רוגן, יוצר הסרט והשחק הראשי, ירד למחתרת, הקרנת הבכורה בוטלה ובתי הקולנוע גנזו את העותקים לאור האיום בפעולת טרור. הנזק הכלכלי לחברה היה חסר תקדים. <u>**מדיניות התגובה של ארה"ב**</u> כללה התייחסות פומבית של הנשיא אובאמה: "הפריצה לSONY היא סייבר מסוג ונדליזם ולא הכרזת מלחמה" והבטיח כי ארה"ב "**תגיב בצורה פרופורציונאלית**"[63]. אובאמה הוסיף כי אסור לאפשר לדיקטטור להטיל צנזורה[64] וטען כי החברה שגתה בהחלטתה לבטל את ההקרנה. בתום דבריו הדגיש כי "**יש צורך בהול בחקיקת חוקים ברורים בעולם האינטרנטי. האופן שבו האינטרנט עובד כרגע זה המערב הפרוע**". במסגרת בחינת הדינים הבינלאומיים נראה כי תנאי השימוש בכוח לאור האיום הממשי לפגיעה באזרחים מתקיים. בתוך כך, פומביות האיום מקנה לארה"ב בסיס לטענה משפטית לפעול כחריג לסעיף 2(4) האוסר על שימוש בכוח במידה ותצליח להצביע על צפון קוריאה כמקור האיום. בפועל, מספר ימים לאחר התבטאות אובאמה בדבר תגובה פרופורציונאלית, ארבעת הרשתות הרשמיות שמחברות את צפון קוריאה לאינטרנט סבלו מבעיות תקשורת[65]. מומחי חברת Dyn Research, טענו כי נפילת רשתות מסוג זה אינה סבירה והחשדות הופנו כלפי ארה"ב אשר **נמנעה מלקיחת אחריות באופן רשמי** על כך. מארי הארף דוברת מחלקת המדינה, טענה שאין בכוונתה לאשר את

[62] http://www.themarker.com/advertising/1.2516885
[63] http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0
[64] http://news.walla.co.il/item/2812157
[65] http://www.calcalist.co.il/internet/articles/0,7340,L-3648074,00.html

הפרסומים ועדכנה כי "**ארה"ב שוקלת מגוון אפשריות תגובה, חלקן יהיו גלויות וחלקן אולי לא גלויות**". ארה"ב נמנעה מלקיחת אחריות רשמית על מתקפת הנגד ועל ישנו קושי מייחוס בעיות התקשורת בצפון קוריאה כפועלת תגובה. באם אכן ארה"ב אחראית למתקפה ניתן לראות אישור להבטחת הנשיא אובאמה ל**תגובה פרופורציונאלית** המלמדת על מדיניות התגובה האמריקאית כפרופורציונאלית לאיום וחשאית. ארה"ב הגיבה באמצעות המרחב הקיברנטי ועשתה **שימוש במרחב ההכחשה** להשלמת התגובה.

<u>פרק ד' - תובנות מרכזית מהמחקר</u>

1. <u>הצעת הגדרה עדכנית למונח 'טרור סייבר'</u>

ניתוח המונח טרור מסוג סייבר נמצא כיום תחת קושי הגדרתי. העובדה כי בדין הבינלאומי אין הסכמה גורפת בדבר הגדרת המונח טרור מערימה קשיים להגדיר את הטרור מסוג סייבר. מניתוח מקרי הבוחן ניתן ללמוד כי אירוע טרור מסוג סייבר טרם התרחש. תקיפת חברת SONY המיוחסת לקוריאה הצפונית הינה התקיפה היחידה אשר כללה איום ממשי בפיגוע טרור ועל כן משמשת כראיה לאיום הפוטנציאלי המשמעותי מטרור מסוג סייבר. בדומה לכך, ניתן לראות במתקפת מתקפת Stuxnet באיראן [66] ומתקפת החשמל באוקראינה[67] כאירועים אשר עשויים לענות על הגדרת המונח טרור סייבר. המשותף לאירועים אלו היא היכולת לאמוד את מידת הנזק מהמתקפה. להמחשה, ניתן לראות ברכבת שירדה מהפסים עקב תקיפה קיברנטית את מערכות המחשוב שלה , כתקיפת טרור מסוג סייבר. אני סבור כי, הגדרת טרור מסוג סייבר מחייבת התייחסות למידת הנזק פוטנציאלי מהמתקפה הקיבנרטית בהשוואה לנזק ממתקפה במרחב הקינטי. בדומה לדנינג[68], אני סבור כי ההגדרה צריכה להכיל גם **תקיפות לא חוקיות ואיומים על תקיפות נגד מחשבים, רשתות ומידע** השמור בתוכם. לאור זאת, הצעתי להגדרת המונח 'סייבר-טרור' המבוססת על הגדרת הטרור של פרופ' בועז גנור ודנינג:

"**מאבק אלים או לחלופין איום מהותי אשר במסגרתו נעשה שימוש במרחב הקיברנטי כלפי אזרחים על מנת להשיג מטרות פוליטיות-חברתיות ותוצאותיו שקולות למתקפה במרחב הקינטי**".

2. <u>ניתוח מגוון החלופות לבחירת מדיניות תגובה</u>

א. **הכלת האירוע והתאוששות**

במסגרת בחירת מדיניות תגובה, מדינה יכולה לבחור בהכלת האירוע מבלי להגיב למתקפה כמדיניות תגובה. עם זאת, ההכלה עשויה לשמש את המדינה כשלב ראשוני להסרת האיום וכקרקע לנקיטת מדיניות תגובה התקפית. ישנם יעדי תקיפה כדוגמת מערכות ממוחשבות של גופים ציבוריים חיוניים אשר בהם המדינה תתמקד תחילה בהכלת האירוע ב**תשתיות המדינה הקריטיות** ולאחר מכן עשויה לנקוט מדיניות תגובה

[66] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[67] http://heb.inss.org.il/index.aspx?id=4354&articleid=11446

[68] ראו הרחבה בפרק א' – הגדרת טרור סייבר

נוספת. לעיתים ישנו קושי מהותי למדינה להכיל את האירוע כפי שזה בא לידי ביטוי בניתוח מקרי הבוחן ועל כן מדינה עשויה להכיל את האירוע באמצעות **שיתוף פעולה בין מדינתי**. שיתוף פעולה זה יכול להתקיים באמצעות גורמי ביטחון ומודיעין או לחלופין באמצעות גופים ממשלתיים רשמיים. שיתוף פעולה מסוג זה יכול שיקבל תוקף משפטי במידה והמדינות חותמות על אמנה המחייבת את שני הצדדים לשיתוף פעולה. סין ורוסיה חתמו על אמנה למניעת מתקפות קיברנטיות אחת כלפי השנייה. אמנה זו בעלת תוקף משפט במסגרת הדין הבינלאומי. נוסף על כך, מדינה ,כחלק מנקיטת מדיניות הכלה והתאוששות, עשויה לייצר **שיתוף פעולה פנים- מדינתי** בין גופי הביטחון, המודיעין לטובת טיפול מיטבי באירוע. ראיה לכך, ניתן לראות את שת״פ בין צה״ל לשירות הביטחון הכללי בטיפול במתקפת ה-DDOS האיראנית על מרחב האינטרנט הישראלי במהלך מבצע צוק איתן[69]. נקיטת מדיניות הכלה והתאוששות עשויה להיעזר בסמכות **המשטרה המקומית**. לעיתים האירוע חוצה את גבולות המדינה הנתקפת והכלת האירוע מחייבת סיוע מדינות נוספות המעוברות בתקיפה. לפיכך, ניתן לעשות שימוש בסמכות המשטרה המקומית לטובת הכלת האירוע במדינה נוספת באם העבירה הינה בעלת אופי פלילי. לטובת הכלת אירוע הגנה רחב היקף במגוון מגזרים נדרש ראייה לאומית אשר עושה שימוש בסמכויות החוקיות של גופי ההגנה. לעיתים ישנם יעדי תקיפה אשר לגופי המודיעין והביטחון לא נתנה הסמכות לפעול בהן לדוגמא חברה פרטית. לפיכך, לעיתים מועברת **בקשה להסכמת** יעד התקיפה לאפשר לגופי המודיעין והביטחון להכיל את האירוע. הסמכת יעד התקיפה לטיפול באירועי הגנה עשויה לזרז את משך הטיפול באירוע ולמזער את הנזק מהאירוע. יודגש, כי אין חובה לחברה פרטית לשתף פעולה עם גופי הביטחון והמודיעין שלא בהוראת בית משפט. ראיה לכך, חברת Apple סירבה לסייע ל FBI האמריקאי בחקירות מתוך רצון לשמור על פרטיות לקוחותיה[70]. ישנו מתח בין פרטיות האזרחים ושמירה על זכויותיהם לבין שמירה על הביטחון המהווה אינטרס ציבורי. מתח משפטי זה הינו במוקד הליווי המשפטי הניתן למקבלי ההחלטות בגופי הביטחון והמודיעין. תפקיד היועץ המשפטי לאפשר את פעילות ההגנה בדרך התואמת את הסמכות החוקית. בדומה לשירות הביטחון הכללי אשר פועל במסגרת סמכותו מכוח בחוק שב״כ, נכתב בשעה זו חוק רשות לאומית להגנה בסייבר אשר עתיד לשמש כסמכות החוקית לפעולת הרשות. חקיקה זו מעידה על שאיפתה של מדינת ישראל לספק הגנה על אזרחיה במרחב הקיברנטי. לעומת זאת, לצורך עמידה על המדיניות האמריקאית, ניתן להבחין כי ארה״ב נמענה מסיוע טכני לחברה מפני המתקפה. נשאלת השאלה מהי מידת **המעורבות המדינית** הנדרשת בעת אירוע תקיפה קיברנטית. תשובה לשאלה זו עשויה להשתנות ממדינה למדינה בהתאם לתפישת הביטחון והמדיניות הנהוגה במדינה. תקיפה קיברנטית בהיקף רחב ,כדוגמת פגיעה במגזר הפיננסי בישראל, עשויה לגרור מעורבות טיפול מדינתית. לעומת זאת, תקיפה קיברנטית המוכוונת בנק גדול בישראל, אינה מאיימת על כלכלת ישראל ולפיכך סביר כי הבנק יפעל להכיל את האירוע בכוחותיו. כתוצאה מכך, מדינות עשויות להפעיל שיקול דעת בבחינת אירועי התקיפה הקיברנטיים בשטחה ובהתאם לניתוח האירועים לבחור באילו מהאירועים נדרשת התערבות מדינתית. ייחודו של המרחב הקיברנטי מקשה על מדינה לספק הגנה מתמשכת על אזרחיה כפי שנדרשת לכך במרחב הקינטי. ישנן גישות מנוגדות למידת **אחריות מדינה** על אזרחיה במרחב הקיברנטי. מחד, גישה המייחסת למדינה אחריות מוחלטת כחלק מהאחריות הביטחון במרחבים נוספים ומאידך, גישה המבדלת את המרחב הקיברנטי מהמרחב הקיברנטי

[69] ראו הרחבה פרק ג׳ מקרה בוחן שלישי

[70] https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

ומשחררת מאחריות המדינה על הביטחון מפני מרחב זה וקוראת לאזרחים לנקוט באמצעי זהירות סבירים לצמצום פוטנציאל הנזק. סיווג פעולה במרחב הקיברנטי אשר תסווג כ**פעולת טרור** תסייע לכוחות הביטחון להפעיל את סמכותם לטיפול בתקיפה. לעיתים, ארגוני הטרור לוקחים אחריות על התקיפה באופן רשמי ופומבי דבר אשר מסייע לשירות הביטחון הכללי להפעיל את סמכותו לטיפול בתקיפה.

ב. **שיקולים מדיניים המשפיעים על קבלת ההחלטות**

בבחירת מדיניות תגובה ישנה חשיבות מכרעת לשיקולים מדיניים. מקבלי ההחלטות מנהלים מערכות יחסים משתנות עם מדינות יריב, מדינות אויב ומדינות עמיתות. מקבלי ההחלטות עשויים לפעול באופן שונה בבחירת מדיניות תגובה למתקפה קיברנטית מטעמים אשר אינם קשורים באופן ישיר למאפייני התקיפה. כראיה לכך, ניתן לראות בבחירתה של מדינת ישראל להימנע מתגובה למתקפה הקיברנטית האיראנית במהלך 'צוק איתן' כבחירה מדינית להימנע מיצירת חזית לחימה נוספת לרצועת עזה. לעומת זאת, באם המתקפה האיראנית הייתה מתרחשת במועד שצה"ל אינו מצוי בעיצומה של מערכה קינטית, יתכן והמתקפה האיראנית הייתה משמשת את הדרג המדיני כעילה לפתיחה במערכה קינטית מול האויב האיראני. לפיכך, החלטות הדרג המדיני, עשויות להשפיע באופן מהותי על מדיניות התגובה ולעיתים אף לייצר קרקע להזדמנויות המשרתות את השיקולים המדיניים.

ג. **<u>תגובה פומבית</u>**

קיים מתח בין רצון המדינה לשדר חוסן לאומי כלפי אזרחיה לבין חובת מדינה לעדכן את אזרחיה בדבר מתקפות קינטיות וקיברנטיות כאחד. בחירה במדיניות תגובה פומבית למתקפה קיברנטית, מאפשרת למדינה לעדכן את האזרחים בדבר התקיפה, מסייעת בהכוונת התנהגותם העתידית באירועים דומים ומעבירה מסרים לתוקף בנוגע ל'קו האדום' המדינתי. מדיניות זו חייבת לעמוד בדרישות המשפטיות הקבועות בדין הבינלאומי ובדין הפנימי כאחד. גישה המעודדת תגובה פומבית רואה בכך כלי משמעותי המשמש להסברה ולהעברת מסרים לאזרחים. הסברה זו נמצאה יעילה בטיפול באירועי תקיפה קינטיים ולפיכך אין מניעה שיסייע בטיפול באירועי תקיפה קיברנטיים. גישה מנוגדת לכך, גורסת כי מדינה צריכה לעיתים להימנע מתגובה פומבית. הימנעות מתגובה פומבית מבטלת את תחושת ההצלחה של התוקף, משמרת את החוסן הלאומי ומטשטשת את יעד התקיפה והיקפה אשר פרסומם עתיד לשמש תוקפים נוספים בעתיד. החלטה בדבר מדיניות תגובה פומבית מושפע משיקולים מדיניים. מדיניות תגובה הכוללת הכלה והתאוששות יכולה להסתיים בהודעה לציבור בגין הטיפול באירוע מבלי להתייחס לאופן התגובה אשר עשוי להיות באמצעים חשאים. לפיכך, מדיניות תגובה פומבית עשויה לשרת את מקבלי ההחלטות בהתמודדות עם האירוע באופן משלים לשיקולים המדיניים. בהקשר זה יצוין, כי השימוש במרחב הסייבר ככלי תגובה עשוי לסייע למדינה הנתקפת ללמידת התגובה, כליה ומתודולוגיית המדינה המגיבה. לפיכך, שימוש בתגובה פומבית באמצעות המרחב הקיברנטי עשוי לשמש את הנתקף ללמידה לקראת קידום מתקפה עתידית.

ד. **<u>מרחב ההכחשה בסייבר</u>**

אחד המאפיינים המרכזיים המבדילים את המרחב הקיברנטי מהמרחב הקינטי הוא האפשרות העומדת בפני מדינה להכחיש קיומה של מתקפה קיברנטיות או לחלופין להכחיש תגובה קיבנרטית. כראיה לכך, ניתן לראות

כי ארה"ב לא לקחה אחריות על נפילת ארבעת רשתות האינטרנט המרכזיות למרות שהחקירה הטכנית סברה כי אין נפילה זו מקרית[71]. באם אכן ארה"ב ביצעה מתקפה זו, ניתן לייחס לה נקיטה במדיניות תגובה אשר מכחישה את התגובה האמריקאית ובכך נמנעת מלקיחת אחריות. יודגש, כי מרחב ההכחשה עשוי לשמש את גורמי ההגנה במסגרת הטיפול באירוע ובהתאמה את גורמי ההתקפה אשר אחראים לפעילות תגובה קיברנטית. יצוין, כי מרחב ההכחשה אינו ייחודי למרחב הקיברנטי, אולם השימוש במרחב ההכחשה במסגרת פעילות קינטית הנראית לעין מאתגר יותר ביחס למרחב הקיברנטי. הפערים הטכניים אשר מקשים על המגן לאתר את מקור התקיפה מאלצים לעיתים מדינות לעשות שימוש במרחב ההכחשה, להימנע מפרסום חלקי ובכך לשמר את החוסן הלאומי. יתרה מכך, פערים טכניים אלו מאפשרים למדינה להימנע מתגובה ובכך לנקוט במדיניות הכחשה בהתייחסותה למתקפה הקיברנטית[72]. בהקשר זה יצוין, כי במקרים בהם גופי המודיעין במדינה מחזיקים במידע מסווג אודות מקור התקיפה, ימנעו מפרסום המידע לציבור הרחב, באמצעות מרחב ההכחשה, על מנת לשמר את המקור המודיעיני. לעיתים השיקול בפרסום מידע הינו חלק משיקולים מדיניים אסטרטגי, במקרים אלו מדינה מוכנה לפרסם מידע מסווג במחיר של פגיעה במקור המודיעיני. ראיה לכך, מדינת ישראל לאחר מלחמת ששת הימים פרסמה הקלטה מסווגות של שיחת בין נשיא מצרים ג'מאל עבד אל נאצר לבין חוסיין מלך ירדן, כדי להצדיק את יציאתה למלחמה. ההחלטה בדבר פומביות הטיפול באירוע או לחלופין התגובה לאירוע קיברנטי תלויה בשיקולים מדיניים אשר משפיעים באופן ישיר על מדיניות התגובה ומידת פרסומה.

ה. **<u>תגובה חשאית</u>**

מרחב ההכחשה מאפשר למדינות להגיב באמצעות גורמי המודיעין והביטחון מבלי לפרסם פעולות אלו. גופי המודיעין והביטחון מורגלים בעבודה חשאית שאינה מפורסמת לציבור. המרחב הקיברנטי משמש קרקע פורייה לתגובה מדינתית חשאית לעומת המרחב הקינטי בו תתקשה מדינה להגיב באופן חשאי. מקבלי ההחלטות עשויים לעשות שימוש במרחב ההכחשה, להימנע מתגובה פומבית ולקדם פעילות תגובה חשאית. נקיטה במדיניות הכחשה עשויה לשמש קרקע לגופי המודיעין והביטחון להגיב באופן חשאי למתקפה. בתוך כך, מדיניות תוגבה חשאית מהווה חלופה ראויה למדינה אשר מעוניינת להימנע מפרסום יכולותיה ההתקפיות במרחב הקיברנטי.

ו. **<u>סיכול פעילויות סייבר</u>**

פגיעה מקדימה ביכולות ההתקפה של אויבים וריבים מכונה 'סיכול' במרחב הקיברנטי. פעולת סיכול במרחב הקינטי כדוגמת הפצצה אווירית מעוררת קשיים ביכולת מדינות להכחיש אחריותן לפעולות אלו. לעומת זאת, במרחב הקינטי מדינות יכולות לפעול באמצעות מרחב ההכחשה לביצוע מגוון פעולות בהן סיכול מערכי תקיפה של גורמי אויב. פעילות סיכול מחייבת שימוש בכלים ויכולות אשר אין המדינה מעוניינת בפרסומם ולפיכך לרוב פעולת סיכול תתבצע באמצעות גופי מודיעין וביטחון באופן חשאי. פעולת הסיכול במרחב הקיברנטי מתבססת על מידע אודות זהות התוקף, מתודולוגיית פעולתו, מערכי התקיפה ברשותו, כליו

[71] ראו הרחבה בפרק ג' – מתקפת צפון קוריאה על חברת Sony האמריקאית.
[72] ראו הרחבה בפרק ג' – מתקפה קיברנטית איראנית על מרחב האינטרנט הישראלי במהלך 'צוק איתן'

ויכולותיו הטכנולוגיות. לפיכך, לקידום פעילות סיכול ישנה חשיבות מכרעת במודיעין המסווג המגיע מסוכנויות המודיעין והביטחון. הצורך במידע המסווג מחייב את גופי המודיעין והביטחון לרגל אחר אויביה באופן שוטף. ישנה הנחה לפיה ריגול התקיים בעבר, מתקיים כעת וימשיך להתקיים בעתיד. בבחינת הדין הבינלאומי, ריגול למטרות איסוף מודיעין אינו מהווה איום על מדינה ולפיכך אין מדינה רשאית להפעיל כוח כתגובה לפעולת ריגול בשטחה.

סיכול מערכי תקיפה בשימוש האויב מהווה כלי מרכזי בסל הכלים המדינתי לתגובה. הסיכול הינו **פעולת הגנה מקדימה** אשר תכליתה לפגוע במערכי התקיפה של האויב בשלב הקודם למתקפה. לפיכך, נדרשת הפעולה לעמוד במסגרת הדין הבינלאומי בדבר פעולת הגנה מקדימה[73]. סיכול מערכי תקיפה של אויבים מצריכה שימוש במשאבים מוגבלים, לפיכך ישנה חשיבות לזהות התוקף, יכולותיו ופוטנציאל הזנק הצפוי בקביעה כי ישנו צורך בסיכול המערך. במסגרת היחסים בין מדינה לארגוני טרור, ישנו יתרון מובהק למדינה במשאבים העומדים ברשותה לסיכול מערכי תקיפה קיברנטיים של ארגוני טרור. ארגוני הטרור עשויים לרכוש יכולות תקיפה מהאקרים פרטיים ובכך להקשות על ארגוני המודיעין לאתר קשרים אלו ולהקשות על סיכול המערכים.

ז. **<u>תגובה קינטית בכפוף לדינים הבינלאומיים</u>**

התגובה המדינתית עשויה לכלול רכיב תקיפה קינטי כתגובה למתקפה הקיברנטית. במסגרת הדין הבינלאומי פומבי ישנו איסור על שימוש בכוח (סעיף 2(4) למגילת האו״ם). לאיסור בשימוש בכוח ישנם חריגים המקנים למדינות **זכות להגנה עצמית** (סעיף 51 למגילת האו״ם) ובכך מהווה פתח משפטי להצדקת פעולות קינטיות כתגובה למתקפות קיברנטיות. לצורך השוואה, פגיעה כלכלית אשר בעבר נחשבה לתנאי להפעלת הזכות להגנה עצמית, נדחה וכעת אינה משמשת עילה ראויה. השימוש במתקפה קינטית כזכות להגנה עצמית נדרש לקיים את דרישות הסעיף, דרישת הצורך ודרישת המידתיות. דרישות אלו מקשות על יישום הסעיף כמקנה זכות למדינות להפעיל יכולות קינטיות בתגובה למתקפות קיברנטיות ופוגעות בהצדקת תגובה מסוג זה. בדומה לאיסור השימוש בכוח, ישנו קושי הגדרתי להתקיימות '**עימות מזוין קיברנטי**'. הגדת 'עימות מזוין' באמצעות השוואת היקף העימות ותוצאותיו למרחב הקינטי מסייע ביישום הדין הבינלאומי למרחב הקיברנטי. בבחינת הזנק הפוטנציאלי ממתקפת הסייבר נדרשת השוואה לנזק הפוטנציאלי של פעולות במרחב הקינטי. לטובת השוואה זו, מסמך טאלין מסייע במדידת הנזק בכך שמגדיר קריטריונים כתנאי וכעילה לשימוש בכוח בעימות המזוין.

ישנם מקורות נוספים המשפיעים על התגובה הקינטית למתקפה קיברנטית, המרכזי שבהם הינו **מדריך טאלין**, המכונה 'טאלין 1', אשר התמקד בניסיון ליישם את הדין הבינלאומי למרחב הקיברנטי. המדריך משמש את היועצים המשפטיים כספר עזר ואינו בעל תוקף משפטי מחייב. המסמך נכתב על ידי משפטנים מומחים במרחב הקיברנטי ומכאן חשיבותו. המדריך קבע שמונה קריטריונים אשר מהווים הצעה לבסיס בחינת הפעולה כשימוש בכוח. קריטריונים אלו עשויים לשמש את היועצים המשפטיים של מדינות בשלב המקדים לבחירה בתגובה קינטית, הגם שאין מדריך זה מחייב מבחינה משפטית. יצוין, כי עתיד להתפרסם

73ראו הרחבה פרק ב' – בחינת הדינים המשפטיים – הדין הבינלאומי פומבי

מדריך 'טאלין 2' אשר יעסוק בדיני האחריות המדינית. תוכן המדריך עתיד לסייע למשפטנים בניתוח הדין הבינלאומי למרחב הקיברנטי ובקביעת מגוון החלופות העומדות בפני מדינה. נוסף על כך, יצוין כי בזירה הבינלאומית הרשמית, ישנה **קבוצת מומחים של האו"ם UNGEE** המטפלת בנושא הסייבר כנשק אסטרטגי. בתוך כך, עמדתן של רוסיה וסין היא שהדין הבינלאומי לא מספק מענה הולם ולכן נדרש הסדר ספציפי למרחב הקיברנטי. לעומתן, עמדת המערב גורסת כי ניתן ליישם את הדינים הקיימים למרחב הקיברנטי ולא נדרשת חקיקה מיוחדת. כמו כן, **אמנת בודפשט מספר 185 COE** מסייעת לאכיפת החוק המדינתי בסייבר. האמנה עוסקת בפעולות פליליות ומהווה תשתית לשיתופי פעולה בין מדינות להפעלת כוח עקיף, כדוגמת איסוף ראיות בשטחה מדינה זרה. לאור היעדר הסכמים רבים בין מדינות, סביר כי הדין הבינלאומי יתפתח כ**דין מנהגי**. הדין המנהגי הינו מקור משפטי מחייב מכוח סעיף 38(1)ב לחוקת בית הדין הבינלאומי בהאג. האופן בו מדינה נוהגת מעיד כל הסכמה משתמעת למנהג הרווח ורק במידה ותביע התנגדות פומבית המנהג לא יחייב אותה. לאור זאת, טענתו של אובאמה במסגרת תקיפת צפון קוראיה את חברת SONY, כי אין כללים במרחב הקיברנטי אינה מדויקת. **הכללים הנורמות והעקרונות אשר נקבעו בדין הבינלאומי חלים על המרחב הקיברנטי** גם בהיעדר תקיפות המסייעות לגיבוש דין מנהגי.

<u>פרק ה - סיכום</u>

טרור מסוג סייבר הינו איום אשר סביר כי יתפתח וישפיע על חיינו בעתיד הקרוב. מטרת המחקר לעורר שיח בקרב מקבלי ההחלטות בדבר אופן תגובתם למתקפת הטרור מסוג סייבר הבאה. במסגרת בחינת מדיניות התגובה הראויה למדינה, עלה הקושי ההגדרתי למונח טרור אשר מקשה על הסכמה בינלאומית למושג 'טרור סייבר'. כתוצאה מהמחקר, החוקר מציע הגדרה מחודשת למונח טרור- סייבר: "מאבק אלים אשר במסגרתו נעשה שימוש במרחב הקיברנטי באופן המוכוון כלפי אזרחים, על מנת להשיג מטרות פוליטיות ותוצאתו שקולה למתקפה במרחב הקינטי". איום הטרור מסוג סייבר, מחייב היערכות הגנתית בקרב מדינות מפותחות אשר מבססות פעילותן על מערכות ממוחשות. מדינת ישראל מבצעת בשנים האחרונות מספר שינויים מהותיים אשר תכליתם שיפור ההגנה הלאומית במרחב הקיברנטי. שינויים אלו, מעידים על הפנמת האיום בקרב מקבלי ההחלטות במדינת ישראל. בחירה במדיניות תגובה מושפעת רבות מהדין הפנימי והדין הבינלאומי הנהוג. בתוך כך, ישנה חשיבות מכרעת לניתוח ויישום דינים אלו למרחב הקיברנטי לטובת בחירת מדיניות תגובה מיטבית למתקפה קיברנטית. הדין הפנימי במדינת ישראל מתייחס באופן מצומצם לפעולות תגובה אפשריות למתקפה קיברנטית, עם זאת חוק הרשות הלאומית להגנה בסייבר אשר עתיד להתפרסם בקרוב עשוי לעצב את המסגרת החוקית לפעולות תגובה מסוג זה. כמו כן, פעולת תגובה מדינתית קינטית כפופה לדין הבינלאומי אשר לאור ניתוח 'מדריך טאלין' נראה כי ניתן ליישם את עקרונות הדין הבינלאומי למרחב הקיברנטי הגם שנכתב במקור עבור המרחב הקינטי. הימנעות מיישום הכללים הקבועים בדין הבינלאומי למרחב הקיבנרטי, עשויה לאפשר למדינות מרחב פעולה רחב להפעלת כוח בניגוד לעקרונות המקובלים בדין הבינלאומי. מקרי הבוחן אשר נבחנו במסגרת המחקר, עשויים להעיד על מדיניות תגובה אפשרית, אך יתכן כי אותן מדינות ינהגו אחרת בנסיבות מקרה שונות. במקרה הבחון החמישי אשר עסק במתקפת צפון קוריאה את חברת SONY האמריקאית וכלל איום בפעולת טרור כלפי צופי הסרט 'ראיון סוף',

ניתן להבחין במדיניות התגובה האמריקאית. אובאמה הבטיח תגובה פרופורציונאלית למתקפה וטען כי "יש צורך בהול בחקיקת חוקים בעולם האינטרנטי". ארה"ב עשתה שימוש במרחב ההכחשה והכחישה מעורבות בפגיעה בארבעת הרשתות הרשמיות שמחברות את צפון קוריאה לאינטרנט, הגם שנפגעו שבוע לאחר הבטחת אובאמה לתגובה פרופורציונאלית.

בפני מדינות עומדות מגוון חלופות לתגובה למתקפת טרור מסוג סייבר. מדינה יכולה לבחור במדיניות של הכלה והתאוששות להסרת האיום. תקיפה קיברנטית על תשתיות מדינה קריטיות עשויה למקד את פעילות ההגנה בהכלה והתאוששות לאור חשיבות הרציפות התפקודית של מערכות אלו. על מנת לשפר את יכולות ההכלה וההתאוששות, מדינה יכולה להסדיר שיתופי פעולה עם מדינות עמיתות לטובת טיפול משוטף במתקפות. יודגש, כי מדיניות התגובה נגזרת משיקולים מדיניים אשר עשויים להשפיע על אופי התגובה, היקפה ומידת חשיפתה לתקשורת. המרחב הקיברנטי מאפשר למדינות לעשות שימוש במרחב ההכחשה כמגן הנמנע מפרסום תקיפה בשטחו וכתוקף אשר נמנע מייחוס פעולת תגובה התקפית בשטח האויב. כמו כן, בפני מדינה עומדת האפשרות להגיב באמצעות גופי המודיעין והביטחון באופן חשאי לצורך סיכול מערכי התקיפה של האויב. תגובה קינטית למתקפה הקיברנטית נדרשת לעמוד בכללים ובנורמות אשר נקבעו בדין הבינלאומי.

מדיניות התגובה למתקפה קיברנטית מושפעת מזהות התוקף, יכולותיו ומידת הנזק הצפוי מהמתקפה. לאור זאת, המחקר מהווה ניסיון ראשוני בהתמודדות עם שאלת בחירת מדיניות התגובה הראויה למתקפה קיברנטית. שאלת בחירת מדיניות תגובה למתקפות קיברנטיות עשויה להעסיק את מקבלי ההחלטות בעתיד הקרוב ועל כן ראוי להעמיק בנושא קביעת מדיניות תגובה הראויה כחלק מההתמודדות עם הטרור מסוג סייבר.

נספח א' - פגישות מחקריות אישיות

במסגרת המחקר, החוקר נפגש עם אישים המהווים מדגם מייצג למקבלי החלטות ברמה המדינית, משפטנים מומחים למרחב הקיברנטי ומומחי טרור מסוג סייבר. בהזדמנות זו הכותב מוסר תודתו לאישים אלו אשר סייעו בקידום המחקר ובמתן מענה מיטבי לשאלת המחקר.

- תת אלוף (במיל') שחר ארגמן, ראש אגף במטה הסייבר הלאומי, משרד ראש הממשלה
- סא"ל (במיל') נועם קרקובר ראש תחום בכיר, מטה סייבר לאומי, משרד ראש הממשלה
- עו"ד עמית אשכנזי, יועץ משפטי מטה סייבר לאומי, משרד ראש הממשלה
- סא"ל א , ראש אגף בכיר ברשות הלאומית להגנה בסייבר, משרד ראש הממשלה
- עו"ד דבורה האוזן, מומחית למרחב הקיברנטי ושותפה לקבוצת המומחים אשר חיברו את 'מסמך טאלין'
- אלוף משנה (במיל') ד"ר איתן עזאני סמנכ"ל המכון למחקר טרור ICT, המרכז הבינתחומי הרצליה
- ד"ר אליאב ליבליך , מומחה למשפט בינלאומי פומבי, המרכז הבינתחומי הרצליה

נספח ב' - ביבליוגרפיה

[1] http://ictlib.cet.ac.il/pages/item.asp?item=16561
[2] http://knesset.gov.il/committees/heb/material/data/H07-10-2015_14-42-37_.pdf
[3] http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf
[4] http://michal.harel.org.il/cmc.htm
[5] Adv. Deborah Housen-Couriel, The envolving law on Cyber Dilemmas in International Law and Israeli law, 2013.
[6] DCSINT Handbook No. 1.02, Cyber Operations and Cyber Terrorism, 15 August 2005, p. I-4: "Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves."
[7] CSIS has defined it as "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population." (James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," Center for Strategic and International Studies, 2002, p.1).
[8] FBI- "The unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, ICTWPS March 2013 [13]/28. in furtherance of political or social objectives." As cited in S. Gordon and R. Ford, Cyberterrorism?, Symantec White Paper, p.4 (no date).
[9] Referenced in ENISA Threat Landscape, 8.1.2013 (https://www.fas.org/sgp/crs/terror/RL32114.pdf).
[10] Brussels Ministerial Declaration of 7 December 2006, Decision No. 7/06, "Countering the Use of the Internet for Terrorist Purposes", at #9 (http://www.osce.org/mc/23078). http://www.osce.org/cio/126475
[11] UNODC, supra note 12
[12] See the ITU's 2010 Toolkit for Cybercrime Legislation , and its analysis below.
[13] http://www.cleanitproject.eu/about-the-project/
[14] Council of Europe, "Cyberterrorism - the use of the internet for terrorist purposes", 2008
[15] http://www.pmo.gov.il/MediaCenter/Spokesman/Pages/spokecyber150215.aspx
[16] CERT - Community Emergency response team.
[17] https://cert.gov.il/About2/mission/Pages/mission.aspx
[18] http://gpo.gov.il/NewsRoom/GPOnews/Pages/pm230615q.aspx
[19] http://www.idf.il/1133-22318-he/Dover.aspx
[20] http://www.arcyber.army.mil/org-uscc.html
[21] http://www.tikshuv.idf.il/901-8536-he/tikshuv.aspx#.Vtx4LPl97IU
[22] http://news.walla.co.il/item/2911579
[23] 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
[24] ראו הרחבה בפרק ג' מקרי בוחן - בחינת מדיניות ארה"ב כנגד מתקפת הסייבר על חברת סוני האמריקאית.
[25] Tallinn Manual on The International Law Applicable to Cyber Warfare (2013). http://issuu.com/nato_ccd_coe/docs/tallinnmanual/37?e=5903855/1802381
[26] NATO- Cooperative Cyber Defense Centre for excellence ; ccdcoe.org/index.html
[27] http://www.haaretz.co.il/captain/net/1.1971006
[28] http://tech.walla.co.il/item/2844066
[29] סעיף 11 במדריך טאלין "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 "

[30] "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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-defense 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"

[31] Necessity and Proportionality .כלל מספר 14 במדריך טאלין

[32] 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).

[33]סעיף 11 במדריך טאלין

[34] https://www.asil.org/insights/volume/14/issue/37/international-law-drones

[35] S.C. Res. 1373, U.N. DOC. S/RES/1373 (Sept. 28, 2001);

[36] 2011 ,Watts

[37] http://weblaw.haifa.ac.il/he/Journals/lawatch1/lawatchF/2004c_wall.htm

[38]מדריך טאלין עמודים 59-60

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

[40]מדריך טאלין עמוד 79

[41] http://www.harvardilj.org/2012/12/online-articlesonline_54_schmitt/.

[42]מדריך טאלין 76

[43] http://www.nevo.co.il/law_html/Law01/214_001.htm

[44] http://www.shabak.gov.il/about/yoamash/pages/law.aspx

[45] http://www.dinimveod.co.il/hashavimcmsfiles/Pdf/sh1685.pdf

[46] http://knesset.gov.il/committees/heb/material/data/H07-10-2015_14-42-37_.pdf

[47] https://www.ict.org.il/Article/1634/Position-Paper-Counter-Terrorism

[48]ראו הרחבה בפרק א'

[49]http://www.isa.gov.il/GeneralResearch/179/Documents/%D7%9E%D7%98%D7%91%D7%A2%D7%95%D7%AA%20%D7%93%D7%99%D7%92%D7%99%D7%98%D7%9C%D7%99%D7%99%D7%9D%209.pdf

[50]החוק להסדרת הביטחון בגופים ציבוריים 1998

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

[52]ראו הרחבה בנושא דיני מלחמה בפרק ב'

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

[54] http://www.israeldefense.co.il

[55] http://www.calcalist.co.il/internet/articles/0,7340,L-3592648,00.html

[56] http://news.walla.co.il/item/2605254

[57] http://www.dni.gov/index.php

[58] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[59] http://heb.inss.org.il/index.aspx?id=4354&articleid=7583

[60]חוקר בכיר העומד בראש תכנית ביטחון סייבר במכון למחקרי ביטחון לאומי INSS

[61] http://www.dentech.org/articles/article_9_2015_f.pdf

[62] http://www.themarker.com/advertising/1.2516885

[63] http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html?_r=0

[64] http://news.walla.co.il/item/2812157

[65] http://www.calcalist.co.il/internet/articles/0,7340,L-3648074,00.html

[66] http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[67] http://heb.inss.org.il/index.aspx?id=4354&articleid=11446

[68]ראו הרחבה בפרק א' - הגדרת טרור סייבר

[69]ראו הרחבה פרק ג' מקרה בוחן שלישי

[70] https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html

[71] ראו הרחבה בפרק ג' - מתקפת צפון קוריאה על חברת Sony האמריקאית
[72] ראו הרחבה בפרק ג' - מתקפה קיברנטית איראנית על מרחב האינטרנט הישראלי במהלך 'צוק איתן'
[73] ראו הרחבה פרק ב' - בחינת הדינים המשפטיים - הדין הבינלאומי פומבי