

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

שרון אפק¹

2	תקציר
2	מבוא - המרחב הקיברנטי והמשפט הבינלאומי
3	א. התקפה במרחב הקיברנטי
5	ב. התקפות הדגל הקיברנטיות בזירה הגלובלית
5	ההתקפה על אסטוניה
6	ההתקפה על גיאורגיה
7	התקפת Stuxnet באיראן
7	התקפות סיניות בארצות הברית
8	ג. מבט להמשך - האטרקטיביות של התקפות קיברנטיות
9	ד. עיצוב כללי המשחק
9	גיבוש מדיניות קיברנטית
10	הפעילות באו"ם
12	ד. המרחב הקיברנטי והמשפט הבינלאומי - ביחד או לחוד?
14	ה. האתגר בהחלת כללי המשפט הבינלאומי במרחב הקיברנטי
15	ו. הזכות להשתמש בכוח כהגנה עצמית כתגובה ל"התקפה מזוינת"
17	סיכום

¹ אלוף משנה שרון אפק מכהן כיום כמפקד קורס פיקוד ומטה (פו"ם) 'אפק' במכללות הצבאיות. מאמר זה נשען על פרסומו "ההתקפה הקיברנטית - קווים משפטיים לדמותה, יישום כללי המשפט הבינלאומי על לוחמה במרחב הקיברנטי", בבמת הפרסום של מרכז המחקר של המכללה לביטחון לאומי, עשתונות, גיליון מס' 5, אוקטובר 2013.

תקציר

המרחב הקיברנטי מאתגר את הסדר המשפטי הבינלאומי מכמה בחינות. בראש ובראשונה, הוא מהווה מרחב נטול אכיפה אפקטיבית של החוק בכלל – סוג של "מערב פרוץ" מודרני – מטעם הקושי בזיהוי שחקנים ובאיסוף סיפית ראיות. מעבר לקשיים הטכניים, דורש המרחב הקיברנטי דורש הסכמות לגבי החלת המשפט הבינלאומי הקיים, שאיננו נוסח בצורה המתאימה לעידן הקיברנטי. לכן יש צורך ביצירת מסגרת משפטית חדשה ומשותפת – משטר קיברנטי שיגדיר את המותר והאסור. הקושי הוא שלכל מעצמה הגדרות משלה למונחים שנויים במחלוקת, כמו "התקפה", כאשר פרשנויותיהן של המעצמות נקבעות בהתאם להנחות יסוד, לאידיאולוגיה ולאינטרסים אישיים. בד בבד, סיכון ההתקפות רק גובר, ואם מדינות לא ימצאו מענה מתאים מצד המשפט הבינלאומי, הן עלולות להתעלם ממנו לגמרי.

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

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

מבוא - המרחב הקיברנטי והמשפט הבינלאומי

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

סיפורה של המלחמה ודיניה הוא גם סיפור של התפתחויות טכנולוגיות. זאת החל מעידן הכלים (המצאת הגלגל), דרך עידן המכונות (למשל השימוש בארטילריה), עידן המערכות (כגון רדאר ומטוסים ארוכי טווח) ועד עידן האוטומציה והמידע (מערכות תקשורת ומחשוב מתוחכמות).² את הלחימה המודרנית מרבים לתאר כלוחמת מידע, לאור המקום הנכבד שתופס בה השימוש בטכנולוגיית מחשבים.³ במאה העשרים ואחת, רשתות תקשורת ומחשבים הם מרכיב משמעותי ביותר בביטחון הלאומי של מדינות. הם מעצימים את כוחן של מדינות ופותחים בפניהן אופקים חדשים, אך בה בעת, התלות בהם מחדדת את הפגיעות והרגישות של מדינות להתקפות עליהן במרחב המכונה 'קיברנטי'.⁴

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

² William Owens, **Lifting the Fog of War** (2001).

לעניין ההקבלה בין התפתחות המרחב הקיברנטי לבין התפתחות הכוח האווירי, והצורך בשני המקרים לפתח תיאוריה צבאית מתאימה:

Brett T. Williams, "The Joint Forces Commander's Guide to Cyberspace Operations", *73 Joint Forces Quarterly* 12 (2nd Quarter 2014).

המונח "עידן המידע" לקוח מספרו הידוע של אלווין טופלר, הגל השלישי.

³ Martin C. Libicki, "What is information warfare?", *ACIS Paper* 3 (August 1995).

Available at:

<http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html>

⁴ Rex Hughes, "Towards a Global Regime for Cyber Warfare", in: Christian Czosseck and Kenneth Geers, eds., **The virtual battlefield: perspectives on cyber-warfare** (2009), pp. 528-529.

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers"⁵.

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

בלבו של המרחב הקיברנטי מצויה רשת האינטרנט ('מרשתת', בעברית תקנית). האינטרנט, אסופה של רשתות המקושרות ביניהן, פותחה בשנות השישים בארצות הברית כ-ARPANET, תוכנה צבאית שנועדה לקשר בין הרשתות של משרד ההגנה האמריקני, קבלנים שעבדו עמו ורשתות שנפרשו במספר אוניברסיטאות⁶. הרשת, שנשענה בראשיתה על מספר קווי טלפון שחיברו מחשבים בודדים, היא כיום ענק גלובלי, המקשר חלק נכבד מהאנושות⁷. במציאות המודרנית, למרחב הקיברנטי חלק משמעותי בכל תחום כמעט של חיינו, ומגמת ההרחבה של השפעתו צפויה להתעצם.

רשת האינטרנט נשאה עמה בשורה חדשה. היא תוכננה במטרה להיות פתוחה, מינימליסטית וניטרלית⁸. מבחינה טכנולוגית היא חסרת גבולות, חוצה גבולות וגלובלית⁹. אדם הניצב מול מסוף מחשב, עשוי בלחיצת כפתור לבצע פעולה, שתהדהד במקום הרחוק ממנו אלפי מיליון. הוא עשוי לתרום בכך לידע, לרפואה, לכלכלה ולחברה, אך לפעולתו עלולה להיות גם תוצאה מזיקה. לצד היתרונות העצומים של המרחב הקיברנטי, והאפשרויות הבלתי מוגבלות של שימוש בו לתכלית טובה, הוא משמש גם כר פורה לריגול, פגיעה בזכויות אזרח, פשיעה, גרימת נזק וטרור¹⁰.

כאשר התפתח המרחב הקיברנטי, היו שציירו אותו כ-'מערב פרוע' נטול סדר וחוקים¹¹. למעשה, אופיו החתרני והפתוח של המרחב היה אחד ממוקדי המשיכה אליו. עם הזמן, לצד הפיכת המרחב למרכזי כל כך בהווה האנושית, הולך ומתפתח שיח בעניין יצירת 'משטר קיברנטי'¹². על רקע האופי הגלובלי וחוצה הגבולות של המרחב, ברור שהסדרה תחייב מעורבות של שחקנים רבים ושיתוף פעולה בינלאומי. יצירת משטר קיברנטי כרוכה, בין השאר, בגיבוש כללי משחק מתחום המשפט הבינלאומי. כללים שיגדירו את המותר והאסור בין שחקנים בינלאומיים, ובין השאר, יפתרו את סימני השאלה ביחס לפעילות התקפית במרחב הקיברנטי.

א. התקפה במרחב הקיברנטי

אחד מאתגרי העיסוק המשפטי במרחב הקיברנטי הוא הצורך לגשר בין המונחים המקצועיים (הקיברנטיים), לבין עולם המושגים המשפטי. הדבר בולט ביחס למונח מרכזי, אשר עתיד לעמוד בלב ההסדרה המשפטית - 'התקפה' (Attack)¹³.

התקפות קיברנטיות הפכו כבר לשגרה, אך טרם התגבשה הבנה מוסכמת ומקובלת בזירה הבינלאומית ביחס להגדרתן. הדבר אינו כה מפתיע, שכן מונחים משמעותיים אחרים, כמו 'טרור', טרם זכו להגדרה בינלאומית מוסכמת¹⁴.

⁵ להרחבה ביחס להגדרות המרחב:

Clifford S. Magee, "Awaiting Cyber 9/11", 70 *Joint Forces Quarterly* 76 (3rd Quarter 2013).

⁶ George K. Walker, "Information Warfare and Neutrality", 33 *Vand. J. Transnat'l L.* 1079 (2000), pp. 1094-1095.

⁷ Vida M. Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places", 51 *Naval Law Review* 132 (2005). pp. 135-136.

⁸ Joseph S. Nye, "Cyber Power", Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010), p3..

⁹ אם כי בפועל, הרשת מוגבלת לעתים על ידי מדינות, חוקים לאומיים וטכנולוגיות שונות. להרחבה:

Tim Maurer, "Cyber Norm Emergence at the United Nations - An Analysis of the UN's Activities Regarding Cyber-security", Discussion Paper 2011-11, Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School (September 2011). p. 8.

¹⁰ *Ibid.* p. 16.

¹¹ *Ibid.* p. 14.

¹² *Ibid.* p. 9.

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

להרחבה בקושי שקשור למינוח:

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

¹⁴ המונח 'טרור' נטבע לראשונה כבר בשלהי המאה השמונה עשרה, במהלך המהפכה הצרפתית, אך עד היום טרם נמצאה לו הגדרה מחייבת ומקובלת, שזכתה לקונצנזוס עולמי. להרחבה:

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

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

בארצות הברית, לאחר שהוקם פיקוד ייעודי למרחב הקיברנטי¹⁵, החלו להתפרסם, משנת 2011, הגדרות רשמיות להתקפה קיברנטית. בהכללה, ההגדרות שאומצו על ידי ארצות הברית, נאט"ו ומדינות מערביות אחרות, כוללות שלושה רכיבים: אמצעי התקיפה (פעולה באמצעות מחשבים ורשתות); גרימת נזק; והתשתית המותקפות (מחשבים, מידע ורשתות של הגורם המותקף).

העמדה של רוסיה וסין, מנגד, שמה דגש על כך שפעולות מסוימות במרחב הקיברנטי הן פסולות. ניתן למשל ללמוד עליה מתוך גישת

Shanghai Cooperation Organization.¹⁶ הארגון שולל הפצת מידע, שנועדה להזיק למערכות חברתיות, פוליטיות וכלכליות, ומבקש לאסור שימוש במרחב הקיברנטי, באופן המערער את היציבות הפוליטית¹⁷. למותר לציין שגישה זו אינה מתיישבת עם ערכים מערביים, הנתפסים כאבן יסוד של המרחב הקיברנטי, כגון חופש הביטוי, הזכות לקבל מידע ולהחליף מידע בזמן אמת ועוד¹⁸.

הספרות המשפטית מנתחת על פי רוב שלושה סוגים מרכזיים של התקפות קיברנטיות¹⁹:

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

השנייה, שתילת מידע שגוי - התוקף מחדיר מידע שגוי למערכת מחשב, כאשר זו ממשיכה לכאורה לפעול בצורה תקינה, גם כאשר היא סוטה ממשיותיה²⁰. כך למשל, נטען כי ארצות הברית תכננה בשנת 1999 להזין מידע שגוי במערכת ההגנה האווירית של סרביה ולנטרל כך את יכולתה לפגוע במטוסי נאט"ו²¹.

השלישית, חדירה לרשת מחשבים וביצוע פעולות באמצעותה - להתקפה מסוג זה פוטנציאל לשבש מערכות רגישות, למשל כאשר מערכות מחשבים שולטות על מפעלים גדולים ותשתיות כמו חשמל ומים (מערכות SCADA - Supervisory Control and Data Acquisition).

¹⁵ הפיקוד הוקם במאי 2010, מתוך הכרה בחשיבות הממד הקיברנטי כממד חמישי, על מנת לתאם את הפעילות של כל הזרועות בתחום הקיברנטי. מטרתו לשמר את היכולת של ארצות הברית לפעול באופן חופשי במרחב הקיברנטי, לשם קידום האינטרסים הביטחוניים הלאומיים. בישראל טרם הוקם פיקוד קיברנטי. להרחבה:

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

¹⁶ ארגון שיתוף פעולה ביטחוני, המורכב מסיין, רוסיה, רפובליקות אסיאתיות (שהיו בעבר בברית המועצות) ומשקיפות כמו איראן, הודו ופקיסטן.

¹⁷ להרחבה בעניין מאמצים סיניים ורוסיים להפעיל מנגנוני פיקוח ושליטה:

Tom Gjelten, "Seeing the Internet as an 'Information Weapon,'" Sep. 23 2010. Available at:

<http://www.npr.org/templates/story/story.php?storyId=130052701>

¹⁸ להרחבה בעניין ההשקפות השונות של מדינות בהקשר הקיברנטי, כמבטאות סיכונים והזדמנויות אסטרטגיים:

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

¹⁹ Oona A. Hathaway, Crootof Rebecca, Levitz Philip, Nix Haley, Nowlan Aileen, Perdue William and Spiegel Julia, "The Law of Cyber-Attack", *California Law Review*, 100, 4 (2012); Yale Law & Economics Research Paper No. 453; Yale Law School, Public Law Working Paper No. 258.

Available at:

<http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf>

²⁰ Libicki, 1995; 77. ראו:

²¹ פעולה שלא יצאה לפועל. להרחבה:

Arkin M. William, "The Cyber Bomb in Yugoslavia", Wash. Post (Oct. 25, 1999). Available at:

<http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.html>

ב. התקפות הדגל הקיברנטיות בזירה הגלובלית

מלחמה קיברנטית, יום הדין הטכנולוגי, נתפסה בעבר כמדע בדיוני. בשנים האחרונות, התקפות קיברנטיות מדווחות, לא אחת, בראש מהדורות החדשות²², כפי שארע לאחרונה ביחס לחילופי המהלומות הקיברנטיים בין צפון קוריאה לבין ארצות הברית, על רקע סרט שעסק בשליט צפון קוריאה. כותבים מצביעים על תרחישים מטרידים, בהם התקפות אלו מסיטות רכבות נוסעים ממסילותיהן, מחשיכות ערים, מפוצצות צינורות נפט וגז ומשביתות שדות תעופה²³. הדעה הרווחת היא שסכסוכי העתיד (ולמעשה כבר במאבקי ההווה), יכללו גם לחימה קיברנטית, שמטרתה פגיעה בתשתיות, במידע, בכלכלה וברוח האנשים²⁴. אין זה מפתיע שביטחון המרחב הקיברנטי הוכתר על ידי האו"ם כאחד האתגרים המשמעותיים במאה העשרים ואחת²⁵.

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

ההתקפה על אסטוניה

באפריל - מאי 2007 נערכו התקפות מסיביות על רשת המחשבים של אסטוניה²⁶. זאת בתגובה לכוונת ממשלת אסטוניה להעביר אנדרטת זיכרון למלחמת העולם השנייה ממרכז עיר הבירה, טאלין, לבית קברות צבאי בפרברי העיר. ההתקפות נמשכו כחודש וכוונו נגד תשתיות אינטרנט ציבוריות וכלכליות, לרבות של הנשיא, ראש הממשלה, הפרלמנט, מפלגות, בנקים, גופי תקשורת וספקי אינטרנט²⁷. ההתקפות היו מסוגים שונים - DDoS, השחתת אתרי אינטרנט, הרס מידע ממוחשב ועוד, והובילו לנפילת שרתים ואתרי אינטרנט.



תמונה מס' 1: אנדרטת הזיכרון בטאלין²⁸

²² William Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber War", 89 *Int'l L. Stud.* 157 (2013), pp. 157-158.

²³ Richard A. Clarke & Knake Robert K., **Cyber War: The Next Threat to National Security and What to Do About It** (2010), pp. 64-68.

²⁴ Waxman, 2011; 423; המחבר מצטט דו"ח של מכון המחקר הבריטי, ה-IISS, לשנת 2010. ²⁵ 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).

²⁶ Eneken Tikk, Kaska Kadri & Vihul Liis, **International Cyber Incidents: Legal Consideration** (2010).pp. 14-33.

²⁷ Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, Vol. 56, 569 (2011). p. 569. (Schmitt 2011 (1))

²⁸ צילום: סוכנות AP

באסטוניה מהווה האינטרנט כלי משמעותי בתחומים רבים, והמדינה אף תוארה כמדינה הפגיעה ביותר להתקפות קיברנטיות.²⁹ חצי מהאוכלוסייה השתמשה בשנת 2007 באינטרנט לקבלת שירותים ממשלתיים; הממשלה פעלה 'ללא נייר'; 95% מהפעילות הבנקאית נהלו באופן דיגיטלי ו-98% משטח המדינה היה מרושת קיברנטית.³⁰ בהתאם, להתקפות היו השלכות משמעותיות: יכולת הפעולה האפקטיבית של שני הבנקים המרכזיים במדינה שותקה למספר ימים, חצי מסוכנויות החדשות המרכזיות נתקלו בקשיים³¹, נפגעה גביית המסים, נותקו קווי החירום במדינה למשך שעה, ניזוקה התקשורת הפרטית והציבורית, ולא פחות חשוב - נפגע האמון בכלכלת המדינה. הנזק הכלכלי של התקיפות נאמד בין 27.5 ל-40 מיליון דולרים.

בהתקפות נגד אסטוניה נוצלו כמיליון מחשבים. חלקם הקטן בשימוש ישיר ורובם כ'זומבים', לאחר שהוחדרה בהם תוכנה זדונית. התקפות רבות בוצעו מרוסיה, אך העקבות הובילו ל-177 מדינות לפחות.³² רוב ההתקפות בוצעו ממחשבים בעלי כתובת (IP) פרטית, אך אותרו גם מחשבים בשליטת מוסדות ממשלתיים רוסיים.

החדש לביצוע ההתקפות נפל, מטבע התפתחות האירועים, על רוסיה. יש הטוענים כי רוסיה הפעילה לשם כך ארגוני חסות. עם זאת, לא הוצגו הוכחות חזקות וחד משמעיות שממשלת רוסיה ביצעה את ההתקפות או עמדה מאחוריהן. אסטוניה עצמה קבעה שההתקפות בוצעו על ידי קבוצות פטריוטיות של פצחנים (האקרים) רוסיים, מבלי שייחסה אותן ישירות לממשלת רוסיה.³³ אסטוניה הגיבה בעיקר בפעולות כמו הרחבת פסי התקשורת, ובמאמץ דיפלומטי משותף עם גורמי נאט"ו. חשיבותן של ההתקפות על אסטוניה בהיותן 'קריאת השכמה', המבשרת על העידן החדש. לראשונה, מדינה מצאה עצמה מתמודדת עם התקפה רחבת היקף ומשמעותית, שבוצעה, ככל הנראה, בחסות מדינה אחרת, במרחב הקיברנטי.

ההתקפה על גיאורגיה

בקיץ 2008 פרץ סכסוך בין גיאורגיה לבין רוסיה, לאחר שכוחות גיאורגים חדרו לחבל דרום אוסטיה. מבחינה משפטית, היה זה סכסוך מזוין בינלאומי (International Armed Conflict), כלומר כזה המתקיים בין מדינות וחלים עליו דיני המלחמה. המאבק הפיזי לא היה ממושך והוכרע במהרה לטובת רוסיה. עוד בטרם החלה תנועת כוחות הצבא הרוסי, בוצעו התקפות קיברנטיות רחבות היקף נגד גיאורגיה,³⁴ לרבות תקיפות DDos על אתרי אינטרנט ממשלתיים והשחתת מידע באופן קיברנטי. התקיפות ארכו כחודש ונמשכו גם לאחר שהושגה הפסקת אש בשדה הקרב. גיאורגיה אינה אסטוניה מבחינת משקל המרחב הקיברנטי, ולכן הפגיעה בה הייתה, באופן יחסי, פחות חמורה. עדיין, נפגעו שירותים ממשלתיים, זמינות הבנקים ואמינות המערכות הממוחשבות במדינה.³⁵ מטרת ההתקפות לא היו רק פיזיות, אלא גם (ובעיקר) יצירת לחץ על האוכלוסייה בגיאורגיה.³⁶ גם במקרה זה, לא נמצאו ראיות חד משמעיות, שאפשרו לייחס אחריות להתקפות או מעורבות בהן. הסברה המקובלת היא שרוסיה לכל הפחות עמדה מהצד, שעה שפצחנים (האקרים) רוסיים ביצעו את ההתקפות נגד גיאורגיה.³⁷

²⁹ Li Sheng, "When Does Internet Denial trigger the Right of Armed Self-Defence?", 38(1) *Yale Journal of International Law* (November 15, 2012), p. 200.

³⁰ Tikk, 2010; 17.

על הקדמה הטכנולוגית של אסטוניה יעידו, למשל, העובדה שבה פותחה אפליקציית Skype ונערכו בה בחירות באופן מקוון.

³¹ Katharine C. Hinkle, "Countermeasures in the Cyber Context: One More Thing to Worry About", *Yale Journal of International Law Online*, 37 (2011), p. 13.

Available at:

<http://www.vjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf>

³² Charles Glover, "Kremlin-Backed Group behind Estonian Cyber Blitz", *Fin. Times*, March 11, 2009.

³³ Tikk, 2010; 23.

³⁴ Ibid. pp. 66-90.

³⁵ Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues", *Naval War College International Law Studies* (2011). p. 113. (Schmitt, 2011 (2))

³⁶ Richard M. Crowell, **War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare**, (2012), p. 14.

³⁷ Hathaway, 2012; 838.

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

התקפת Stuxnet באיראן

בשנת 2010 נפגעה התכנית הגרעינית של איראן, כתוצאה מפעולת וירוס, המכונה Stuxnet, במתקן להעשרת אורניום בנתנו. תולעת (Worm) שחדרה למערכות במתקן, גרמה לצנטריפוגות להסתובב במהירות גבוהה מהרצוי, מבלי שמנגנוני השליטה במתקן יאתרו את התקלה, דבר שהוביל לכך שהצנטריפוגות נהרסו³⁸.

פעולה זו מתוארת בכתיבה המשפטית כתקדים משמעותי (יש אף הרואים בה 'שינוי של כללי המשחק'). זהו וירוס המחשבים הידוע הראשון, שגילם יכולת להתקיף באופן ספציפי מערכת תעשייתית³⁹ (מהסוג המכונה - SCADA, Supervisory Control and Data Acquisition) ולגרום לה נזק רב. אם עד אז, התקפות קיברנטיות גרמו לשיתוק מחשבים ולאובדן מידע, לראשונה גרמה התקפה כזו הרס פיזי לרכוש⁴⁰. הדבר חידד את הפוטנציאל של התקפות קיברנטיות כאמצעי של יצירת אפקט הרס ליריב.

גורמים באיראן ובמדינות אחרות ייחסו את ההתקפה לארצות הברית ולישראל⁴¹, אך לא הוצגו ראיות של ממש למעורבות של מדינה כלשהי בפיתוח הווירוס או בהפצתו.

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

התקפות סיניות בארצות הברית

בשנים האחרונות הצטברו סימנים לקיומה של תכנית רחבת היקף, במסגרתה נערכות התקפות קיברנטיות בחסות ממשלת סין⁴². חברות אבטחת מחשבים בארצות הברית שבות ומדווחות כי 'שחקן מדינתי' (הכוונה לסין), מבצע במשך שנים התקפות נגד גופי ממשל וכלכלה רבים בארצות הברית. כך למשל, אחת ההתקפות הידועות, אשר בוצעה כבר בשנת 2005, כונתה "Titan Rain"⁴³.

בחשיפה משמעותית לכאורה, פרסמה בפברואר 2012 חברת האבטחה Mandiant, כי יחידה בצבא סין שמספרה 61398 פרצה את מערכות המחשוב של שלוש חברות ענק אמריקניות לפחות (קוקה קולה, ענקית האבטחה הממוחשבת RSA, וחברת לוקהיד-מרטין - יצרנית מטוסי הקרב הגדולה במערב). בנוסף, בוצעו התקפות סיניות משמעותיות נגד חברות אמריקניות ומערביות אחרות, לרבות כאלו המפעילות תשתיות קריטיות בתחומי האנרגיה והמים⁴⁴.

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

³⁸ Marco Roscini, "Cyber Operations as Nuclear Counterproliferation Measures", *Journal of Conflict and Security Law*, Vol. 19 (2014), p. 137.

³⁹ Hathaway, 2012; 819.

⁴⁰ Banks, 2013; 157-158. Kenneth Geers, "Pandemonium: Nation States, National Security, and the Internet", *The Tallin Papers*, Vol. 1 No. 1 (2014). pp. 5-6.

Available at:

https://www.ccdcoe.org/publications/TP_Vol1No1_Geers.pdf

⁴¹ לדוגמה:

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

⁴² בתוכנית טלוויזיה אף צולמה, בזמן אמת, התקפה קיברנטית (בשיטת DDoS), על ידי צבא סין, נגד אתר של תנועת Falun Gong בארצות הברית:

Ellen Nakashima & Wan William, "China's Denials About Cyberattacks Undermined By Video Clip", *Wash. Post* (Aug. 24, 2011).

⁴³ Crowell, 2012; 16.

⁴⁴ להרחבה:

<http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&r=0>

ג. מבט להמשך - האטרקטיביות של התקפות קיברנטיות

התקפות במרחב הקיברנטי מאתגרות את כללי המשחק הקיימים והתפיסות המקובלות. במובן זה, הן מזכירות סוג אחר של התקפות, אשר מצאו את הקהילה הבינלאומית בלתי מוכנה - הטרור העולמי, בעיקר מאז שנת 2001. באופן לא מפתיע, ארגוני טרור מוצאים במרחב הקיברנטי כר פורה לפעילות, בין נגד גופים ממשלתיים ובין נגד גורמים מהמגזר הפרטי.⁴⁵

למרבה הצער, דרך הטרור אומצה כדרך פעולה מועדפת על ידי קבוצות ופרטים רבים, והשפעתה על הזירה האזורית והגלובלית רבה. ניסיון לנתח את ההתפתחויות ביחס להתקפות קיברנטיות, מוביל למסקנה כי גם הן נתפסות וצפויות להמשיך ולהיתפס בקרב מדינות, ארגונים ופרטים כאטרקטיביות. בהתאם, היקפן ועוצמתן עלולים לצמוח.

טעמים רבים עומדים בבסיס המשיכה אל התקפות קיברנטיות כדרך פעולה.⁴⁶ להלן יוצגו, על רגל אחת בלבד, חלק מאותם טעמים.⁴⁷

ראשית, יכולת ההסתרה של פעולות קיברנטיות. שחקן מתוחכם יכול להסתיר את זהות מבצע ההתקפה ומקורה הגיאוגרפי, ולעיתים אף את עיתויה, אמצעיה והשפעותיה. פעולות קיברנטיות ניתנות גם לביצוע באופן מקוטע, כמארג של פעולות נפרדות, כך שתיתפסנה כאירועים מבודדים, מבלי שניתן להתחקות אחר 'התמונה הגדולה'.⁴⁸

בנוסף, ניתן להפעיל גורמים פרטיים בעלי ידע לביצוע ההתקפות, בין אם גורמים עבריינים הפועלים בתשלום ובין אזרחים הפועלים מתוך רגש פטריוטי.⁴⁹ הדבר מסייע למסך את מעורבות הגורם היוזם. לעיתים, פעולות שנתפסות כוונדליזם או פיראטיות במרחב הקיברנטי, הן בעצם יוזמה מדינית.

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'.⁵⁰

שנית, עלותה של הטכנולוגיה הנדרשת לביצוע התקפה היא נמוכה (באופן יחסי), זמינותה גבוהה ואין היא מחייבת כוח אדם בהיקף רחב. זאת ועוד, התקפות קיברנטיות אינן מוגבלות בשיקולי זמן ומרחק או בגבולות מדיניים פיזיים. מבחינה טכנולוגית, באופן בו המרחב הקיברנטי התפתח, ההתקפה במרחב תהיה ככל הנראה תמיד חזקה מההגנה, והגנה מושלמת אינה קיימת.⁵¹

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

רביעית, התקפות קיברנטיות עשויות לאפשר פגיעה בהתפתחות התעשייתית, הטכנולוגית, הכלכלית והחברתית של היריב. אלו תחומים שפגיעה קונבנציונלית או קינטית בהם מצויה מחוץ למשחק. ליכולת, למשל, להשיג באמצעים קיברנטיים את הפיתוחים הטכנולוגיים העדכניים ביותר של היריב, עשויים להיות יתרונות כלכליים וצבאיים, שלא ניתן להפיק בדרך אחרת וקשה להפריז בחשיבותם.⁵²

הנקודה האחרונה לא נעלמה מעינם של קובעי המדיניות ומנסחי התפיסות במדינה כמו סין (שם גם נעשה שימוש במינוח מתחום הביטחון הלאומי: סין כ- "Cyber Power"). בראייה הסינית, הפעילות הצבאית היא חלק מתחרות אסטרטגית רב תחומית, המתקיימת בממדים כמו לוחמת מידע, מסחר,

⁴⁵ Banks, 2013; 159.

⁴⁶ Watts, 2011; 72.

⁴⁷ ראו גם: יצחק בן-ישראל וליאור טבנסקי, "מבט בינתחומי על אתגרי הביטחון בעידן המידע", צבא ואסטרטגיה, 3(3), 2011, עמ' 19.

⁴⁸ Antoine Lemay, Fernandez José M. & Knight Scott, "Pinprick Attacks, a Lesser Included Case?", in: Czosseck Christian & Podins Karlis eds., **Conference on Cyber Conflict, Proceedings**, 183 (2010). p. 191.

⁴⁹ Rain Ottis, "From Pitchforks to Laptops: Volunteers in Cyber Conflicts," in: Czosseck & Podins, 2010; 97.

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

⁵⁰ הגורם התוקף מנסה לא אחת לפעול מתחת ל'סף התגובה' של מדינות, ולייצר לעצמו מעין 'חסינות קיברנטית' מפני תגובה.

Watts, 2011; 72-75.

⁵¹ John N.T. Shanahan, "Achieving Accountability in Cyberspace - Revolution or Evolution", 73 *Joint Forces Quarterly* 20 (2nd Quarter 2014). p. 25.

וגם: בן-ישראל וטבנסקי, 2011.

⁵² Lemay, 2010; 190.

⁵³ Li Zhang, "A Chinese Perspective on Cyber War", *International Review of the Red Cross*, Vol. 94, (2012).

מטבע ומדיה⁵⁴. מדינות המבקשות להיאבק בממדים אלו ביריביהן, בעצימות נמוכה ומבלי לחצות את הסף שיוביל לתגובה צבאית, ימצאו במרחב הקיברנטי מגרש מהמעלה הראשונה לקידום מטרותיהן⁵⁵. חמישית, כשם שהמשטר המשפטי בתחום ההתמודדות עם טרור טרם הבשיל לכדי הסדרה מלאה, כך טרם הוסדר הפן המשפטי של המרחב הקיברנטי. היעדר משטר משפטי בינלאומי אפקטיבי וחוסר מורא מענישה, מעודדים בחירה באמצעי של התקפות קיברנטיות ואת אי-היציבות העלול להיגרם מכך. המשך המאמר יעסוק בכינון המשטר המשפטי ואתגריו.

ד. עיצוב כללי המשחק

בשנים האחרונות הלכה והתחדדה תשומת הלב של מדינות למרחב הקיברנטי, תוך הפנמת חשיבותו הגדולה של המרחב וחיוניותו לביטחון, לכלכלה ולחברה. זהו תהליך הדרגתי, המונע על ידי מספר גורמים, כמו הבנת משקל המרחב על חיי היום יום והאינטרסים הכלכליים הטמונים בו; הרצון של ממשלות מסוימות להגביר את הפיקוח על מידע 'מערער יציבות' ברשת האינטרנט; ההתקפות הקיברנטיות שכבר התרחשו ב'זירת הלחימה' החדשה והחשש מהתקפות עתידיות וחמורות יותר. השנים הקרובות צפויות להיות תקופה מכוננת ורבת חשיבות בעיצוב המשטר העתידי שיחול במרחב הקיברנטי. קצרה היריעה מלספק, במסגרת זו, ניתוח עמוק של ההקשר האסטרטגי הרחב והגורמים המעצבים והמשפיעים. עם זאת, דומה שראוי להצביע על מספר מהלכים המצויים בעיצומם: במישור המדינתי - גיבוש מדיניות בהקשר הקיברנטי; השיח באו"ם בתחום בקרת הנשק הקיברנטי; והחתימה ליצירת כללי משחק משפטיים.

גיבוש מדיניות קיברנטית

אשר למישור המדינתי, בהכללה, ההתפתחות המהירה של המרחב הקיברנטי תפסה את מדינות העולם בלתי מוכנות להתמודד עם אתגרי השעה. מדינות רבות, בעיקר במערב, נדרשו לפתח, תוך זמן קצר, מדיניות חוץ וביטחון בהקשר הקיברנטי; לנסח דוקטרינה; להקים גופי מטה ומבנים ארגוניים; להקצות משאבים; ואף לגבש מדיניות משפטית⁵⁶ 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"⁵⁷. הממשל האמריקני מודע היטב לכך שההישענות על טכנולוגיה מודרנית ועל המרחב הקיברנטי, עלול להיות עקב אכילס של ארצות הברית⁵⁸. בהתאם, זוהה הצורך בריסון השימוש ברשת, שיסכן את העליונות הכלכלית והצבאית האמריקנית. נשיא ארצות הברית עצמו התייחס לכך ביולי 2012:

"It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill. This is the future we have to avoid"⁵⁹.

⁵⁴ ספר משמעותי שנכתב בסין בנושא ופורסם כבר בשלהי המאה הקודמת:

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

⁵⁵ Watts, 2011; 74.

⁵⁶ 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

⁵⁷ The White House, National Security Strategy 27 (2010)

www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

⁵⁸ Andrew F. Krepinevich, **7 Deadly Scenarios: A military Futurist Explores War in the 21st Century** (2009). p. 194.

⁵⁹ ראו:

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

ציטוט נוסף מלמד על האינטרס האמריקני:

"Having some effective limits on what nations actually do with their cyber war knowledge might, given our asymmetrical vulnerabilities, be in the U.S. national interest"⁶⁰.

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 וחלל⁶¹. 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 הקיברנטי⁶².

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' שלה⁶³.

בדומה לארצות הברית, הנושא זוכה לעיסוק נרחב גם בבריטניה, בארגון נאט"ו, ואף במדינות שאינן מערביות כמו סין ורוסיה⁶⁴. רוסיה, למשל, פרסמה בשנת 2011, באופן חריג, מסמך תפיסתי, המנחה את הכוחות המזוינים של המדינה ביחס לפעילות במרחב המידע⁶⁵.

הפעילות באו"ם

צמיחת המרחב הקיברנטי, ההתקפות שבוצעו, הסיכונים הכרוכים בכך והתפתחותו של מעין מרוץ חימוש קיברנטי - כל אלו צפויים היו להוביל לדיונים בעלי אופי משפטי באו"ם⁶⁶. כך קרה בפועל, תחילה באופן מהוסס ובשנים האחרונות היקף הדיונים הולך וצובר תאוצה.

בהכללה, הדיונים באו"ם מתקיימים בשני הקשרים מרכזיים: הפוליטי-צבאי, בו דנים בלוחמה קיברנטית, לעיתים תחת הכותרת של בקרת נשק (בעיקר במסגרת הוועידה הראשונה של האו"ם); וההקשר הכלכלי, בו דנים בעיקר בפשיעה במרחב הקיברנטי⁶⁷. בהקשר הפוליטי-צבאי, לב הדיון הוא בשאלות, כיצד טכנולוגיות וכלים במרחב הקיברנטי, עלולים לשמש למטרות שאינן מתיישבות עם שמירת היציבות והביטחון הבינלאומיים ולסכן את הביטחון של מדינות, וכיצד הקהילה הבינלאומית נדרשת להגיב לכך. זירת האו"ם היא מיקרוקוסמוס, ממנה ניתן ללמוד על מרוץ החימוש שמתרחש במרחב הקיברנטי, ועל האינטרסים השונים במסגרתו. באופן אירוני, רוסיה היא שמובילה קריאה בינלאומית לבקרת נשק במרחב הקיברנטי, ואילו ארצות הברית נתפסת לעיתים כמי שחוסמת מהלך כזה⁶⁸. מבלי להרחיב, בשלב זה מוקדם להעריך את כיווני ההתפתחויות של היוזמות המקודמות במסגרת האו"ם והאם תבשלה למשטר מחייב בהובלת הארגון.

כינון המשטר המשפטי

⁶⁰ Richard D. Clarke, שהיה אחראי לתיאום ביטחון קיברנטי בבית הלבן עד שנת 2003, כפי שצוטט ב:

Maurer, 2011; 5.

⁶¹ Department of Defense, Strategy for Operating in Cyberspace (2011).

⁶² להרחבה ראו דברים שפרסם משרד ההגנה האמריקני בעת הקמת הפיקוד החדש:

<http://www.defense.gov/news/newsarticle.aspx?id=59295>

⁶³ Maurer, 2011; 5.

⁶⁴ להרחבה:

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

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

⁶⁵ 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

⁶⁶ Waxman, 2011; 425. המחבר מציע ללמוד מלקחי ההיסטוריה ומהדיונים שנערכו בעבר בסוגיות דומות באו"ם, ובפרט מהדיונים בנושא משמעות 'שימוש בכוח' בתקופת המלחמה הקרה.

⁶⁷ Maurer, 2011; 6. המחבר מרחיב אודות זירות הדיונים באו"ם והזיקה בין הדיונים להתפתחויות הגלובליות.

⁶⁸ Clarke & Knake, 2010; 219-218. יש לציין שהיחסים בין המעצמות אינם רק מנוגדים ויש גם סימנים לשיתופי פעולה, לדוגמה פורסם דבר קיומו של "קו חם" בין ארה"ב לבין רוסיה בהקשרים קיברנטיים, ראו: Geers, 2014; 13.

בעת הזו מצוי המשטר המשפטי הבינלאומי, שיסדיר את המרחב הקיברנטי, בשלבי התהוות ראשוניים (Norm Emergence, במונחי אחד המודלים, המתאר התפתחות נורמות ביחסים בינלאומיים⁶⁹). זהו שלב של עיצוב כללי משחק משפטיים, בו גורמים שונים מנסים לזום הצעות למשטר עתידי ולשכנע כמה שיותר מדינות וארגונים בינלאומיים לאמץ את הצעותיהם, בדרכים שונות. חלק מהיוזמות ממוקד בניסיון לפתח משטר משפטי, המכונה Soft Law, כלומר כזה שאינו מחייב ואינו ניתן לאכיפה. זהו משטר הכולל נורמות ועקרונות לא מחייבים, שמטרתו הסמויה, ולעתים המופגנת, היא להשפיע על הפרקטיקה של מדינות⁷⁰. מסלול משפטי זה, המשולב בדיפלומטיה ציבורית ובשיח אקדמאי, מבקש לעצב גרסאות 'רכות' יותר של המשטר המשפטי העתידי, במטרה לעודד התקדמות בעיסוק המשפטי, כשלב מוקדם בתהליך רב שלבי⁷¹.

תהליך משמעותי ברוח זו היה ניסוח מדריך טאלין (להלן גם - המדריך)⁷². המדריך נוסח על ידי קבוצת מומחים, בהובלת פרופ' מייקל שמיט מארצות הברית. התהליך שהביא לניסוח המדריך קודם על ידי גוף הפועל בחסות נאט"ו, שעניינו שיתוף פעולה בהגנה במרחב הקיברנטי - NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). זהו גוף צבאי בינלאומי, שמקום מושבו בטאלין, אסטוניה. לפני מספר שנים, הוזמנה על ידו קבוצת מומחים בינלאומית לשם הפקת מדריך בנושא הדין החל על לוחמה קיברנטית⁷³. עם קבוצת המומחים נמנו משפטנים בעלי ניסיון פרקטי רב, אקדמאים ומומחים טכניים⁷⁴. התהליך שהחל בשנת 2009, הבשיל בקיץ 2012, אז הושלם המדריך ופורסם, תחילה באופן מקוון, ובמארס 2013 גם בדפוס⁷⁵.

⁶⁹ מודל שפותח על ידי Finnemore & Sikkink, לא יורחב לגביו במסגרת זו.
⁷⁰ להרחבה:

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

⁷¹ Maurer, 2011; 14.

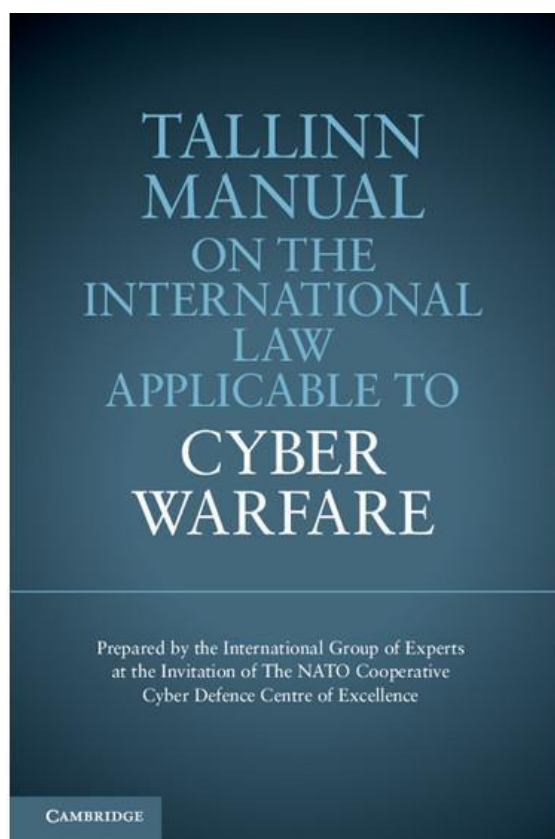
⁷² Tallinn Manual on The International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.

(להלן: "מדריך טאלין" או "המדריך").

⁷³ 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.

⁷⁴ לא היה ישראלי בקרב המומחים.

⁷⁵ הכללים המופיעים במדריך נוסחו על בסיס של קונצנזוס בקרב המומחים, ככאלו שמבטאים לדעתם את המשפט הבינלאומי הקיים. השאיפה להגיע להסכמה על דעת כל המומחים, כרוכה לעתים בפשרה וביצירת מכנה משותף רחב. מנסחי המדריך אינם מציעים, למשל, פרדיגמה חדשה להסדרה המשפטית של המרחב הקיברנטי, כגון אמנה חדשה או החלה סלקטיבית של כללים קיימים, אלא מבקשים, בהכללה, לספק מענה לאתגרי המרחב באמצעות פרשנות לכללי המשפט הקיימים.



תמונה 2: מדריך טאלין

ד. המרחב הקיברנטי והמשפט הבינלאומי - ביחד או לחוד?

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

המענה לשאלה זו אינו חד משמעי. הדבר נובע, בראש ובראשונה, מכך שאותן אמנות בינלאומיות, המהוות את עמוד השדרה של כללי המשפט הבינלאומי, נוסחו בעידן שבו המרחב הקיברנטי היה בגדר מדע עתידי, ואינן מתייחסות כמובן ישירות למרחב זה. יתר על כן, לא קיימת פרקטיקה של מדינות, ממנה ניתן לגזור את הכללים שמנחים אותן בפועל בהתמודדות המשפטית עם המרחב⁷⁶.

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

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

אם בכל זאת נבקש להתחקות אחר עמדות בשאלת היסוד האמורה, נראה כי העמדה הסינית מכירה בצורך להחיל כללים בינלאומיים במרחב הקיברנטי, לרבות כללים המיועדים למנוע מיליטריזציה של המרחב, לעודד פתרון סכסוכים בדרכי שלום ולאסור שימוש בכוח⁷⁷. סין מדגישה את היותה קורבן

⁷⁶ מדריך טאלין, 5.

⁷⁷ להרחבה: Zhang, 2012.

להתקפות במרחב הקיברנטי, בפרט מצד ארה"ב, יפן וקוריאה הדרומית⁷⁸, ומגנה את ניסיונות המערב למנוע ממנה פיתוח יכולות קיברנטיות.

אשר לגישה הרוסית, זו מכירה בכללי המשפט הבינלאומי הקיימים כנקודת מוצא לדיון במרחב הקיברנטי, אך מציגה להם פרשנות החורגת מפרשנותם המקובלת במערב, לצד דרישה להכללת עקרונות משפטיים נוספים⁷⁹.

סין ורוסיה ממוקדות בקידום אסטרטגיה שתיצור מרחב, המתאים יותר לאינטרסים שלהן. בראייתן, השליטה הדומיננטית של המערב במידע היא חלק מאסטרטגיה גדולה יותר של הגמוניה, האינטרנט בסגנונו המערבי מהווה איום על המשטרים שלהן, והמידע הוא נשק שחובה לפקח עליו⁸⁰.

אשר לעמדות במערב, ניתן להצביע על קשת של דעות, החל מכאלה המצדדות בהחלה מלאה של כללי המשפט הבינלאומי במרחב הקיברנטי; דרך דעות לפיהן ההחלה מחייבת שינויי פרשנות ותפיסה; וכלה בדעה החולקת על תחולת הדין הקיים ביחס לפעולות קיברנטיות⁸¹.

העמדה הדומיננטית בקרב גורמים רשמיים בממשלת ארצות הברית, כמו גם בקרב כותבים מובילים במדינה, היא שיש ליישם את כללי המשפט הבינלאומי גם על המרחב הקיברנטי⁸². עמדה זו באה לידי ביטוי במסמך האסטרטגיה הבינלאומית למרחב הקיברנטי, שפורסם בשנת 2011. שם נכתב:

"[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behaviour - in times of peace and conflict - also apply in cyberspace"⁸³.

דברים דומים נאמרו בנאום חשוב שנשא היועץ המשפטי של מחלקת המדינה בארצות הברית (להלן - נאום Koh) בספטמבר 2012.⁸⁴

לצד הקביעה העקרונית, המקובלת בארצות הברית ובמדינות מערביות, כי יש להחיל את כללי המשפט הבינלאומי במרחב הקיברנטי, קיים מגוון של דעות בעניין מידת ההתאמה של הכללים למרחב הקיברנטי והקלות בה ניתן ליישם. במסמך האסטרטגיה שהוזכר לעיל, נכתב כי נדרשת עבודה משפטית, במטרה לקבוע כיצד בדיוק הכללים חלים ומה נדרש כדי להשלים אותם. הכותבים מדגישים, כי ישנה אי בהירות ביחס לאופן בו ראוי ליישם את כללי המשפט הבינלאומי ביחס להתקפות בתחום הקיברנטי⁸⁵, וכי נדרשת בחינה משמעותית של כללי המשפט הבינלאומי לאור ההתפתחויות הקשורות לפריחת המרחב הקיברנטי⁸⁶.

⁷⁸ הסינים מוטרדים ממלחמה נגדם במרחב הקיברנטי. לטענתם, נכון לשנת 2012, מבוצעות נגדם כ- 80,000 תקיפות בחודש. ראה: Zhang, 2012; 805.

⁷⁹ הדבר עולה למשל מטיטת אמנה בנושא ביטחון מידע בינלאומי, מספטמבר 2011, שהציג מזכיר המועצה הרוסית לביטחון לאומי, ניקולאי פטרושב. בסעיף 7 לטיטה, נכתב שבמהלך מלחמות מידע יש לציית לדין ההומניטרי הבינלאומי.

http://www.conflictstudies.org.uk/files/20120426_CSRC_IISI_Commentary.pdf

⁸⁰ לואיס ג'יימס א', "להגנת וירוס הסטקסנט", צבא ואסטרטגיה, 4 (3), 2012, עמ' 57.

⁸¹ מדריך טאלין, 3. במדריך מצוטטת, בין השאר, עמדת ארגון הצלב האדום הבינלאומי, לפיה הדינים חלים במרחב הקיברנטי. לדעה מעניינת, לפיה המשפט הבינלאומי צריך להתפתח כדי להסדיר את התחום הקיברנטי, ואף לעודד פעילות התקפית קיברנטית כתחליף למלחמה קונבנציונלית, ראו:

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

⁸² מדריך טאלין, 5. ראו גם הוגה אסטרטגי חשוב: Charles Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly* (Spring 2011).

⁸³ למסמך המלא:

The White House, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World 9 (2011).

Available at:

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

⁸⁴ Harold Koh Honhgu, "Legal Advisor of the Dep't of State, International Law in Cyberspace Address to the USCYBERCOM Inter-Agency Legal Conference," (Sept. 18, 2012)

Available at:

<http://www.state.gov/s/l/releases/remarks/197924.htm>

⁸⁵ לדוגמה:

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

⁸⁶ לדוגמה:

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

ה. האתגר בהחלת כללי המשפט הבינלאומי במרחב הקיברנטי

גם המאמינים ההדוקים ביותר בתחולתם הרחבה של כללי המשפט הבינלאומי, יסכימו לקביעה שהחלתם ויישומם במרחב הקיברנטי מאתגרים, בלשון המעטה⁸⁷. המרחב הקיברנטי חותר תחת פרדיגמות מסורתיות של המשפט הבינלאומי. מספיק לאזכר חלק מהמאפיינים של כללי המשפט הבינלאומי והאופן בו התפתחו, כדי לעמוד על המורכבות של החלתם במרחב הקיברנטי.

כך למשל, המשפט הבינלאומי התפתח כאמצעי להסדרת יחסים בין מדינות, להן גבולות, טריטוריה וריבונות. במרחב הקיברנטי, לעומת זאת, פועלים שחקנים משמעותיים שאינם מדינות, בהם גופי ענק כלכליים כמו גוגל (Google), פייסבוק (Facebook) ואחרים, ארגונים כמו הקבוצה המכונה אנונימוס (Anonymous) ולהבדיל - ארגוני טרור, פצחנים (Hackers), גופים לא רשמיים המופעלים על ידי מדינות ועוד. יתר על כן, קשה להתייחס לפעילות קיברנטית במונחים כמו 'טריטוריה' 'הפרת ריבונות', 'כבוד לגבולות גיאוגרפיים', 'פעילות מדינתית' וכו'⁸⁸. מונחים מרכזיים אלו מתחום המשפט הבינלאומי, כמעט זרים למרחב הקיברנטי, הפתוח והגלובלי.

אחת ההתפתחויות החשובות במשפט הבינלאומי בעשורים האחרונים היא הטלת אחריות על מדינות ועל פרטים, למשל במקרה של ביצוע פשעי מלחמה. הטלת אחריות במישור המשפטי מחייבת זיהוי של המדינה או הגורם שביצע את הפעולה וייחוס הפעולה לו, בהתבסס על ראיות. המרחב הקיברנטי, כפי שכבר הודגש, לא תוכנן על מנת לאפשר זיהוי של הפועלים בו. שחקנים מתוחכמים לא יותירו עקבות למעשיהם, ימנעו ייחוס (Attribution) של התקיפות אליהם⁸⁹ ואף יוכלו 'להפליל' גורמים תמימים. תקיפות הדגל במרחב הקיברנטי לוו אמנם בשלל ספקולציות ביחס לגורמים האחראים, אך ההשערות הללו לא נתמכו בראיות והוכחות של ממש, ולא בכדי.

כללי המשפט הבינלאומי, המסדירים לחימה, מבוססים על מספר עקרונות, בהם עקרון האבחנה (Distinction). העיקרון מחייב, בין היתר, להבחין בעת תקיפה בין לוחמים ומטרות צבאיות של האויב לבין אזרחים ורכוש אזרחי, תוך הימנעות מפגיעה באחרונים. עמידה בדרישת האבחנה מאתגרת בלחימה המודרנית בכלל, ועלולה להיות קשה ליישום פי כמה וכמה במרחב הקיברנטי.

במרחב הקיברנטי שורר טשטוש כמעט מוחלט בין 'אזרחים' לבין 'לוחמים' ('הלוחמים' עשויים להיות אזרחים, בלבוש אזרחי ובמשרד אזרחי, שנשקם מקלדת ומחשב)⁹⁰. קיימת מזיגה כמעט מלאה של תשתיות אזרחיות ותשתיות צבאיות, ללא הפרדה של ממש בין רשתות, מתקנים ומוסדות צבאיים לבין אלו האזרחיים⁹¹. מונחים כמו 'לוחם', 'מטרה צבאית', 'פרופורציונאליות' ו-'נזק אגבי', מחייבים, לכל הפחות, מחשבה חדשה ויצירתית בהקשר הקיברנטי.

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

המרחב הקיברנטי מאיים לשבור (ואולי כבר שובר) את האבחנות המשפטיות המסורתיות, אינו מיישר קו עם הרציונל שבבסיס הכללים המקובלים, וחותר תחת דרך המחשבה המשפטית (והצבאית) האופיינית⁹².

⁸⁷ Hathaway, 2012; 840.

⁸⁸ Luciano Floridi, "The Ethics of Cyber-Conflicts in Hyperhistorical Societies", in: Ludovica Glorioso & Anna-Maria Osula eds., **1st Workshop on Ethics of Cyber Conflict 3**, (2014). p. 4.

⁸⁹ Larry Greenemeier, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers", *SCI. AM.*, June 11, 2011.

Available at:

<http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers>.

בתקיפות DDoS ניתן לעיתים להציג ראיות נסיבתיות לעניין הגורם האחראי, אך לא בטוח שהדבר מספק, להרחבה:

Sheng, 2012; 202-203.

⁹⁰ להרחבה בדבר טשטוש מעמד הלוחמים במרחב הקיברנטי:

Maurizio D'urso, "The Cyber-Combatant: A New Status for a New Warrior", in: Glorioso & Osula, 2014.

⁹¹ מת'יו קרוסטון, "דילמת דוקו": הנחת העמימות והשאיפה חסרת התוחלת למלחמת סייבר סטרטגית, צבא ואסטרטגיה, (1)5, 2013, עמ' 99.

המחבר מדגים את חוסר היכולת להבחין בין צבאי לבין אזרחי תוך ניתוח וירוס DuQu. לגישתו אין במרחב הקיברנטי תשתית אזרחית 'טהורה'.

⁹² ואכן יש הכופרים באפשרות לגבש משטר משפטי ראוי למרחב הקיברנטי, ושמים את יהבם על אסטרטגיה של הרתעה, כמו: קרוסטון, 2013.

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

בשעה שיש למשל מעט מדינות, אם בכלל, המסוגלות לאיים (באופן ריאלי) בתקיפה קינטית משמעותית על מדינות המערב, הרי שעם ההתפתחות הטכנולוגית, מדינות, ארגונים וגופים רבים הם תוקף פוטנציאלי (או הלכה למעשה) של מדינות המערב. במרחב הקיברנטי גם לשחקנים 'קטנים' יכולת להשפיע באופן משמעותי, הרבה מעבר לגודלם היחסי⁹³, על הביטחון הלאומי של מדינות אחרות. זאת ועוד, מדינות המערב היו בעבר המעצמות הדומיננטיות שהובילו את עיצוב כללי המשפט הבינלאומי. הסדרה משפטית עתידית של המרחב הקיברנטי אינה צפויה להיות פריבילגיה של המערב. יתר השחקנים לא יהיו חותמת גומי ושותפים סבילים. סין ורוסיה הן מעצמות קיברנטיות ובעלות אינטרסים ומשקל בכל תהליך של הסדרה עתידית. ניתן להניח כי גם למדינות אחרות הפעילות במרחב (הודו ואיראן למשל) תהיה השפעה בתחום זה.

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

1. הזכות להשתמש בכוח כהגנה עצמית כתגובה ל'התקפה מזוינת'

אחד העקרונות החשובים במשפט הבינלאומי הוא איסור השימוש בכוח. האיסור מעוגן בסעיף 2(4) למגילת האו"ם, ונחשב, כפי שקבע בית הדין הבינלאומי בהאג, אחד מאדני היסוד של המגילה⁹⁴. הסעיף קובע, בתרגום חופשי: "כל חברי האו"ם יימנעו ביחסיהם הבינלאומיים מאיום או משימוש בכוח נגד שלמותה הטריטוריאלית או עצמאותה המדינית של מדינה כלשהי, או בכל דרך אחרת שאינה מתיישבת עם מטרות האו"ם".

אם נעשה שימוש בכוח נגד מדינה מסוימת, עלולות להיות לכך השלכות מרחיקות לכת. כאשר השימוש בכוח חמור מספיק, ונחשב בגדר 'התקפה מזוינת' (Armed Attack), קמה למדינה המותקפת זכות לעשות שימוש נגדי בכוח, כהגנה עצמית⁹⁵. מכאן, המרחק למלחמה עלול להיות קצר וכואב.

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

בית הדין הבינלאומי בהאג כבר פסק ביחס לאיסור השימוש בכוח, כי זה חל על כל שימוש בכוח, בלי קשר לשאלה באיזה נשק נעשה שימוש. היועץ המשפטי של מחלקת המדינה האמריקנית הצהיר, כי ארצות הברית תממש את זכותה להגנה עצמית, גם במקרה שתותקף באמצעים קיברנטיים, אם הפעילות נגדה תגיע לכדי 'התקפה מזוינת'⁹⁶.

אם כך, השאלה המתבקשת - אילו פעולות קיברנטיות עלולות להוות 'התקפה מזוינת'? העמדה הדומיננטית במערב היא שהתקפה קיברנטית תהיה 'התקפה מזוינת' כשהיו לה מאפיינים ותוצאות, המזכירים 'התקפה מזוינת' קינטית⁹⁷, כלומר גרימת מוות או פגיעה של אנשים או פגיעה ברכוש.

גישה זו אומצה למשל במדריך טאלין, ובאה לביטוי במסגרתו בכלל מספר 13. בקרב מחברי המדריך היה קונצנזוס, כי פעולות קיברנטיות עלולות להיות כה חמורות, עד שיוצדק להגדירן כ'התקפה מזוינת'.

⁹³ צ'ילופ, קרדאש וסלמואירגי, 2012.

⁹⁴ Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v. Uganda) 2005 I.C.J. Rep. 168, 223.

⁹⁵ בהתאם לסעיף 51 למגילת האו"ם, מוקנית זכות להגנה עצמית, אינדיבידואלית או קולקטיבית, למדינה כאשר בוצעה נגדה 'התקפה מזוינת' (Armed attack). זאת כל עוד לא נקטה מועצת הביטחון אמצעים החיוניים לשמירת השלום והביטחון הבינלאומיים. זו אחת מזכויות היסוד החשובות במשפט הבינלאומי.

⁹⁶ נאום 4, Koh.

⁹⁷ Sheng, 2012; 188.

הם הוסיפו, כי לא כל שימוש בכוח יהווה 'התקפה מזוינת'. נדרשים היקף וחומרה מסוימים ('Scale and Effects'), על מנת ש'שימוש בכוח' יגיע לכדי 'התקפה מזוינת'⁹⁸.

הגישה הרשמית האמריקנית הוצגה בספטמבר 2012 על ידי היועץ המשפטי של מחלקת המדינה (נאום Koh). לפי עמדה זו, התוצאות הפיזיות של הפעולה הקיברנטית הן המפתח להגדרתה: אם התוצאות הן מוות, פגיעה או הרס רכוש משמעותי, התקיפה תיתפס כשימוש בכוח המהווה 'התקפה מזוינת' ומצדיק הגנה עצמית בכוח. כך למשל יהיה, כאשר התוצאות הפיזיות של התקפה קיברנטית תהיינה שקולות לתוצאות של הטלת פצצה או ירי טיל. כדוגמאות לפעולות קיברנטיות מסוג זה, הוצגו תרחישים תיאורטיים של גרימת התכה במתקן גרעיני, פריצה של סכר באזור מיושב או נטרול של בקרת תעופה. האם פגיעה במידע היא פגיעה ברכוש? הפרשנות המקובלת היא שאיסוף מידע קיברנטי, גניבת מידע ואפילו השמדת מידע או שינויו, אינם 'התקפה מזוינת' בפני עצמם⁹⁹.

הגישה האמריקנית והמערבית מבטאות תפיסה מסורתית של עולם המלחמה. לאורך ההיסטוריה, שיבשו מדינות את הסדר העולמי באמצעות פגיעה בבני אדם וגרימת נזק לרכוש. תוצאות פיזיות אלו נתפסו כהרסניות ליציבות העולמית ולביטחון המדינות, ולכן הקהילה הבינלאומית הסכימה לאמץ כללים שימנעו את התרחשותן¹⁰⁰.

האתגר שמעורר המרחב הקיברנטי קשור למצבים בהם נגרמת למדינה, כתוצאה מהתקפה קיברנטית, פגיעה קשה ומשמעותית שאינה מתבטאת בנזק פיזי ישיר לאדם או לרכוש. דמיינו למשל התקפה קיברנטית על הבורסה בניו יורק, שתגרום לפגיעה קשה בזרימת המידע ובאמינותו ולהתרסקות הבורסה. הפגיעה בכלכלה האמריקנית והעולמית תהיה קשה מאוד. לכאורה, נגרם נזק כלכלי גרידא, אין לפעולה מאפיינים של פגיעה פיזית ישירה, ולכן אינה בגדר 'התקפה מזוינת'.

הבעיה, אם כך, היא שבמרחב הקיברנטי ניתן לערער את היציבות של מדינות באמצעות פעולות שאינן קינטיות, באמצעות הקשה על לוח המקשים של מקלדת מחשב או מסך מגע. כלים ויכולות קיברנטיים, שאיש בעבר לא חשב לאסור, עלולים לגרום תוצאות קשות, שייתפסו על ידי מדינות כ-Casus Belli (עילה למלחמה)¹⁰¹.

במילים כלליות יותר, המרחב הקיברנטי מנתק את החפיפה בין המשטר המשפטי הקיים לבין התוצאות שהמשפט מבקש למנוע. המשטר המשפטי הבינלאומי אמור לאפשר למדינות להגן על עצמן ולמנוע תוצאות שנתפסות כחמורות מאד בראייתן¹⁰². בעולם המודרני, המשפט אינו יכול להסתפק באיסור על פגיעה פיזית ותו לא. מדינה שבה האזרחים לא יוכלו לגלוש באינטרנט, האמון במערכת הבנקאית ייפגע, הבורסה תשוקת ושירותי הממשלה הממוחשבים לא יתפקדו, תראה זאת בחומרה רבה. היא תחוש פגיעה שאינה נופלת מזו של התקפה קינטית-צבאית. מדינה שתיפגע כך, תרצה להגיב ותחוש הצדקה מלאה לכך. המשפט יהיה חייב לתת מענה גם לסוג ההתקפות הקיברנטיות הללו¹⁰³. גם אם הדין ימלא פיו מים, הפרקטיקה של מדינות תכתיב כללי משחק חדשים.

הקושי בהשלמה עם המצב המשפטי כבר זכה לביטוי, בעיקר בכתיבה האקדמית. כותבים רבים סבורים שלא האופי הפיזי של תוצאות התקיפה (פגיעה גופנית או הרס רכוש בלבד) צריך להיות המבחן הקובע בהקשר שתואר לעיל. לגישתם, למשל, צריך לבחון בצורה רחבה יותר את היקף האפקט הנגרם מהתקיפה, כך שהתקפה קיברנטית שתוצאותיה הכלכליות קשות, תיחשב 'התקפה מזוינת'¹⁰⁴. בראייה זו, התקפה קיברנטית הגורמת, למשל, שיבושים קשים ברשתות תקשורת וברישומים פיננסיים, מצדיקה שימוש נגדי בכוח כהגנה עצמית.

כך, השוואה מעניינת שעלתה בכתיבה היא בין חסימת גישה למידע דיגיטלי לבין חסימת נתיבי שיט, הנחשבת ככלל אסורה לפי המשפט הבינלאומי¹⁰⁵. לפי הקבלה זו, התלות המודרנית בתשתית דיגיטלית אינה פחותה מהתלות בתשתית פיזית, ויש לאסור על פגיעה בשני סוגי התשתיות.

המורכבות בהחלת הכללים המשפטיים בעניין הזכות להשתמש בכוח בהגנה עצמית כתגובה ל'התקפה מזוינת' במרחב הקיברנטי, היא דוגמה אחת בלבד מני רבות לקושי רחב בהרבה. גם ניסיון להחיל עקרונות משפטיים אחרים במרחב הקיברנטי יוליד פערים וסימני שאלה דומים.

⁹⁸ מונח שלקוח מפסק הדין של בית הדין הבינלאומי בהאג בפרשת ניקרגואה.

⁹⁹ יש הטוענים שאחרת, המשמעות תהיה שכמעט כל הפעולות במרחב הקיברנטי תהיינה 'התקפה מזוינת' - פרשנות בלתי סבירה שתוצאותיה קשות. יש המוסיפים בכל זאת חריג, במקרה בו נפגע מידע, המיועד להיחפץ באופן מיידי לחפצים מוחשיים, כגון מחיקת חשבון בנק ששקול לכסף מזומן. במקרה כזה, הפגיעה במידע עשויה, לפי פרשנותם, להיחשב פגיעה ברכוש. להרחבה: Schmitt, 2011; 589.

¹⁰⁰ Schmitt, 2011 (1); 603.

¹⁰¹ הדברים עלו גם מפי נשיא ארה"ב, שציין שמתקפות קיברנטיות אשר אינן פיזיות, עודן עלולות לגרום משבר פיננסי ומצבי חירום רפואיים:

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

¹⁰² Schmitt, 2012; 287.

¹⁰³ Ibid, pp. 288-289.

¹⁰⁴ מדריך טאלין, 56.

¹⁰⁵ Sheng, 2012.

סיכום

ביטחון המרחב הקיברנטי הוגדר על ידי ארגון האומות המאוחדות ועל ידי מדינות רבות כאחד האתגרים המשמעותיים של המאה הנוכחית. ראש ממשלת ישראל רואה בו את אחד מארבעת האיומים הגדולים ביותר על ישראל¹⁰⁶.

תפיסות אלו התגבשו על רקע ההתקפות שכבר בוצעו ומבוצעות במרחב הקיברנטי, ויותר מכך - על הבנה כי השימוש בהן ילך ויגבר ועל מודעות לפוטנציאל הנזק הטמון בהן. התקפות קיברנטיות הן דרך פעולה אטרקטיבית עבור מדינות, ארגונים ופרטים. הן ניתנות להסתרה בקלות יחסית, זולות, זמינות, קשה להתגונן מפניהן, בכוחן לאיין יתרונות טכנולוגיים וכלכליים של יריבים ולתרום לביטחון הלאומי של התוקף. בנוסף הנורמות המשפטיות ביחס אליהן טרם עוצבו, כך שהתוקף אינו מסתכן בפעילות המצויה 'מחוץ לכללי המשחק'.

השנים הקרובות צפויות להיות תקופה מכוננת בעיצוב המשטר המשפטי העתידי, שיסדיר את המרחב הקיברנטי. כיום, כבר שוררת הסכמה רחבה למדי (הן במערב והן בסין וברוסיה) כי יש להחיל את כללי המשפט הבינלאומי במרחב זה. בד בבד, קיימת תמימות דעים כי החלה זו היא מאתגרת, בלשון המעטה.

מה מקור האתגר? המרחב הקיברנטי חותר תחת פרדיגמות מסורתיות של המשפט הבינלאומי. מונחי המשפט הבינלאומי (כמו גבולות, טריטוריה, מדינות, לוחמים ועוד) כמעט זרים למרחב הקיברנטי; קשה לייחס אחריות משפטית לפעילות קיברנטית; המשפט הבינלאומי נשען על אבחנות דיכוטומיות בין אזרחי לבין צבאי, ואילו המרחב הקיברנטי מאופיין בעמימות טבועה ומכוננת.

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

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

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

הרחבה ביחס לכיווני הפעולה הנדרשים מחייבת חריגה מהיקפו של מאמר זה. ברור כי המשפט הבינלאומי יצטרך להשתנות ולהתפתח כדי לתת מענה למציאות החדשה. אם הדבר לא יקרה, מדינות יחוו מוגבלות על ידי המשפט הקיים ונטולות מענה אפקטיבי לאיומים עליהן¹⁰⁷. שמירה על כללי המשפט הבינלאומי 'המסורתיים' עלולה לעמוד בניגוד לאינטרסים שלהן בתחום הביטחון הלאומי ולעורר דילמות קשות ביחס לדרך הפעולה. ככל שהטכנולוגיה תצמד קדימה וירבו התקפות קיברנטיות, מדינות תידרשנה בתדירות גבוהה לקבל החלטות, האם להגיב באמצעות שימוש בכוח, קיברנטי או פיזי. על המשפט הבינלאומי להמציא עצמו מחדש ביחס למרחב הקיברנטי ולספק כללים שיסייעו בשמירה על היציבות והביטחון. ימים יגידו האם המשפט עמד בהצלחה באתגר זה.

¹⁰⁶ "מי יגן על ישראל ממתקפות מחשב? נתניהו העדיף את מטה הסייבר על פני השב"כ" ("הארץ", 21 בספטמבר 2014). להרחבה:

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

¹⁰⁷ להרחבה: Watts, 2011; 76.