"לוחמה כלכלית רחבה" בעידן הסייבר

שמואל אבן

"לוחמה כלכלית רחבה" היא מכלול פעולות לשם פגיעה, או איום בפגיעה, במשק האויב/היריב במטרה להפעיל עליו לחצים או להחלישו, וזאת כדי להשיג את יעדיו האסטרטגיים של מפעיל הלוחמה. "לוחמה כלכלית רחבה" כוללת בתוכה: לוחמה כלכלית מקובלת (כגון סנקציות), לוחמה קינטית ולוחמת סייבר נגד כלכלת האויב.
עידן הסייבר משַנה את תחום הלוחמה הכלכלית הרחבה. בהיבט ההתקפי, יכולות סייבר מאפשרות לפגוע בכלכלת האויב בעת מלחמה ובין המלחמות. לוחמת סייבר עשויה להעצים את הפגיעה במשק האויב, וזאת בנוסף לסנקציות כלכליות ו/או התקפות קינטיות. בהיבט ההגנתי מדובר בסיכון נוסף לתפקוד המשק. תרחישי קיצון של התקפות סייבר על כלכלות של מדינות אמנם טרם התממשו, אולם למרות זאת יש להתאים כבר כיום את קצב בניית ההגנה על הסייבר המדינתי לקצב התבססותו המואצת של המשק במרחב הסייבר.

מילות מפתח: לוחמה כלכלית רחבה, כלכלה, לוחמה, סייבר, ישראל, איראן

הקדמה

מטרתו של מאמר זה היא להציג את "הלוחמה הכלכלית הרחבה" ולפרט את יישומה במרחב הסייבר. המאמר מחולק לשניים. בחלקו הראשון מוצגת "לוחמה כלכלית רחבה" כשדה משותף לכל פעולות הלוחמה שכלכלת האויב היא היעד שלהן. שדה זה מקיף לוחמה כלכלית מקובלת (כגון סנקציות), לוחמה קינטית ולוחמת סייבר נגד כלכלת האויב, והוא נוגע גם לממד ההגנתי של תחום זה. בחלקו השני מתמקד המאמר בלוחמת סייבר בתור אמצעי במסגרת "לוחמה כלכלית רחבה", תוך הבחנה בין לוחמה "רכה" ללוחמה "קשה". במאמר מובאות דוגמאות לסוגים שונים של כלי לוחמה זה.

ד"ר שמואל אבן הוא חוקר בכיר במכון למחקרי ביטחון לאומי.

רקע

אסטרטגיות לחימה בעלות מאפיינים כלכליים מוכרות עוד מהעת העתיקה. אז היה המצור אחד מכלי המלחמה הנפוצים, והשלל היה חלק מאספקה הכרחית לצבאות המתקדמים ומהתמורה למנצחים. מאז עבר הנושא התאמות, שנבעו מהשינויים במציאות הכלכלית, המדינית והצבאית בעולם. לפי אנציקלופדיה בריטניקה, "לוחמה כלכלית הינה שימוש, או האיום בשימוש, באמצעים כלכליים נגד מדינה, כדי להחליש את כלכלתה, ובכך לפגוע בכוחה המדיני והצבאי".[1] לפי מילון אוקספורד, מדובר ב"אסטרטגיה כלכלית, המבוססת על שימוש באמצעים כגון מצור, או איום בשימוש באמצעים כאלה, שמטרתה הישירה היא להחליש את הכלכלה של מדינה אחרת".[2]

הנטייה המקובלת, לפחות בעשורים האחרונים, היא לראות את הלוחמה הכלכלית ("לוחמה כלכלית מקובלת") כלוחמה המוגבלת לפעולות שאינן מבקשות להפעיל אש נגד משק האויב. כלומר, תקיפה של משק אויב בנשק קינטי כדי לפגוע בכושר הייצור שלו אינה נמנית עם ארגז הכלים של הלוחמה הכלכלית המקובלת. ברם, מצור, שהוא אמצעי צבאי שעלול להוביל לשימוש בנשק קינטי, נכלל בארגז הכלים של הלוחמה הכלכלית המקובלת. מכאן עולה ששימוש בנשק קינטי במסגרת לוחמה כלכלית מקובלת אינו חד־משמעי. הדבר מעורר שאלות גם לגבי סיווגן של התקפות סייבר רבות־עוצמה נגד יעדי המשק של האויב, שהתוצאות הצפויות מהן אינן נופלות בהכרח מעוצמתן של התקפות קינטיות. מדובר, למשל, בהתקפות סייבר רבות־עוצמה על תחנות כוח, מפעלי תעשייה ומערכות תחבורה, שלפגיעה בהם עשוי להיות אפקט קינטי (לרבות פגיעה בנפש והרס). באנלוגיה לתקיפות קינטיות, גם לתקיפות סייבר מסוג זה אין, אפוא, מקום בהגדרות המקובלות של לוחמה כלכלית.

לאור האמור לעיל, נשתמש במושג "לוחמה כלכלית רחבה" כמסגרת לכל סוגי הפעולות שמטרתן היא פגיעה, או איום בפגיעה, במשק האויב/היריב במטרה להחלישו, וזאת כדי להשיג יעדים אסטרטגיים של מפעיל הלוחמה. הבחנה בין "לוחמה כלכלית רחבה" ללוחמה כלכלית מקובלת מוצגת בלוח הבא. יצוין כי ל"לוחמה כלכלית רחבה" יש גם צד הגנתי.

1 George Shambaugh, "Economic Warfare", *Encyclopedia Britannica*, https://www.britannica.com/topic/economic-warfare.

2 *Oxford Dictionaries*, https://en.oxforddictionaries.com/definition/economic_war.

לוח 1: "לוחמה כלכלית רחבה" לעומת לוחמה כלכלית מקובלת

קטגוריה		פעולות אופייניות
לוחמה כלכלית (לפי הגדרה מקובלת)		סנקציות כלכליות למיניהן – הקפאת נכסים בחו"ל, איסורים בתחומי סחר והשקעות, תנאי סחר מפלים לרעה (לא משיקולים כלכליים גרידא), חרם בתחומי כלכלה שונים (Boycott), אמברגו (Embargo) ומצור (Blockade) למניעת סחר של האויב.[3]
"לוחמה כלכלית רחבה"	**לוחמה "רכה"**	סנקציות כלכליות למיניהן – הקפאת נכסים בחו"ל, חרם, איסור על סחר ואמברגו (שאינו כולל פגיעה קינטית בכלי תובלה של האויב). הרעת תנאים ביחסים הכלכליים עם היריב, למשל בתחומי הסחר וההשקעות, וזאת משיקולים אסטרטגיים־מדיניים ולא משיקולים כלכליים גרידא. לוחמת מידע ולוחמת סייבר "רכה". שימוש בכלים לא לגיטימיים לשם השגת יתרון אסטרטגי, כגון גניבת קניין רוחני בהיקף נרחב.
	לוחמה "קשה"	סגר/מצור בכוח צבאי למניעת סחר של האויב, שעלול להיות כרוך בעימות באש. התקפות קינטיות על יעדים במשק האויב התקפות סייבר רבות־עוצמה על תשתיות ומפעלים.

"לוחמה כלכלית רחבה": הגדרה, מאפיינים ומשרות

"לוחמה כלכלית רחבה" ניתנת להגדרה כמכלול פעולות לשם פגיעה, או איום בפגיעה, במשק האויב/יריב[4] במטרה להפעיל עליו לחצים או להחלישו, וזאת כדי להשיג את יעדיו האסטרטגיים של מפעיל הלוחמה.[5] בתוך מכלול זה נמצאות גם פעולות שנועדו להגן מפני מהלכים התקפיים מסוג זה מצד האויב. במילים אחרות, "לוחמה כלכלית רחבה" היא שדה משותף לכל פעולות הלוחמה שכלכלת האויב היא היעד שלהן, כגון: סנקציות, לוחמת מידע, חרם, אמברגו, סגר צבאי, לוחמה

3 *Encyclopedia Britannica.*

4 למשל, נשיא ארצות הברית, דונלד טראמפ, הגדיר את נשיא רוסיה, ולדימיר פוטין, כיריב ולא כאויב, לאחר שארצות הברית הטילה סנקציות על ארצו: "טראמפ טוען לניצחון בנאט"ו: אנגלה, תעשי משהו", *Ynet*, 12 ביולי 2018, https://www.ynet.co.il/articles/0,7340,L-5308872,00.html

5 תכלית הפעולה היא לרוב מדינית־צבאית, כגון לחץ אסטרטגי על האויב כדי שישנה את מדיניותו, או לחץ שנועד להחליש את שלטונו מבית ואת כוחו הצבאי. עם זאת, ייתכנו מצבים שבהם ללוחמה ישנה גם תכלית כלכלית־אסטרטגית, למשל, כאשר מדובר במאבק בין מדינות על נכסים כלכליים, כמו מחלוקת על מים כלכליים שבתחומם נמצאים שדות גז, או כאשר מדינה הנתונה תחת סנקציות פועלת לחלץ כספים (באמצעות התקפות סייבר). ייתכנו גם מצבים שבהם מאבקים בזירה הכלכלית (כמו מלחמות סחר) יסלימו ויתדרדרו למאבקים בעלי אופי מדיני־ביטחוני.

קינטית ולוחמת סייבר נגד משק האויב; וכן פעולות הגנתיות נגד מהלכים כאלה, למשל יכולות תגובה, היערכות מוקדמת לסנקציות, הגנה פסיבית ואקטיבית, הגנת סייבר על המשק ועוד.

לפי ההגדרה דלעיל, "לוחמה כלכלית רחבה" אינה מוגבלת לכלי הלוחמה הכלכלית המקובלת, אלא מוסיפה עליהם תקיפות קינטיות ותקיפות סייבר רבות־עוצמה נגד יעדים במשק האויב. לדוגמה, פעולות נגד מערכת החשמל של האויב עשויות לכלול: הפסקת מכירת חשמל כסנקציה מדינית; סנקציות על ייבוא חלקי חילוף לתחנות כוח; התקפת סייבר או התקפה קינטית שתביא להפסקת חשמל זמנית; התקפת סייבר רבת־עוצמה או התקפה קינטית, שתגרום לנזק בלתי הפיך לטורבינות של תחנות כוח.

"לוחמה כלכלית רחבה" עשויה לבוא בשילוב מלא או חלקי עם אמצעים אחרים, וזאת בהתאם למטרות, לאמצעים ולאסטרטגיה עליהם יוחלט. היא עשויה להיות חלק מלוחמה "רכה", כמו שילוב של סנקציות כלכליות עם התקפות סייבר על המשק במטרה להפעיל לחץ אסטרטגי כבד על האויב ללא שימוש באש. היא גם עשויה להיות חלק מלוחמה "קשה", שתכלול התקפות קינטיות והתקפות סייבר רבות־עוצמה נגד יעדים במשק האויב.

מטרותיה של "לוחמה כלכלית רחבה" הן:

- להפעיל על אויב/יריב לחצים כלכליים אסטרטגיים כדי שישנה את התנהגותו בכיוון הרצוי למפעילי הלוחמה.
- להקשות על אספקת משאבים להתעצמותו הצבאית של האויב במטרה להחליש את כוחו ("בניין כוח"); לפגוע במשאבים, בתשתיות ובנכסים כלכליים של האויב כדי לפגוע בפעילותו הצבאית ("הפעלת כוח").
- לערער את מעמדו ויציבותו של שלטון האויב, להפעיל עליו לחצים ולהביא לשינוי בסדר העדיפויות שלו ובמדיניותו (למשל, בעניין פרויקט הגרעין באיראן), לחזק את האופוזיציה נגדו ואולי אף להביא לנפילתו.
- להרתיע מפני מלחמה או לקצר את אורכה, ואף לגבות מחיר מלחמה מהאויב ולהאריך את תקופת השיקום שלו אחריה, וזאת כדי לדחות את מועד המלחמה הבאה.
- להשתמש במשאבי האויב כנגדו, או כפיצוי מצידו על פעילותו (למשל, חילוט כספי טרור לצורך מתן פיצוי לנפגעי טרור).

האמצעים והכלים של "לוחמה כלכלית רחבה"

"לוחמה כלכלית רחבה" תוצג להלן בחלוקה לשתי קטגוריות: לוחמה "רכה" – כזו שאינה עושה שימוש ישיר בכוח קינטי או בכוח ההרס של הסייבר; לוחמה

"קשה" – כזו הכרוכה בהפעלת כוח מסוגים שונים, החורגים בעוצמתם מתחום הלוחמה "הרכה".

כלי לוחמה "רכה"

מדובר בלוחמה כלכלית מצד מדינות או קבוצת מדינות, ואף ארגונים, שנועדה להפעיל לחץ כלכלי ופוליטי משמעותי על יריב/אויב, במטרה להביאו לשנות את מדיניותו ואף להחלישו, וכל זאת ללא הפעלת כוח צבאי.

פעולות עונשין

פעולות עונשין כוללות סנקציות, אמברגו וחרם על משק האויב/היריב, כמו צמצום יחסים כלכליים או השעייתם (סחר, בנקאות, תיירות, השקעות, הסכמים כלכליים למיניהם), לרבות הטלת מכסים מפלים מסיבות מדיניות; הפעלת לחצים על חברות ומדינות אחרות להפסיק את יחסיהן הכלכליים עם מדינת האויב/היריב; הרחקת מדינה סוררת ממנגנוני המשק העולמי; הקפאת כספים ונכסים של אותה מדינה בחו"ל. דוגמאות לפעולות עונשין הן הטלת הסנקציות המקיפות על איראן (לרבות הטלת חרם על ייצוא הנפט האיראני)[6] ועל צפון קוריאה[7] בשל הפרויקטים הגרעיניים שלהן; הטלת סנקציות אמריקאיות על רוסיה בגין מעורבותה בבחירות בארצות הברית באמצעות הסייבר;[8] הקפאת נכסים של עיראק בחו"ל לאחר פלישתה לכווית בשנת 1990; אמברגו הנפט של מדינות ערב על המערב ב־1974, שנועד להפעיל לחץ על הכלכלה המערבית באמצעות יצירת מחסור בנפט והאמרת מחירים; החרם של ארגון BDS על ישראל.

מעבר להשפעה הישירה של צעדי הענישה על המשק, יש להם השלכות בתחום התודעה, בכך שהם עשויים ליצור אווירה של חנק כלכלי וחוסר מוצא אצל הצד הנפגע. עם זאת, ישנן מחלוקות בין חוקרים לגבי האפקטיביות של מכשיר הסנקציות, כך שמוטב לבחון כל מקרה לגופו.[9]

---

6 כיום מוטלות הסנקציות על ידי ארצות הברית, שפרשה מהסכם הגרעין עם איראן: טל שניידר, "כל מה שצריך לדעת על הסנקציות הכלכליות שיוטלו על איראן", **גלובס**, 8 במאי 2018, https://www.globes.co.il/news/article.aspx?did=1001235164.

7 "האו"ם אישר פה אחד סנקציות חדשות נגד פיונגיאנג", **הארץ**, 12 בספטמבר 2017, https://www.haaretz.co.il/news/world/america/1.4437072.

8 רן דגוני, "בגלל התערבות בבחירות: ארה"ב מטילה סנקציות על רוסיה", **גלובס**, 15 במארס 2018, https://www.globes.co.il/news/article.aspx?did=1001228035; Missy Ryan, Ellen Nakashima and Karen DeYoung, "Obama Administration Announces Measures to Punish Russia for 2016 Election Interference", *The Washington Post*, December 29, 2016.

9 רקע תיאורטי בנושא הסנקציות ראו: ניצן פלדמן, **בצילה של מתקפת דה־לגיטימציה: רגישותה של כלכלת ישראל לסנקציות**, מזכר 154, תל אביב: המכון למחקרי ביטחון לאומי, 2016, פרק 1.

פעולות אחרות שנועדו לפגוע בכלכלת היריב באמצעים "רכים"

מדובר, בין השאר, בהתקפות סייבר לשיבוש אתרים חיוניים של הממשל והמשק של האויב/היריב; בלוחמת מידע לערעור החוסן הכלכלי של המשק שלו (למשל, הפצת מידע מטריד בעניין חולשת ערך המטבע, חולשת המערכת הבנקאית, בריחת הון, מחסור בסחורות) ובהתערבות במערכת המוניטרית של האויב/היריב (למשל, זיוף שטרות של לירות שטרלינג על ידי הנאצים במלחמת העולם השנייה); ריגול טכנולוגי ותעשייתי בין מדינות, שנועד לגניבת קניין רוחני בהיקף נרחב במטרה לשנות את המאזן האסטרטגי הכלכלי בין אותן מדינות (אף שאיסוף מידע אינו נחשב לפעולה מלחמתית). בקטגוריה של "לוחמה כלכלית רחבה" ניתן לכלול שימוש בעוצמות כלכליות להחלשת היריב לתכלית מדינית וצבאית, לרבות הטלת מכסים מפלים מסיבות מדיניות.

עניינים נוספים

פעולות רבות מתנהלות במרחב הכלכלי הגלובלי, אם במסגרת הסכמים בין מדינות ואם מחוצה להם, ואף שלעיתים צד אחד יוצא מהן נשכר וצד אחר מפסיד, אין לייחס להן משמעות של לוחמה כלכלית. הדבר נובע מההבחנה, לפיה "לוחמה כלכלית רחבה" מיועדת בעיקרה להשגת תכלית מדינית וצבאית, גם במחיר של עלויות כלכליות למפעיל הלוחמה.

פירוש הדבר הוא ש"לוחמה כלכלית רחבה" אינה אופטימלית מבחינה כלכלית גם בעיני המתכנן. זאת, לעומת מאבקים כלכליים, לרבות מלחמות סחר,[10] שבהן מצפה המתכנן להשיג יתרון כלכלי מול שותפות הסחר שלו, שחלקן הן בעלות בריתו, באמצעים המקובלים במשק העולמי. דוגמה לכך הם מכסי המגן על אלומיניום ופלדה שהטיל הממשל האמריקאי על חברות האיחוד האירופאי, קנדה ומקסיקו.

להשלמת התמונה יש להזכיר את מנופי ההשפעה הכלכליים החיוביים. זהו הצד הנגדי של "לוחמה כלכלית רחבה", אם כי מטרתם של מנופים אלה זהה לאלה של המנופים השליליים – להניע מדינות וארגונים לפעול בכיוון הרצוי למפעיל. מדובר בשימוש בתמריצים כלכליים כדי לקדם יעדים צבאיים ומדיניים, ובהם סיוע במענקים ובהלוואות נוחות, הסכמים כלכליים, תנאי סחר מועדפים, מחיקה ופריסה של חובות, העברת טכנולוגיות ועוד. שני הצדדים עשויים לצאת נשכרים משימוש במנופי השפעה כלכליים: הצד הנותן נהנה מרווח מדיני, ואילו הצד המקבל זוכה

10 המושג "מלחמת סחר" שאול משדה המלחמה, אך אינו שייך לשדה זה ואינו נמנה עם לוחמה כלכלית. מלחמת סחר היא סכסוך כלכלי המאופיין במצב שבו מדינות מעלות או יוצרות מכסי מגן, או מחסומי סחר אחרים, זו מול זו. עם זאת, מלחמות סחר עלולות להידרדר למצב של לוחמה כלכלית.

ברווח כלכלי. לדוגמה, סיוע החוץ האמריקאי לסוגיו מחזק את הלגיטימציה של ארצות הברית לבוא בדרישות אל המדינות מקבלות הסיוע.

מנופי השפעה כלכליים אלה אינם כלי לוחמה על פי הגדרתם. עם זאת, יש הרואים בהפסקת הטבות כלכליות, באיום להפסיקן או בהתניית הסיוע בהשגת תכלית מדינית של נותן הסיוע מעשה בתחום הלוחמה הכלכלית הרחבה, או על גבול הלוחמה הזאת. כך, למשל, ארצות הברית קיצצה את הסיוע לפלסטינים בשל אי־שיתוף פעולה מדיני עימה; ערב הסעודית יוצרת קשר בין הסיוע הכלכלי שהיא מעניקה לירדן ובין מילוי דרישתה לקדם את יעדיה המדיניים והביטחוניים, ובראשם בלימת ההשפעה האיראנית במזרח התיכון;[11] במלחמת המפרץ הראשונה, בשנת 1991, קיבלה מצרים מבעלות הברית שלחמו נגד עיראק סיוע במזומן בהיקף של מיליארדי דולרים, וחובותיה קוצצו ב־25 מיליארד דולר, בתמורה להשתתפותה לצידן במלחמה נגד סדאם חוסיין. גם סוריה זכתה לסיוע כלכלי בגין השתתפותה במלחמה זו.

כלי לוחמה "קשה"

סגר צבאי (blockade)

משמעותו של סגר כזה היא הפעלת כוח צבאי למניעה או להגבלת אספקה של סחורות ושירותים אל מדינת האויב וממנה לעולם, במטרה להפעיל עליה לחצים כלכליים, בעיקר לשם השגת מטרות מדיניות וצבאיות. פעילות זו עשויה להיות כרוכה לפעמים גם בהפעלת נשק קינטי.

ניתן להבחין בין סגר על מדינה סוררת, שנסמך על הסכמה וכללים בין־לאומיים, כגון סגר של הקואליציה הבין־לאומית על עיראק לאחר פלישתה לכווית בשנת 1990, ובין סגר שמנסות מדינות שונות להטיל על נתיבי הסחר של מדינות אחרות כחלק ממלחמה ביניהן. דוגמאות לסגר מהסוג השני ניתן לראות בסגר שהטילה איראן על נתיב ייצוא הנפט של עיראק במפרץ הפרסי במהלך מלחמת עיראק־איראן בשנות השמונים של המאה העשרים, באמצעות תקיפות על מכליות נפט; בחסימת נתיב השיט של ישראל במצרי טיראן על ידי מצרים במאי 1967 (שהייתה אחד הגורמים העיקריים למלחמת ששת הימים); ובשימוש שעשתה גרמניה בצוללות במלחמות העולם הראשונה והשנייה כדי להטביע אוניות סוחר של אויביה.

תקיפה של יעדי תשתית וכלכלה

מדובר בתקיפה, או באיום בתקיפה, באמצעות נשק קינטי ו/או התקפות סייבר רבות־עוצמה למטרות הרתעה של האויב או החלשתו, קיצור משך המלחמה,

11 דן ארקין, "סיוע כלכלי בתנאים של סעודיה", *IsraelDefense*, 13 ביוני 2018, http://www.israeldefense.co.il/he/node/34572.

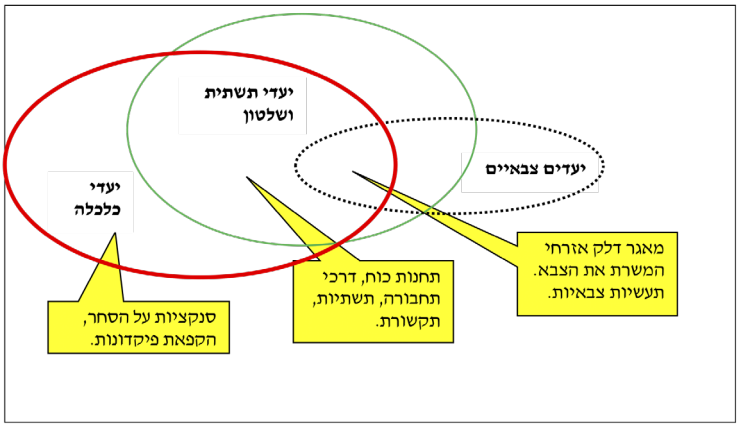
הרתעה מפני הסלמה והעלאת מחיר המלחמה. דוגמאות לכך הן: ההרתעה של ישראל כלפי חיזבאללה ולבנון באמצעות איום לפגוע בתשתיות בלבנון; פגיעה של ארצות הברית במתקני נפט עיראקיים במלחמת המפרץ הראשונה; התקפות חיל האוויר הישראלי על מטרות אסטרטגיות בעומק מצרים וסוריה במלחמת יום הכיפורים (מתקני נפט, מוסדות שלטון, בתי זיקוק ותחנות ממסר).

טרור כלכלי

טרור כלכלי הוא פגיעה של ארגוני טרור, או איומים שלהם לפגוע במטרות במשק המדינה או בתחושת הביטחון הכלכלי שלה. דוגמאות לכך הן איומיו של ארגון חיזבאללה לפגוע בתחנות כוח בישראל;[12] טרור העפיפונים מרצועת עזה בקיץ 2018, שהבעיר יבולים חקלאיים בנגב; גניבות והשחתות של ציוד חקלאי בישראל ממניעים לאומניים; פיגועי טרור במצרים שנועדו לפגוע בתיירות למדינה.[13]

ניתן להפעיל "לוחמה כלכלית רחבה" גם נגד ארגוני טרור, למשל איום על המשק של האוכלוסייה התומכת בארגונים אלה (במקרה של ארגונים סמי־מדינתיים), או פגיעה במקורות המימון ובמערכות הפיננסיות שלהם (כפי שנעשה במקרה של דאע"ש).

לוח 2: יעדי תקיפה של "לוחמה כלכלית רחבה" (דוגמאות)



12 רועי קייס, "נסראללה: אין צורך בנשק כימי, נפגע בתחנות כוח", *Ynet*, 3 בספטמבר 2012, https://www.ynet.co.il/articles/0,7340,L-4276742,00.html.

13 "מיעדי תיירות ליעדי טרור: איום ממשי למצרים", **שורטי**, המכון למחקרי ביטחון לאומי, 14 בינואר 2016, http://www.inss.org.il/he/blogs/?pauthor=55226.

הגנה נגד "לוחמה כלכלית רחבה"

ל"לוחמה כלכלית רחבה" יש גם צד הגנתי. אמצעי הגנה מדינתיים נגד לוחמה כזו כוללים:

- הרתעה – הכנת יכולת תגובה אמינה ואיום בתגובת נגד.
- הגנה פיזית אקטיבית, דוגמת "כיפת ברזל", ופסיבית, לרבות מיגון מתקנים כלכליים.
- פיזור של תשתיות ומתקנים כלכליים אסטרטגיים ברחבי המדינה והכנה של יכולות גיבוי ומערכות תשתית חלופיות, למשל בתחומי תקשורת ואנרגיה.
- הגנת סייבר על המשק (פירוט בהמשך).
- אחזקת מלאים של דלק, מזון, חלפים ועתודות מטבע חוץ בכמות גדולה מהנדרש לצרכים שוטפים.
- שימור ופיתוח יכולות ייצור עצמי של מוצרים קריטיים, כמו אנרגיה (למשל, פיתוח שדות הגז הטבעי בישראל), מזון, מלט ועוד.
- גיוון של מקורות הייבוא, ובעיקר של מוצרים חיוניים, וכן של יעדי הייצוא. מתן עדיפות לחוזים ארוכי טווח עם גורמים אמינים, שאינם מושפעים מהסכסוך הפוליטי באזור.
- הכנת תוכנית להמשכיות עיסקית במצבי חירום, לרבות בניית יכולות להתאוששות ולניהול אפקטיבי של המשק בשעת חירום, וכן תרגול והדרכה שלו לקראת מצבי חירום.

יתרונות ומגבלות השימוש ב"לוחמה כלכלית רחבה"

לשימוש ב"לוחמה כלכלית רחבה" יש, כמובן, הן יתרונות והן חסרונות. בין היתרונות ניתן למנות:

- יכולת להפעיל לוחמה כלכלית בספקטרום גדול של אמצעים ועוצמות, כמו חרם, סנקציות, סגר, התקפות סייבר והתקפות קינטיות, ובכך לנהל ולבקר את המערכה עד להשגת יעדיה.
- "לוחמה כלכלית רחבה" ניתנת להפעלה מרחוק ובלא סיכונים רבים למפעיל, למעט במקרים של תקיפות קינטיות מסוימות.
- "לוחמה כלכלית רחבה" בעת מלחמה יוצרת לחצים כלכליים על האויב להפסקת הלחימה, או משמשת לגביית מחיר כלכלי מהאויב שמטרתו היא להרחיק את המלחמה הבאה, וכל זאת תוך מזעור האבידות בנפש לאוכלוסייתו.
- ניתן לעשות שימוש ב"לוחמה כלכלית רחבה" גם במערכה שבין המלחמות (מב"ם).
- "לוחמה כלכלית רחבה", או איום להפעילה, עשויים להיות גם גורם מרתיע.

מגבלות וסיכונים הכרוכים בשימוש ב"לוחמה כלכלית רחבה" כוללים:

- מיסקלקולציה – שימוש ב"לוחמה כלכלית רחבה" עלול לגרור או להאיץ תהליכים שליליים, ואף להוביל למלחמה. למשל, בתחילת יוני 2018 הודיעה איראן על

האצה בפעילותה להעשרת אורניום, בתגובה לחידוש הסנקציות עליה מצד ארצות הברית.[14] בראייה היסטורית, הסנקציות הכלכליות שהטילו ארצות הברית ובריטניה על יפן בגין פלישתה לסין בשנת 1937 הביאו לשרשרת תוצאות לא רצויות: ברית בין יפן לגרמניה הנאצית ולאיטליה, ובהמשך – למתקפה היפנית על פרל הרבור בדצמבר 1941, שבתגובה לה הכריזה ארצות הברית מלחמה על יפן, ואילו בעלות בריתה של יפן (בהן גרמניה הנאצית) הכריזו מלחמה על ארצות הברית. השתלשלות זו הביאה, בסופו של דבר, לכניסתה של ארצות הברית למלחמת העולם השנייה.

- האוכלוסייה במדינת האויב עלולה לחוש איבה כלפי מפעיל הלוחמה, כך שהלחץ הכלכלי עשוי להביא דווקא לחיזוק התמיכה בשלטון המותקף.
- לחץ כלכלי חמור יכול ליצור פגיעה רחבה באוכלוסייה אזרחית חלשה, דבר שעלול להוביל למשבר הומניטרי ולגרור ביקורת בין־לאומית נוקבת.
- תגובת נגד – היריב עלול לפתח יכולות ולהגיב באותם כלים או בכלים אחרים. כתוצאה מכך, עלולה להתפתח מלחמה עתירת נזקים גם לתוקף.
- תיתכן פגיעה בנכסים או באינטרסים כלכליים של מדינות ידידותיות או ניטרליות לתוקף. דוגמה לכך היא פגיעה בנכס כלכלי של מדינת אויב המבוטח במדינה ידידותית, או תקיפת מחשב שזלגה ליעדים לא קרואים. מקרים כאלה עלולים להביא לתגובות נגד מפעיל הלוחמה.

"לוחמה כלכלית רחבה" בעידן הסייבר

להלן יתואר המרחב המשותף הקיים בין "לוחמה כלכלית רחבה" ובין הסייבר.[15] מהפכת המידע והטכנולוגיה העוברת על המשק והחברה נמצאת כיום בעיצומה: ענן מחשוב, ביג דאטה, מציאות רבודה, בינה מלאכותית, כלים אוטונומיים ו"האינטרנט של הדברים" הם תחומים המתפתחים ומאיצים את יחסי הגומלין בין השדה הכלכלי והחברתי ובין מרחב הסייבר, שהופך למשמעותי יותר ויותר בחייהם של פרטים, ארגונים, מדינות והמשק העולמי כולו.

כבר כיום קיימים מגזרים כלכליים, כמו מגזרי הבנקאות והפיננסים, שפעילותם העיקרית מתקיימת בעולם הווירטואלי של מרחב הסייבר, תוך שהם מצמצמים את הפעילות מחוץ למרחב זה. אמנם, השדה הכלכלי הוא ממשי, וכולל צרכנים, כוח עבודה, קרקע, חומרי גלם ואת התוצרים של תעשיות המתכת, הבנייה, המזון וכדומה, אלא שלכל אלה יש ייצוג דיגיטלי בסייבר, המתעד אותם וקושר ביניהם,

14 דניאל סלאמה וליעד אוסמו, "אירן: בחודש הבא יושלם מתקן לבניית צנטריפוגות מתקדמות", *Ynet*, 7 ביולי 2018, https://www.ynet.co.il/articles/0,7340,L-5280313,00.html.

15 ההרחבה המושגית מ"לוחמה כלכלית" ל"לוחמה כלכלית רחבה" מאפשרת לדון גם בהתקפות סייבר רבות־עוצמה, שקשה להכליל אותן בהגדרה המקובלת של "לוחמה כלכלית".

כך שלפגיעה בסייבר יש אפקט משמעותי גם מחוצה לו. תופעה חשובה נוספת היא הגלובליזציה של הסחר העולמי ושל שוקי ההון העולמיים, הנשענים על האינטרנט ועל מערכות סייבר המקושרות זו עם זו.

לוחמת סייבר היא לוחמה שבה משתמשים במרחב הסייבר כדי לפגוע ביעדים שונים של האויב, בעיקר לתכלית מדינית וצבאית. לוחמת סייבר יכולה להתלוות ללוחמה קונבנציונלית כממד לחימה נוסף, או להיות זירה בפני עצמה. היא יכולה להתממש בין המלחמות או תוך כדי מלחמה ולשאת אופי התקפי והגנתי כאחד. "לוחמה כלכלית רחבה" בסייבר משתמשת במרחב הסייבר הן כדי לתקוף יעדים כלכליים של האויב והן כדי להגן על נכסים כלכליים ותשתיות סייבר של המדינה, או על כאלה המקושרים אל מרחב הסייבר שלה (למשל, מפעלים, תחנות כוח ושדות תעופה), מפני מתקפות סייבר של האויב.

התקפת סייבר על הכלכלה

התקפת סייבר כוללת תקיפה **של** מערכות סייבר שמהוות תשתיות דיגיטליות (למשל, בסיסי נתונים ותוכנות של ארגונים), או תקיפה **דרך** הסייבר (מבלי לפגוע בו) על מערכות משובצות מחשב שפועלות מחוץ למרחב הסייבר, כמו תחנות כוח, מגדלי פיקוח, מערכות בקרת רמזורים וכדומה. המאפיין ההתקפי הייחודי ללוחמת סייבר הוא היכולת לבצע פעילות מרחוק באמצעות הסייבר ומבלי להיחשף ישירות.[16] כלומר, התוקף אינו מסתכן ויכול לנקוט מדיניות של עמימות (לרבות אי־נטילת אחריות). לעיתים, התקיפה אינה נראית על פני השטח ונדרש זמן לזהותה (למשל, בעת שיבוש בסיסי נתונים).[17]

התקפות סייבר נגד כלכלת האויב ניתנות לביצוע בדרכים שונות ויכולות להיעשות בשילוב עם סנקציות או עם התקפות קינטיות (באש), בעצימות נמוכה או גבוהה. בעת מלחמה יש לסייבר יתרון בתקיפת מוסדות פיננסיים על פני תקיפתם בדרך קינטית. לעיתים ניתן לעשות שימוש בהתקפות סייבר כתחליף להפעלת נשק קינטי.

התקפות סייבר עשויות להיות אמצעי נוסף של ארגוני טרור לשיבוש אורח החיים במדינות יעד שלהם, במיוחד נוכח העובדה שניתן להוציא אותן לפועל מכל נקודה בעולם, ולא רק באמצעות מגע קרוב. התקפות סייבר רבות־עוצמה מצד ארגוני טרור אינן נפוצות בשלב זה, אם כי יש לצפות להן כאשר לארגוני הטרור יהיו יכולות לבצע פיגועי ראווה בסייבר, כלומר התקפות סייבר עוצמתיות שתוצאותיהן ייראו לעין. התקפות בסייבר משמשות או עשויות לשמש את ארגוני

16 מה שקרוי Non-face to face business relationships or transactions

17 שמואל אבן ודוד סימן טוב, **לוחמה במרחב הקיברנטי: מושגים, מגמות ומשמעויות לישראל**, מזכר 109, תל אביב: המכון למחקרי ביטחון לאומי, יוני 2011.

הטרור גם להשגת כספים למימון פעילותם. בנוסף, הסייבר משמש ארגוני טרור, כמו חיזבאללה וחמאס, לביצוע פעולות איסוף[18] ולוחמה פסיכולוגית.

מדינות שביקשו להשיג יכולת התקפית הקימו ארגוני סייבר צבאיים. כך, למשל, ביוני 2009 הוקם פיקוד הסייבר האמריקאי, ובמאי 2018 הוא קיבל מעמד של פיקוד לוחם.[19] עם הקמתו פורסם שהפעולה ההתקפית בסייבר מול האויב או היריב נועדה ליצור חמישה אפקטים (חמישה D): למנוע את יכולת הפעולה של האויב/היריב בסייבר (Deny); להחליש אותו ולפגוע במעמדו (Degrade); לשבש את פעילות המערכות שלו (Disrupt); לבצע הונאה (Deceive); להרוס (Destroy) את יכולותיו. חמשת האפקטים הללו רלוונטיים גם ל"לוחמה כלכלית רחבה" בסייבר.

הסייבר הינו פלטפורמה שבמסגרתה נעשות פעולות כלכליות רבות, ובאמצעותה ניתן להעצים לוחמה כלכלית, כמו הגברת האכיפה של סנקציות כלכליות. הסייבר גם מאפשר שליטה ובקרה במרחב הכלכלי, כגון: מניעת גישה של מדינת אויב למערכת סחר וכספים; חסימת תנועות כספים; מניעת העברת הוראות סחר; ביצוע פעילות איסוף מידע וחשיפת חברות המפרות סנקציות; הקפאת חשבונות בנקים ופיקוח עליהם; בקרה על תנועות מט"ח חוצות גבולות באמצעות דיווחים של מוסדות פיננסיים מחוץ למדינת האויב; בקרה על הסחר באמצעות אימות נתונים עם ספקים מחוץ למדינת האויב.

כלכלה, מעצם טבעה, מפגינה רגישות גבוהה למידע, וחלק ניכר מהמערכות הכלכליות מבוסס על אמון הציבור במשק ומוסדותיו, כמו הבנקים, המטבע של המדינה והמערכות הממונות על שוקי ההון. "לוחמה כלכלית רחבה" בסייבר עשויה לשמש לערעור האמון במערכות המשק, בין היתר באמצעות הפצת מידע רלוונטי. עם זאת, אין זה פשוט להגיע להישג משמעותי במלחמת מידע כזו, מאחר והסייבר מאפשר גם לנתקף להגיב במהירות ולהזים שמועות נגדו.

תקיפת יעדים של מוסדות שלטון בסייבר, למשל באמצעות חסימת הגישה אליהם מצד הקהל, עלולה לפגוע במשילות, במשק ובהכנסות המדינה. זאת, מאחר והסייבר מהווה אמצעי לקשר בין העסקים והאזרחים ובין השלטון, קשר שאינו אינפורמטיבי בלבד, אלא כזה שהופך, יותר ויותר, לקשר מעשי, כמו השימוש ההולך וגובר באתרים של הממסד השלטוני לתשלומי מיסים ואגרות.

פריצה לסייבר ואיסוף מודיעין טכנולוגי ותעשייתי בסייבר מאפשרים לרוקן ארגונים מקניינם הרוחני. מהלכים כאלה, כאשר הם נעשים בסדרי גודל ניכרים,

18 טל שחף, "זירת הקרב הבאה של החמאס – הסייבר", **גלובס**, 18 ביולי 2018.

19 עמי רוחקס דומבה, "פיקוד הסייבר האמריקאי מקבל מעמד של פיקוד לוחם", *IsraelDefense*, 6 במאי 2018, http://www.israeldefense.co.il/he/node/34080.

עשויים לשנות את המאזן האסטרטגי בין חברות עיסקיות גלובליות, ואף בין מדינות. ארצות הברית טוענת, למשל, כי סין מבצעת פעילות כזאת בתחומה.[20]

ניתן לנהל התקפות בסייבר בדרגת עוצמה גבוהה, שמטרתן לשבש מסחר, ייצור ופעילות פיננסית של המדינה הנתקפת, למשל על ידי שיבוש בסיסי נתונים של מערכות סחר, מחסני לוגיסטיקה, תקציבים ועוד. פעולות אלו נמצאות על גבול הלוחמה "הרכה" ויכולות להגיע אף לדרגת לוחמה גבוהה יותר (תלוי בעוצמה ובהיקף הנזק).

ניתן לבצע התקפות בסייבר בדרגת עוצמה גבוהה יותר, במסגרת לוחמה "קשה", שתכליתן היא לפגוע בתפקודן של מערכות תשתית וכלכלה (חשמל, מים, בנקאות, תחבורה, תקשורת), עד כדי שיבוש מהותי של שגרת החיים ותפקוד המשק במדינת האויב. היכולת לפגוע מרחוק בתפקודן של מערכות כלכליות, מבלי לחצות גבול טריטוריאלי ומבלי להפעיל אש, היא יתרון ייחודי לסייבר. עם זאת, פעולות התקפיות מסוימות בסייבר יכולות להיות הרות אסון למדינה הנתקפת, לרבות בחיי אדם ובנזקים לתשתיות חיוניות. במקרה זה, מעמדן דומה לזה של התקפה קינטית, ותגובת המדינה הנתקפת עלולה להיות בהתאם.

בין המדינות המשתמשות בסייבר לתקיפת יעדים כלכליים ניתן לציין את איראן. באוגוסט 2012 נערכה התקפת סייבר באמצעות הווירוס "שאמון", המיוחסת לאיראן, נגד חברת הנפט הלאומית הסעודית עראמקו. הווירוס הדביק כ־30,000 מחשבים ופגע בתפקודה של החברה.[21] בשנת 2013 דווח כי האקרים איראנים ביצעו סדרת התקפות סייבר על מטרות אמריקאיות, כמו בנקים גדולים וחברות אנרגיה הפועלות במפרץ הפרסי, אך התקפות אלו לא גרמו נזק משמעותי.[22] התקפה נוספת באמצעות הווירוס "שאמון", המיוחסת לאיראן, בוצעה בשלהי שנת 2016 על הבנק המרכזי של ערב הסעודית וגופים ממשלתיים נוספים במדינה.[23] לפי ההערכות, איראן עלולה להגיב על הסנקציות שהטיל עליה נשיא ארצות הברית טראמפ במתקפת סייבר מסיבית,[24] אלא שאז היא תסתכן בחשיפת עצמה לתגובות נגד קשות. צפון קוריאה, הנתונה גם היא תחת סנקציות, הקימה מערך

---

20 "ארה"ב מאשימה את סין בגניבת מידע עיסקי בשווי 400 מיליארד דולר", *TheMarker*, 17 בפברואר 2012, https://www.themarker.com/wallstreet/1.1644216?=.

21 עמוס הראל, "הערכות: איראן מאחורי מתקפת הסייבר על חברות נפט במפרץ הפרסי", **הארץ**, 11 בספטמבר 2012, http://www.haaretz.co.il/news/world/1.1821619.

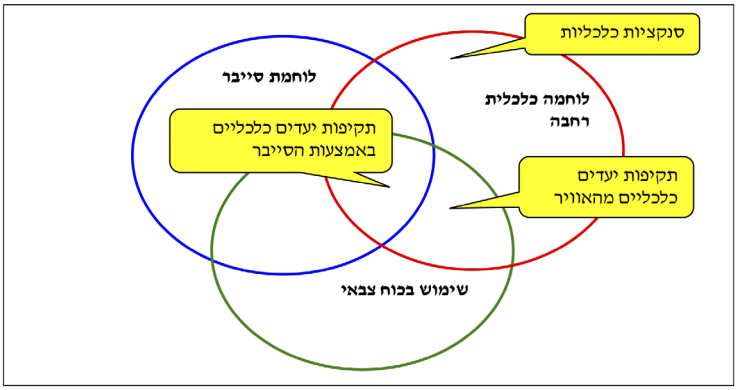
22 "דיווח: איראן מנהלת מתקפה מקוונת נגד ארה"ב", *Ynet*, 13 באוקטובר 2013, https:// www.ynet.co.il/articles/0,7340,L-4291493,00.html.

23 "האקרים איראנים פרצו למחשבי הבנק המרכזי של סעודיה", *TheMarker*, 3 בדצמבר 2016, https://www.themarker.com/wallstreet/1.3140741.

24 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks", *The New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

לתקיפות סייבר ומבצעת תקיפות כאלו בעיקר על דרום קוריאה ומדינות המערב.[25] הדוגמאות שהובאו לעיל מצביעות על כך שלוחמת הסייבר משמשת, בין היתר, כאמצעי תגובה של מדינות הנתונות תחת סנקציות.

לוח 3: "לוחמה כלכלית רחבה" ולוחמת הסייבר (דוגמאות)



הגנה מפני התקפות סייבר

איום הסייבר על המשק

המשק המדינתי והגלובלי תלוי במערכות מידע, בסיסי נתונים, תקשורת ואוטומטיזציה, ותלותו בסייבר הולכת וגוברת. ענפי כלכלה מסוימים, כגון תקשורת ובנקאות, מצויים כבר כיום עמוק במרחב הסייבר, ואחרים, כגון תחנות כוח, מפעלים ואמצעי תחבורה, פועלים באמצעות מערכות משובצות מחשב וסייבר.

תרחיש "יום הדין" של התקפת סייבר על המשק כולל מצב שבו בנקים ייסגרו; המסחר בבורסה ייפסק; התפקוד של תחנות כוח, מערכות מים, מפעלים ומערכות תחבורה ישובש מאוד; בשדות תעופה תיעצר תנועת המטוסים; מפעלים ומשרדים יסגרו את שעריהם; סחר החוץ ייבלם. כתוצאה מכך, אזרחים יתקשו לבצע פעולות בסיסיות, כמו משיכת כספים, קבלת שכר באמצעות הבנקים, תדלוק, רכישה במרכולים, תנועה ממקום למקום, מציאת תעסוקה ותקשורת עם מוסדות השלטון. השלטון, מצידו, יתקשה לנהל את המשק ולגבות מיסים, והפעילות במשק כולו תיעצר. למעשה, אין צורך בפגיעה כה רחבה כדי לעצור את התהליכים במשק, ודי לפגוע באחדות מהחוליות הרגישות בו. יחד עם זאת, עד היום לא נרשם אירוע

25 David E. Sanger, David D. Kirkpatrick and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More", *The New York Times*, October 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

מדינתי בסדר גודל של "יום הדין". בין הסיבות האפשריות לכך: מגבלות יכולתם של שחקני סייבר רבים, על רקע מנגנוני הגנה שהוקמו במדינות שונות (יש הבדל גדול בין פגיעת סייבר ביעד כזה או אחר לבין פגיעה מערכתית במשק); זהירות מצד מעצמות סייבר בחשיפה מוקדמת של נשקי סייבר; חשש מתגובות נגד, ואף החשש מפני הצתת מרוץ חימוש בסייבר ומלחמת סייבר גלובלית.[26]

להשלמת התמונה יש לציין שאירועי הסייבר הדרמטיים ביותר בשנים האחרונות, הנוגעים לביטחון הלאומי, היו בתחום המשילות במדינות דמוקרטיות. כך, ארצות הברית טוענת שרוסיה ביצעה מתקפת סייבר שנועדה להשפיע על תוצאות הבחירות לנשיאות בה בשנת 2016, דבר שנתפס כאיום ממשי על הדמוקרטיה האמריקאית. ניסיון להתערב בבחירות לנשיאות אירע גם בצרפת בשנת 2017, ובשיטה דומה – באמצעות הפצת מידע רגיש ברשתות חברתיות נגד המועמד, מידע שהושג, בין השאר, באמצעות פריצות למחשבים הקשורים אליו.[27] לעומת זאת, הסייבר אִפשר לנשיא טורקיה, ארדואן, לסכל ניסיון הפיכה צבאית נגדו ביולי 2016: ארדואן עלה לשידור טלוויזיה באמצעות אפליקציה סלולרית וקרא לתומכיו להפר את העוצר שהטיל הצבא ולצאת לרחובות.

קבוצה חשובה במשק, הזוכה לעדיפות מצד המדינה בהגנה בסייבר, הן "תשתיות מדינה קריטיות" (תמ"ק). קבוצה זו כוללת בישראל את תשתיות החשמל, המים, הגז הטבעי, הרכבות, רשות שדות התעופה, בתי הזיקוק, שרשרת ייצור החשמל והולכתו, משרדים ממשלתיים ובתי חולים. מדובר ב־26 תשתיות קריטיות, שאותן מנחה מערך הסייבר הלאומי באופן ישיר.[28]

המגזר הפיננסי (בנקים, חברות אשראי, מערכת הסליקה, שוק ההון, ביטוח, קרנות פנסיה) הוא אחת החוליות הרגישות במיוחד להתקפות סייבר, שכן הוא קריטי לתיווך פעולות כלכליות וחברתיות. בשונה ממגזר התשתיות הכבדות, מגזר הפיננסים חשוף לתקיפות סייבר יותר מאשר לתקיפות קינטיות. המערכת הפיננסית הינה מבוססת סייבר, רגישה לאמון הציבור וקריטית לתפקודן של מדינות.

דוגמה להתקפת סייבר על המערכת הפיננסית היא גניבה של 81 מיליון דולר מהבנק המרכזי של בנגלדש בפברואר 2016, במסגרת מתקפה שבה הצליחו האקרים (יתכן מצפון קוריאה) להעביר לפיליפינים כסף מחשבונות של הבנק המרכזי

---

26 גדי עברון ובועז דולב, "משחקי מלחמה: למה ארה"ב לא עורכת מתקפת סייבר על צפון קוריאה", *Ynet*, 19 בספטמבר 2017, https://www.ynet.co.il/articles/0,7340,L-5017828,00.html.

27 דודי סימן טוב, גבי סיבוני, גבריאל אראל, "איומים קיברנטיים על תהליכים דמוקרטיים", **סייבר, מודיעין וביטחון**, כרך 1, גיליון 3, דצמבר 2017.

28 דן ארקין, "ערוכים היטב לאיומים", *IsraelDefense*, 24 במאי 2018, http://www.israeldefense.co.il/he/node/34321.

של בנגלדש בבנק הפדרלי של ניו יורק.[29] אירוע דומה של גניבת כסף אירע בבנק וייטנאמי בתחילת 2016, שבמסגרתו נעשתה חדירה של האקרים למערכת "סוויפט", הנחשבת למערכת התשלומים הבין־בנקאית המאובטחת ביותר בעולם.[30] דוגמאות אלה מציגות יכולות שאותן ניתן להפעיל במידה גדולה יותר במסגרת "לוחמה כלכלית רחבה".

חברות אחרות במשק הרגישות למתקפות סייבר הן: חברות העוסקות בתשתיות, חברות ביטחוניות, חברות תקשורת, חברות סחר באינטרנט וארגונים העושים שימוש במידע רגיש (משרדי עורכי דין, מאגרים של קניין רוחני, של סודות מסחריים, של סודות רפואיים וכדומה). בשנים האחרונות גוברת המודעות לכך ששרשרת האספקה של ארגונים (גופים המספקים לאותם ארגונים תוצרי ביניים ושירותים) מהווה ציר כניסה למתקפות סייבר רבות עליהם. המשמעות היא שיש להגן לא רק על יעדים חיוניים במשק, אלא גם על המעטפת שלהם.

האיום עלול להגיע גם מקרב עובדי החברות, לרבות עובדים בתעשיות הביטחוניות העוסקות בסייבר. דוגמה לכך היא פרשה ביטחונית חמורה שנחשפה ביולי 2018, כאשר עובד בחברת הסייבר ההתקפי NSO נעצר בחשד שגנב נשק סייבר של החברה (תוכנת "פגאסוס") וניסה למכור אותו ברשת האפלה (Dark Web) תמורת חמישים מיליון דולר. ניסיונו של העובד סוכל לאחר ש"הקונה הפוטנציאלי" פנה לחברה. האירוע מצביע על הצורך שהמדינה תפקח על הנעשה גם בחברות העוסקות בתחום הסייבר.[31]

עיקר הנזק הכלכלי שנגרם עד היום למשק בתחום הסייבר אינו נובע מ"לוחמה כלכלית רחבה" של מדינות וארגונים פוליטיים, אלא מפשיעה, שמניעיה הם בעיקר כלכליים. עם זאת, יש להניח שכל מה שמגזר הפשיעה יודע לעשות בתחום הסייבר יודעות או יידעו לעשות גם מדינות, שיכולותיהן מאפשרות להן לעשות אף יותר מכך, אם וכאשר הן יחליטו להפעיל לוחמת סייבר מסיבית. המחשה ליכולת מדינתית עוצמתית כזו ניתנה בחשיפתן בשנת 2010 של התקפות סייבר (באמצעות תולעת "סטוקסנט"), שהרסו צנטריפוגות איראניות להעשרת אורניום.[32] התקפות אלו הבהירו לעולם שהאיום הנשקף מהתקפות סייבר כולל גם פגיעות פיזיות במפעלי

---

29 "מבצע לזרוס: כך צפון קוריאה גונבת כספים מבנקים במערב באמצעות מתקפות סייבר", *Nana10*, 5 באפריל 2017, http://media.nana10.co.il/Article/?ArticleID=1240370.

30 "מתקפת סייבר על הבנקאות הגלובלית: האקרים שוב פרצו למערכת התשלומים המאובטחת בעולם", *TheMarker*, 13 במאי 2016, https://www.themarker.com/wallstreet/1.2942637.

31 אלה לוי־וינריב, טל שחף, "הותר לפרסום: NSO ופרשת הסייבר מהחמורות בתולדות ישראל", **גלובס**, 5 ביולי 2018, https://www.globes.co.il/news/article.aspx?did=1001244618.

32 "תיק איראן נפתח: מלחמת הסייבר", **ערוץ 2**, **תוכנית עובדה**, 2 בנובמבר 2012, https://www.mako.co.il/tv-ilana_dayan/specials/Article-a996bba5fccba31006.htm.

תעשייה, בתשתיות ובתחום התחבורה, המצוידים כולם במערכות שליטה ובקרה ממוחשבות, ואינו מוגבל לפגיעות בבסיסי נתונים בתוך מרחב הסייבר בלבד.

המענה לאיום

פגיעה קשה במרחב הסייבר המדינתי עשויה להיחשב לבעיה של ביטחון לאומי. הגנת סייבר בהקשרה הכלכלי היא מכלול פעולות, בתוך מרחב הסייבר ומחוצה לו, שתכליתן להגן על המשק המדינתי, הן במרחב הסייבר והן במרחבים אחרים, מפני תקיפות העושות שימוש בסייבר. את הגנת הסייבר יש להפעיל מול מדינות, ארגונים אויבים, ארגוני פשע, אנשי זדון וגם לצורך התאוששות מתקלות.

ההבדל העיקרי בין לוחמה כלכלית של מדינות הנעשית בסייבר ובין פעולות פשיעה במרחב זה הוא בכך, שהמניע של פושעי הסייבר הוא לרוב כלכלי־פלילי (גניבת כספים, גניבת סודות מסחריים וקניין רוחני, מעילות והונאות, סחיטה, גביית כופר).[33] עם זאת, יש מקרים בהם מדינות מתייחסות לפעילות של פשיעה בהיקף נרחב בסייבר, ואף לפעילות כלכלית חריגה של גופים שפועלים למטרות רווח, כאיום הנוגע לביטחון הלאומי שלהן.[34]

להבדיל מתחומים אחרים, כמו ההגנה על הגבולות והגנה על העורף מפני טילים, שעליהם ממונה הצבא, ההגנה על נכסי המשק בסייבר, הן בישראל והן ברחבי העולם, מבוססת בעיקרה על שירותי אבטחה, תוצרים ואסטרטגיות של המגזר הפרטי[35] ועל משאביו של מגזר זה. קיימת תעשייה ענפה של חברות המפתחות, מייצרות ומשווקות מערכות הגנה בסייבר ותומכות בהן.

הגורם העיקרי להתפתחותה של תעשיית אבטחת הסייבר במשק המקומי והעולמי בעשורים האחרונים אינו הממסד, אלא הצורך של המגזר הפרטי להתגונן מפני חדירות של פורצים, שמניעיהם מגוונים: גניבת כספים, גניבת קניין רוחני וסודות מסחריים וטכנולוגיים ותקיפות סייבר ממניעים אידיאולוגיים או פסיכולוגיים (כמו אגו, ונדליזם וכדומה). תפקידם העיקרי של גורמי הביטחון הממשלתיים בהגנת

---

33 Alan Blinder and Nicole Perlroth, "Atlanta Hobbled by Major Cyberattack that Mayor Calls 'a Hostage Situation'", *The New York Times*, March 28, 2018, https://www.seattletimes.com/nation-world/atlanta-hobbled-by-major-cyberattack-that-mayor-calls-a-hostage-situation/.

34 לדוגמה, בתחילת 2010, בעיצומו של המשבר הכלכלי באירופה, סומנו ספקולנטים כ"טרוריסטים כלכליים". שר האוצר של גרמניה אמר אז שגרמניה עשויה לשקול להורות לסוכנויות הביון שלה להתחיל לנהל מעקב אחר התארגנויות של משקיעים ספקולנטים כדי להגן על האירו. בעיתון הספרדי **אל פאיס** נכתב כי השירות החשאי של ספרד פתח בחקירה של "התקפות" מצד ספקולנטים על המדינה.

35 גבי סיבוני, הדס קליין, "פיתוח יכולות ארגוניות לניהול משברי סייבר", **סייבר, מודיעין וביטחון**, כרך 2, גיליון 1, אפריל 2018, http://www.inss.org.il/he/publication/developing-organizational-capabilities-to-manage-cyber-crises/?offset=1&posts=2&type=715

המשק הוא הנחיה של גופים בולטים בעלי חשיבות לאומית ופיקוח עליהם. המדינה עוסקת בעיקר בהגנה על מוסדותיה ובהנחייה של ארגונים בקטגוריה של "תשתיות מדינה קריטיות". כלל המשק והציבור נהנים, לכל היותר, מהיכולת לפנות למוקד החירום הלאומי (CERT) ומהכתוב במדריך למתגונן בסייבר.

קצב השינוי של טכנולוגיית הסייבר הוא מהיר, כך שקשה לחזות כיצד היא תיראה בעוד מספר שנים. משום כך, קשה להכין תוכנית רב־שנתית בתחום הגנת הסייבר.[36] להשתנות המהירה ישנן גם עלויות גדולות של פחת טכנולוגי: אמצעים שיותקנו היום לא יהיו בהכרח רלוונטיים תוך מספר שנים, ויש לעדכן בהתמדה גרסאות של תוכנות, דבר שמגביר את התלות בספקי המחשוב.

העובדה שברוב מתקפות הסייבר קשה לזהות את התוקף (הנוקט אמצעי הסתרה וחמקנות), וכן ריבוי התוקפים, מחייבים את הארגונים והחברות במשק לאמץ אסטרטגיית הגנה רחבה בסייבר, שאינה מכוונת דווקא לתוקף מסוים, אלא להגנה מפני תקיפות מסוגים שונים, מכיוונים שונים וברמות קושי גוברות – הכל בשל ההתפתחויות הטכנולוגיות המהירות בתחום זה. בתחילה התפתחו מערכות הגנה היקפיות, ששמו את עיקר הדגש על הגנה מפני חדירה מרחוק ועל הסרת הווירוס שחדר, אך בעשור האחרון נפוצות בחברות גם מערכות שתכליתן לבלום או להתריע על פעילות לא מורשית, ואף עוינת, מצד אדם שחדר פיזית לארגון (חדירה ממגע קרוב), ובכלל זה עובד או ספק של אותו ארגון. כיום ממלאים תפקיד חשוב במערך ההגנה בסייבר גם מערכות ההגנה הפיזיות, קב"טים ומערך מיון כוח האדם ביחידת משאבי אנוש של הארגונים.

במהלך השנים הפכה ההגנה על התשתיות ועל המגזר הפיננסי מפני התקפות סייבר לדרישה רגולטורית מצד המדינה. במסגרת זו גם הוקמו גופים העוסקים בהגנה על הסייבר ברמה הלאומית: בישראל הוקמה כבר בשנת 2002 הרשות הממלכתית לאבטחת מידע, הפועלת במסגרת השב"כ; בשנת 2011 הוקם מטה הסייבר הלאומי; בשנת 2015 הוקמה הרשות הלאומית להגנת הסייבר;[37] בסוף 2017 הוחלט על הקמת מערך הסייבר הלאומי במשרד ראש הממשלה, כגוף שיאחד את מטה הסייבר הלאומי עם הרשות הלאומית להגנת הסייבר.[38] למרות כל הצעדים הללו, עדיין רבה הדרך להשגת הגנה מלאה על מרחב הסייבר הלאומי. כחזון לעתיד, ניתן לצפות מהמדינה שתיטול על עצמה אחריות מעשית רבה יותר להגנת מרחב הסייבר המדינתי עבור כלל המשק והאוכלוסייה. כשם שהמדינה מספקת מים

36 יצחק בן ישראל, "כי מציון ייצא סייבר", **הארץ**, **תוצרת ישראל – מוסף מיוחד ליום העצמאות**, אפריל 2018.

37 עמי רוחקס דומבה, "רשות הסייבר תחליף את השב"כ בפיקוח על אבטחת מידע בבנקים", *IsraelDefense*, 9 במאי 2016.

38 אתר מערך הסייבר הלאומי, https://www.gov.il/he/Departments/about/newabout.

צלולים וזרם חשמל יציב הן לעסקים והן לבתי המגורים, כך ראוי שהיא תדאג ליציבותה של תקשורת המחשבים ולהיותה נקייה מנוזקות.

לאור האמור לעיל, קיימת חשיבות רבה לשילוב בין המגזר הממשלתי למגזר הפרטי בתחום הגנת הסייבר. על המדינה לשלב את המגזר הפרטי בפעילות להגנת הסייבר הלאומי, הן כצרכן עיקרי והן כמשתתף במערך ההגנה.[39] דוגמה לכך ניתן למצוא בהקמתו, בינואר 2017, של מרכז בנקאי להגנת הסייבר בישראל, שהוא פרי יוזמה משותפת של הרשות הלאומית להגנת הסייבר, משרד האוצר, הפיקוח על הבנקים, התאגידים הבנקאיים וחברות כרטיסי האשראי.[40] לישראל יתרון בתחום זה, מאחר שיש בה מספר מועט יחסית של בנקים, פיקוח ממשלתי הדוק ויכולות סייבר גבוהות. עם זאת, מיעוט בנקים עלול להיות גם חיסרון, בהיבט של פיזור הסיכונים.

העובדה שמרחב הסייבר נטול גבולות טריטוריאליים מחייבת שיתופי פעולה בין־לאומיים לצורך הגנת הסייבר הלאומי. ואכן, בפסגת נאט"ו ביולי 2018 הסכימו מנהיגי המדינות החברות על הגברת המוכנות של מדינותיהם גם מול התקפות סייבר.[41] בהקשר הישראלי, יש לציין את דבריו של ראש השב"כ, נדב ארגמן, כי "מדינת ישראל נמצאת היום עם מעצמות הסייבר המובילות בעולם, בתוך זה מערכת הביטחון וקהילת המודיעין הישראלית. אנחנו כמובן משתפים פעולה עם שירותי מודיעין ומערכות ביטחון מרחבי העולם. לנו כארגון יש יכולת סייבר, גם הגנה וגם התקפה, די משמעותית. אנחנו כמובן משתפים פעולה עם כלל מערכת הביטחון הישראלית ולא עושים כלום לבד. אנחנו עם יכולת רחבה מאוד".[42]

דוגמה לשיתוף פעולה בין־לאומי בתחום הכספים הוא ארגון Financial Action Task Force (FATF),[43] שהוקם בשנת 1989 במטרה לפתח ולקדם מדיניות למלחמה בהלבנת הון ובמימון טרור ונשק להשמדה המונית. אלה תחומים שעל אף שונותם, עוסקים כולם בכסף שיש כוונה להסתיר את מקורו או את ייעודו, ואמצעי הטיפול בהם דומים. אחד הסיכונים שעליהם הצביע הארגון בעידן הסייבר הוא היכולת לבצע עסקאות לא חוקיות, או לעשות שימוש בכספים לא כשרים בסייבר, ללא חשיפה ישירה של המבַצע (פנים אל פנים). הארגון גם פרסם רשימה של קריטריונים, על פיהם

---

39 שמואל אבן, "אסטרטגיה לשילוב המגזר הפרטי בהגנת הסייבר הלאומי בישראל", **צבא ואסטרטגיה**, כרך 7, גיליון 2, אוגוסט 2015, http://www.inss.org.il/he/publication/?pauthor=50089&load_offset=30.

40 "מרכז סייבר בנקאי הוקם והחל לפעול בינואר", *READ IT NOW*, 20 במארס 2017, https://www.readitnow.co.il/news.

41 "נאט"ו שרדה את טראמפ, בינתיים", **הארץ**, 15 ביולי 2018.

42 איתי בלומנטל, "ראש השב"כ: סיכלנו השנה מתקפות סייבר מכל העולם", *Ynet*, 30 בינואר 2018, https://www.ynet.co.il/articles/0,7340,L-5078254,00.html.

43 http://www.fatf-gafi.org/home.

ייבָדקו מדינות שאינן חברות במסגרתו, ואם יוחלט שאינן עומדות בקריטריונים, הן עלולות להיכנס ל"רשימה שחורה", שתאפשר להטיל עליהן סנקציות כבדות.

הסיכון של העברת כספים לא כשרים גבר בשנים האחרונות, עם התפתחות השימוש במטבעות וירטואליים כגון ביטקוין, אטריום ודומיהם, שמאפשרים עסקאות מחוץ למערכת הפיננסית המדינתית והגלובלית הממוסדת. התפתחות של אמצעי תשלום ומערכות פיננסיות הנמצאים מחוץ לתחום שליטתן של מדינות עלולה להוביל להשלכות מרחיקות לכת, כמו מימון פעילות טרור, גיוס הון מצד ארגוני טרור וארגונים חתרניים, עקיפת סנקציות, תשלומים חשאיים עבור חומרים וטכנולוגיות רגישים ואסורים (נב"ק, טק"ק, יכולות סייבר), ערעור מערכות פיננסיות ממוסדות, פגיעה בגביית מיסים, פשעי סייבר וכופר, הלבנת הון, תשלומי שוחד ופגיעה בכספי ציבור. מדינות שונות נוקטות גישות שונות כלפי מטבעות אלה, אך המערכת הבין־לאומית טרם קיבלה החלטה משותפת לגביהם. ראשי המערכת הפיננסית במערב אינם רואים במטבעות הווירטואליים איום קרוב, נוכח הממדים המוגבלים של התופעה ביחס לשוק ההון העולמי. אם תופעת המטבעות הדיגיטליים תתפשט, יהיה צורך בנקיטת צעדי חקיקה ואכיפה ברמה המדינתית ובהסכמות בין־לאומיות, ואלה עשויים להיות חלק משמעותי מהפתרון לבעיה.[44]

הצורך בשיתוף פעולה גלובלי להגנת הסייבר הינו ברור. ארגון התקשורת הבין־לאומי (International Telecommunication Union – ITU) פועל לקדם הסכמה גלובלית סביב הגנת מרחב הסייבר. היו גם יזומות לגיבוש אמנה בין־לאומית בתחום הגנת הסייבר, בדומה לאמנות בתחום הגבלת תפוצת הנשק הכימי והביולוגי, אך ההערכות הן שהסיכויים לכך נמוכים כיום, משום שהדבר מחייב מנגנון פיקוח ואימות אמין, דבר שקשה ליישמו בתחום הסייבר.[45] גם נראה שארצות הברית חוששת שאמנה כזאת תגביל את יכולותיה ולא תתרום משמעותית להגנתה, מה שמפחית עוד יותר את הסיכוי להשגת הסכמה סביב אמנה אפקטיבית בתחום זה.

סיכום

חלקו הראשון של המאמר הציג את "הלוחמה הכלכלית הרחבה", שהיא סוג של לוחמה שהיקפה רחב יותר מהלוחמה הכלכלית על פי הגדרתה המקובלת. בחלקו השני של המאמר נדונה הלוחמה בסייבר כחלק מ"הלוחמה הכלכלית הרחבה". תחום "הלוחמה הכלכלית הרחבה" מאפשר לדון באופן מערכתי במגוון פעולות נגד כלכלת האויב, תוך שימוש בשורה של כלים – כלכליים, דיפלומטיים, תודעתיים, קינטיים

44 שמואל אבן, "מטבעות האינטרנט והביטחון הלאומי", **מבט על**, 28 בדצמבר 2017.

45 קמרון בראון ודוד פרידמן, "אמנה בינלאומית להתמודדות עם לוחמת סייבר? לקחים מהאמנות בתחום הנשק הכימי והביולוגי", בתוך: אמילי לנדאו וענת קורץ (עורכות), **בקרת נשק וביטחון לאומי: אופקים חדשים**, מזכר 136, תל אביב: המכון למחקרי ביטחון לאומי, מאי 2014.

וסייבר. מטרתן של פעולות אלו היא להפעיל לחץ על הכלכלה של האויב במטרה להרתיעו או להחלישו, בעיקר לשם השגת יעדים מדיניים וצבאיים. ניהול "לוחמה כלכלית רחבה" בעידן הסייבר מותנה בפיתוח יכולות התקפיות והגנתיות כאחד. היכולת ההתקפית חיונית גם לצורכי הגנה – לשם הרתעה ולתגובות נגד – ואילו יכולות ההגנה בסייבר הכרחיות גם למצבי התקפה, כדי לעמוד בפני התקפות נגד.

עידן הסייבר משַנה את תחום "הלוחמה הכלכלית הרחבה". מבחינה התקפית הוא מאפשר לפגוע בכלכלת האויב בעת מלחמה ובין המלחמות, הן באמצעות לוחמת סייבר "רכה" והן באמצעות תקיפות סייבר רבות־עוצמה, שעשויות להיות עדיפות על פני תקיפות קינטיות, המלוות במקרים רבים בפגיעות בנפש. מבחינה הגנתית, התלות הגוברת של מדינות בסייבר מעצימה את איומי הסייבר על המשקים הכלכליים, ועל כן מחייבת מאמצים מרובים והשקעות כבדות להגנה על המשק, לצד שיתופי פעולה בתוך המשק, בין המשק הפרטי לממשלה ובין מדינות במערכת הגלובלית.

תרחישי קיצון של התקפות סייבר על כלכלות של מדינות אמנם טרם התממשו, אולם הדבר אינו מונע את הצורך להתאים בכל מקרה את קצב בניית ההגנה על הסייבר המדינתי לקצב התבססותו המואצת של המשק במרחב הסייבר.