לוחמת מידע

התדירה המסיבית של המחשבים לתחום הצבאי פותחת פתח לניהול מלחמה מסוג חדש לחלוטין. מושגי היסוד של מלחמות העתיד יהיו "סוסים טרויאניים", "וירוסים", "תולעים" ו"פצצות לוגיות"

אלוף ד"ר יצחק בן־ישראל

כללי

בספרות המקצועית העולמית — ובמיוחד האמריקנית — מקובל לראות את לוחמת המידע כאחד המאפיינים היותר מובהקים של המהפכה הצפויה בשדה הקרב העתידי. הנושא הוא סבוך, בתולי, ורב הנעלם בו על הידוע. בכל אופן, ברור כי חדירת המחשבים לכל תחומי החיים, ובכלל זה לתחום הצבאי, מחייבת רוויזיה במושגי יסוד — ואפילו, כמו שיתברר בהמשך, במושג המלחמה עצמו. משום ראשוניות הנושא בחרתי הפעם לפתוח דווקא בהצגת הבסיס העיוני לתחום.

הקדמה עיונית — מלחמות הגל השלישי בעולם השלישי

הכותרת של פיסקה זו מחייבת הסבר: מהו הגל השלישי, ומהו העולם השלישי? מהו הקשר בין הגל השלישי לבין לוחמת המידע, ובמה שונה מלחמת הגל השלישי ממלחמות אחרות? נפתח תחילה בהבהרת המושגים.

המונח "הגל השלישי" לקוח מבית מדרשם של זוג הסופרים רבי־המכר אלווין והיידי טופלר. בסדרה של ספרים,[1] החל מ"הלם העתיד" וכלה ב"מלחמה ואנטי מלחמה", הם חוזרים ומפתחים רעיון בסיסי, ולפיו ניתן לראות את ההיסטוריה האנושית כמתחלקת לשלוש תקופות (או "גלים" כלשונם):

א. הגל החקלאי.
ב. הגל התעשייתי.
ג. הגל השלישי (הנוכחי) — גל המידע.

לכל גל יש כלכלה משלו, דרכים ליצירת עושר, תרבות וצורת מלחמה משלו. סמלו של הגל הראשון הוא המעדר, של הגל השני — קו הייצור התעשייתי, וסמלו של הגל השלישי — המחשב. כלכלת הגל הראשון התבססה על חקלאות, ועשיר היה אז מושג נרדף לבעל אדמות. המעבר לכלכלת הגל השני החל עם המהפכה התעשייתית במאה ה־17 (מהפכה שהקבילה למהפכת הרנסאנס באמנות ובתרבות ולמהפכה המדעית מבית מדרשו של ניוטון). כלכלה זו התבססה על קו הייצור התעשייתי, ועשירי התקופה ההיא היו התעשיינים. כיום אנו נמצאים בעיצומו של המעבר לגל השלישי, שבו מבוססת הכלכלה על ידע ועל שליטה במידע[2] ולאו דווקא על קווי ייצור תעשייתיים, עתירי מכונות.

טבלה מס' 1: הגל השלישי (לפי טופלר)

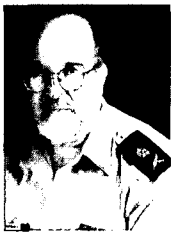
	מאפיין	מיהו עשיר?	סמל	צורת מלחמה
הגל הראשון	חקלאות	בעל אדמות	מגל	חרב
הגל השני	תעשייה (קו ייצור)	תעשיין	מכונות	טנק, מטוס
הגל השלישי	ידע	ביל גייטס	מחשב	לוחמת מידע

> מלחמות הגל השלישי יהיו שונות בתכלית השינוי. שם המשחק יהיה השגת מידע על האויב ומניעת מידע על עצמך. מי שישלוט בטכנולוגיות המידע, ינצח במלחמה, גם אם יעמדו מולו כלים רבים, שייפלטו מקווי הייצור של הגל השני

כאמור, לכל גל גם צורת מלחמה משלו. באופן ציורי אפשר לקבוע את החרב כסמל המלחמה של הגל הראשון, את המטוס ואת הטנק ("מכונות") כסמלי הגל השני ואת המחשב הצבאי (או את לוויין המודיעין) כסמלה של המלחמה בגל השלישי.

צורת המלחמה בגל השלישי

מלחמות הגל השני מוכרות לנו היטב. אלה מלחמות המבוססות על צבא המוני (מאז ימי נפוליאון) ועל "מכונות" (פלטפורמות) המיוצרות בקווי ייצור תעשייתיים והנושאות את עיקר המערכה על שכמן (מטוסים, טנקים, אוניות וכו'). שם המשחק הוא קו



ראש מפא"ת במשרד הביטחון ובמטכ"ל

הייצור, ובמלחמה זו מנצח, בסופו של דבר, מי שמסוגל (כלכלית, טכנולוגית וכו') לפלוט יותר מכונות מקו הייצור שלו. כך, למשל, ניצחה ארה"ב את גרמניה במלחמת העולם השנייה, אף שבתחילת המלחמה היה הסד"כ שלה נחות כמותית: במהלך המלחמה ייצרו האמריקנים כמעט 100 אלף טנקים ו־300 אלף מטוסים![3] מלחמות הגל השלישי — טוענים בני־הזוג טופלר — יהיו שונות בתכלית השינוי. שם המשחק יהיה השגת מידע על האויב ומניעת מידע על עצמך. מי שישלוט בטכנולוגיות המידע, ינצח במלחמה, גם אם יעמדו מולו כלים רבים, שייפלטו מקווי הייצור של הגל השני.

אתנחתא פילוסופית: שלושת העולמות של פופר

לפני שנעבור לניתוח ולדיון בתיזה של בני־הזוג טופלר, ניעזר בכמה מושגים מבית היוצר של הפילוסוף קרל פופר, שהלך לעולמו לפני כשלוש שנים.

נקודת המוצא שלו היא השאלה: איזה מין דברים קיימים בעולם?

באופן מסורתי נהוגה בפילוסופיה (מאז ימי היוונים) החלוקה לשניים: חומר ורוח. העולם מכיל עצמים מסוג "חומר" (אבנים, כיסאות, טנקים וכו'). לאלה יש מיקום מוגדר (זמן ומרחב), והם מורכבים מאבני היסוד האלמנטריים של החומר. לעומתם, החוויות המנטליות (מחשבות, רגשות תחושות וכו') אינן חומריות. קיומם של העצמים החומריים הוא אובייקטיבי, ואילו החוויות הרוחניות הן סובייקטיביות. פופר[4] מכנה את אוסף העצמים החומריים בשם "עולם ראשון", ואת עולם הרוח (הסובייקטיבי) בשם "עולם שני".

אבל, שואל פופר, מה מעמדו של הידע האנושי? לאן שייך, למשל, משפט פיתגורס? לעולם הראשון או לעולם השני? ברור כי אינו "חומר". אבל האם הוא "חוויה מנטלית"? האם הוא סובייקטיבי? אף שהוא תוצר של הרוח האנושית, אומר פופר, אין הוא משתייך לעולם השני. מרגע שנוצר, הוא אמת אובייקטיבית, ששוב אינה תלויה ברוח שיצרה (או גילתה) אותו. למעשה, קיים "עולם" שלם של ידע אנושי — פופר מכנה אותו "העולם השלישי" — המאוכלס על־ידי "יצורים" כמו משפט פיתגורס, חוקי הפיסיקה וכו', אשר אינם "חומר" ואינם "חוויות מנטליות" סובייקטיביות. הידע הוא אובייקטיבי, אף שהוא תוצר של הרוח האנושית (הסובייקטיבית).

כך אומר פופר במילותיו שלו:[5]

> בלי לקחת יותר מדי ברצינות את המילה "עולם", ניתן להבחין בין שלושת העולמות הבאים: ראשית, העולם של אובייקטים פיסיקליים או של מצבים פיסיקליים; שנית, העולם של מצבי תודעה או של מצבים מנטליים או אולי של נטיות התנהגותיות לפעולה; ושלישית, העולם של תוכן אובייקטיבי של מחשבה, במיוחד של מחשבות מדעיות, שירה ועבודות אמנות...
>
> בין התושבים של "העולם השלישי" נמצאות במיוחד מערכות תיאורטיות, אבל תושבים אחרים, חשובים לא פחות, הם בעיות ומצבי בעיות. לטענתי, התושבים החשובים ביותר של עולם זה הם טיעונים ביקורתיים... וכמובן גם התוכן של כתבי־עת, של ספרים ושל ספריות.

כדי להוכיח את הקיום האוטונומי של העולם השלישי מביא פופר בדרך־כלל את הטיעון הסטנדרטי הבא:[6]

> לכל גל צורת מלחמה משלו. באופן ציורי אפשר לקבוע את החרב כסמל המלחמה של הגל הראשון, את המטוס ואת הטנק כסמלי הגל השני ואת המחשב הצבאי כסמלה של המלחמה בגל השלישי

נתבונן בשני ניסויי מחשבה:

ניסוי 1: כל המכשירים והמכונות שלנו וכל הלמידה הסובייקטיבית שלנו הושמדו, כולל הידיעה הסובייקטיבית שלנו על המכשירים ועל המכונות ודרכי השימוש בהם, אבל נותרו הספריות והיכולת שלנו ללמוד מהן. ברור כי אחרי סבל רב העולם שלנו ייצא שוב לדרכו.

ניסוי 2. כמו מקודם — המכשירים והמכונות שלנו הושמדו, כמו גם למידתנו הסובייקטיבית, כולל הידיעה הסובייקטיבית שלנו על המכשירים, על המכונות ועל דרכי השימוש בהם. אבל הפעם כל הספריות הושמדו גם הן, כך שיכולתנו ללמוד מספרים נעשית בלתי אפשרית. אם נחשוב על שני ניסויים אלה, אזי הממשות, המשמעות ומידת האוטונומיה של העולם השלישי (כמו גם פעולתו על העולם השני ועל העולם הראשון) ייעשו אולי קצת יותר ברורים, משום שבמקרה השני לא תהיה שום צמיחה מחדש של התרבות שלנו למשך אלפים רבים של שנים.

טבלה 2 שלהלן מסכמת את המאפיינים העיקריים של שלושת העולמות הפופריאניים.

טבלה מס' 2: שלושת העולמות של פופר

	תכולה	מעמד	דוגמאות
העולם הראשון	חומר	אובייקטיבי	שולחנות, מטוסים
העולם השני	חוויות מנטליות	סובייקטיבי	כאב, שמחה
העולם השלישי	ידע	אובייקטיבי	מתימטיקה, פיסיקה

פלכלת עידן המידע והטכנולוגיה

בניגוד לחומר, ניתן להשתמש בידע שוב ושוב ולחלק אותו לצרכנים רבים, בלי שהוא יתמעט. לכך יש השלכה חשובה גם על תורת הכלכלה: הידע אינו "סחורה" רגילה, אשר כמותה מתמעטת אם חלק ממנה נמכר; הידע הוא "סחורה" בלתי נדלית. נושא

זה זוכה רק בשנים האחרונות לטיפול נרחב בתורת הכלכלה. כך, למשל, אומר הכלכלן פול רומר, שמוביל כיום את המחקר בנושא זה בעולם, במאמר שבו הוא מניח יסודות ל"כלכלה אחרת":[7]

> התוצר לשעת עבודה בארה"ב כיום הינו בעל ערך הגבוה פי עשרה מהתוצר לשעת עבודה לפני 100 שנה. בשנות ה־50 של המאה הזאת שייכו כלכלנים כמעט את כל השינויים בתוצר לשעת עבודה לשינויים טכנולוגיים. ניתוח נוסף הגביר את הערכתנו לגבי חשיבות הגידול בכוח העבודה ובמאגרי ההון האפקטיביים כגורמים המניעים צמיחה של תוצר לעובד, אך השינוי הטכנולוגי היה חשוב לפחות באותה מידה. אומנם לא היה שינוי בחומרי הגלם שבהם השתמשנו, אבל כתוצאה מניסוי וטעייה, התנסות, דיוק הולך וגובר וחקירה מדעית נהפכו ההוראות, שלפיהן אנו משלבים את חומרי הגלם [להפקת המוצר המוגמר], להרבה יותר מתוחכמות. לפני מאה שנה כל מה שיכולנו לעשות בתחמוצת ברזל כדי לקבל גירוי ויזואלי היה להשתמש בה בתור פיגמנט. כיום אנו מצפים בה רצועות פלסטיק ומשתמשים בהן ליצירת קלטות וידאו.

שלא ככור היתוך בודד או קו ייצור, בידע אפשר להשתמש בשתי חברות בעת ובעונה אחת. הן אף יכולות לנצל אותו ליצירת ידע נוסף

הטענה המוצגת במאמר זה מבוססת על שלוש הנחות:

ההנחה הראשונה היא ששינוי טכנולוגי — כלומר שיפור בהוראות לשילוב חומרי הגלם [כדי להפיק את המוצר המוגמר] — הינו הלב של הצמיחה הכלכלית... שינויים טכנולוגיים ממריצים צבירה מתמדת של הון. צבירת הון ושינויים טכנולוגיים אחראים לרוב הגידול בתוצר לשעת עבודה.

ההנחה השנייה היא ששינוי טכנולוגי נובע ברובו הגדול כתוצאה מפעולות מכוונות של אנשים אשר מגיבים לגירויי השוק...

> ההנחה השלישית והבסיסית ביותר היא כי ההוראות לעבודה עם חומרי גלם שונות במהותן מאלה של מוצרים כלכליים אחרים. לאחר שכבר הוצאה העלות ליצירת מערך חדש של הוראות, ניתן להשתמש באותו מערך שוב ושוב ללא תוספת עלות. פיתוח של מערכי הוראות חדשים וטובים יותר שקול להוצאת עלות קבועה נוספת. תכונה זו היא האפיון המגדיר של הטכנולוגיה...

כלכלנים החוקרים את תורת המימון הציבורי זיהו שתי תכונות בסיסיות של כל מוצר כלכלי: המידה שבה הוא בלתי נדלה[8] והמידה שבה הוא בלעדי. בלתי נדלות היא תכונה טכנולוגית טהורה. מוצר (או סחורה) נדלה טהור מתאפיין בכך ששימושו על־ידי חברה אחת או אדם אחד מונע את שימושו [בו זמנית] על־ידי אחרים. מוצר בלתי נדלה טהור מתאפיין בכך ששימושו על־ידי חברה אחת או אדם אחד אינו יכול להגביל את שימושו על־ידי אחרים.

בלעדיות (excludability) היא פונקציה גם של טכנולוגיה וגם של המערכת המשפטית. מוצר הוא בלעדי, אם בעליו יכולים למנוע מאחרים להשתמש בו. מוצר כמו תוכנת מחשב יכול להיעשות בלעדי באמצעות מערכת חוקים, שתאסור להעתיקו, או באמצעות הצפנה ואמצעי הגנה נגד העתקה. סחורות כלכליות רגילות הן סחורות נדלות ובלעדיות. הספקתן נעשית בערוץ השיווק הפרטי, והן נסחרות בשווקים תחרותיים. מעצם ההגדרה, מוצרים/סחורות ציבוריים אינם נדלים ואינם בלעדיים...

המקרה המעניין עבור תורת הצמיחה הוא אוסף הסחורות שאינן נדלות, אך בכל זאת בלעדיות. מההנחה השלישית המובאת בהקדמה משתמע כי טכנולוגיה היא מוצר בלתי נדלה...

לתכונת הבלתי נדלות יש שתי השלכות חשובות על תורת הצמיחה:

ראשית, מוצרים בלתי נדלים ניתנים לצבירה ללא חסם התלוי במספר האנשים, בעוד שמרכיבי הון אנושי, כמו היכולת לחבר מספרים, אינם ניתנים לצבירה זו. לכל אדם יש רק מספר סופי של שנים, שבהן הוא יכול לרכוש מיומנויות. כאשר הוא מת, כל המיומנויות שלו נעלמות, מלבד המוצרים הבלתי נדלים שאדם זה הפיק, כמו: חוק מדעי; עיקרון בהנדסה מכנית, אלקטרונית או כימית; תוצאה מתימטית כלשהי; תוכנת מחשב; פטנט; שרטוט מכני או תוכן. כל אלה נשארים הרבה אחרי שהאדם כבר הלך לעולמו.

שנית, ההתייחסות לידע כאל מוצר בלתי נדלה מאפשרת לדבר על דליפת ידע, כלומר על בלעדיות לא מושלמת. שתי תכונות אלה של ידע — צמיחה בלתי חסומה ובלעדיות לא מושלמת — הן אשר בדרך־כלל מזוהות כרלוונטיות לתורת הצמיחה.

אלווין והיידי טופלר מתבטאים כמעט באותן המילים בבואם לתאר את כלכלת הגל השלישי:[9]

> בעוד שאדמה, עבודה, חומרי גלם והון היו "גורמי הייצור" הראשיים בכלכלת הגל השני של העבר, ידע — המובא כאן בהגדרתו הרחבה, הכוללת נתונים, מידע, דמויות, סמלים, תרבות, אידיאולוגיה וערכים — הוא המשאב המרכזי של כלכלת הגל השלישי. רעיון זה, שפעם זכה לקיתונות של בוז, היה בינתיים לאמת חיים. השלכותיו, לעומת זאת, ברובן עדיין אינן מובנות. בעזרת הנתונים, המידע ו/או הידע המתאימים ניתן להפחית את כל שאר התשומות המשמשות לעשיית עושר. תשומות הידע הנכונות יכולות להפחית את הצורך בידיים עובדות, לצמצם מלאים, לחסוך אנרגיה וחומרי גלם ולקצץ בזמן, במקום ובכסף הדרושים לייצור...
>
> מה שהופך את כלכלת הגל השלישית למהפכנית באמת הוא העובדה שבעוד אדמה, ידיים עובדות, חומרי גלם ואולי אף ממון יכולים להיחשב כמשאבים בעלי כמות סופית, הידע הוא מכל הבחינות משאב בלתי נדלה. שלא ככור היתוך בודד או קו ייצור, בידע אפשר להשתמש בשתי חברות בעת ובעונה אחת. הן אף יכולות לנצל אותו ליצירת ידע נוסף.

אם ננסה לאחד עתה את הבסיס המטפיסי של פופר עם הסוציולוגיה של טופלר (המתוארת, למעשה, ע"י תורת הכלכלה של רומר), נוכל לטעון כי מלחמות הגל השני (והראשון) התנהלו בעיקר בעולם הראשון ("חומר"). במלחמות אלו ניצח מי שהשכיל להעמיד צבא גדול וחזק יותר, ומי שידע לגייס לעזרתו ולטפח את הגורמים המנטליים (העולם השני) של גייסותיו (כמו רוח קרב, מוטיבציה, אומץ לב וכו'). מלחמות העתיד, לפי תיאור זה יתפשטו גם לעולם השלישי, עולם המידע. מבלי להפחית בערכם של גורמים אלה גם בעתיד, הרי בעוד שמלחמות העבר (הגל הראשון) נשענו על כוח הזרוע, ומלחמות ההווה (הגל השני) נשענות על כוח המכונות, יישענו מלחמות העתיד יותר ויותר על כוח המוח.

מהי לוחמת מידע?

טבלה 3 שלהלן מפרטת את הנושאים הנכללים בדרך־כלל תחת הכותרת לוחמת מידע (Information Warfare): איסוף והעברה של המידע הגולמי (תקשורת), עיבוד וסינון, הפצת המידע המעובד, ובמקביל — מניעת הגעתו לידי גורמים שאינם מורשים.

למעשה אלה שטחים קלאסיים, שהעיסוק בהם הוא עתיק יומין, וימיהם כימי המלחמה עצמה. במרוצת ההיסטוריה פותחו כמה שיטות קלאסיות ללוחמת מידע — החל מאיסוף מודיעין באמצעות "חיישנים" אנושיים (ראו פרשת המרגלים בימי יהושע בן־נון) וכלה בפיתוח טכנולוגיות איסוף מיוחדות (כמו חיישני מודיעין

טבלה מס' 3: לוחמת מידע

נושא	מערכות רלוונטיות
איסוף מידע	חיישנים
שינוע מידע לתחנת עיבוד	תקשורת (DL)
עיבוד מידע	מחשבים, אינטלגנציה מלאכותית (AI), אלגוריתמים לזיהוי אוטומטי (ATR), מיזוג נתונים (Data Fusion)
הפצת מידע	מערכות תצוגה, תקשורת רחבת סרט
מניעת מידע	הסתרה, שיבוש, לוחמה אלקטרונית (ל"א), הטעיה
מה חדש?	לוחמת מחשבים

מוטסים, לוויינים וכו'). גם בתחום המניעה פותחו שיטות קלאסיות בלוחמת מידע, כמו הסוואה, בניית דמיים, מיסוך, הונאה, הטעיה, שיבוש, חסימה וכדומה.[10]

עיון במערכות הרלוונטיות המתוארות בטבלה 3 יכול להוביל אותנו למסקנה כי החידוש (הכמעט) יחיד בתחום זה הוא התלות ההולכת וגוברת של מערכות המידע במחשב. במילים אחרות, בעוד שלוחמת מידע אינה תחום חדש, הרי שאין הדבר כך ביחס למערכות המידע הממוכנות, כלומר המערכות משובצות המחשב. ה־FM 100-6 האמריקני מגדיר בתמציתיות את אפשרויות המלחמה החדשות, הקשורות למערכות אלה:

> במקום להיות מוגבלים להשמדה פיסית של אנשים או של מכונות מלחמה כנתיב היחיד המוביל להצלחה בשדה הקרב, יכולים עכשיו הצבאות להפוך את מערכות המידע של היריב למטרות כדי לשנות את "הכימיה" של שדה הקרב ולהביא להצלחה במלחמה.

בקצרה, מה שיכול בהחלט להיחשב כתחום ייחודי למלחמה המודרנית אינו לוחמת מידע, אלא לוחמת מחשבים. משום כך אני מציע לצמצם את תחום הדיון ללוחמת מחשבים (ל"מ).[11] חשוב להבין כי לא רק מערכות צבאיות מתאפיינות בכך שהן משובצות מחשב. גם חלק גדול ממערכות המשק האזרחי הולכות

טבלה מס' 4: מערכות מחשב - דוגמאות

מערכות צבאיות	מערכות אזרחיות
מרכזיות טלפון ותקשורת	מערכות טלפון ותקשורת
מערכות נשק וניווט	— — — — —
מערכות בקרת טיסה	— — — — —
— — — — —	תחבורה (בקרת רמזורים, רכבות)
מערכות מידע מרכזיות	מערכות מידע מרכזיות
שו"ב	— — — — —
— — — — —	בנקים / בורסה
מערכים לוגיסטיים	מערכים לוגיסטיים
— — — — —	מערך האשמל / מים / דלק
מערכות ל"א	— — — — —
מערכות התרעה	— — — — —

ונעשות תלויות יותר ויותר במחשבים. עובדה זו פותחת אפשרויות חדשות ללחימה. טבלה מס' 4 מפרטת דוגמאות בולטות למערכות עתירות מחשב הן בתחום הצבאי והן בתחום האזרחי־כלכלי — מערכות שפגיעה בהן יכולה להיות משמעותית ביותר. בין המערכות הבולטות מצויות מרכזיות טלפון ותקשורת, מערכות הבנקים, מערכות מידע לוגיסטי ומערכות שליטה ובקרה (שו"ב).

לוחמת מחשבים — דילמות מרכזיות

עובדה זו מעלה מייד הרהור לגבי מושג המלחמה עצמו: האם תקיפת מחשבים המרכזים את המידע הכלכלי (נאמר של הבנקים) במדינה מסוימת היא אקט של מלחמה? נניח כי יום בהיר אחד יתמוטטו מערכות המחשבים של הבנקים בישראל. נניח גם כי נצליח לגלות את הסיבה ולקבוע בוודאות כי הנזק (אשר גודלו לא ישוער) נעשה במכוון על־ידי חדירה פיראטית שבוצעה מתוך

טבלה מס' 5: טכניקות לוחמת מחשבים (ל"מ)

טכניקות מעולם המחשבים	
סוסים טרויאניים וירוסים תולעים פצצות לוגיות/פצצות זמן	החדרה בתקשורת הפעלת סייענים מבפנים להחדרה, החדרה דרך תוכנות "מסחריות", תקיפת ציוד במהלך הייצור ההעברה, האחסון, ההתקנה, התחזוקה והתפעול
טכניקות לא קונווציונליות דופק אלקטרומגנטי (EMP) נשק ביולוגי נגד רכיבים אלקטרוניים קרינה רבת עוצמה (HPM)	
טכניקות קלאסיות חסימה (ל"א) שיבוש הטעיה	
טכניקות ברוטליות פגיעה פיסית (הפצצה) שיבוש הספקות (חשמל, מיזוג אוויר וכו')	

שטחה של מדינה שכנה. האם זהו אקט של מלחמה? כיצד נגיב? באשי? לכאורה הנזק שנעשה הוא "רק" כלכלי ולא נפגעו חיי אדם (ישירות). אבל במקרים מסוימים עלול נזק כלכלי לגרום לשיתוקה של מדינה שלמה, ומה אז? הבעיה נעשית, כמובן, סבוכה יותר, משום שתקיפת מחשבים אינה מחייבת טריטוריה מוגדרת כבסיס, והיא יכולה להיעשות לא רק על־ידי מדינות, אלא גם על־ידי ארגונים (כולל ארגוני טרור או פשע מאורגן) ועל־ידי יחידים.[12] הדילמה שתוארה לעיל מעוררת מייד מספר שאלות הקשורות אליה ישירות:

א. כיצד מזהים את התקיפה (במקרה של לוחמת מחשבים)?[13] כיצד מזהים את התוקף?
ב. מהי מטרת המלחמה בכלל ולוחמת המחשבים בפרט? האם היעד לתקיפה הוא רק מערכות צבאיות, או שמא גם מערכות כלכליות או שלטוניות?
ג. האם מלחמה ללא אש היא גם מלחמה?
ד. האם יש להפעיל לוחמת מחשבים רק במצב מלחמה, או שמא ראוי להפעילה גם בימי שלום למטרות מסוימות (למשל - השגת מודיעין)?

הגדרתה של לוחמת המחשבים

כנקודת פתיחה לדיון אני מציע את ההגדרה הבאה לעיסוק בתחום: "חדירה למערכות המחשב של האויב לשם איסוף מודיעין, שיבוש, הטעיה, מניעת שימוש והשהיית המידע. כל זאת במקביל למניעת הישג דומה של היריב במערכות שלנו".

טכניקות לוחמת מחשבים

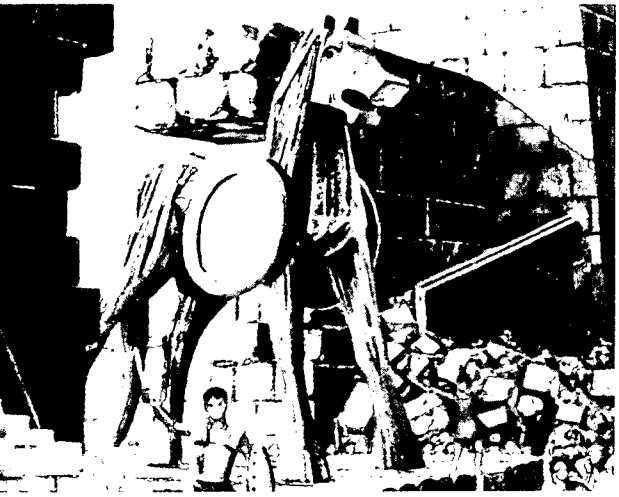
כיצד ניתן לפגוע במערכות מחשב? לשם כך ישנן טכניקות מגוונות, חלקן עתיקות יומין — עוד מלפני עידן המחשב — כמו, למשל, הרס פיסי באמצעות הפצצה. טבלה 5 מפרטת את הטכניקות המקובלות בתחום זה — החל משתילת וירוסים, סוסים טרויאניים ושאר מיני תוכנות מזיקות,[14] דרך שיתוק באמצעות פגיעה פיסית (קונוונציונלית או לא קונוונציונלית, כמו דופק אלקטרומגנטי או נשק ביולוגי, המשמיד רכיבים אלקטרוניים) וכלה בדרך הקלאסית המקובלת בלוחמה אלקטרונית (חסימה, שיבוש והטעיה). מטבע הדברים אתרכז במסמך זה רק בטכניקות מעולם המחשבים, משום שרק בהן יש משום חידוש מהפכני בשדה הקרב העתידי.

טכניקות מעולם המחשבים

טכניקות אלו מתאפיינות בדרך־כלל בהחדרה של תוכנה עוינת או מזיקה למחשב הקורבן. בהקשר זה יש לדון בסוג התוכנה המזיקה, בדרכי החדרתה למחשב הקורבן ובדרכים להפעלתה. להלן סוגי התוכנות המזיקות המוכרות לנו:

א. **סוס טרויאני:** תוכנה המבצעת משימה רצויה במקביל לביצוע חשאי של פונקציות בלתי רצויות, בלי שהמשתמש חש בכך.
ב. **וירוס:** קטע תוכנה (המוסתר בתוכנה לגיטימית), המשתכפל באמצעות הדבקת העתקים של עצמו לתוכנות אחרות בכל פעם שמופעלת התוכנה הנגועה.
ג. **תולעת:** תוכנה עצמאית, המשתכפלת מעצמה ללא צורך בהתערבות המשתמש תוך ניצול פרצות במערכת ההפעלה. התוכנה משתמשת בשירותי הרשת כדי להתקדם למערכות אחרות.
ד. **פצצה לוגית:** תוכנה פרזיטית, המחכה לאות הפעלה, שיכול להיווצר כאשר מתקיים תנאי לוגי כלשהו,[15] או כאשר מוכנס קלט מסוים למערכת.

וירוסים ותולעים גורמים בדרך־כלל נזקים מיידיים למחשבים



הטרויאנים בטוחים כי היוונים ויתרו על המצור. הם הורסים חלק מהחומות כדי להכניס את סוס העץ לעיר

הנגועים בהם ולמי שמחובר איתם ברשת. הסיכוי להחדיר אותם בדיוק ברגע הנכון אינו גבוה, ומשום כך תופנה להלן תשומת הלב יותר לסוסים טרויאניים ולפצצות לוגיות.

החדרת סוס טרויאני/פצצה לוגית[16]

החדרת סוס טרויאני יכולה להיעשות על־ידי הכללתו בתוכנה מראש או דרך מאגרי תוכנה שנועדו לשימוש ציבורי. כדוגמא לדרך הראשונה אפשר להביא את "מייקרוסופט", שכללה במערכת ההפעלה חלונות 95 פונקציות נסתרות לדיווח על התוכנות שבמחשב האישי. הדרך השנייה חושפת, למעשה, את כל מי שמעתיק תוכנה — ברשות או ללא רשות.

במקרים שבהם מדובר במחשב קורבן שהינו חלק מרשת, ניתן לחדור אליו דרך התקשורת. בכל מקרה אחר יש לבצע את החדירה באמצעות השתלת חומרה או תוכנה. השתלה כזאת יכולה להיעשות בכל אחד משלבי מחזור החיים של המערכת, וככל שהיא נעשית מוקדם יותר, היא קשה יותר לגילוי.

השתלת חומרה יכולה להיעשות ברמות שונות. למשל: הוספת יחידה, הוספת כרטיס מודפס ליחידה קיימת, הוספת מעגל משולב על כרטיס מודפס קיים או החדרת תוספת לתוך מעגל משולב.[17] ככל שהתוספת הפיסית קטנה יותר, קשה יותר לגלותה — לפחות ויזואלית. השתלה כזאת אקטואלית במיוחד בהתקנים ייעודיים (ASIC), המפותחים לשימוש ספציפי ונפוצים עתה מאוד — במיוחד בציוד ממוזער או בציוד אלקטרוני המיוצר בכמויות גדולות.

הפעלת התוכנה המזיקה

כאמור, במקרה של סוס טרויאני/פצצה לוגית ניתן להגדיר שורה של תנאים, שהתמלאותם תהיה trigger להפעלת התוכנה המזיקה. אם המחשב הקורבן הינו חלק מרשת, ניתן לבצע את ההפעלה באמצעות תקשורת חיצונית. במקרים אחרים אפשר להסתייע בסוכן פנימי לא רק לחדירה, אלא גם להפעלה.

במקרה של סוס טרויאני/פצצה לוגית ניתן להגדיר שורה של תנאים, שהתמלאותם תהיה Trigger להפעלת התוכנה המזיקה

האלמנט המושתל (חומרה או תוכנה) יכול לבצע פונקציות שונות: שיבוש, הטעיה או מודיעין. אלמנט כזה עשוי לפעול באופן עצמאי או בשילוב עם אלמנט אחר. למשל: אלמנט תוכנה, הממתין להופעת קוד מסוים, עשוי להפעיל וירוס לשיבוש, לשנות נתונים בטבלה (הטעיה) או להפעיל משדר להעברת נתונים מהמערכת (מודיעין). ככל שההשתלה תיעשה מוקדם יותר במהלך הפיתוח – ובמיוחד לפני גיבושן של תוכניות בדיקה – הסיכוי לגלותה בבדיקות שגרתיות יהיה קטן יותר.

התגוננות

ככלל, פעילות ההתגוננות נחלקת לשלושה מעגלים:

א. מעגל המניעה: הפעלת אמצעים (כמו, למשל, תוכנת firewall או תוכנת אנטי־וירוס) לעצירת התוקף לפני החדירה.

ב. מעגל הגילוי: זהו עקב אכילס של התחום כולו — כיצד נדע כי בוצעה תקיפת מחשבים?

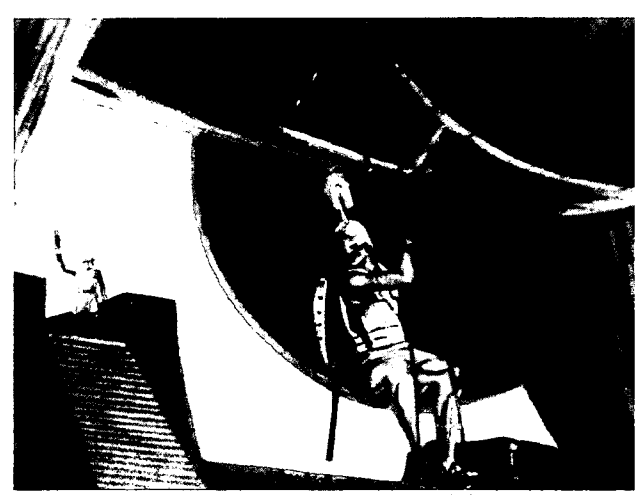
ג. מעגל התגובה: הכולל אמצעי התאוששות.

הבעיה מספר אחת בנושא ההתגוננות היא איתור הפגיעה. נניח שמתרחשת נפילת מחשבים מסיבית. מניין לנו שזו קרתה כתוצאה מלוחמת מחשבים ולא כתוצאה מאיזו תקלה מקרית?

הטכניקה הבסיסית לגילוי תקיפות מחשבים היא בדיקת תצורה תקופתית: "מצלמים" את תצורת המערכת במצב "תקין", ואחר־כך בודקים תקופתית שאין שינוי בתצורה. כדי שתהיה אפקטיבית, על בדיקה זו לכסות את כל רכיבי החומרה והתוכנה במערכת. כלי הבדיקה הידועים ביותר הן תוכנות אנטי וירוס, הבודקות תצורת תוכנה בלבד. תוכנות אלה פועלות בשיטות שונות — למשל חיפוש מאפיינים של וירוסים ידועים נוסף על בדיקת תצורה. מתנהל מאבק נמשך בין מפתחי הווירוסים, המוסיפים ל"מוצריהם" תחכום כדי למנוע את גילוים באמצעות תוכנות האנטי וירוס הקיימות, לבין ספקי תוכנות אלה, המפיקים בקביעות גרסאות חדשות, האמורות לזהות את הווירוסים החדשים על בסיס מאפיינים שלא נכללו קודם.

כלי גילוי אחרים בודקים את גודל התוכנות ואת מערכי הנתונים ועשויים להיות מבוססים גם על טכניקות שיגלו לא רק תוספות, אלא גם שינויים. ייתכנו גם תוכנות שיבדקו תקופתית — ובאופן אוטומטי — את תצורת החומרה, אם כי הדבר מחייב תוספות ברכיבי החומרה השונים, שיגיבו לפניות של תוכנת הגילוי. חשוב מאוד לקיים גם מנגנון תגובה מסודר להודעות גילוי, שיבטיח תגובה מהירה ויעילה.

מנגנון גילוי אחר מבוסס על ניהול יומן (log) מפורט של כל האירועים במערכת. מנגנון כזה עשוי גם להצביע על ניסיונות חדירה שלא הצליחו ולציין את מקורם. גם כאן לא מספיק לאסוף את הנתונים, אלא חשוב שיהיה מנגנון שיפרש את הנתונים ויגיב על אירועים חשודים.



באשמורת לילה יוצאים אודיסוס ואבריו מהסוס החלול כדי לפתוח את שערי העיר לפני חבריהם

זהו, הצלחתי להסיר את הבאג....

האמצעים העיקריים למניעת פגיעה מתקיפות מחשבים הם:

א. שימוש בסיסמאות לגישה ולהצפנת המידע. בדרך־כלל מקובל כי למגן בשיטות אלה יש יתרון על התוקף, ויתרון זה גדל עם התפתחות הטכנולוגיה.

ב. הגבלת גישה פיסית (כולל בזמן הובלה) נגד השתלות חומרה או תוכנה.

ג. בדיקה תדירה של בעלי זכות הגישה (משתמשים, מתחזקים, נותני שירותים).

ד. בקרת תצורה קפדנית של חומרה ושל תוכנה לכל אורך מחזור החיים.

ה. הפרדה מוחלטת בין מערכות מחשוב צבאיות לתקשורת האזרחית.

המשתמשים החוקיים מהווים סיכון גדול למערכות המחשוב. לכן יש להקדיש תשומת לב רבה להגברת מודעותם לנושא, להכשרה מקצועית ולבדיקות ביטחון קפדניות.

בעיות יסוד בתקיפת מחשבים[18]

תקיפת מחשבים כרוכה במספר בעיות יסוד, המיוחדות לה והשונות מהבעיות המוכרות בלוחמה קלאסית. בעיות אלה הן בעיקר בקרת תוצאות התקיפה (BDA), האפשרות לפגיעה עצמית והמגבלות החוקיות והאתיות החדשות הכרוכות בלוחמה מסוג זה.

בקרת תוצאות (BDA: Battle Damage Assessment)

כדי שאפשר יהיה להסתמך על תקיפת מחשבים בתכנון המשך הלחימה, דרוש דיווח על תוצאותיה. מבחינה זו, לתקיפה המבוצעת "בחוג פתוח", כלומר כזו שלא ידוע אם הצליחה, יש תועלת מוגבלת. בעיה זו חריפה במיוחד בתקיפות "רכות".

פגיעה עצמית (או פגיעה לא מכוונת במדינה ידידותית)

תקיפות בלתי ממוקדות במסגרת לוחמת מחשבים, כגון החדרת וירוס, עלולות לחזור לתוקף, אם יש קשר בין המערכות של שני הצדדים, למשל דרך רשת תקשורת עולמית. מבחינה זו דומה לוחמת המחשבים ללוחמה ביולוגית, שבה כלל ידוע הוא שאינך תוקף באמצעות חיידק שאין לך חיסון נגדו.

ללוחמה קונונציונלית יש "חוקי משחק" המוגדרים באמנות בינלאומיות שונות, שאינן רלוונטיות ללוחמת מחשבים

מגבלות חוקיות ואתיות

ללוחמה קונונציונלית יש "חוקי משחק" המוגדרים באמנות בינלאומיות שונות (ז'נווה, האג). אמנות אלו נוסחו בתקופה שבה איש לא חשב במושגים של לוחמת מידע, וכלליהן מתייחסים למאבק מזוין, לעימות פיסי, לפגיעה טריטוריאלית וכדומה. מושגים אלה אינם רלוונטיים ללוחמת מחשבים. ייתכנו כמה סיבוכים אפשריים:

א. השימוש הצבאי הנרחב בתשתיות אזרחיות (בעיקר לתקשורת) מקשה על ההבחנה בין פגיעה באובייקטים צבאיים לפגיעה

באובייקטים אזרחיים.

ב. במקרים רבים קשה לדעת מיהו התוקף, בשליחות מי פעל, ומהיכן תקף, ובוודאי שקשה להוכיח דברים אלה.

ג. אין פרופיל ברור ל"לוחם". אזרחים (גם ילדים ונשים) יכולים להיות יעילים כלוחמי מחשבים לא פחות מחיילים. האם זה הופך אותם למטרות לגיטימיות?

ד. "לוחם מחשבים", הפועל באמצעות רשת תקשורת עולמית, למשל באינטרנט, כלל איננו יודע באיזה מסלול יעברו התשדורות שלו. כך הוא עלול לערב בסכסוך — ללא ידיעתו — גורמים חיצוניים שאינם מעוניינים בכך שהתשדורות יעברו דרך צמתים בשטחם. גורמים אלה אינם מסוגלים למנוע מעבר תשדורות באופן סלקטיבי, ללא פגיעה במשתמשים שלהם באותה תשתית תקשורת.

ה. לוחמת מחשבים יכולה להתנהל גם בין מדינות ידידותיות. האם ראוי בכלל לקרוא לזה "לוחמה"?

נראה שהאמנות הבינלאומיות אינן מהוות במצב הנוכחי מגבלה משמעותית ללוחמת מחשבים. ייתכן מאוד שבעתיד יותאמו אמנות אלה למלחמות "הגל השלישי" ויגדירו בצורה מפורשת פעולות אסורות.

הערות

1. הוצאת ספריית מעריב, 1994. לקורא המעוניין בתמצית משנתם על רגל אחת מומלץ לעיין בספר: Alvin and Heidi Toffler, **Creating a New Civilization - The Politics of the Third Wave**, Turner Publishing Inc., 1995

2. ניתן להבחין בין מידע (Information) או נתונים (Data) לבין ידע (Knowledge) המחייב גם המשגה והבנה של המידע הגולמי. לצורך מסמך זה ההבחנה אינה עקרונית.

3. ליתר דיוק, במהלך המלחמה ייצרו האמריקנים 86,330, טנקים ו־296,400 מטוסים. ראו דיוויד זיוק, רובין הייאם, **קיצור תולדות המלחמות**, הוצאת מערכות, 1981 (הופיע במקור ב־1966)

4. פופר פיתח את רעיונותיו בסדרה של מאמרים שפורסמו בשנות ה־50 וה־60. העיקריים שבהם (במיוחד "Epistemology Without a Knowing Subject" ו־"On the Theory of the Objective Mind") כונסו והופיעו מחדש כפרקים מס' 3 ו־4 בהתאמה בספרו: **Objective Knowledge - An Evolutionary Approach**, Oxford University Press, 1972

5. **שם**, עמ' 107

6. **שם**, עמ' 107־108

7. Paul M. Romer, "Endogenous Technological Change", **Journal of Political Economy**, 1990, Vol. 86, no. 5, pt 2, pp. S71-S102

8. דהיינו המידה שבה ניתן לחלק את המוצר שוב ושוב מבלי לגרום להתמעטותו. רומר משתמש כאן בביטוי הטכני Non-Rival.

9. **מלחמה ואנטי מלחמה**, עמ' 73־74

10. ראו למשל את התיאור של שיטות הלוחמה הקלאסיות לצד השיטות החדישות יותר בספר היסוד של הצבא האמריקני FM 100-6: Field Manual No. 100-6, **Information Operations**, US Army, 1997
הספר מכיל (בסופו) רשימה ענפה של ספרות מומלצת, הכוללת הנחיות של משרד ההגנה האמריקני, פרסומים אסטרטגיים, ספרות גלויה, ספרות צבאית ומסמכים אחרים הרלוונטיים ללוחמת מידע.

11. דיון מעניין בנושא של תת־התחומים (וההגדרות המתאימות) של לוחמת המידע ניתן אצל ד"ר מ' ורנר, **סקר ספרות בנושא לוחמת מידע**, רפא"ל, דו"ח מס' 97/88/1230, ספט' 97'

12. ללוחמת מחשבים גם אין קו "חזית" מוגדר, ואין בה (כמעט) משמעות למרחקים גיאוגרפיים.

13. תקיפת מחשבים יכולה להתבטא ב"נפילות מחשב", בשינוי בלתי מורגש של הנתונים האגורים במחשב ובשאר תופעות ממין זה, העלולות להיות בלתי מורגשות או להתפרש כתקלות "טבעיות".

14. בספרות מקובל להשתמש במונח Malicious Software.

15. כאשר התנאי הוא תאריך נתון, נהוג לדבר על "פצצת זמן".

16. בדיון להלן בנושא החדרת התוכנות המזיקות והפעלתן – ובמיוחד בדיון (שיובא בסוף המסמך) על טכניקות ההתגוננות בלוחמת מחשבים – נסמכתי במידה רבה על ד"ר מ' ורנר, **סקר ספרות בנושא לוחמת מידע**, רפא"ל, דו"ח מס' 97/88/1230, ספט' 97'

17. כך, למשל, ניתן להשתיל חומרה ביחידה של ספק המתח (שבה יש בדרך־כלל מקום פנוי).

18. ראו ד"ר מ' ורנר, **סקר ספרות בנושא לוחמת מידע**, רפא"ל, דו"ח מס' 97/88/1230, ספט' 97'