מבוכו של המינוטאור
או: פרדוקס הסייבר – עיון מערכתי באתגרים ובהזדמנויות של המרחב המקוון

ליאור לבד[1]

תקציר 2
א. תורת המערכות המורכבות – התפתחות ומאפיינים 3
על זהירות, צניעות ומתודולוגיות יישום 7
ב. התבוננות מערכתית במרחב הסייבר 8
על מלחמה בוירוסים – ממערכות הגנה בסייבר למערכת החיסונית של גוף האדם 8
לוחמת מידע וחופש מידע – התבוננות מערכתית על מרכיבי מימד הסייבר 13
סיכום 21

[1] סרן ליאור לבד משרת כעוזר מחקר במרכז דדו.

תקציר

למרות הנטייה להבין את מרחב הסייבר על פי ניתוח פרטני של מרכיביו, יש לאמץ את גישת המערכות המורכבות. גישה זו לא מסתפקת בהבנת סכום המרכיבים של מערכת נתונה אלא מתמקדת ביחסים שמתקיימים בין המרכיבים. הטענה העיקרית במאמר היא שחסרה גישה מערכתית לאבטחת מידע, וכן שכדי להבין את מרחב הסייבר כמערכת אפשר להשוות אותו למערכות מורכבות אחרות, כמו המערכת החיסונית של גוף האדם. הבנה הזאת מאתגרת את תפיסת ההגנה בעומק, שמבקשת ליצור מענה אבטחתי לכל מרכיב ומרכיב, על בסיס שכבות הגנה (לדוגמה באמצעות תוכנת "אנטי וירוס"). מצד שניאידך, תורת המערכות מגלה את האפשרות של "הגנה קדמית", שפועלת כמו המערכת החיסונית הגופנית למניעת חדירה של גורמים עוינים באמצעות שכבת הגנה קדמית אחת חזקה.

"אתם חייבים לשמוע מה אחיין שלי עשה אתמול!" צעק לפני כמה שבועות מכר שלי בכניסתו לבית. "נו, מה?" שאלתי באדישות, מוכן לעוד סיפור על חיתולים ונפלאות המגבונים הלחים. "הוא ישב ממושכות מול החלון והביט בנוף, אחר כך דידה לעברו, הושיט יד, והחליק כמה פעמים את אצבעו על החלון משמאל לימין, כאילו מנסה להחליף את הנוף על גבי מסך האייפד!" התלהב הדוד. כולנו צחקנו, לא עברו רגעים ספורים ועלתה בי המחשבה – "העתיד" כבר כאן.

על פי נתונים שהציג מולי אדן, נשיא אינטל ישראל, בכנס הסייבר הבינלאומי האחרון שנערך באוני' ת"א, בזמן שקראתם על סיפורו של אורי והחלון בפסקה הראשונה, באתר יוטיוב הועלו מעל 30 שעות של סרטוני וידאו, בטוויטר פורסמו מעל מאה אלף טוויטים, ובסביבות השישה מיליון דפים נצפו ברשת הפייסבוק. אורי לא הספיק להושיט ידו את החלון ומעל 20 מליון תמונות נסרקו בפליקר, כ- 47,000 אפליקציות הורדו לסמארטפונים שונים, וכ- 45 תוכנות זדוניות (Malware) חדשות הועלו לרשת. בכל דקה שעוברת, היקף תנועת המידע המועבר על פני הרשת יכול למלא 230,000 דיסקים – מספר יחסית קטן, לעומת התחזיות המביטות אל עבר שנת 2015 (!), בה צפויים להיות 15 מיליארד מכשירים שונים מחוברים לרשת האינטרנט, היקף תעבורת התקשורת הניידת (סמארטפונים, טאבלטים ודומיהם) צפוי לזנק פי 11, ואילו היקף כלל התקשורת העולמית צפוי לגדול פי שלושה.

הגידול האקסטנסיבי הצפוי בנפח תעבורת המידע איננו פועל יוצא רק של גידול בכמות המשתמשים על פני הגלובוס כולו, אלא בשינוי מן היסוד הצפוי בחוויית התקשורת בקרב משתמשים בעולם המפותח. חזון ה"אינטרנט של הדברים" (IOT - Internet Of Things), או "האינטרנט של הכל" (IOE – Internet Of Everything), אשר הואץ במיוחד במהלך השנה החולפת, צפוי להתממש הרבה יותר מהר מכפי שדמיינו אותו. בקרוב, נוכל להציץ על הולוגרמה שקופה על ידנו ולדעת את רמת הסוכר בדם או אחוזי שומן הגוף, המקרר שלנו יזמין בעצמו קניות בסופר, הרכב שלנו יאותת לבית שלנו שאנחנו מתקרבים והכניסה לחניה תחכה פתוחה, או שהקומקום כבר ירתח, ואילו העיר שבה נגור תנתב אותנו הרחק מפקקים באמצעות מערכת רמזורים חכמה ותדע לנצל חשמל ומים ביעילות מרבית.

כיום, כ – 85% מכלל המכשירים החשמליים בעולם אינם נכנסים לקטגוריית ה – IOT, שכן הם אינם עומדים בשלושת תנאי הסף – יכולת חישוב, תקשורת וחיבור לענן מידע (Data Cloud). עם זאת, כבר בשנת 2020 צפויה האנושות להשתמש בכ – 50 מיליארד מכשירים מבוססי עיבוד ותקשורת, אשר יהיו

מחוברים לענן מידע עצום. אגב, כבר ישנם התוהים על השמות שינתנו ליחידות המידה הגדולות יותר שתבואנה לאחר היוֹטה-בייט (יוטה-בייט אחד שווה לאלף מיליארד טרה-בייט, או בקיצור, 10^{24} בייטים, בשיטה העשרונית).

הנוחות הדיגיטאלית הזו, כאמור, תהיה ככל הנראה חלק בלתי נפרד מעולמנו ושגרת חיינו בעוד לא זמן רב כלל. אך כגודל ההבטחה אותה מביאה קדמה זו, כך גם גודל הסיכון הטמון בחובה. הסיכון אינו קיים רק בכך שהמקרר שלי יזמין מהחנות שבעים טון פסטרמה, או בכך שהרכב שלי יתעקש שוב ושוב להביאני לביתה של חמותי (שתחיה) במקום לזה שלי. הסיכון אף אינו טמון כולו רק בשדות הריגול, גניבת הזהויות ואיסוף המידע כפי שאנו, אנשי הצבא, עלולים לחשוב.[2] מהותו של הסיכון במסירת השליטה על הסדר בכל מישור המוכר לנו, הוא באבדן השליטה על תפיסת העצמי – כפרט, כחברה, כאומה, ומרחיקי הלכת יאמרו – כאנושות.

עם זאת, אין בכוונתי לגזול את מנת לחמם לא של פילוסופים, לא של פסיכולוגים, וגם לא את זו של חברות הביטוח. על כן, במאמר זה אתמקד, באמצעות גישת המערכות המורכבות, בהבניית מערכת מושגית שתאפשר, כך תקוותי, להאיר ולבאר את חוסר הנוחות המאפיין את "בעיית הסייבר". חוסר נוחות זה נובע משלל המתחים המתקיימים וגוברים ככל שהולך וגדל מספר הילדים שמנסים להחליף נוף בחלון. פרטיות מול נוחות, אישי מול משותף, חשאיות מול אפקטיביות מבצעית– כל אלה, ועוד רבים נוספים, הם מתחים ודילמות איתם אנו מתמודדים כבר היום הן בחיינו הפרטיים, הן בעבודתנו במערכת הביטחון. העדר הגבולות והפוטנציאל האינסופי הטמונים במרחב הסייבר מביאים עמם אולי את השאלה הפרדוקסאלית שטרם נענתה – כיצד חובתה של מדינה לפעול במרחב חדש מתיישבת עם אופיו החותר, לכאורה, תחת עצם קיומה?

אופיו הכאוטי, אינספור הגורמים המרכיבים אותו, נטייתו להתארגנות עצמית, ומאפיינים נוספים, מעמידים את ניתוח מימד הסייבר כמקרה בוחן טוב לחקירה של מערכות מתהוות. על כן, המתודולוגיה המוצעת במאמר זה לניתוחו היא מתודולוגיה הוליסטית – מערכתית, המבוססת על תורת המערכות המורכבות, עליה ארחיב בחלק הראשון.

חלקו השני של המאמר יפתח בהרחבה על מימד ההגנה בסייבר. באמצעות סקירה של תהליך למידה שנעשה בחיל הים האמריקני לצורך פיתוח תפיסה מערכתית להגנה בסייבר והרחבה על התפתחות תפיסת 'מחשוב ענן' והגנתו, יראה הפרק את המעבר המתבצע בימינו ממש ממודל חשיבה של "הגנה בעומק" למודל חשיבה של "הגנה קדמית" בתחום אבטחת המידע. שאר מרכיבי מרחב הסייבר, כגון איסוף, הרתעה, השפעה ומלחמה בהאקרים יידונו, בהקשר ניתוח מערכתי, באחריתו של החלק. נדבכים אחרים בפעילות במרחב הסייבר נעדרים ממאמר זה עקב מגבלות שונות.

א. תורת המערכות המורכבות – התפתחות ומאפיינים

בתחום חקר החברה והדינאמיקות החברתיות המאפיינות חברות שונות, קיימות גישות רבות ואסכולות מנוגדות זו לזו בפירוש התופעות הנצפות. עם זאת, במשך מאות שנים קיימת הסכמה בסיסית אחת לגבי התנהגות "החברה"- בהסתמך על חוקיות כזו או אחרת, ניהול חברתי נבון הינו בר השגה. אי ההסכמה

---

[2] הגנרל דיוויד פטראוס, בשעתו כראש ה – CIA, כבר התבטא בעניין "שינוי תפיסת הסודיות" לה אנו נדרשים לאור העידן הדיגיטאלי אליו אנו צועדים, בהקשר ליכולות הצפויות שתהיינה לארגוני ביון שונים. להרחבה ראו:
Spencer Ackerman, "CIA Chief: We'll Spy on You Through Your Dishwasher," *Wired*, 15.03.2012. http://www.wired.com/2012/03/petraeus-tv-remote/

סבבה תמיד סביב מהות החוקים הללו. תפיסה זו, ניתן לתמצתה בנוסחה פשוטה: פעולה מוגדרת בהכרח תביא לתוצאה מוגדרת. כך עולה מתפיסת העולם הלינארית הקרטזיאנית[3].

כמות המידע האינסופית המעשירה את עולם המחקר, מורכבות הניתוח והמבנים התיאורטיים הרבים אליהם נדרשים חוקרים בעבודותיהם, הופכים את המדע המודרני לגלגל הולך וגדל המכיל יותר ויותר תחומים מחקריים חדשים ומחודשים. כך, מוצא עצמו המדע מתחלק שוב ושוב לכמות עצומה של ספירות המתפצלות לתת- ספירות וכן הלאה. עם זאת, סקירת התפתחותו של המדע המודרני מעלה את העובדה המפתיעה לפיה, למרות היעדרותה של המשגה כללית ועצמאותם של תחומים אלה מאחרים, בעיות, תהיות ותפיסות עולם דומות, ולעיתים אף זהות, מועלות באופן נרחב בתחומי מחקר שונים, שלכאורה אינם משתפים בינם שום מאפיינים דומים.[4] גישה אנליטית- מכניסטית ישנה זו הולידה במהלך המאה העשרים ספקנות בקרב הקהילה המדעית באשר ליכולתה לענות על האתגרים אותם מציבה חדשות לבקרים מורכבותן של החברה והטכנולוגיה המודרניות. כתוצאה מכך גברה ההכרה בדבר הצורך בהבנה חדשה, המבוססת על גישות מערכתיות כוללות ובעלות אופי בין- תחומי נרחב.[5] אחד מחלוצי ומפתחי גישת המערכות הכללית, פון ברטלנפי, כתב בספרו המרכזי בתחום כי "מדובר בשינוי בקטגוריות החשיבה הבסיסיות, ומורכבותה של הטכנולוגיה המודרנית הינה רק אחת מגילויו ואולי לא החשוב שבהם. אנו נאלצים, בצורה זו או אחרת, להתמודד עם מורכבויות, עם מכלולים או מערכות, בכל תחומי הידע. דבר זה מחייב אוריינטציה מחודשת לחשיבה המדעית."[6] התפתחותה של הבנה מערכתית חדשה זו הולידה את הצורך בניסוחה של תיאוריה כללית למערכות, אשר לא בהכרח תבטל את התיאוריות הקודמות למערכות ספציפיות, אלא תפעל במקביל להן, אם לא תאגדן תחת המשגה מחקרית אחת, על בסיס עקרונות אוניברסאליים. כך, בתחילת שנות החמישים חברו לודוויג פון ברטלנפי (ביולוג), אנטול רפופורט (מתמטיקאי), קנת בולדינג (כלכלן) וראלף ג'רארד (פיסיקאי) כדי לייסד את התחום המדעי החדש. למעשה, גישתם אינה מהווה תשובה נגדית לדרך המחשבה הקרטזיאנית שהוצגה לעיל, אלא מהווה תשובה מודרנית, או ביטוי מודרני, לאותו הלך הרוח.

ברטלנפי מגדיר מערכת כמכלול של אלמנטים אינטראקטיביים. לכן, הבעיות אשר בפניהן ניצבת מערכת כלשהי הינן, לשיטתו, בעיות של יחסי גומלין בין מספר רב של משתנים, הקיימים בתחומי הפוליטיקה, הכלכלה, התעשייה, המסחר, הניהול הצבאי, וכו'. ברטלנפי מציע כלי חשיבה לצורך הערכה וביקורת של מערכות, בהתבסס על שלושה פרמטרים: הראשון הינו הפרמטר הכמותי, העוסק במספר האלמנטים המרכיבים את המערכת; השני הינו החומר, שכן הוא עוסק באופי האלמנטים; והשלישי הינו הפרמטר האיכותי או, ליתר דיוק, מהותי, והוא מתמקד בתכונות היחסים שבין האלמנטים השונים במערכת.[7] בעקבות זאת מגדיר ברטלנפי שתי קטגוריות בסיסיות של מערכות אוניברסאליות, מערכות פתוחות ומערכות סגורות: "אנו מבטאים זאת על ידי האמירה שמערכות חיות הינן למעשה מערכות פתוחות. מערכת פתוחה מוגדרת כמערכת המצויה במצב של חילופי חומר עם סביבתה, כולל

---

[3] K. A. Richardson, Mathieson, G. & Cilliers, P. "Theory and practice of complexity science: Epistemological considerations for military operational analysis," *SysteMexico*, vol. 1, No. 1, 2000, pp. 25-66.

[4] L. von Bertalanffy, **General System Theory- Foundations, Development, Applications**, (New York: George Braziller, 1968), p. 30.

[5] שמעון נוה, **אמנות המערכה- התהוותה של מצוינות צבאית**, (תל אביב: "מערכות"/ משהב"ט, 2001), עמ' 24.

[6] שם. (תרגום הציטוט מתוך Bertalanffy, 1968; 3.).

[7] שם, עמ' 24- 25.

יבוא ויצוא, בניה והריסה של מרכיביה החומריים... מערכות סגורות הינן כאלה שניתן להחשיבן כמבודדות מסביבתן."[8]

במרוצת השנים ידעה תורת המערכות הכללית פיתוחים, שינויים ו"תיאוריות נגזרות" שהתפתחו ממנה. בשל קוצר היריעה לא ארחיב כאן על כל שלבי ההתפתחות, אך לא ניתן שלא להזכיר את תיאוריית הקיברנטיקה שהתפתחה בשנות הארבעים, תחום הדינאמיקה המערכתית שהחל להתפתח בשנות השישים, ותיאוריית הכאוס שהפכה פופולארית במיוחד בשנות התשעים.[9]

כאמור, תורת המערכות הכללית משנות החמישים לא ייצגה אלטרנטיבה לצורת החשיבה הקרטזיאנית הדטרמניסטית, אלא היוותה ביטוי מודרני לדרך החשיבה הישנה. לאורך הזמן, ועם ההתפתחויות התיאורטיות במהלך העשורים האחרונים, התפתחה גישה אלטרנטיבית, "מדעי המורכבות" או "Complexity Sciences", אשר הולכת וחודרת יותר ויותר למדעי החברה. ליבת הגישה היא בהכרה בעובדה שישנן מערכות (פיזיות, ביולוגיות וחברתיות)[10] שאופן התנהלותן אינו עומד בקנה מידה אחד עם התפיסה הלינארית המאפיינת את התנהלות המערכות לפי ברטלנפי. המערכות המורכבות נקראות כך מעצם אופי התנהלותן- מורכבת ואי-ליניארית. לפי תיאוריה זו, ובניגוד לתפיסה הקרטזיאנית, הקשר בין פעולות לתוצאותיהן נע על פני רשת (Network[11]) בה מתקיימים אינספור קשרי גומלין שונים בין מכלול רב של אלמנטים. במילים אחרות, במערכת נתונה הכל משפיע על הכל – מעין "אפקט הפרפר". בשל כך, גירוי מזערי ביותר בחלקה האחד של המערכת, עשוי להוביל לתוצאות מרחיקות לכת בחלקיה האחרים, ואף עלול לפגוע ביציבות המערכת כולה או להביא להשמדתה. כך, לדוגמא, פגם גנטי זניח, הגורם למחסור באנזים מסוים בגוף, שבלעדיו האדם אינו מסוגל לעכל מרכיב מזון כלשהו, עלול לגרום למותו עם אכילת מזון המכיל מרכיב זה. כך גם שריפתו העצמית של אדם מן הישוב בתוניסיה בדצמבר 2010 הביאה דרך סדרת אירועים בלתי צפויים לשרשרת אירועים היסטוריים במהלך השנים האחרונות, המכונים "האביב הערבי" או "הטלטלה האזורית". הקשר הבלתי- קווי (הפעלה שולית שעשויה להביא לשינוי משמעותי או להפך) עושה את המערכות המורכבות לבלתי צפויות פר הגדרה[12].

כדי להבין התנהגותן של מערכות מורכבות יש צורך בהבנה לא רק של התנהגות החלקים המרכיבים את המערכות, אלא בהתנהגותם המשותפת המעצבת את התנהגות הכלל. איננו יכולים לתאר את הכלל בלא לתאר כל מרכיב ממנו, ואין אנו יכולים לתאר כל מרכיב שהוא אלא ביחס לשאר המרכיבים.[13] על כן, תמציתה של המערכת טמונה יותר ביחסי הגומלין בין מרכיביה מאשר בכל דבר אחר.

תכונה נוספת של המערכות המורכבות היא קיומן המתמיד "על סף התוהו". משום שהשינויים הבלתי צפויים במערכות מורכבות הם באופן התפקוד הנורמטיבי שלהן, המערכות תמיד מתנהלות "על הקצה".

---

[8] שם. (תרגום הציטוט מתוך. Bertalanffy, 1968; 14, 38).

[9] אבי אלטמן, "גישת המערכות – היסטוריה, עקרונות ופרקטיקות של חשיבה מערכתית," *חשיבה מערכתית – חומר עזר מקצועי*. צה"ל/אמ"ץ- תוה"ד/ מרכז דדו לחשיבה צבאית בינתחומית. אוקטובר 2014. מסמך פנימי.

על הקיברנטיקה ראו:

Norbert Wiener. **Cybernetics: Or Control and Communication in the Animal and the Machine**. (Paris: (Hermann & Cie) & Camb. Mass. MIT Press, 1948).

על ייסוד גישת הדינאמיקה המערכתית ראו:

Jay W. Forrester, **Industrial Dynamics**. (Waltham, MA: Pegasus Communications, 1961)

על ייסוד תיאוריית הכאוס ראו:

James Gleick, **Chaos: Making a New Science**, (New York: Viking Penguin Inc., 1987).

[10] M. A. Boden, "Autopoesis and life," *Cognitive science quarterly*, Vol. 1, 2000, pp. 117-145;

[11] Y. Bar- Yam, **the Dynamics of Complex Systems**, (Westview Press, 1997).

[12] C. Gershenson & Heylighen, F., "How can we think complex?" In: A. K. Richardson (Ed*.),* **Managing organizational complexity: Philosophy, theory, and applications- A Volume in Managing the complex**, (Greenwich, Connecticut: Information Age pub., 2005), pp. 47-61.

[13] Bar- Yam, 1997; 1.

כלומר, לא ניתן לצפות ממערכות מורכבות שתתנהגנה על פי תכנית כלשהי, ותגובתן תמיד תהא פרטיקולארית, ובהתאמה לנסיבות הנתונות לאותו מצב ורגע. כך, לדוגמא, מבלי להתכוון לכך, כבר במאה ה- 18 ניסח קלאוזביץ טענה מערכתית מורכבת בקביעתו כי שדה הקרב הינו ממלכת אי הודאות, בו לעולם לא יקרו הדברים כפי שתוכננו מבעוד מועד.

אופיין הכאוטי של המערכות המורכבות, והתהייה על השאלה "אם כך, אז איך זה בכל זאת עובד?", נענו בתשובה- מחקר בתחום המערכות המורכבות מראה שכנגד הכאוס והאי-סדר המובנים בתוכן, עומד כוח מאזן ומסדר המכונה "התארגנות עצמית".[14] כוחה של ההתארגנות העצמית גדול ולא נחות מכוחו של אי-הסדר. לדוגמה, הדמוקרטיה החברתית היא צורה של התארגנות עצמית המהווה ערך תרבותי המקודש לחברה המערבית. דוגמא נוספת מתבטאת במיליציות אזרחיות המתארגנות לצורכי הגנה עצמית בשעת מצוקה והיחלשות השלטון המרכזי. כבר מאז "מצב הטבע" של תומאס הובס והתארגנותם העצמית של הפרטים לכדי חברה אחת, ספרות אקדמית ענפה מתארת מקרים המדגימים כיצד מתוך קבוצות מבוהלות של פרטים (תמיד) צומחת מנהיגות המפחיתה את הכאוס ואי-הסדר.[15]

התארגנות זו נעשית על פי עקרון המשיכה ל"מוקד כוח" (Attractor) החזק ביותר מבין כלל הגורמים האחרים הפעילים בהקשר קונקרטי. המושג "מוקד כוח", בו משתמשת תורת המערכות המורכבות יכול להיות מקורב במידה מסוימת למושג "מוטיבציה". אלא שמוקד הכוח מושך אליו כמו מגנט, וזאת משום שהוא נתפס על ידי המערכת כמוקד "ההצלה" החזק ביותר בעת הנתונה. מאחר והמערכת כולה נמצאת על סף קריסה מתמדת, היא נעה ללא הרף בין "מוקדי כוח" שונים. התחלופה הקבועה בין מוקדי הכוח נובעת מהעובדה כי התנהגות זו היא פועל יוצא של השפעתם הבלתי פוסקת של כוחות חיצוניים ופנימיים רבים, מגוונים ועצמתיים, באופנים שונים ובקשרים רשתיים (בלתי- קוויים) על מרכיבי המערכת המורכבת. אך גם כאן חל עקרון התזה והאנטי-תזה - פרט למוקדי הכוח, אלמנט נוסף אשר משפיע על התנהלותה של המערכת ותמרונה בין מוקדי כוח, הוא אלמנט מוקדי הדחייה (Repulsion)[16]. מוקדי הדחייה משפיעים על המערכת בצורה הפוכה מהשפעת מוקדי הכוח, ובמקום למשוך את מרכיבי המערכת להתארגנות עצמית סביבו, הם דוחפים אותה מעצמם ובכך משפיעים על עיצובה העצמי של המערכת. אגב, לפי גישה זו, סוד הצלחתו של ארגון דאע"ש, הוא בהיותו גורם 'מושך' היוצר סדר (לפי ראיית עולמו) במערכת הכאוטית הנקראת 'המזרח התיכון של ימינו'. וכמו כל גורם מושך אחר, הוא מצוי בתחרות מול גורמי מושכים ודוחים אחרים, המעצבים את המערכת האזורית לא פחות ממנו.[17]

כאמור, מערכות מורכבות מתאפיינות בכמות אינסופית של אלמנטים, ובכמות אינסופית של קשרים בין האלמנטים הללו. מצב זה מקשה עד מאוד, ויש האומרים עושה לבלתי אפשרי[18], את יישום שיטת המחקר המדעית הבסיסית ביותר- הפשטה ("רדוקציה"). באופן מסורתי, בהתבסס על השקפת העולם הדטרמיניסטית, הפשטה לצורך מחקר נועדה בכדי לאפשר את למידתו והבנתו של חלק כלשהו מן

---

[14] L. M. Rocha, "Selected self-organization and the semiotics of evolutionary systems," In S. N. Salthe, Van de Vijver, G., Delpos, M. (Eds.), **Evolutionary Systems: Biological and Epistemological Perspectives on Selection and Self-organization**. (Boston, Mass.: Kluwer Academic Publishers, 1998), pp. 341-358.

[15] S. Guastello, "Self-organization and leadership emergence in emergency response teams," *Nonlinear Dynamics, Psychology, and Life Sciences,* Vol. 14, No. 2, 2010, pp. 179-204.

[16] V. Dimitrov, **A New Kind of Social Science- Study of Self- Organization of Human Dynamics,** (Morrisville, NC: Lulu Press Morrisville, 2005), p. 22.

[17] Felix Lebed & Michael Bar-Eli, **Complexity and Control in Team Sports – Dialectics in Contesting Human Systems,** (London, New York: Routledge, 2013, 2014). pp. 11-18.

[18] L. Biggero, "Sources of complexity in human systems," *Nonlinear dynamics, psychology and life sciences*, Vol. 5, No. 1, 2001, pp. 3-19.

השלם, למען הכללת התובנות הנגזרות מן הניתוח, על השלם כולו. אולם בשל הכמות האינסופית של חלקים וקשרים במערכות המורכבות, הן אינן בנות הפשטה.[19] לכן, במהלך העשורים האחרונים התפתח מספר רב של מתודולוגיות מודרניות להתמודדות עם מערכות מורכבות.

על זהירות, צניעות ומתודולוגיות יישום

"המערכת המורכבת" כשמה היא- מורכבת, בלתי צפויה בעליל, ובלתי ניתנת לחקירה והבנה על ידי שיטות המדע המסורתיות. בהשאלה מן העולם הצבאי – מתודולוגיית "הערכת המצב" המסורתית אולי רלוונטית ומתאימה ללמידת מצבה הפיסי של דיביזיית האויב שמעבר לגבעה, אך כשמדובר בלמידה על ארגון דאע"ש, למשל, או על התפתחות איומי טרור בחבלי ארץ שוממים – הערכת המצב עלולה לספק מענה חלקי בלבד, שיכול להיות רלוונטי לגיבוש מידע, אך לא תורם לפיתוח הידע. חשוב לציין, כי ליישומה בפועל של תורת המערכות המורכבות קיימות מתודולוגיות יישום רבות. הקלות היחסית בה נופלים שבי, פרקטיקנים ומומחים כאחד, בידי מתודולוגיית יישום אחת בה הם רואים חזות הכל, ומוצאים עצמם לעתים "דוחסים" מציאות אל מידותיה של השפה אליה הם מורגלים, מקנה חשיבות לזהירות וביקורתיות עצמית.

במרוצת העשורים האחרונים התפתחו פרקטיקות שונות לניתוח מערכות מורכבות ולהתמודדות עמן. כנראה בגלל התחרות הקשה וההתמודדות היומיומית עם מציאות של "על סף תהום", התחום העיקרי בו התפתחו פרקטיקות אלו הוא התחום העסקי. במסגרתו, פורסמו במהלך השנים עשרות רבות של ספרי ייעוץ על התמודדות "נכונה" של ארגונים עם המציאות המשתנה הסובבת אותם.[20] למשל, פרקטיקה בולטת העולה מהררי ההמלצות, היא כי מתוקף אופיה הרב-תחומי של גישת המערכות (שכן מערכת מורכבת מאופיינת באלמנטים משלל תחומים מגוונים), הבכיר הארגוני או הדירקטוריון אינו עוסק ב"קבלת החלטות" ובניית תכניות ליניאריות ארוכות טווח, אלא ב"עיצוב" (Design) מתמשך, הער לשינויים המתרחשים תוך כדי תנועה, ומנווט את ספינת הארגון דרך המים הגועשים של המציאות המתהווה.[21]

פרט לארגונים עסקיים, גם צבאות מודרניים אימצו את גישת העיצוב המערכתי. כנראה בשל רוח התקופה המהפכנית, הנחשון בתחום היה הצבא הסובייטי, אשר אימץ את הגישה ופיתח את התחום עוד בשנות השלושים של המאה הקודמת ובתקופת מלחמת העולם השנייה.[22] מתודולוגיות של חשיבה מערכתית לתכנון (עיצוב) מערכה נוצרו בהמשך גם בצבאות הישראלי והאמריקאי, ובראשם ה- SOD (System Operational Design) – עיצוב מערכתי אופרטיבי). פיתוחים נוספים לתפיסה זו נוצרו בהמשך השנים.

---

[19] כאמירתו המפורסמת של העיתונאי והסופר הנרי לואיס מנקן:
".For every complex problem there is an answer that is clear, simple, and **wrong**"

[20] בין רבים אחרים, ראו למשל:
Senge, Peter M. **The Fifth Discipline: The art and practice of the learning organization**, Doubleday, New York, 1990; Russell L. Ackoff, **Systems Thinking for Curious Managers**. Triarchy Press, 2010; Jamshid Gharajedaghi, **Systems Thinking: Managing Chaos and Complexity - A Platform for Designing Business Architecture**. Butterworth-Heinemann, 2005;

[21] לדוגמא, ראה ספרו של הפילוסוף האמריקאי צ'רצ'מן, שפורסם כבר בשנת 1971:
C. West Churchman, **The Design of Inquiring Systems: Basic Concepts of Systems and Organization**. (New York: Basic Books, 1971).

[22] להרחבה יתרה, ראו: נווה, 2001**;** רפי רודניק, "אבולוציית המערכה הצבאית – הזיקה בין הפעלת הכוח הצבאי למאפייני סביבת המלחמה," *בין הקטבים*, גיליון 2 – שינוי והשתנות, יולי 2014, עמ' 135-133.

ידיעת העקרונות של חשיבה מערכתית איננה מבטיחה שאכן נחשוב מערכתית. במהלך השנים התפתחו מתודולוגיות שונות לניתוח מערכתי, אשר באו מגישות שונות לתורת המערכות. עם זאת, כל המתודולוגיות השונות כוללות שיטה לניתוח מערכות, איתור הבעיה/ תהליך למידה והתאמת פתרונות למצבים נתונים. בברירה שבין המתודולוגיות השונות, ניתן להפעיל שלושה מבחנים של ישימות בתהליך העבודה על פי מתודולוגיה: א. האם ביחד עם המתודולוגיה אנו מפעילים גם חשיבה מערכתית? ב. האם בחרנו את המתודולוגיה המתאימה למערכת אותה אנו חוקרים? ג. האם המתודולוגיה נגישה גם למי שאינו מומחה מקצועי בשימוש בה?[23]

ייתכן כי מתודולוגיה טובה אכן לא מחייבת נוכחות של מומחה למתודולוגיה בחדר, אך הבחירה במתודולוגיה מתאימה להקשר הנתון הנלמד – כדאי שתיעשה לאחר מחשבה רבה.

ב. התבוננות מערכתית במרחב הסייבר

בחלק זה של המאמר טמון פרדוקס. כפי שתואר בפרק הקודם, ניתוח בעיות מורכבות לפי מאפייני תורת המערכות המורכבות מחייב גישה הוליסטית – מערכתית ללא פירוקה של הבעיה למרכיביה השונים. מדוע, אם כך, ימצא הקורא התוהה בפרק זה פירוקו של מרחב הסייבר לכדי מרכיביו המוכרים? ולא, נאמר, ניתוח מערכתי של מרחב הסייבר כמערכת-על מורכבת? היות ומטרתו של המאמר היא להציע מבט אחר על קטגוריות הייחוס המקובלות למרחב הסייבר, ולהעניק לאיש המקצוע כלים להתמודדות טובה יותר עמו, ימצא הקורא פרשנות מערכתית על כל אחת מקטגוריות מרחב הסייבר בנפרד. עבודת הבנייתה של מערכת-על אחת, הכוללת את כלל הקטגוריות כנדבכים מרושתים זה בזה, יכולה להיות בת מימוש על ידי אנשי מקצוע בלבד, "אמני סייבר", בעלי הסתכלות מערכתית, וכתוצאה מתהליך למידה מבנה.

על מלחמה בוירוסים – ממערכות הגנה בסייבר למערכת החיסונית של גוף האדם

בעיית ההגנה בסייבר היא הנדונה, המנותחת והפופולארית ביותר הן בעולם הפרקטיקה של חברות אבטחת מידע וארגונים ממשלתיים, הן בעולם האקדמי. יתכן כי בזכות שיח ער זה, מימד ההגנה הוא גם המפותח ביותר מבחינה תיאורטית (לפחות במקורות גלויים) ועל כן גם תפיסות ההפעלה הנוצרות בקרבו מתקדמות יותר לעומת תחומי סייבר אחרים.

כניסתו המהירה של מרחב הסייבר כמעט לכל נדבך בחיינו (וכפי שתואר בפתיח – כניסה שצפויה לגדול ולהעצים עד מאוד) הינה הגורם המרכזי לחשש מפני השתלטות עוינת והשפעה זדונית על מערכות בהן אנו נעשים תלויים יותר ויותר. תוכנות זדוניות קיימות מזה ארבעים שנים[24], אך לפי דו"ח חברת אבטחת המידע הספרדית Panda Security כ – 20% מכלל התוכנות הזדוניות הקיימות נוצרו רק במהלך שנת

---

[23] אלטמן, 2014.

[24] ההנחה הרווחת היא כי התכנות הזדוניות הראשונות היו "The Creeper System" מ - 1971 ו – "Rabbit" או "Wabbit" מ – 1974.

2013.[25] בסיכום שנת 2013 הציגה החברה נתונים לפיהם מדי יום נוצרות בממוצע 82,000 תוכנות זדוניות המופצות ברשת,[26] אך בדו"ח הרבעון השלישי של 2014 מספר זה מאמיר לכמעט 230,000 תוכנות מדי יום, כאשר רק בין החודשים יולי – ספטמבר 2014 נוצרו למעלה מ – 20 מליון תוכנות זדוניות חדשות.[27]

במהלך שלושת העשורים האחרונים נכתבו והופצו לשוק עשרות תוכנות אנטי וירוס אשר התפתחו ושודרגו במקביל להתפתחותם ושדרוגם של האיומים השונים על הרשת. תפיסת האבטחה כמובן השתנתה עם השנים, ותוכנות אבטחה מתקדמות ביותר הופצו לשוק, אך, לרוב, מדובר היה בתוספת שכבות הגנה על אתרי הרשת השונים ומשתמשיהם. תפיסת שכבות ההגנה שואבת מעוגנה המרכזי של תפיסת ההגנה המקובלת - אסטרטגיית ה"הגנה לעומק" ("Defence in Depth") השאולה מהתחום הצבאי הטקטי - מערכתי.[28] לפי גישה זו, מיקוד ההגנה הוא אינו במניעת הפגיעה כליל, אלא בעיכובה ככל הניתן, בעיקר באמצעות יתירות מבנה, וזאת לשם מתן זמן זיהוי ותגובה הולמת למערכת המגנה. מכשולי נ"ט, לדוגמא, הם ביטוי לגישת "הגנה לעומק" – הם אינם מונעים כניסת טנקי אויב, אלא מעכבים ודוחים אותה. גישת "שכבות ההגנה" היא המקובלת כיום על ידי רוב חברות אבטחת המידע, ומהותה ביצירת מענה אבטחתי לכל רובדי התנועה המקוונת – החל מעמדת המחשב הפרטי בביתנו ('עמדת הקצה') וכלה בספקית האינטרנט. ביטוי ויזואלי אופייני ניתן, למשל, לראות בהצגת תפיסת ההגנה של חברת אינטל, כפי שהוצגה בינואר השנה בועידת "CyberStart14 Security Conference" בהלסינקי:[29]

---

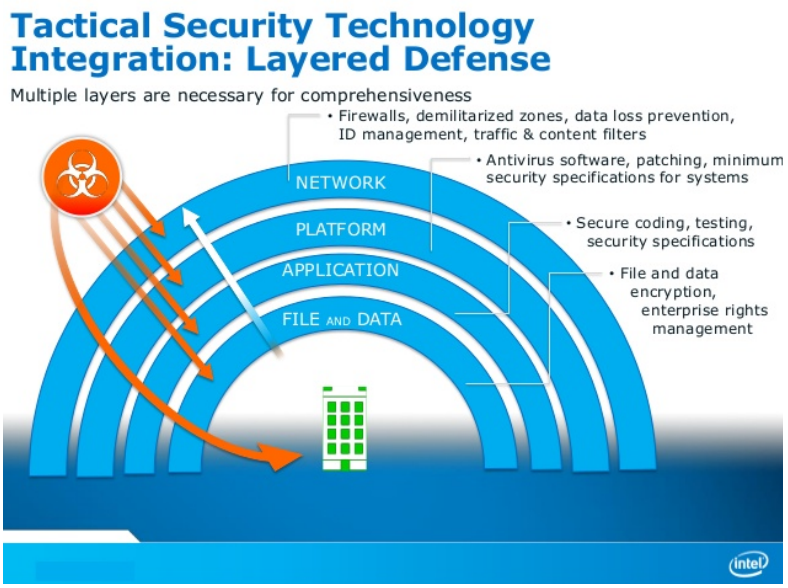
25 http://mediacenter.pandasecurity.com/mediacenter/wp-content/uploads/2014/07/Annual-Report-PandaLabs-2013.pdf

26 Ibid.

27 http://mediacenter.pandasecurity.com/mediacenter/wp-content/uploads/2014/11/Quarterly-Report-PandaLabs_Q3.pdf

28 ה**"הגנה בעומק"** הוא מושג בו השתמש ההיסטוריון ומדען המדינה אדוארד לוטוואק בספרו המכונן "האסטרטגיה רבתי של האימפריה הרומית". אחת השאלות המרכזיות עמן מתמודד ספרו היא "כיצד הרומים שמרו על גבולותיהם?" לטענתו, במאה השלישית ובתחילת המאה הרביעית לספירה עברה האימפריה הרומית מאסטרטגיה של **"הגנה קדמית"**, המונעת כל חדירה של כוחות זרים לשטחי האימפריה ומנטרלת אותה בשטחי האויב, לאסטרטגיה של "הגנה בעומק", המתייחסת לחדירת כוחות זרים כמצב נתון, אותו ניתן לנצל לטובת הכוחות המגנים באמצעות הכלה, ארגון כוחות ותקיפה. לצורך ההמחשה, ניתן לטעון כי אסרטגיית ההגנה של מדינת ישראל, על פי תפיסת הביטחון לבן גוריון, היא תפיסת "הגנה קדמית", מתוקף דוקטרינת העברת המלחמה לשטחי האויב, ואילו תפיסת ההגנה של סוריה (טרם מלחמת האזרחים, כמובן), בהתאם לדוקטרינה הסובייטית, היא תפיסת "הגנה בעומק", במסגרתה חגורת הביטחון הרחוקה ביותר ממרכז העצבים (דמשק) היא גם החלשה ביותר, ועל כן הדיפת כוח פולש תהיה על אדמת סוריה ובאמצעות הכוחות ההולכים וחזקים עם ההתקרבות לבירה. המקרה הסורי הוא גם ההמחשה לכך שתפיסת "הגנה בעומק" היא בהכרח תפיסה של שכבות הגנה.
אדוארד לוטוואק, **האסטרטגיה רבתי של האימפריה הרומית,** (הוצאת מערכות, 1982).
המונח "הגנה בעומק" הפך, כאמור, משמעותי בהקשר מימד ההגנה בסייבר. להרחבה על התפיסה ומימושה במרחב אבטחת המידע ראו הסבר באתר הסוכנות לביטחון לאומי (ה - NSA):
https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

29 Intel® Cyber Security Briefing: Trends, Challenges, and Leadership Opportunities. Matthew Rosenquist, Cyber Security Strategist, Intel Corp January 2014.
http://www.slideshare.net/MatthewRosenquist/cyberstrat14-helsinki-matthew-rosenquist-2014-public



תמונה 1: גישת "שכבות הגנה" באבטחת המידע של חברת אינטל

רוס אשבי, פסיכיאטר בריטי ואחד מאבות תחום הקיברנטיקה וגישת המערכות המורכבות, גרס בספרו הנודע "An Introduction to Cybernetics" משנת 1956 כי מערכת מנהלת מוכרחה להיות מורכבת יותר מהמערכת שהיא מנהלת בעצמה.[30] כך, ניסו במשך העשורים האחרונים חברות האבטחה לשמור על קצב התפתחות זהה, ובשאיפה – מהיר יותר, מקצב התפתחות ושדרוג התוכנות הזדוניות על שלל סוגיהן. בשנים האחרונות נשמעים בשיח האקדמי (והמעשי) בתחום ההגנה בסייבר קולות שונים, המבקשים לבחון דרכים אחרות לפיתוח נוסף של "גישת השכבות". הולכת ומתעצבת הבנה כי אם כבר היום ההגנה בסייבר מאותגרת יותר מפעם ומתקשה להתמודד עם כמות רבה כל כך של תקיפות (מתוחכמות במיוחד בחלקן), הרי שעל אחת כמה וכמה יאותגרו מערכות אלו בעתיד, כאשר היקף תעבורת המידע במרחב יגדל בעשרות מונים. נשמעים קולות לחשיבה 'אחרת' ולשינוי תפיסתי בגישה הבסיסית, עד כדי כך שמייסד חברת האבטחה נורטון אנטי וירוס, בריאן די, הכריז השנה חגיגית על "מותו של האנטי וירוס", בהתייחסו לתהליך שינוי גישה מערכתית בה נוקטת החברה.[31]

על רקע השינוי בשיח חוגי הפרקטיקנים בהגנה במרחב הסייבר, ואף עוד לפני שהנושא הפך פופולארי במיוחד, שיתוף פעולה מחקרי[32] בין ה- SSG (Chief of Naval Operations Strategic Studies Group) של חיל הים האמריקני (Navy) לבין מכון ניו אינגלנד למערכות מורכבות (New England Complex Systems Institute) בראשותו של פרופ' יניר בר ים, הוביל למסקנות מערכתיות מקוריות:[33]

הנחת המוצא של סטייסי (עמית מחקר במכון) ובר ים היא כי גישות מסורתיות להגנה בסייבר הופכות לרלוונטיות פחות ופחות עם התגברות האיומים, תחכומם, והקצב בו הם משתנים. בנוסף, כך הם גורסים, בעולם האבטחה ניתן לזהות דפוסי פעולה כלליים דומים, וכי זיהוי מאפייני מערכות אבטחה כלליות יעילות יכול להועיל בהתמודדות עם אתגרים מורכבים חדשים ברשתות טרור גלובאליות ובאבטחה בסייבר. בנייר המסכם את תהליך הלמידה המשותף עם ה - SSG, משתמשים החוקרים במערכת החיסונית האנושית כהשראה למערכת המתמודדת עם אתגרים ואיומים מקבילים לאלה הקיימים במרחב הסייבר.

---

[30] W. R. Ashby, **An Introduction to Cybernetics,** (London: Chapman & Hall LTD., 1957) [2nd Ed.], pp. 219-259.

[31] Brad Chacos, "Antivirus is dead, says maker of Norton Antivirus," *PCWorld*, 5 may 2014. http://www.pcworld.com/article/2150743/antivirus-is-dead-says-maker-of-norton-antivirus.html

[32] שיתוף הפעולה המדובר התקיים במהלך שנת 2008, ולכן אין ספק כי מימד ההגנה בסייבר ידע שינויים והתפתחויות מאז. היות ואין עניינו של המאמר בהעלאת חידושים ומהפכנות, אלא בהצעת כלים לחשיבה אחרת, תיאור תוצאות המחקר מובאות בתור דוגמא לתהליך למידה פתוח שאפשר הכנסת מושגים לכאורה לא קשורים, כגון המערכת החיסונית האנושית, אך הוביל לפיתוח תפיסות מקוריות וחדשניות.

[33] כלל תיאורי תוצאות המחקר מובאים מתוך:
Blake Stacey and Yaneer Bar-Yam, "Principles of Security: Human, Cyber and Biological," New England Complex Systems Institute, reported to William G. Glenney IV, Chief of Naval Operations Strategic Studies Group, June 1st 2008. http://necsi.edu/research/military/cyber/netsecurity.pdf

השוואה זו מתאפשרת, לטענת החוקרים, עם הפיכתה של תקשורת המחשבים למתפתחת, מתמשכת ומהירה. המערכת החיסונית האנושית מורכבת ממיליארדי תאים המתואמים ביניהם להגיב על אתגרי אבטחה בגוף האנושי. לדידם, הפעילות של המערכת החיסונית אינה יכולה להיות מובנת כמערכת ריכוזית הנשלטת על ידי "מוח" אחד, אלא מתקיימת באמצעות מספר רב של קשרים מקומיים בין מרכיבים ייעודיים לצורך ביצוע תגובת חירום מיידית. הברירה הטבעית האבולוציונית הביאה את המערכת החיסונית לכדי שכלול כזה שהיא משיגה תוצאות טובות, היא גמישה, מדידה, ומסוגלת להבחין תוך כדי פעולה בין "ידיד" ל"אויב".

את פעילותה של המערכת החיסונית ניתן לחלק לשלוש שכבות: הראשונה, מורכבת מחסמים בין 'אזורי אבטחה' לסביבתם – שכבות העור המפרידות בין גוף האדם לסביבתו החיצונית, כמו גם חסמים פנים גופניים המפרידים בין סביבות שונות. בשכבה השנייה מתבצעת תגובה לפגיעות במערכת המשפיעות על מספר רב של תאים, וכוללת איחוי רקמות ו"החלפת" חסמים. השכבה השלישית, "חוד החנית", היא המערכת החיסונית הסתגלנית (Adaptive immune system), מגיבה לאתגרים המשמעותיים ביותר הפוגעים במערכת, ואחראית על איתור תאים ומולקולות המופצים במערכות הגוף, בדגש על זיהוי וירוסים ובקטריות המסוגלים לשכפל עצמם לכדי כמויות גדולות תוך פרק זמן קצר, ותגובה מיידית לנטרולם. לכל אחת מהשכבות הללו, כך טוען בר ים, יש את המקבילה שלה במימד ההגנה בסייבר, ואילו השכבה השלישית – היא החשובה והמתוחכמת ביותר, ועליה נרחיב.

התכונות החשובות ביותר של שכבת המערכת החיסונית הסתגלנית הן הזיהוי והתגובה, מה שנכון לגבי כל מערכת אבטחה באשר היא. הזיהוי מושג באמצעות מיפוי המרחב המאובטח על תכולותיו והתנהגויותיו השגרתיות – מה שמאפשר בשעת התקפה את היכולת להבדיל בין איום ל'לא איום' (בין "ידיד" ל"אויב"). כאשר מאובחן "אויב" שחדר לסביבה המאובטחת, מופעלת תגובת נגד מיידית. הזיהוי והתגובה הן שתי פונקציות נפרדות של מרכיבי המערכת, הדורשים רגולציה עדינה שתאפשר פעולה מסונכרנת. ניתוח מעמיק של מערכות התקשורת המתקיימות בין האלמנטים השונים של המערכת החיסונית מגלה דפוסים המאפשרים למערכת 'ללמוד מחיכוך' ולהגביר את יכולתה להגיב במהירות לאיומים חדשים. מערכת תקשורת זו מפיצה בגוף את ידע 'מנגנוני הגילוי' שנשארים או נשכחים בהתאם ליעילותם בברירה הטבעית.

החוקרים ממשיכים וטוענים כי מערכות ההגנה בסייבר הקיימות היום גם הן חולקות מרכיבים דומים עם המערכת החיסונית האנושית. תפיסת החסמים וההגבלה המאפיינת את שכבת ההגנה הראשונה של המערכת החיסונית באה לידי ביטוי ב'חומות אש' (Firewalls) והפרדת רשתות. השכבה השנייה של ההגנה, בה מתבצעת התגובה לפגמי המערכת מתבטאת, למשל, באמצעות קיום "רשימות שחורות" של שמות תחום (DNSBLs) לצורך חסימת מפיצי ספאם. השכבה השלישית, היא תוכנות האנטי וירוס ומסנני דואר אלקטרוני המזהים תוכנות זדוניות וחוסמים אותם. בעוד שכאמור, מתקיים דמיון בין המערכת החיסונית לתפיסת ההגנה בסייבר הקיימת היום, עם ההשוואה למערכת החיסונית מתגלים שני פערים משמעותיים בארכיטקטורה של הרשת, המונעים ממנגנוני אבטחתה את הרלוונטיות לאתגרי המחר. ראשית, לא מתקיים מנגנון הפצה של הידע הנוצר מהתגובה לזיהוי תוכנות זדוניות, למנגנוני אבטחה אחרים. הפצת הידע הזו היא אופציונאלית, המתאפשרת רק עם רישום פעיל של משתמשים בודדים למערכות אבטחה. בעוד שתוכנות זדוניות מקיימות מנגנוני שכפול והפצה עצמית ברשת (וחלקן אף 'לומדות תוך כדי' ומתחזקות ככל שתנועתן נמשכת), הידע שנוצר מחסימתן בעמדות קצה שונות אינו מופץ ואינו 'מלמד' עמדות קצה אחרות, מה שמיידית מציב את ההגנה בעמדת נחיתות לעומת התוקף.

שנית, התפיסה המקובלת של מערכות ההגנה איננה תפיסה מערכתית משום שהיא איננה מערכת הגנה קולקטיבית. המיקוד הוא בהגנה של מרכיבים בתוך האינטרנט (בין אם אתרים ספציפיים או עמדות קצה של משתמשים) ולא בהגנה על האינטרנט כמערכת שלמה. ללא מערכת הגנה קולקטיבית, הפתרון היחידי להתמודדות עם אתגרים מתגברים ומשתנים, היא הקשחת כל מרכיב נפרד של האינטרנט, מלאכה לא פשוטה בפני עצמה. כתוצאה מכך, מסיקים החוקרים, מרחב הסייבר נעדר מנגנוני חסימה של תקיפות עם כניסתן למרחב המשותף, אלא ממוקד בחסימתן בנקודות תקיפה רבות "בסוף מסלול ההתפשטות".

על אף ההשראה הותיקה של האיומים על המערכת החיסונית האנושית לעולם ההגנה בסייבר (שהרי

לא סתם מחשב הנגוע בתוכנה זדונית כלשהו הוא מחשב "עם וירוס"), רק חמש השנים האחרונות הביאו עמן בשורה של הגנות מערכתיות. המניע המרכזי להתפתחות שיח של גישה מערכתית לאבטחת מידע היה התפתחות תפיסת וטכנולוגיית מחשוב הענן (Cloud Computing). תפיסת מחשוב הענן, המהווה בסיס מרכזי לבשורת ה"אינטרנט של הדברים" (IOT) אותה הזכרנו בתחילת המאמר, מציעה בפנינו מציאות עתידית בה המסמכים, התמונות, התוכנות, ולמעשה – כל מה ששמור לנו במחשב הפרטי בבית, יהיה נגיש לנו באמצעות "ענן" מידע עליו הם יישמרו. במקום שנצטרך לקנות תוכנה ולהתקינה על המחשב הפרטי (או הרשת המקומית), ניתן יהיה להשתמש במידע או בישום הנשמר בחוות שרתים מרוחקת, ולשלם (אם בכלל) רק עפ"י שימוש. ניתן, למשל, להקביל את השימוש המעודכן באינטרנט עפ"י טכנולוגיה זו לשימוש ברשת החשמל - המשתמש תמיד מחובר לרשת אך משלם על פי השימוש בחשמל. למעשה, כל מי שמנהל, למשל, חשבון פייסבוק ושומר עליו תמונות, משתמש כבר היום בשירות אחסון מידע בענן.[34] טכנולוגיית מחשוב הענן מעמידה דרישות חדשות, מחמירות יותר, בכל הנוגע לאבטחת מידע. כעת, כשהמשתמש (או החברה) מאבדים את היכולת ל"קשר פיסי" עם המידע האישי או העסקי שלהם (שהרי כבר לא יהיה "דאבל קליק" על 'המסמכים שלי'), החשש מפני התערבות גורמים זרים ועוינים, ומפני אבדן המידע, רק מעצים. שינוי בסיסי מעין זה מוביל כעת לחשיבה מחודשת על עקרון ה"הגנה בעומק" שהוביל את עולם ההגנה בסייבר שנים כה רבות. ספקי תשתיות כבר לא יכולים להרשות לעצמם "הכלה בשטחנו", היות והם מעמידים בסיכון מידע שהם אמונים על שמירתו. על כן, תפיסת "הגנת הענן" (Cloud Security) המתפתחת, נוטה יותר ויותר לכיוון תורת ה"הגנה

---

[34] דני דניאל, " טכנולוגית מחשוב ענן: 'באזז' בעולם ה-IT, אז מה זה בעצם?," *ביפורטל*, 21.01.2010.
http://wallstreet.bizportal.co.il/articles.php?id=110427
להסבר קצר אך תכליתי על מהות מחשוב הענן ראו:
http://www.davidchappell.com/CloudPlatforms--Chappell.pdf

הקדמית", המיועדת למניעת חדירה של גורמים עוינים עוד בטרם יגיעו ל'גבול'.[35] עם זאת, לפולמוס הער המתרחש היום סביב מהות הגנת הענן, מבנהו ואופן פעילותו (גם נוכח בעיות משמעותיות של הגנה על פרטיות) יש עוד מרחק רב לעבור עד שיחול קונצנזוס כלשהו סביב 'תפיסת הפעלה' על ידי קהילת אבטחת המידע והמשתמשים.[36]

לוחמת מידע וחופש מידע – התבוננות מערכתית על מרכיבי מימד הסייבר

"בכל רחבי העולם, אנשים מבחינים בחלקים שונים ממה שמתרחש בסביבתם. אחרים מקבלים מידע ממקור שני. באמצע נמצאים אנשים שמעורבים בהעברת המידע מהצופים לאנשים שיפעלו על סמך המידע. אלו שלוש בעיות נפרדות שכרוכות זו בזו.

הרגשתי שקשה לנתח נושאים ולהפיץ את הניתוח באופן יעיל, כך שהמידע יגיע לאנשים שבסופו של דבר יפעלו על פיו. אפשר לטעון שחברות כמו גוגל, למשל, מעורבות בעסקי ה'תיווך' האלה, של העברת מידע מאנשים שהמידע מצוי אצלם לאנשים שמעוניינים בו. הבעיה שזיהיתי היתה שהשלב הראשון, ולפעמים גם השלב האחרון, מוגבלים כשמדובר במידע שממשלות נוטות לצנזר.

אפשר להסתכל על התהליך הזה כעל צדק שנעשה על ידי הרשות הרביעית. [...] היה נראה לי שצוואר הבקבוק מצוי בראש ובראשונה בהשגת מידע, שימשיך וייצר שינויים צודקים. בהקשר של הרשות הרביעית, אנשים שמשיגים מידע הם בגדר מקורות; אנשים שמעבדים את המידע ומפיצים אותו הם עיתונאים ומפרסמים למיניהם; ואנשים שעשויים לפעול על סמך המידע הם כולם. זה תיאור ממעוף הציפור אבל הוא מסתכם באופן שבו מהנדסים מערכת שתפתור את הבעיה, ולא סתם מערכת טכנית אלא מערכת כוללת. ויקיליקס היתה, ועודנה, ניסיון – אם כי ראשוני מאוד – להיות מערכת כוללת כזאת."[37]

ג'וליאן אסאנג'

בין ה – 18 בפברואר 2010 ל – 1 בספטמבר 2011 חווה העולם את מה שכונה אחר כך "ההדלפה הגדולה בהיסטוריה", או בשמה הרשמי – "פרשת קייבלגייט". במשך 19 חודשים פרסם אתר ויקיליקס

---

[35] להרחבה ראו:
Vic Winkler, **Securing the Cloud: Cloud Computer Security Techniques and Tactics**, (Elsevier, 2011).
אתר האינטרנט של "ברית הגנת הענן":
https://cloudsecurityalliance.org/

[36] ראו למשל:
Rajiv Gupta, "Why cloud security requires multiple layers," *USA Today*, 25 Nov. 2013. http://www.usatoday.com/story/cybertruth/2013/11/25/why-cloud-security-requires-multiple-layers/3683171/; Cliff Saran, "Cloud security remains a barrier for CIOs across Europe," *ComputerWeekly.com*, 9 December 2014, http://www.computerweekly.com/news/2240236318/Cloud-security-remains-a-barrier-for-CIOs-across-Europe ; Mark Wilson, "Has Microsoft found the answer to cloud security?," *ITProPortal,* 3 December 2014, http://www.itproportal.com/2014/12/03/haven-answer-cloud-security-problems/

[37] ג'וליאן אסאנג', **כשגוגל פגשה את ויקיליקס**, (תל אביב: הוצאת דיונון, 2014), עמ' 71-70.

251,287 מסמכי תכתובות מסווגים שונים שנשלחו במקור אל מחלקת המדינה האמריקאית מ-274 הקונסוליות שלה, השגרירויות שלה, וכן הנציגויות שלה ברחבי העולם, הכוללים ניתוחים מדיניים וציטוטים של מנהיגים ושרים שונים ברחבי העולם אשר נאמרו במקור בדלתיים סגורות. מסמכי התכתובת שהודלפו במסגרת הפרשה נוצרו במקור החל מדצמבר 1966 ועד לפברואר 2010. המסמכים מכילים ניתוחים מדיניים ממנהיגי העולם, וכן הערכותיהם של דיפלומטים אמריקנים במדינות המארחות ושל הפקידים שלהם.

קשה להגזים בתיאור ההשפעה של ויקיליקס על מרחב הסייבר. בספרו, מצטט אסאנג' את המוציא לאור של העיתון התוניסאי "נוואת", סמי בן ע'רביה שכתב כך: "עשרים יום חלפו בין פרסום התכתובות המודלפות על תוניסיה ב – 28 בנובמבר 2010, לבין תחילתו של האביב הערבי ב – 17 בדצמבר 2010. ביום ההוא, רוכל עני בשם מחמד בועזיזי הצית את עצמו. בצ'אט עם עיתונאי בריטי שנערך השנה הודה שר התעמולה של בן עלי, אוסאמה רומדאני, כי 'ההדלפות היו מכת החסד, הקש ששבר את גב הגמל מבחינת המערכת של בן עלי.' לא היה זה המידע על השחיתות ועל העדפת המקורבים, התוניסאים לא היו זקוקים להדלפות כדי לדעת שארצם מושחתת. [...] ההבדל היה בהשפעה הפסיכולוגית של ממסד שנאלץ להתעמת באופן פומבי כל כך עם בבואתו העכורה. [...] ומי שסיפר את הסיפור לא היה מורד או רוחש-רעה פוליטי. זו היתה מחלקת המדינה של ארצות הברית, בעלת ברית לכאורה."[38] רבים נוספים מייחסים להדלפות ויקיליקס תפקיד משמעותי, אם לא מכריע, בפרוץ המרידות ברחבי העולם הערבי נגד משטריהם האוטוקרטיים,[39] אך גם אם נשאיר להיסטוריה לשפוט בעניין זה, הרי שההצלחה המשמעותית ביותר של ויקיליקס היא ביצירת שיח ציבורי חסר תקדים בהיקפו, על פתיחות המידע.

בענייננו, מעניין לראות כי תגובתם הראשונה של גופי סייבר, בין אם פרטיים או ממסדיים, להדלפות ויקיליקס הייתה ניסיון 'להשתלט על המערכת'. אתרי ויקיליקס השונים ספגו אש ארטילרית מכל הכיוונים, האתר הופל והועלה מספר פעמים, ומלחמת חורמה נפתחה נגד ספקי השרתים שעבדו עם אסאנג' ונגד חברות אשראי שסיפקו דרכים לתמיכה כספית בפרוייקט. התקיפות על ויקיליקס נעשו כנראה על רקע רצון בנקמה או בפגיעה באתר, שהרי ברור לכל איש מחשבים בינוני שברגע שמידע כלשהו עולה לאינטרנט – הוא נשאר בו. ולראייה, גם היום ניתן להיכנס לאתר ויקיליקס באין מפריע ולראות את כלל הפרסומים שנעשו בתקופה ההיא, כמו גם הדלפות חדשות שיוצאות מדי פעם.

סיפור ויקילקס לא מובא במאמר זה רק כקוריוז פיקנטי להמחשת הסכנות באינטרנט. ויקיליקס, ובמיוחד פרשת קייבלגייט, מהווים דוגמא קלאסית לניצחונה של מערכת מורכבת על מערכת מורכבת פחות. ויקיליקס לא רק נבנתה באופן מורכב טכנולוגית כדי לעמוד בפרץ ההתקפות על אתריה, אלא היא נבנתה בהיגיון שממוטט את היגיון הפעילות של המערכת ה'יריבה' לה. מחלקת המדינה האמריקנית, בתפקודה השגרתי מול נציגויותיה בעולם ובאמצעות שימוש בעקרון כה נושן הנקרא "סיווג בטחוני" למסמכים, לא הייתה בנויה לעמוד בפני התקפה שכזו.

---

[38] שם, עמ' 16.

[39] ראה למשל:

Brett van Niekerk, Kiru Pillay, Manoj Maharaj, "The Arab Spring| Analyzing the Role of ICTs in the Tunisian and Egyptian Unrest from an Information Warfare Perspective," *International Journal of Communication*, vol. 5 (2011); Benedetta Brevini, Arne Hintz, Patrick McCurdy, **Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society,** (Palgrave Macmillan, 2013); June R. Klein, "Wikileaks, Arab Uprisings, English Riots and Occupy Wall Street: Implications for Internet Policy and Practice from a Business and Industry Outcome Perspective*," Information, Communication & Society Journal*, No. 14.6, 2012; Theresa Sauter & Gavin P. Kendall," Parrhesia and democracy : Truthtelling, WikiLeaks and the Arab Spring", *Social Alternatives*, 30(3), pp. 10-14;

ועוד רבים נוספים.

באותו האופן, הבנוי על פעילות בהיגיון הממוטט את מבנה המערכת ה'יריבה', פועלת גם קבוצת אנונימוס. אנונימוס החלה להתארגן אי שם בשנת 2003 כקבוצת צ'ט בפורום 4chan. כבר בהתחלה פעלו הגולשים בפורום באופן משותף על מנת 'להטריל'[40] פורומים אחרים ומשחקי און ליין שונים. אט אט החלה פעילות משותפת זו לעבור לתחום ה'האקטיביזם' תוך חתירה תחת הממסד. ככל שהתרבו פעילות ההאקינג שלהם – כך גברה הפופולאריות של הקבוצה. עם הזמן, הוכרה הקבוצה כ'תופעה אינטרנטית' והיא נתפסת היום כקבוצה בעלת יכולות פריצה מתקדמות ביותר (בשנת 2012 קבוצת אנונימוס הפילה את אתר משרד המשפטים של ארצות הברית, אתר הבולשת הפדרלית (FBI) והאתרים של חברות בידור ומוזיקה שונות כגון חברת יוניברסל מיוזיק, במחאה על סגירת אתר ההורדות Megaupload וצעדי הממשל האמריקאי כנגד אתרים פיראטיים.(אחד מסמליה של הקבוצה, חליפת איש עסקים עם סימן שאלה במקום ראש, הוא אחד הביטויים הגראפיים להיגיון פעילותה – פעילות סייבר אלימה ומאסיבית ללא גוף שניתן 'לאחוז בו', ללא דוברים, מייצגים, או כתובת למשלוח מכתבים. באתר ויקיפדיה מסווג אנונימוס כ'ארגון'.[41] ככזה, זוכה העמוד למסגרת ("בוקס") של "תעודת זהות" אותה מקבלים כלל הארגונים המתוארים בויקיפדיה, על פי אמות המידה המקובלות ל'מהו ארגון' (מדינת מקור, מייסדים, מיקום המטה, בעלות...). בדקו בעצמכם כמה אנונימוס עונה להגדרות 'מקובלות' בתמונה המצורפת, וראו בכך דוגמא חיה ליכולתן של מערכות ממסדיות "להכיל" תופעות שכאלה.

אין כוונתי כאן, להביע תמיכה או גינוי כלפי גופים, ארגונים או פרטים הפועלים במרחב הסייבר. ללא ספק ישנם גם האקרים המנצלים לרעה את הכישרון הניתן להם ופוגעים פגיעות קשות בפרטיותם של גולשים, בפיתוח כלכלי של חברות מדינות, בקניין רוחני של אמני וכו'. אך עם זאת, להאקרים, כפי שטוענת המומחית לאבטחת מידע קרן אלעזרי, ישנו גם הפוטנציאל להיות מערכת החיסון של מרחב הסייבר, ביכולתם לזהות פרצות אבטחה וכשלי מערכות, ולהתריע מפניהם.[42]

השימוש במרחב הסייבר לצרכי השפעה על ידי ארגוני טרור גם הוא תופעה הראויה לניתוח בראייה מערכתית. על פעילותו של ארגון דאע"ש במרחב הסייבר כבר העמיקו בגיליון זה ברן ולוי, אך קיימות עדויות ומחקרים רבים גם לפעילות מקוונת לצרכי השפעה, וגיוס תמיכה ומשאבים על ידי מדינות כמו איראן[43] וארגוני טרור כמו חמאס וחזבאללה[44]. ארגוני הטרור, כמו גם ארגוני פשע ועבריינים, מנצלים גם

---

[40] 'להטריל' – (מהמילה טרול) לפעול בצורה תוקפנית וטורדנית כלפי גולשים אחרים ברשת האינטרנט, למשל בפורומים, רשתות חברתיות, שליחת הודעות וכד'. *מילוג* – המילון העברי החפשי ברשת.
/http://milog.co.il/%D7%9C%D7%94%D7%98%D7%A8%D7%99%D7%9C/s

[41] http://goo.gl/4bXrc7

[42] Dan Smith, "Hackers are the immune system for the information age," *Weird,* 13 June 2014. http://www.wired.co.uk/news/archive/2014-06/13/keren-elazari

ראו גם הרצאתה ב – TED:
https://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system

[43] גבי סיבוני וסמי קרוננפלד, "התפתחויות בלוחמת הסייבר של איראן 2013-2014," *צבא ואסטרטגיה*, כרך 6, גיליון 2, אוגוסט 2012.

[44] המרכז למורשת המודיעין (מל"מ) - מרכז המידע למודיעין ולטרור, "האינטרנט כזירת מאבק עם ארגוני הטרור: השימוש שעושים חזבאללה וחמאס באינטרנט במלחמה על התודעה ודרכי ההתמודדות עם התופעה," 25 ביולי 2007.
http://www.terrorism-info.org.il/data/pdf/PDF_07_084_1.pdf

את האנונימיות שב"רשת האפלה" (Darknet)[45] על מנת ליצור התקשרויות בינם לבין עצמם, ובינם לבין רשתות קרימינליות ולקוחות פוטנציאליים, וכל זאת מתחת לרדאר ובעילום שם.

תמונה 2: תעודת הזהות של ארגון אנונימוס באתר ויקיפדיה

אין ספק בלבי כי ארגוני הביון המערביים מודעים לתופעה זו, שהרי סערת ויקיליקס לא הספיקה לשכוח ומיד צצה פרשה חדשה, בדמות ההדלפות של אדוארד סנודן. סנודן, עובד לשעבר בסוכנות לביטחון לאומי (ה - NSA), העביר ביוני 2013 לעיתונים "הגארדיאן" ו"הוושינגטון פוסט" חומר מסווג על תוכניות סודיות ביותר של הסוכנות לביטחון לאומי, כולל תוכניות המעקב PRISM (המופעלת ע"י ה - NSA) ו – Muscular (המופעלת בשיתוף פעולה ע"י ה- NSA וה – GCHQ, סוכנות הביון הבריטית).

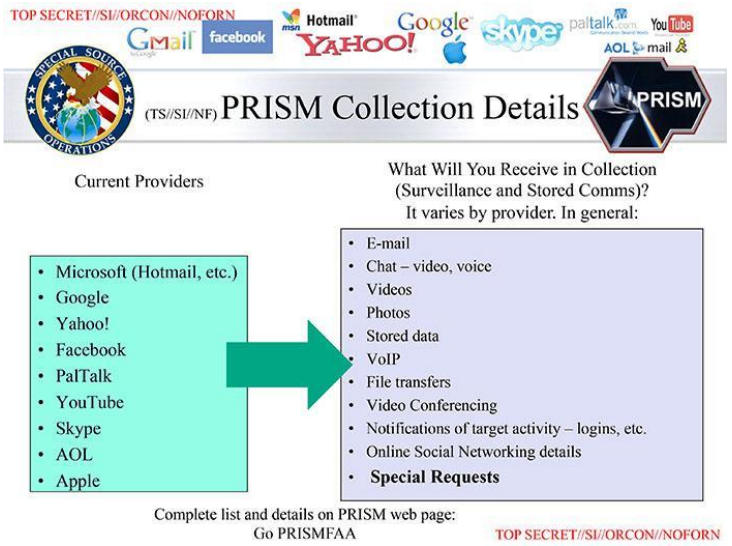
על פי המסמכים שהודלפו, PRISM היא תכנית חשאית לאיסוף מידע מודיעיני מחברות טכנולוגיה אמריקאיות, הפועלת מאז שנת 2007. החברות הכלולות בתוכנית הן מיקרוסופט (מאז 2007), יאהו (Yahoo) (מאז 2008), גוגל, פייסבוק ופאלטוק (Paltalk) (מאז 2009), יוטיוב (מאז 2010), AOL וסקייפ (Skype) (מאז 2011) ואפל (מאז 2012), כאשר 98% מהמידע המופק בתוכנית מקורו ביאהו, גוגל ומייקרוסופט.[46]

Muscular, היא תוכנה שפותחה על ידי סוכנות הביון הבריטית (GCHQ) ומייצרת גישה באמצעות פרצה אל מאגרי המידע של החברות גוגל ויאהו, בדומה לתוכנה ששימשה את ה – NSA בתכנית המעקב שלה.

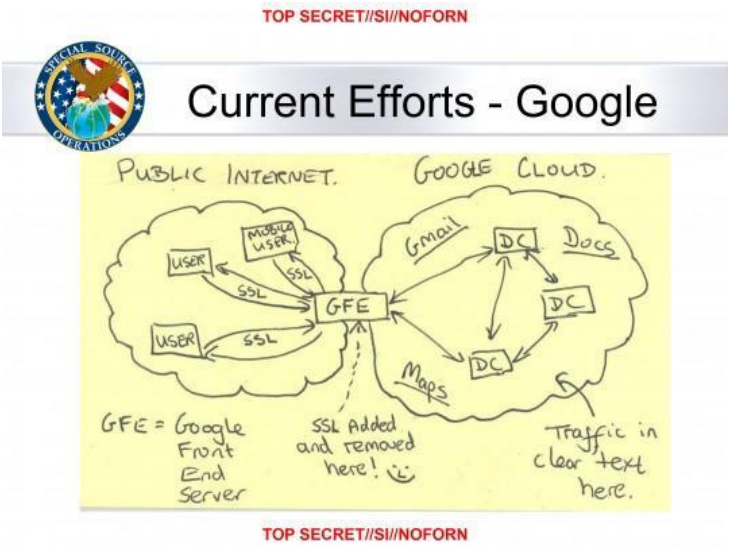
---

[45] "רשתות אפלות" ("Darknets"), הוא שם כולל לרשתות תקשורת אנונימיות ומוצפנות, המבוססות על תשתית אינטרנט. רשתות אלה אמנם משתמשות ב"נתיבי התעבורה" של רשת האינטרנט, אך הן פועלות על פי פרוטוקולי תקשורת שונים ומאפשרות רמת אנונימיות ופרטיות מידע מוגברת.
הכנסת. מרכז המחקר והמידע, רועי גולדשמידט, "שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה," מוגש לוועדת המדע והטכנולוגיה, 1 בינואר 2012.
http://www.knesset.gov.il/committees/heb/material/data/mada2012-01-02.doc

[46] לפירוט מלא על ההדלפה, פרטי התכנית והשלכות הפרסום:
http://www.theguardian.com/us-news/the-nsa-files



תמונה 3: תכנית PRISM- שקופית "פרטי האיסוף" מתוך אחת המצגות המסווגות שהודלפו



תמונה 4: תוכנת Muscular- שקופית ארכיטקטורת המאמץ על גוגל מתוך אחת המצגות המסווגות שהודלפו

מאמצן של סוכנויות הביון בבניית תוכנות איסוף מידע שכאלה ותוכנות ניתוח לכמויות כה גדולות של מידע היה ללא ספק עצום. אך במקביל עלה החשד להפרה גסה של זכויות אזרחיות המעוגנות בחוקת ארה"ב, כפי שטענה במאמרה גם פרופ' לורה דונהיו מאוני' ג'ורג'טאון.[47] נשיא ארצות הברית בעצמו, ברק אובמה, בנאומו ביום למחרת פרסום החומרים המסווגים אמר [ההדגשות שלי]:

[47] Laura K. Donohue, " NSA surveillance may be legal — but it's unconstitutional," *The Washington Post,* June 21 2013. http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html

"You can't have 100 percent security and then also have 100 percent privacy and zero inconvenience. You know, we're going to have to make some choices as a society."[48]

במאמר צד ניתן רק לתהות על השימוש שנעשה במידע הצבור עלינו על ידי חברות התקשורת עצמן. אם סוכנויות הביון היו צריכות למצוא פרצות כדי לשים ידן על מידע כה יקר ערך, הרי שבמקרה של חברות התקשורת– הן שומרות הסף של המידע הזה. בהקשר זה קישר ג'וליאן אסאנג' בספרו בין ציטוט של העיתונאי טום פרידמן, בעל הטור בניו יורק טיימס, משנת 1999: "ידו הנעלמה של השוק החופשי לא תצלח ללא אגרוף נעלם. מקדונלדס לא תשגשג ללא מקדונל-דאגלאס, מתכנן ה – F15. והאגרוף הנעלם שמאפשר לטכנולוגיות של עמק הסיליקון לשגשג בעולם נקרא הצבא, חיל האוויר, חיל הים וחיל הנחתים של ארצות הברית."[49] לבין ציטוט המופיע בספרם של אריק שמידט, מנכ"ל גוגל, וג'ארד כהן, ראש חטיבת Google Ideas, משנת 2013: 'מה שלוקהיד-מרטין היתה עבור המאה העשרים, הטכנולוגיה וחברות לאבטחת מחשבים יהיו עבור המאה העשרים ואחת."[50]

כוונותיהן השאפתניות של סוכנות הביון "לשבת על הברז" של תעבורת כמות מידע כה עצומה בכדי לאתר איומים פוטנציאליים (או קיימים) על שלום המולדת מעידות על גישה הנדסית, לפיה ככל שתהיה לך כמות גדולה יותר של מידע – כך גוברים סיכוייך לגלות איום חבוי. יתכן וגישה זו נכונה לצורך גילוי, למשל, רשתות טרור קטנות המתכננות פעולה כזו או אחרת (בהנחה ורשתות כאלו אכן משתמשות בכלים כגון ג'ימייל, פייסבוק או יוטיוב), אך באשר לזיהוי מגמות או למיפוי מערכות חברתיות מורכבות – הרי שהרשתות החברתיות מלאות במידע שהאזרח המוגן משתף מרצונו החפשי. ניתן כמובן להשתמש בניתוחים מדעיים מעמיקים בתחום זיהוי גורמים משפיעים (attractors) על מערכות מורכבות,[51] אך ניתן גם להשתמש במגוון חברות אזרחיות המפתחות אלגוריתמים אשר סוקרים את הרשתות החברתיות ומספקים מיפוי מוצלח למדי של המערכות על מרכיביהן.

למשל, פרוייקט "People Maps" שבראשו עומד דייב טרוי, הוא פרוייקט שמטרתו לחשוף קשרים חברתיים, קבוצות וקהילות באזור גיאוגרפי תחום.[52] המפה החברתית הנוצרת איננה בהכרח גיאוגרפית, אלא בעיקר מלמדת על שונות חברתית ותחומי עניין נפרדים או משיקים בין קבוצות אוכלוסייה שונות. למשל, נעיף מבט אל עבר מיפוי תחומי העניין הבולטים בעיר בולטימור, באמצעות פילוח הנושאים הפופולאריים העולים ברשתות החברתיות של תושבי העיר:

---

[48] Peter Baker and David E. Sanger, "Obama Calls Surveillance Programs Legal and Limited," *The New York Times,* June 7, 2013. http://www.nytimes.com/2013/06/08/us/national-security-agency-surveillance.html

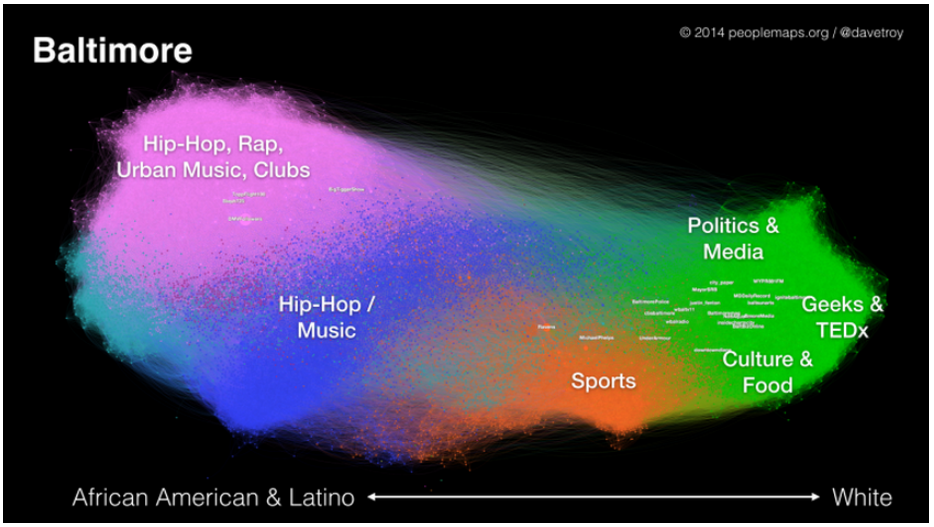
[49] Thomas Friedman, "A Manifesto for the Fast World," *New York Times,* 28 March 1999. archive.today/aQHvy

[50] Eric Schmidt and Jared Cohen, **The New Digital Age,** British paperback edition (John Murray, 2013), p. 98.

[51] ראו, למשל:
Maksim Kitsak, Lazaros K. Gallos, Shlomo Havlin, Fredrik Liljeros, Lev Muchnik, H. Eugene Stanley & Hernán A. Makse, "Identification of influential spreaders in complex networks," *Nature Physics* vol. 6, 2010, pp. 888–893.

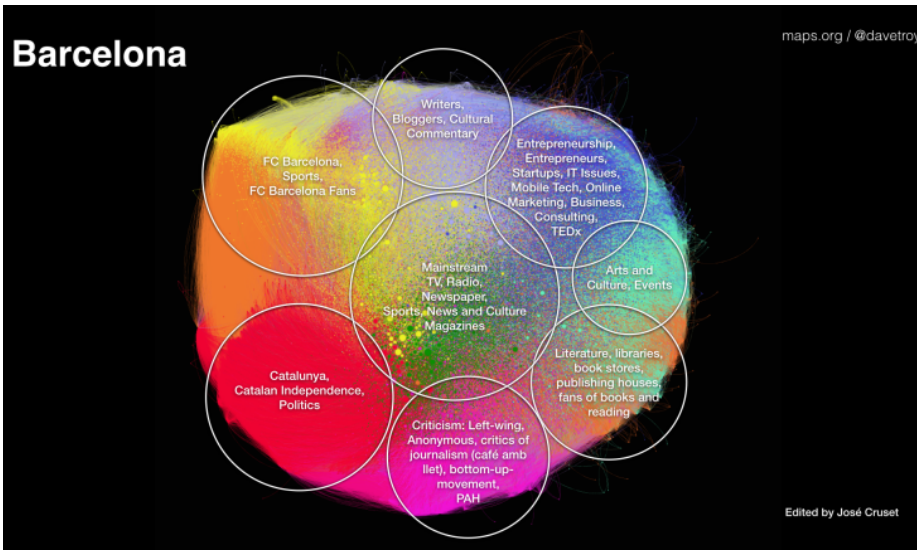
[52] http://peoplemaps.org/

ראו גם הרצאתו ב – TED:
http://www.ted.com/talks/dave_troy_social_maps_that_reveal_a_city_s_intersections_and_separations



תמונה 5: פילוח חברתי של העיר בולטימור, לפי שיטת אתר "People Maps"

במפה, כל נקודה מסמלת אדם (או שם משתמש), כל קו מסמל קשר בין אנשים, ואילו כל קבוצת צבע מסמלת קהילה בעלת תחום עניין משותף.
במפה החברתית של בולטימור ניתן לראות סגרגציה גזעית מובהקת. המפה כמעט מחולקת לשניים – בצד שמאל של המפה נמצאים בעיקר תושבים ממוצא אפרו-אמריקאי ולטיני, ומימינה – בעיקר לבנים. ניתן לראות גם את תחומי העניין המאפיינים את שני הקצוות, כמו גם את העובדה כי לא קיים תחום עניין ברור המקשר בין השניים.
לעומת זאת, המפה החברתית של ברצלונה נראית אחרת לגמרי:



תמונה 6: פילוח חברתי של העיר ברצלונה, לפי שיטת אתר "People Maps"

מעבר לגיבוש החברתי היחסי הניכר מצורת התפזרות תחומי העניין (כדורית), ניתן גם לזהות בבירור נושאים "חמים" עליהם סוערות הרשתות. למשל, ביטויים פוליטיים לעצמאות קטלוניה היא תחום עניין

משמעותי המאגד קבוצה גדולה של אנשים סביבו, המקושרים, באופן לא מפתיע, לקבוצה גדולה של אנשים המזוהים יותר עם אוהדי מועדון הכדורגל ברצלונה (FCB). כלל הקבוצות סובבות סביב תרבות מיינסטרימית (ומכאן שמה...) וסביב חדשות היום. כמו כן, ניכר מהמפה כי למתעניינים בטכנולוגיה, סטארטאפים ועסקים יש מעט מן המשותף עם אוהדי הכדורגל מחד, ועם תושבים המזוהים עם השמאל הפוליטי ותנועות חברתיות (bottom-Up-movement) מאידך.
ניטור קבוע של מפות מסוג זה מאפשר זיהוי היווצרותן של מגמות ופערים, ומאפשר זיהויים של הנעדרים מן השיח המרכזי. מיפוי דעותיה ומחשבותיה של חברה מאפשר לפרקטיקן (הן הממסדי הן אחר) במרחב הסייבר את היכולת להשפיע בצורה אפקטיבית על קהלי יעד רצויים – בין אם לצורך ניווט מגמות ובין אם לצורכי הגנה.

כלל הגורמים והתופעות שנסקרו בחלק זה - ויקיליקס, אנונימוס, האקרים פרטיים, השימוש שעושים באינטרנט ארגוני טרור ומדינות, תכניות PRISM ו- Muscular, ושיטות למיפוי רשתות חברתיות, למעשה מבטאים שני צידי מתרס של המלחמה המתחוללת בתקופתנו על המידע. שלל התופעות שנסקרו מתחלקות לשתי קטגוריות – האחת, היא יצירת השפעה במרחב הסייבר. השנייה, היא הניסיון להתמודד עם יצירת ההשפעה ולהשתלט עליה. שתי הקטגוריות מייצגות גם שתי תפיסות המנוגדות זו לזו. הראשונה, "נשקו של הקטן", מציעה גישה רכה להפעלת כוח במרחב הסייבר, ואילו הגישה השנייה, המדינית, היא הקשה והטוטאלית בתפיסתה. מיותר לציין פעם נוספת כי זירת מרחב הסייבר היא מערכת מורכבת שלא ניתן להשתלט עליה אלא לכל היותר לתרום את כלי הנגינה שלך בסימפוניית הביטים. ואכן, על אף תקציבי עתק המועברים מדי שנה לפיתוח טכנולוגיות שיאפשרו שליטת הממסד ב"בן הקיברנטי הסורר" – נראה דווקא כי השפעת הכוחות הלא מדינתיים, האזרחיים, על פתיחות מרחב הסייבר רק עולה.

סיכום

"ידוע לי כי בני האדם סבורים שענייני העולם נשלטים על ידי המזל ואלוהים, וכי האנשים, עם כל כישרונותיהם, אינם מסוגלים לשנות את מה שקבעו אלה. מכך עלולה לנבוע המסקנה כי אין טעם לטרוח ולשנות דברים ומוטב להניח להם להתגלגל בנתיב גורלם. [...] דומה הדבר לאותם נהרות הרסניים, אשר עולים על גדותיהם ושוטפים עצים ומבנים העומדים בדרכם, מעבירים אדמה מאזור לאזור, מבריחים כל מי שמסוגל להימלט, ללא כל יכולת לעצרם. למרות שכך הוא הדבר, בני האדם, בזמנים כתיקונם, מסוגלים לצפות את הדבר מראש ולהתקין תעלות וסכרים באופן שבעת השיטפונות המים יוטו לתעלות ונזקם לא יהיה כה רב. כך הם פני הדברים גם בכל הקשור למזל. הוא מפגין את עצמתו במקום שבו לא נמצאה תושייה לנקוט באמצעים כדי לעמוד בפניו, והוא מכוון את מכותיו לאותם מקומות שבהם לא הקימו סכרים ותעלות כדי לרסנו."[53]
ניקולו מקיאוולי

בנותנו עצות חכמות (אם כי שנויות במחלוקת) לשליטי איטליה לדורותיהם, העניק לנו מקיאוולי עצה חכמה להתמודדות עם מרחב הסייבר. בעידן שיטפון המידע בו אנו חיים, שיטפון שרק ילך ויגבר, נראה כי הדרך הנכונה להתמודדות ראויה עמו היא לא בניסיון לשלוט בימים ובנהרות, אלא בבניית סכרים ותעלות, בהשפעה ולא בהשתלטות.
השינוי התפיסתי שחל בקרב קהילת אבטחת הסייבר, שתואר בתחילת חלקו השני של המאמר, היא סנונית ראשונה ומבורכת להתמודדות מערכתית מורכבת עם אתגרי המחר. המעבר מתפיסת "הגנה בעומק" המורכבת משכבות שכבות של מגנים לתפיסה של "הגנה קדמית" מקיפה נבע מההבנה כי אין באפשרות חברות האבטחה לשלוט בתעבורת המידע לכלל עמדות הקצה המצויות בכל בית ולהבטיח כשרותה, אלא יש לווסת את תנועת המידע לכדי אזור מוגדר ומאובטח באמצעות שכבת הגנה קדמית אחת חזקה.
בהמשך, תיארתי מגמות, תופעות ופרקטיקות שונות המאפיינות את הפעילות במרחב הסייבר של ימינו. "במאבקי הכוח הללו", כפי שכתבה פרופ' קרין נהון בהקדמה לספרו של אסאנג', "יש צדדים למאבקים, אולם הסתכלות על מאבקים אלה כמאבקים של טוב נגד רע, אנרכיסט נגד קונפורמיסט, לוחם חופש המידע אל מול תאב השליטה, היא פשטנית ומתעלמת מהמורכבות של מאבקים אלו".[54] מדובר במאבק מרתק בין תפיסות עולם שונות (למרות שבכולן הקידמה הטכנולוגית מוצבת כאידיאל דטרמניסטי בהתפתחותו), המיוצגות, אמנם, על ידי גופים וארגונים ענקיים, אך בסופו של דבר, המחזיקים בהן בני אדם. כל גולש אינטרנט, בבחירות שהוא עושה מדי 'לייק' (אם הוא בחר להיות בפייסבוק), הוא בעל פתק הצבעה לתפיסות העולם השונות הללו.
תורת המערכות המורכבות, שהוצגה בקיצור נמרץ בחלקו הראשון של המאמר, היא אחד הכלים להבנת העולם הסבוך בו אנו מתפקדים מדי יום. ההכרה בהיעדר סופיות המידע והאפשרויות, ובטבע המשיכה החברתית ל'מעצבים' זמניים הינם כלים חשובים מאין כמותם במימוש אחריותנו כאנשי צבא (בחשיבתנו על האתגרים וההזדמנויות הביטחוניים והשלומניים של המחר), כאזרחי מדינה (המעצבים כל אחד

---

[53] ניקולו מקיאוולי, **הנסיך**, (בתרגום גאיו שילוני), (תל אביב: זמורה ביתן, 1988). פרק 25.
[54] קרין נהון, הקדמה לג'וליאן אסאנג', 2014; עמ' iii.

בחלקתו את האקוסיסטם החברתי בו ילדנו יגדלו), וכשותפים למערכת אמונות ועקרונות חובקי עולם (כבעלי קול, שבעוצמתו כבר שינה סדרי עולם בעבר).

בטרם אסיים, חש אני חובה בפני הקורא להסביר, סוף סוף, את שמו של המאמר. ובכן, האגדה, מהמיתולוגיה היוונית, מספרת כך: לפני שמינוס היה למלך כרתים, הוא התפלל לאל פוסידון, וביקש סימן שיאשש שהוא זה שצריך לקבל את כס המלכות, ולא אחיו. בתמורה, הוא הבטיח להקריב לפוסידון את היצור שייצא מהים. פוסידון שלח לו פר לבן ויפהפה, אך מינוס, שרחמיו נכמרו על היצור המופלא, הקריב במקומו שור רגיל. פוסידון, נזעם מהפרת ההבטחה, גרם לפסיפאה, אשתו של מינוס, להזדווג עם הפר, וכתוצאה מכך נולד המינוטאור - יצור כלאיים של שור ואדם. המינוטאור היה יצור אכזר ופראי שהטיל את חיתתו על תושבי כרתים, ולכן מינוס, בעצתו של האורקל מדלפי, כלא אותו בלבירינת (מבוך).

באותה תקופה הכריז מינוס מלחמה על אתונה, כיוון שרצה לנקום באתונאים שרצחו את בנו. אתונה נוצחה במלחמה, וכעונש, נדרשה לשלוח, מדי תקופה קבועה, שבעה נערים ושבע נערות אל תוך הלבירינת, כדי שיהיו טרף עבור המינוטאור. בהמשך, תסאוס, בנו של מלך אתונה, התנדב להישלח אל תוך המבוך, במטרה לשים קץ ליצור ולהורגו. למרבה מזלו של תסאוס, לפני שהוא נשלח ללבירינת, אריאדנה, בתו של המלך מינוס, התאהבה בו וגמרה אומר לסייע לו להשמיד את המינוטאור. היא העניקה לו פקעת חוטים, כדי שיוכל לשוב על עקבותיו ולצאת מן המבוך. תסאוס אכן הרג את המינוטאור, והוביל את שאר האתונאים החוצה מן הלבירינת.

מינוס, בזעמו על תסאוס שהצליח לברוח מן הלבירינת, החליט להעניש את דדלוס על כשלונו בבניית הלבירינת כמקום ללא מוצא, וכלא אותו ואת בנו איקרוס במבוך. עם זאת, בזכות תושייתו וכושר המצאתו של דדלוס, הצליחו השניים לברוח לחופשי, בכך שהם בנו לעצמם כנפיים מנוצות ומשעווה.[55]

בראייתי, קווי דמיון רבים נמתחים בין האגדה על מבוכו של המינוטאור לבין סיפור מרחב הסייבר של ימינו. שניהם מעשה ידי אדם, בשניהם מתקיים מאבק, ובשניהם ניתן ללכת לאיבוד. סוד נצחונו של תסאוס לא היה רק בגבורתו על המינוטאור, אלא בשבירתו את היגיון המבוך עם פקעת החוטים. יתכן ואהבה ונועזות הם כלים לא רעים להתמודדותו של כל אחד, עם המינוטאור שלו.

ואם פקששת ונכלאת במבוך – אל תאמר נואש. שבירת הפרדיגמה תבוא גם מחזון הנישא על כנפיים.

---

[55] ויקיפדיה. *מינוטאורוס*. http://goo.gl/f3T20e