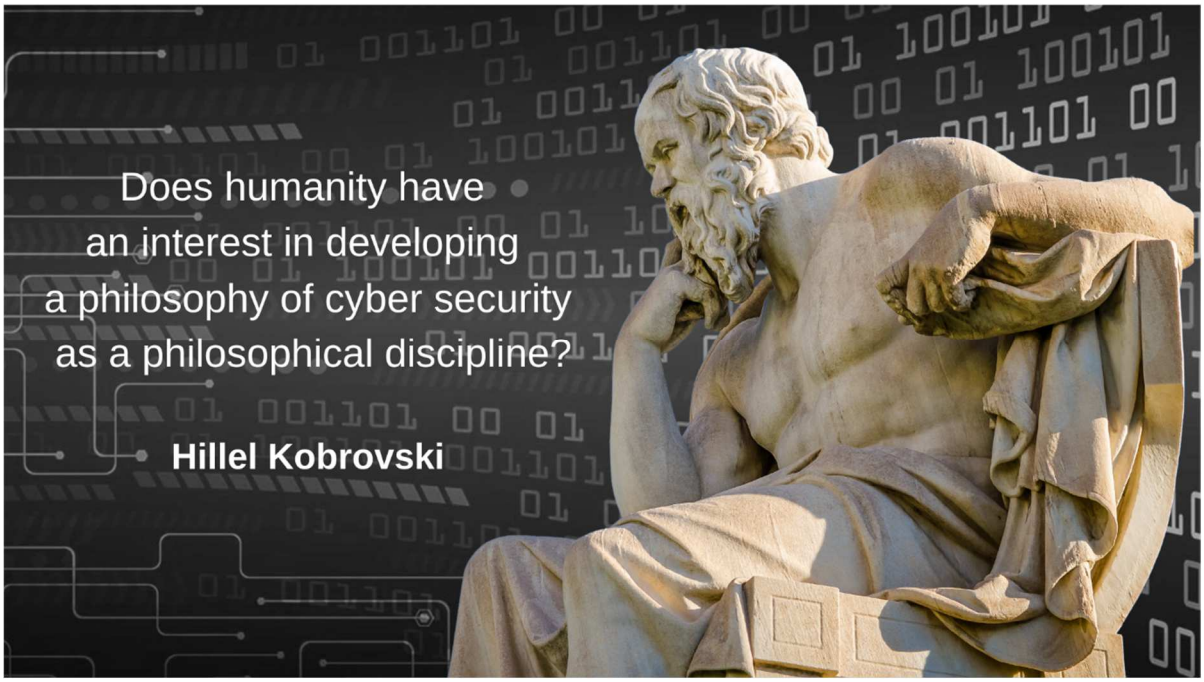


האם לאנושות יש אינטרס לפתח פילוסופיה של אבטחת סייבר כדיסציפלינה פילוסופית ?

מאת: הילל קוברובסקי

חלוקה לנושאים:

1. מבוא - מהם האתגרים בתחילת הדרך על מנת לבנות מהיסוד ולפתח דיסציפלינה חדשה בתחום הפילוסופיה ?.
2. מהי משמעות המושג "מרחב הסייבר" לעומת "אבטחת הסייבר", מהם גבולות התיחום של הענף הקרוי סייבר ?.
3. מהי פילוסופיה ?, מהן הפילוסופיות שיכולות להוות השפעה עבור הפילוסופיה של אבטחת הסייבר ?.
4. מהן הבעיות והשאלות המהותיות בהן צריכה לדון הפילוסופיה של אבטחת הסייבר ?.
5. מהם הגורמים שיכולים להוות קטליזטור להתפתחות דיסציפלינה פילוסופית עצמאית בתחום אבטחת הסייבר.
6. סיכום – האם לאנושות יש אינטרס לפתח פילוסופיה של אבטחת הסייבר כדיסציפלינה פילוסופית ?.

1. מבוא - מהם האתגרים בתחילת הדרך על מנת לבנות מהיסוד ולפתח דיסציפלינה חדשה בתחום הפילוסופיה ?.

1.1 מבוא למאמר: איך בכלל הגעתי לכתוב על הנושא?

בראיון שערכתי **לפילוסוף והפיזיקאי פרופ' יוסף אגסי** [1] במהלך חודש דצמבר 2021, שאלתי אותו מהיכן נובעת המוטיבציה שלו בקריירה שנמשכת כבר מעל 70 שנה לפרסם קרוב ל-600 מאמרים אקדמיים ומעל 35 ספרים שכתב וערך במגוון נושאים: פיזיקה, פילוסופיה (מדע, טכנולוגיה, אסתטיקה, אתיקה, פוליטית ועוד), דת-ולאום, פסיכולוגיה, סוציולוגיה, טכנולוגיה ועוד, התשובה שלו כפי שנשמרה בזיכרוני היתה מאוד פשוטה, "תכתוב על מה שמעניין אותך, ועל השאלות שמטרידות אותך, כך אף פעם לא יהיה חסר לך נושאים לכתוב עליהם".

תשובתו של פרופ' אגסי כמי שאני מקבל ממנו השראה מקצועית רבה מאוד שינתה משהו בהסתכלות שלי על האופן בו כך אפשר לשלב ולחבר בין תחומים מקצועיים שונים. כמי שמתעקש בעצמו להתמחות וללמוד מספר רב של תחומים, באופן עצמאי, מקצועי או אקדמאי, מצאתי שאני מצליח להבין לעומק הרבה יותר טוב את ההתמחות הראשית שלי בתחום אבטחת הסייבר כתחום מקצועי שבו אני עוסק מעל ל-25 שנה, אך ורק כאשר אני מסוגל לפרש את התופעות, הטרנדים והמגמות מתחום אבטחת הסייבר לאחר שאני בוחן, מנתח ומפרש אותן בעזרת "כלים" מתחומי מדעי החברה והרוח בהם: פילוסופיה, פסיכולוגיה, סוציולוגיה, כלכלה, ובעזרת "כלים" (מתודות עבודה) מתחומי פיתוח חדשנות ארגונית \ רעיונאות מוצרית, חקר עתידים לטווח ארוך המתבסס על גישה מדעית של "חקר מערכות מורכבות" [2] , טרנדולוגיה כחקר מגמות עתידיות המתפתחות בטווח קצר, "תרבות תקשורתית" [3] בעידן החדש בו המדיה מעצבת וקובעת את מאפייני התרבות, ולבסוף הסתכלות מקרו הבוחנת את השפעות ההתפתחות הטכנולוגית המואצת על עתיד האנושות מבחינות רב-תחומיות ורב-מימדית.

היות וזה אתגר אִינְטֶלֶקְטוּאֶלִי לרכוש ידע במקביל בהרבה תחומים מקצועיים, מצאתי שכתיבה היא דרך מאוד אפקטיבית "לְפַרְמֵל" [4] מידע ולהפוך אותו לידע או תובנות מעמיקות. **ד"ר ג'ורדן פיטרסון** בהרצאות שלו [5] מסביר כי כתיבה שווה חשיבה, היות וכתיבה זה תהליך הדורש ממך חשיבה מעמיקה מקדימה על מה שאתה רוצה לכתוב עליו, תהליך "פּוֹרְמָלִיזַצְיָה" של הידע שלך עד לשלב בו אתה מחבר תובנות מעמיקות ורב-תחומיות שהפנמת בתהליך הלימוד שלך.

מאמר זה הוא ניסיון הנובע מתוך סקרנות אישית שלי לבחון את השאלה המוצגת, "**האם לאנושות יש אינטרס לפתח פילוסופיה של אבטחת סייבר כדיסציפלינה פילוסופית ?" ,** ברצוני לבחון במאמר צעד אחרי צעד, איך כן אפשר לבנות גשר רעיוני בין **הפילוסופיה המערבית** לבין תחום **אבטחת הסייבר**, בנוסף לבחון מה האנושות תרוויח מפיתוח של פילוסופיה של אבטחת הסייבר כדיסציפלינה פילוסופית נפרדת.

בחרתי "להנגיש" את הדיון בנושא לקהל רחב ככל האפשר, כך שהמאמר אינו מחויב למגבלות או דרישות של מאמר אקדמאי או מאמר מחקרי ולכן המאמר אינו מחויב להנחיות או דרישות של האקדמיה למאמר מסוג כזה. אולם אם מצאתם\ן טעות כלשהי בדבריי, הרי שזו באחריותי בלבד, ואשמח לכל הארה והערה שלכם\ן כדי לתקנה.

---

1 **הפילוסוף פרופ' יוסף אגסי** – רקע כללי – לינק

2 **חקר מערכות מורכבות** - מערכת מורכבת היא מערכת המכילה מספר גדול של מרכיבים אשר משפיעים זה על זה. מערכות מורכבות מופיעות בתחומים רבים כולל פיזיקה , סוציולוגיה, כלכלה , ביולוגיה , פסיכולוגיה, טכנולוגיה, מטאורולוגיה, ניהול וכיוצא בזה. מקור

3 **תרבות תקשורתית** = תרבות היא תוצר של תקשורת המונית.

4 "**לפרמל**" = להפוך לנוסחה – נגזר מהמילה הלועזית פורמולה.

5 **ד"ר ג'ורדן פיטרסון** - מה שכחו ללמד אותך במסגרת התואר באוניברסיטה ומהו הנשק החזק ביותר בעולם? - לינק

1.2 החיבור שבין טכנולוגיה לפילוסופיה – תחילת הדרך:

השאלה הפשוטה כביכול, **האם לאנושות יש אינטרס לפתח פילוסופיה של אבטחת סייבר כדיסציפלינה פילוסופית ?** מטרידה אותי מזה כשנתיים, מאז התחלתי לימודים אקדמאיים מסודרים בתחום הפילוסופיה, שנתיים שבמהלכן השקעתי שעות רבות של חיפושים ברשת, קריאה ועיון בעשרות ספרים שונים העוסקים בחיבור שבין פילוסופיה – חברה – טכנולוגיה [6], במטרה להגיע להסבר רציונלי מהן הסיבות שעד היום לא מתקיים בשום מסגרת אינטלקטואלית כזאת או אחרת, שיח פילוסופי-טכנולוגי שדן באופן ממוקד בכל האתגרים המהותיים שתת-ענף אבטחת הסייבר מציב בפני הקהילה המקצועית שעוסקת בו, ובכלל זה אתגרים שענף הסייבר מציב בפני האנושות כולה.

מחד גיסא מתנהל שיח אקדמי ומחקר פילוסופי בתחומים של "**הפילוסופיה של הטכנולוגיה**" [7] וה "**פילוסופיה של המידע**" [8] ומאידך גיסא, באופן מפתיע, ולמרות הרלוונטיות הגבוהה וההשפעה של פילוסופיות אלו על החיים שלנו בהיבטים שונים (כלכליים, חברתיים, תרבותיים, גיאופוליטיים, טכנולוגיים), תחומים אלו ממש לא בולטים בחשיבותם, ואינם נמצאים ב"קדמת הבמה" הפילוסופית מתוך רשימה מאוד ארוכה [9]. הרשימה כוללת פירוט של כמה עשרות פילוסופיות בתחומים שונים, דיסציפלינות פילוסופיות שרובן התפתח רק בתחילת המאה העשרים.

בעידן של מידע הזמין לכולם ללא גבולות או מגבלות, התחלתי בחיפושים מעמיקים ומורכבים בפלטפורמות שונות [10] , פלטפורמות שיתוף ידע המשמשות חוקרי אקדמיה, מרצים וסטודנטים העוסקים בתחום הפילוסופיה.
בחיפושים אלו גיליתי שעד היום פורסמו מאמרים בודדים בלבד שעוסקים בחיבור שבין אופן החשיבה והחקירה הפילוסופיה לבין הטכנולוגיות הקשורות לענף הסייבר, חלק גדול מאותם מאמרים שעסקו בתחום נשא את הכותרת הכוללת את מילת ההלחם "**CyberPhilosophy**" משמע "**פילוסופית הסייבר**", ברם רובם ככולם (כולל ספר שנכתב בשנת 2003 בתחום זה [11]) **עוסקים בתחומים של "<u>מרחב</u> <u>הסייבר</u>"**, כך שלא גיליתי ולו מאמר אחד שפורסם ושותף ברשות הרבים, בו נבחנות לעומק הסוגיות המאתגרות ביותר התלויות והקשורות לענף הסייבר, ולמען הסר ספק ההתייחסות למונח סייבר היא בהקשר של Cyber Security , מונח הכולל את תת-התחומים: סייבר הגנתי \ סייבר התקפי \ אבטחת מידע \ הגנת הפרטיות, תחומים אשר כל אחד בפני עצמו מציב לחברה האנושית אתגרים מהותיים <u>שכבר היום משפיעים באופן בלתי הפיך על עתיד האנושות</u>, היבטים המשנים את המציאות הכלכליות, החברתיות, התרבותית, הגיאו-פוליטיות והטכנולוגית, החל מסוגיות הקשורות לאתיקה (פילוסופיה של המוסר), סוגיות הקשורות לתחום התפתחות הטכנולוגיה והשימוש שאנחנו עושים בה לטובת או לרעת האנושות (הפילוסופיה של הטכנולוגיה), סוגיות הקשורות בתחומי מחקר של: סוציולוגיה \ פסיכולוגיה על מנת להבין ולנתח לעומק את ההתנהגות האנושית (פילוסופיה של הנפש), סוגיות הקשורות במתודולוגיה לקבלת החלטות מבוססות תבונה מלאכותית או החלטות אנושית בתוך כאוס נתונים אין סופיים (לוגיקה – תורת ההיגיון), סוגיות הקשורות להתפתחות עתידית של ענף הסייבר: כיצד מתועדת ההיסטוריה של הסייבר (היסטוריוסופיה של הסייבר) [12], היות ואין טכנולוגיה בענף הסייבר שהומצאה "יש מאיין", אלא קיימת שרשרת של פיתוחים, בדומה לאבני לגו, אבן יסוד אחת מתבססת על השנייה, כך שפיתוחים חדשים נולדים ומפותחים בהשראתם, בהשפעתם ובהתבוססותם של

---

6 בשפה העברית הספר "**הפילוסופיה של הטכנולוגיה**" מאת **פרופ' יוסף אגסי** , שיצא בהוצאה מיוחדת בשנת 2011, על ידי הוצאת משרד הביטחון \ הוצאת מודן, הוא הספר היחידי שעוסק בתחום זה. הספר הוא תקציר בעברית של הספר: Technology - Philosophical and Social Aspects - Dordrecht Kluwer – 1985 , ספר העוסק בחיבור שבין טכנולוגיה ופילוסופיה ופורסם בשפה האנגלית בלבד.

7 **פילוסופיה של הטכנולוגיה** – תחום פילוסופי חדש יחסית בהשוואה לדיסציפלינות פילוסופיות אחרות. למרות שהפיתוח הטכנולוגי מתקדם בקצב מהיר מאז תחילת המהפכה התעשייתית לפני מעל כ-200 שנה, החלו לעסוק בתחום זה רק בתחילת המאה ה-20 והדיון בנושא תפס תאוצה לאחר מלחמת העולם השנייה, בהקשר של שימוש בטכנולוגיות לפיתוח נשק להשמדה המונית.

8 **פילוסופיה של המידע** – ענף בפילוסופיה החוקר נושאים רלוונטיים לעיבוד מידע, תחום מדעי המחשב ומערכות מידע. בשנים האחרונות תחום זה נחקר גם הקשרים בתחומים של למידת מכונה \ בינה מלאכותית.

9 קיימות מספר רשימות ברשת המציגות **תחומים שונים של פילוסופיה**, לדוגמא: לינק

10 **אתרי אינטרנט בהם יש מאגרים ופרסומים של מאמרים או מחקרים אקדמיים** כדוגמת: researchgate.net , philevents.org, academia.edu ,jstor.org ועוד.

11 ספר בשם "**Cyberphilosophy: The Intersection of Philosophy and Computing**" שפורסם בשנת 2003 על ידי העורכים: James H. Moor & Terrell Ward Bynum

12 **היסטוריוסופיה** = חקר ההיסטוריה של התפתחות בתחום מסוים

הצלחה במימוש בפועל של טכנולוגיה קיימת. בתחום **הטרנדולוגיה** [13] בגלל ההשפעות הרבות של תופעות "**החדשנות המשבשת**" מקובלת הטענה בקרב העוסקים בחקר טרנדים ומגמות לטווח קצר כי "העבר אינו מעיד על העתיד". לא כך הדברים בתחום אבטחת הסייבר היות ושום טכנולוגיה נוכחית אינה נזרקת לפח ובטח שאינה מוחלפת בין לילה, **למעשה ברוב המקרים אנחנו רואים בעיקר השתכללות והתייעלות של שימוש בטכנולוגיה קיימת**. החשיבות הגבוהה של תחום היסטוריוסופיה (חקר ההיסטוריה) של הסייבר היא על מנת להבין ולבחון לעומק איזה טכנולוגיה \ מתודולוגיית עבודה \ רגולציה השפיעה באופן ישיר או עקיף על התפתחות של זאת הבאה בתור זאת שהחליפה אותה.

חשוב לציין כי בשנים האחרונות התפתח תחום אקדמי חדש ומרתק המשלב את תחומי **המדע, טכנולוגיה וחברה** (**STS**) [14] אבל גם הוא עוסק רק במעט מאוד היבטים הממוקדים והמיוחדים לענף אבטחת הסייבר.

2. מהי משמעות המושג "מרחב הסייבר" לעומת "אבטחת הסייבר", מהם גבולות התיחום של הענף הקרוי סייבר ?.

2.1 מה ההבדל בין "סייבר" ל "סייבר" ?

יש הפרדה מוחלטת בין שני שימושים לשוניים ומאד נפוצים שחשוב מאוד שנבחין בהן כאשר נאמרת או נכתבת המילה "סייבר", המשמעות הראשונה למילה סייבר היא כהתייחסות ל "**מרחב הסייבר**", מאידך ההתייחסות השנייה למילה סייבר היא במשמעות של "**אבטחת מידע**" בהיבט הכוללני והרב-ממדי שלה, דהיינו דיסציפלינה מתוך ענף טכנולוגית המידע שעוסקת בכל ההיבטים של שמירה והגנה של מידע במערכות ממוחשבות.

לצערי אף התיאור המקובל של "**מרחב הסייבר**" ("המרחב הקיברנטי" [15]) כפי שנתפס בקרב הציבור הנרחב, אינו ברור היטב למי שלא עוסק בתחום:

"המרחב הקיברנטי או הסייברספייס, סביבת רשת הוא מרחב מטפורי של מערכות מחשב ורשתות מחשב בו נאגרים נתונים אלקטרוניים ומתבצעת תקשורת מקוונת ואינטראקטיבית ללא תלות במיקום הגאוגרפי של המשתמשים בו.

...

מבחינה חברתית, המרחב הקיברנטי מאפשר למשתמשים בו לקיים דרכו אינטראקציה, להחליף רעיונות, לשתף מידע, לספק תמיכה חברתית, לקיים עסקים ומסחר, ליצור אמנות, לשחק במשחקים, לעסוק בדיון פוליטי וכן הלאה.

...

אין להתבלבל בין המונח לרשת האינטרנט עצמה. המונח מתייחס לעיתים רבות לאובייקטים ולזהויות הקיימים ברשת האינטרנט, כך שניתן לומר, מבחינה מטאפורית, כי אתר אינטרנט נמצא במרחב הקיברנטי. לפיכך, האירועים אשר מתרחשים באינטרנט אינם לוקחים חלק במדינות בהן המשתתפים או השרתים נמצאים פיזית, אלא "במרחב הקיברנטי."

המונח "**מרחב הסייבר**" או ה-**Cyberspace** בשפת המקור, גדל והתעצם מאז הוגדר לראשונה בתחילת שנות ה-80, המהירות המואצת בה טכנולוגיה מתפתחת הכניסה בטווח של 35-30 שנה לתוך המרחב ביליארדי אלמנטים שבקצה שלהם לא נמצא גורם אנושי, אותם אלמנטים פעילים ומקיימים אינטרקציה בינם לבין עצמם גם ללא

13 **טרנדולוגיה** - חקר טרנדים ומגמות לטווח קצר, בדרך כלל בהתייחסות לטווח של שנה עד שלוש שנים. כדי להבין לעומק מחקר טרנדולוגי מהו, ומהי המתודה המומלצת לבנות תחזיות ותרחישים לחיזוי פעילות עסקית עתידית בטווח קצר, אני ממליץ לעיין בספר "**הבא – השיטה לחזות טרנדים בעולם משובש**" של **עדי יופה** שיצא לאור בשנת 2019 , הספר המקצועי היחידי בעברית שעוסק בתחום הטרנדולוגיה.

14 **מדע, טכנולוגיה וחברה (STS - Science, Technology and Society)** תחום מחקר צעיר שהפך להיות אקדמי באופן רשמי רק בשנות ה-80 של המאה ה-20, תחום ה-STS הוא שדה מחקרי בין-תחומי הבוחן את השפעותיהם ההדדיות של פיתוחים מדעים וטכנולוגיים יחד עם גורמים חברתיים ופוליטיים. החוקרים בתחום מעלים שאלות לגבי ההשלכות של התפתחויות מדעיות וטכנולוגיות על החברה והתרבות, וכיצד תפיסות תרבותיות, חברתיות ופוליטיות שונות משפיעות על התפתחות המדע והטכנולוגיה. בנוסף, המחקר בתחום פועל לקידום מעורבות אזרחית וחשיבה ביקורתית לגבי התפתחויות מדעיות וטכנולוגיות. מקור: לינק

15 **המרחב הקיברנטי \ מרחב הסייבר** – מקור: לינק

התערבות גורם אנושי.

העתידן והפילוסוף הטכנולוגי, **קווין קלי**, (שזכה גם לכינוי "הדארווין של הטכנולוגיה") מי שהיה בעבר העורך והמייסד המגזין המפורסם Wired, פרסם בשנת 2010 ספר בשם "What Technology Wants" [16] ("מה הטכנולוגיה רוצה") בו הוא תיאר לראשונה את מושג "***הטכניזם***" (Technium) , **הטכנולוגיה כסופר אורגניזם חי**, טכנולוגיה הפועלת באופן עצמאי, מתקיימת באופן אוטונומי, ובמקביל הטכנולוגיה גם משנה את ההתפתחות האבולוציונית של בני האדם, קלי מגדיר את הטכנולוגיה "כממלכה השביעית של החיים" [17] זו הסתעפות חדשה מן הצורה האנושית. התחזית של קווין קלי [18] שעד לפני כ-15 שנה נשמעה דמיוניות, וכיום לכולם כבר ברור שזה העתיד שאליו האנושות "שועטת", כך ש"מרחב הסייבר" יכלול יותר אלמנטים טכנולוגים בעלי קיום עצמאי מאשר מספר בני האנוש החיים ברגע נתון בעולם. כדי להמחיש את המשמעות של מושג "הטכניזם" ממש לא צריך ללכת רחוק, אנחנו כבר קרובים ליום שבו כל אמצעי התחבורה בעולם המערבי יהיו אוטונומיים, כך שנשאלה השאלה לאיזה שינויים האנושות תצטרך להסתגל כדי שתחבורה אוטונומיות תפעל מקצה לקצה ללא תלות בבני אדם לצורך פעילותה, כאשר יש אינטרקציה אוטונומית מלאה בין הרכבים לבין עצמם, לבין הרמזורים (שבעתיד לא נצטרך אותם בכלל) לבין הכביש עצמו, לבין בני אדם אשר ישתמשו באותם רכבים אשר פועלים עצמאית ואוטונומית בתוך המרחב התחבורתי.

דוגמה נהדרת אחרת לתיאור הטכנולוגיה כ "סופר אורגניזם חי" היא החזון העתידי של ערים חכמות בו פחי אשפה ידווחו למשאיות איסוף האשפה האוטונומיות, איזה פח דורש פינוי מידי, כך שהמשאית תבנה מסלול אוטונומי על בסיס תנאים משתנים וקדימות, וכל ההתנהלות הזאת של פינוי אשפה תתנהל באופן אוטונומי ללא צורך של התערבות אנושית. עם צפי הגידול והצפיפות ההולכת וגוברת מיום ליום בערים המתועשות, למעשה לא תהיה לאנושות ברירה אלא להתמודד עם הצורך הבסיסי בכל עיר של פנוי אשפה ושמירה על רמת תברואה נאותה, אלא באופן אוטונומי כמתואר לעיל. לפי תחזית של הלמ"ס בישראל בשנת 2048 (בחגיגות ה-100 שנים להיווסדה) יחיו במדינת ישראל הצפופה מעל 17 מיליון תושבים [19] (לעומת 9 מיליון כבר היום). קשה לדמיין את החיים בערים צפופות הרבה יותר מבני ברק או תל אביב של היום, ללא טכנולוגיה כפי שתיארתי לעיל, כזאת שנהיה תלויים בה 24/7 על מנת לאפשר חיים סבילים בערים כל כך צפופות.

בסוגיות המהותיות המטרידות אותנו בהתייחסות למושג **סייבר בהקשר של "מרחב הסייבר"** דנים בהן במסגרות של תחומים שונים במדעי החברה, כדוגמת תארים אקדמאים המשלבים לימודים בתחומים של מדע, חברה וטכנולוגיה (תחום ה-STS כפי שהוזכר לעיל). בנוסף קיימת אליהן התייחסות שטחית גם בלימודים של מינהל עסקים, כלכלה התנהגותית, סוציולוגיה ואף בתחום השיווק. עיקר ההתייחסות ממוקדת באתגרים "שמרחב הסייבר" על שלל התופעות שבו, משפיעות עלינו כחברה רב-לאומית ורב-תרבותית, והשפעות באופן ישיר על כלל תחומי החיים בהיבטים: גיאו-פוליטיים, כלכלים, טכנולוגים, תעסוקה בעולם גלובאלי, ועוד.

מאידך גיסא, בהתייחסות להגנה על נכסי מידע דיגיטליים, **סייבר בהקשר של אבטחת מידע**, האתגרים והסוגיות הרבות בינהם היבטים: חברתיים \ משפטיים \ כלכליים \ פסיכולוגים \ גאו-פוליטיים \ טכנולוגיים, אתגרים מהותיים שקיימים ונוכחים בתוך ענף אבטחת הסייבר, הן אתגרים וסוגיות שדנים בהן באופן חלקי ביותר (אם בכלל). כפי שזה נראה כיום מבחינת האקדמיה לא נראה באופק התקדמות משמעותית ורצינית לממן ולקדם מחקרים בתחומים אלו.

16 כלכליסט, איתי להט, 18.11.2010, "**ניצחון טכני: קווין קלי מאמין שלטכנולוגיה יש חיים משל עצמה**" | ההארה של **קווין קלי**, עורך "Wired" ופילוסוף הטכנולוגיה המוביל בעולם, הטכנולוגיה עוד תשנה לגמרי את האופן שבו בני אדם תופסים את עצמם - לינק.

17 TED, 22 בפבר' 2010, הרצאת TED של קווין קלי בשם "**Kevin Kelly tells technology's epic story**" – לינק.

18 עוד על **Kevin Kelly** אפשר לקרוא באתר האינטרנט שלו – לינק.

19 ערוץ הדיגיטל של כאן 11, 15 באוג' 2022, "**בלי פאניקה!**" – פרק 4, **איך תיראה ישראל בחגיגות המאה?**, תאור הפרק: גורי אלפי ולוסי איוב מוצאים את עצמם בשנת 2048, מנסים לחיות במדינה שיש בה שבעה עשר מיליון תושבים ויוצאים למסע דוקומנטרי כדי לבדוק האם המדינה ערוכה למנוע את האסון הידוע מראש, לינק

ככל שהתעמקתי לנסות ולהבין **מה השפעת החדשנות הטכנולוגית המואצת על עתיד האנושות** [20], מבחינתי זה בלתי נתפס, הרי כל בר דעת אמור להבין על סמך ההיסטוריה הפרוסה לפנינו, כי ההשפעות של **המהפכה המדעית** שהחלה לפני מעל 500 שנה **והמהפכה התעשייתית הראשונה** מלפני 200 שנה [21] הן מהפכות שהשפיעו מקצה לקצה על כלל האנושות בכל ההיבטים. צריך להיות מובן לכל אדם החי במאה ה-21 כי בעיות ואתגרים שלא מטפלים ונותנים עליהם את הדעת בתחילת דרכם, משולות לכדור שלג במפולת שאי אפשר לעצור. את ההשפעות של המהפכה התעשייתית הראשונה אנחנו חשים על בשרנו כבר היום, קראנו לכדור השלג המתגלגל הזה: "**התחממות גלובלית**", ההשפעה והשינויים הקיצוניים באקולוגיה של כל כדור הארץ, כך שאף אחד מתושבי הכדור אינו יכול להתעלם מכך, ואינו חסין מההשפעות של "כדור שלג" זה שמתגלגל לעברנו כבר בעשור הקרוב עם תחזית מדעית מבוססת שהטמפרטורה בכל כדור הארץ תעלה בשתי מעלות [22].

ההתעלמות שלנו כיום מהבעיות והאתגרים של המהפכות הקודמות וזאת שכרגע רק בראשיתה, **מהפכת הבינה מלאכותית**, מהפכה שמכילה בתוכה הרבה טכנולוגיות חדשות, שחלקן רק בתחילת דרכן ולכן אנחנו עוד לא מסוגלים להבין לעומק מה האופן שבו הן ישנו את האנושות מקצה לקצה. צריך להיות מובן לכל אדם בר-דעת כי אף מדינה או אפילו מעצמה גדולה אינה יכולה לבדה לתת מענה לבעיות והאתגרים הגלובליים, לאנושות יש רק ברירה אחת, להגיע להבנות משותפות ולהתמודד עם האתגרים באופן גלובלי, שכן אם האנושות כולה לא תתאחד כבר היום לתת מענה כלשהו לאותם אתגרים לא פתורים, אתגרים שיש להם השפעה ישירה ובלתי הפיכה על העתיד של כלל הציוויליזציה האנושית: **האתגר הגרעני** (שימוש בטכנולוגיה אטומית), **האתגר האקולוגי** (ההתחממות הגלובלית), **האתגר הטכנולוגי** (אבטחת הסייבר\מרחב הסייבר הם בהחלט חלק מהותי ומרכזי בו), הם יהפכו להיות בעיות משותפת של כלל תושבי כדור הארץ (צמחיה, בעלי חיים, בני אדם).

כפי שלמדו הלודיטים על בשרם במהפכה התעשייתית הראשונה, וכפי שהוכח מאז אין ספור פעמים, את הטכנולוגיה לא ניתן לעצור או להאט את מהירות ועוצמת התפתחותה, אפשר רק להסתגל אליה במהירות ובחוכמה ע"מ להפיק ממנה, בתהליך ארוך, תועלות מגוונות לרווחת האנושות. הפילוסוף הגרמני-יהודי **הנס יונאס** [23], טען לפני כ-40 שנה כי **האנושות כבר מזמן אינה שולטת בטכנולוגיה, אלא הטכנולוגיה שולטת באנושות**. בתחרות של "הטכנולוגיה למול האנושות" יש הצופים כי ההתנגשות בין המכונה לאדם היא בלתי נמנעת [24]. בהסתכלות רחבה על הווה, אפשר לעת עתה להסיק כי האנושות כבר הפסידה לטכנולוגיה, הטכנולוגיה מתפתחת מהר יותר ממה שרוב בני האדם מצליחים להסתגל אליה, והציוויליזציה האנושית תלויה באופן מלא בטכנולוגיה להמשך קיומה. אולם אין פה שאלה מי שולט במי, ואיך האנושות תנצח, היות שבשל הטבע האנושי זו מלחמה אבודה שלא ניתן להשיג בה ניצחון. השאלה שאנחנו כאנושות חייבים לשאול את עצמנו היא איך "תוך כדי

---

20 קהילת פייסבוק הנושאת את אותו השם ועוסקת בנושאים של "**השפעת החדשנות הטכנולוגית המואצת על עתיד האנושות**" – לינק.

21 **מקובל לחלק את המהפכות התעשיות הגדולות שהאנושות עברה ועדיין עוברת לארבע מהותיות** | הראשונה: "**מהפכת הקיטור**" האדם מנצל את כוח הקיטור כדי להעצים את כוחו של האדם המפעיל מכונה במפעלים. נק' מפנה: 1784 - נול מכני הראשון | השנייה: "**מהפכת החשמל**" האדם מנצל את כוח החשמל כדי לבנות ולהעצים את קווי היצור בתעשייה, תחילתו של עידן הייצור ההמוני. נק' מפנה – 1870 – מסוע חשמלי ראשון | השלישית: "**מהפכת הדיגיטל**" האדם מנצל את היכולת של מערכת המחשב להפוך את קווי הייצור לאוטומטים עם פחות כ"א אנושי, ועד שימוש נרחב במחשבים אישיים ורשת האינטרנט. נק' מפנה – 1969 – בפעם הראשונה נעשה שימוש בבקר לוגי הניתן לתכנות | הרביעית: "**מהפכת הבינה מלאכותית**" התלכדות של טכנולוגיות, כוח העיבוד גדל בצורה משמעותית, מחשוב קוונטי, ביג דאטה, AI/ML, מחשוב ענן ציבורי, המעבר מאוטומציה לאורקסטרציה. נק' מפנה: בינה מלאכותית: תוכנה שכותבת את עצמה, עיבור נתונים מהיר מכל מוח אנושי, שיפור ותיקוף אין סופי.

22 מאמר מתוך האתר של **נאס"א** (סוכנות החלל האמריקאית) נכתב על ידי Alan Buis, פורסם בתאריך 19-June-2019 תחת השם A Degree of Concern: Why Global Temperatures Matter – לינק

23 **הנס יונס** (1903 – 1993) פילוסוף יהודי-גרמני, עסק בפילוסופיה של המדע \ הטכנולוגיה (ובהשלכות המוסריות של המדע \ טכנולוגיה) , היה תלמידו של הפילוסוף אדמונד הוסרל ,של הפילוסוף (הנאצי) מרטין היידגר (עד שנת 1933) ושל התאולוג רודולף בולטמן. היה חבר כיתה של הפילוסופית חנה ארנדט ואף השפיעה עליה מבחינה פילוסופית. ספרו "ציוויה של האחריות" שיצא לאור בגרמנית ב־ 1979 ותורגם לאנגלית ב־ 1984, מתרכז בבעיות המוסר החברתי שהטכנולוגיה מעמידה בפני המין האנושי. יונאס עומד על כך כי הישרדותו של האדם תלויה במאמצינו לשמור על כוכב הלכת שעליו אנו חיים ועל עתידו. הוא פיתח עיקרון מוסרי חדש: "עלינו ללמוד לחיות כך שפעילותנו תהלום חיים אנושיים אמיתיים ועקביים." ספרו זה המריץ את מדע האקולוגיה ואת הנושא של חשיבה סביבתית. מקור – לינק.

24 בספרו של העתידן **גרד לאונהארט** , "**הטכנולוגיה מול האנושות – ההתנגשות הקרובה בין אדם למכונה**" * שיצא לאור בשנת 2016 נטען כי האנושות תשתנה ב-20 שנה הקרובות יותר מאשר ב-300 שנה האחרונות, קצב השינויים ילך ויגבר באופן מהיר ואקספוננציאלי (מעריכי) כך שנכון להיום אין ביכולתנו להבין ולאמוד כיצד תראה האנושות בעוד מספר עשורים.

* "Technology vs. Humanity: The coming clash between man and machine" - Gerd Leonhard's

תנועה" נקטין ונצמצם את הפערים והנזקים שכבר נגרמו, נתקן ונשפר את הנזקים הדחופים, כדי שנבטיח את המשך קיום האנושות בכדור הארץ. אין בכוונתי לצבוע את העולם בדיסאוטופיה או לזרוע פחד ואימה לקראת העתיד, אולם יש להסתכל למציאות בעיניים פקוחות, ולפעול כבר היום כדי לבנות יסודות רחבים של שיתופי פעולה בינלאומיים על מנת שהאנושות בעתיד, לאחר שתתעשת על עצמה, תתחיל לעבוד בשיתוף פעולה גלובאלי למען האינטרסים של כלל האנושות.

בהיבטים של אימוץ טכנולוגי על ידי אוכלוסייה רחבה, אחד הדברים **<u>הטובים</u>** שקרו לאנושות בשנתיים האחרונות (2020-2022) הוא משבר מגפת הקורונה שהתפשטה באופן גלובלי. ראשית קיבלנו הוכחה שכאשר האנושות נמצאת במצב של "אין ברירה", אז זה אך ורק ענין של החלטה ומיקוד בהפניית המשאבים כדי לעבור קפיצת מדרגה משמעותית וכלל עולמית באימוץ טכנולוגיות חדשות על ידי ציבור נרחב. שנית קיבלנו הוכחה לשינוי העצום שחל באנושות ב 200 שנה האחרונות, ומהי מידת הגמישות של האנושות לסגל ולאמץ התנהגות חדשה, כך שאם במאה ה-18 נדרש לאנושות מעל 100 שנים כדי לעבור את המהפכה התעשייתית ה-I, מתברר שבמאה ה-21 נדרש לאנושות פחות מכמה חודשים בודדים כדי להכיל ולהסתגל למהפכת הטרנספורמציה הדיגיטלית ולאמץ אותה באופן מוחלט להיות חלק בלתי נפרד מחייו.

<u>2.2 למה סייבר הוא ענף ולא תחום ?.</u>

אחרי שהגדרנו מהו סייבר בהקשר של טכנולוגיות המידע, קיימת חשיבות להבהיר למה בטרמינולוגיה הלשונית עלינו להתייחס להגדרת הסייבר כענף ולא כתחום. המשמעות הלשונית המקובלת של ענף היא תת-קבוצות במסגרת ארגונים או דיסציפלינות, **<u>ענף</u> הוא חלק <u>מתחום</u> מוגדר** [25], כמו שפיזיקה היא ענף בתחום מדעי הטבע, כך "סייבר", או לצורך ההבחנה הברורה נקרא לזה "**אבטחת הסייבר**" היא נדבך <u>מענף</u> גדול יותר הנקרא **אבטחת המידע** (Information Security) שהוא נדבך <u>מענף</u> גדול יותר הנקרא **מערכות המידע** (IT), שהוא נדבך <u>מענף</u> **מדעי המחשב** (Computer Science) שהוא נדבך **<u>מתחום</u> הטכנולוגיה**. מקובלת עלי התפיסה שניתן להציג את ההיררכיה בין הענפים השונים תחת תחום הטכנולוגיה עם ענפים ופיצולים רבים יותר ממה שהצגתי לעיל.

כאשר נבקש לבצע השוואה לתחומים מדעיים שונים בהם עוסקת פילוסופיה אסור לנו לשכוח שמדובר על תחומים "צעירים" של עשרות שנים בודדות [26] תחומים שהתפתחו אך ורק באמצע המאה ה-20 ואילך. מיפוי שערך מגזין הסייבר Cyber Crime Magazine בחודש אפריל 2021 ממפה **<u>מעל 50 תפקידים \ התמחויות</u>** שונות בענף הסייבר, הרשימה [27] הזאת היא המחשה ראשונית למי שלא בקי במקצועות <u>שענף</u> הסייבר מתחלק אליהם, עד כמה הענף הזה מורכב ומפוצל. כמובן שבכל "תפקיד" יש תפקידי משנה שנכללים במסלול הכשרה מקצועית "בדרך" לאותו תפקיד ראשי שמוגדר ברשימה.

<u>2.3 מהם דרישות הידע והכישורים האישיים הנדרשים כדי למלא תפקיד בכיר בתחום "אבטחת הסייבר" ?</u>

הידע שנדרש כיום כדי למלא בהצלחה תפקיד בכיר בתחום אבטחת הסייבר **הוא ידע רב-תחומי (מולטידיסיפלינרי)** שכולל לא רק הבנה טכנולוגית, אלא גם הבנה עסקית וראייה אסטרטגית [28]. אם ניקח כמקרה בוחן את דרישות הידע מתפקיד של מנהל אבטחת מידע ארגוני (Chief Information Security Officer - CISO), על מנת למלא את תפקידו והאחריות שתפקידו כולל עליו לשלוט ולהכיר עשרות של תחומי ידע טכנולוגים בנוסף לכישורים ניהוליים, וכישורים אישיים גבוהים (בינהם: יכולת מנהיגות, יכולות פרזנטציה, שכנוע והעברת מסרים, יכולות ניהול משא ומתן, יכולות של ניתוח טרנדים ומגמות עתידיות, ועוד).
כדי למלא את תפקידו CISO <u>חייב</u> להכיר (<u>גם אם זה באופן בסיסי</u>) היבטי אבטחה והגנה בטכנולוגיות בתחומים שונים בהם (רשימה חלקית):

---

25 **הענף הטכנולוגי באנגלוגיה לעץ**: העץ מתפצל גם לתת ענפים וגם מתפרס לרוחב, לפי אותה אנלוגיה ההגדרה של "תחום" היא אותם ענפים ראשיים שיוצאים מגזע העץ.

26 **חוג מדעי המחשב הראשון הוקם ב-1962 באוניברסיטת פרדו שבארצות הברית**, למרות שמבחינה היסטורית, קיים תיעוד של "מכונות חישוב" שמדענים במאה ה-17 כדוגמת קפלר, לייבניץ, פסקל בנו באופן עצמאי כדי לבצע חישובים מורכבים לצורך עבודתם המדעית, עדין תחום מדעי המחשב הוא תחום צעיר שהחל את דרכו רק בתחילת המאה ה-20.

27 "**50 Cybersecurity Titles That Every Job Seeker Should Know About**" - <u>לינק</u> למאמר שפורסם בחודש אפריל 2021 ב- Cyber Crime Magazine.

28 "**Three types of CISO. Know which one you need**" – <u>לינק</u> למאמר שפורסם ב-28 Nov 2017 באתר FortyTwo.nl.

גוף המחקר בתחום אבטחת הסייבר – **SANS** מפרסם מידי שנה מפה הכוללת את דרישות הידע והיכולות האישיות, והמקצועיות הנדרשות ממי שמקבל על עצמו תפקיד כ-CISO , **<u>היכולות הנדרשות מ-CISO מחולקות לשמונה דיסציפלינות</u>**:
1. תפעול אבטחה מידע (מניעה, זיהוי\ גילוי , תגובה) | 2. ידע משפטי \ רגולטורי | 3. יכולת פיתוח עסקי וראייה אסטרטגית | 4.תרבות אבטחה ארגונית | 5. יכולת מנהיגות | 6. ידע טכנולוגי בניהול זהויות | 7.ידע בתחום ה-GRC | 8. יכולות לבצע הערכת סיכונים טכנולוגים וניהוליים [29].

כמי שמרצה בקורסים להכשרה מקצועית של CISO / DPO מעל מספר שנים, והייתה לי הזכות ללוות באופן מקצועי כמה אלפי סטודנטים בהכשרתם המקצועית או האקדמית, אני יכול להעיד מניסיון אישי כי אם אתה שולט מבחינה מקצועית ברמה גבוהה ב 3-4 תחומים ראשיים (ענן ציבורי, תקשורת, הגנה על תחנות קצה, אבטחה על מערכות אפליקציה, פיתוח מאובטח, GRC, ועוד) זה כבר הישג יוצא דופן בענף הסייבר. המרצים וזה נכון גם כלפי הסטודנטים בקורס, לא מסוגלים להכיל הן מבחינת ידע והן מבחינת משאבים של זמן \ עלות \ מוטיבציה כדי ללמוד את כל קשת התחומים שמופיעים לעיל. מהיכרות רבת השנים שלי עם ענף הסייבר, אני בספק גדול שיש CISO אחד בעולם ששולט ברמת ידע ומומחיות גבוהה בכל התחומים, לראייה גם במסלולי ההכשרה שבהם אני מרצה, יש בכל מסלול, לפחות כחמישה מרצים ראשיים (שמלמדים בין 30 ל-40 שעות כמה תחומים קשורים וקרובים זה לזה) ובנוסף אליהם עוד כעשרה מרצים אורחים, האחראיים להרצות בתחומים ממוקדים או בנושא ספציפי ביותר. כל זאת ומכוון שבענף הסייבר קצב השינויים גבוהה מאוד כך שלא ניתן אלא להתמחות מבחינה מקצועית ובאופן ממוקד בתחומי ידע בודדים, לדוגמה מומחיות בתחום של מודעות הגנת סייבר לעובדים, הגנה אפליקטיבית, הגנה על תשתיות תקשורת, רגולציה של מדינה מסוימת או מגזר עסקי מסוים. כל אחת מהדוגמאות היא תת-התמחות הדורשת שנים של ניסיון מעשי כדי להיחשב כמומחה באותו תת-תחום.

להיות מומחה ברמה גבוהה בכל תחום של **ענף אבטחת הסייבר** דורש מבעל המקצוע להיות בעל **ידע רב-תחומי** (מולטידיסיפלינרי) כאשר הוא מחויב ולתהליך של למידה והתפתחות אישית ומקצועית, לא רק להיות בתחומים טכנולוגים אלא גם מבחינת ראייה עסקית ואסטרטגית של העיסוק בו הוא מתמחה.

29 **SANS CISO MIND MAP** - לינק להורדת המפה

2.4 איזה תת-תחומים קיימים בחלוקה גסה בענף אבטחת הסייבר ?.

כמקובל במתודה צבאית, כדי להתמודד בהצלחה עם משימה גדולה כדאי בשלב הראשון לתחום "ולגדר" את המשימה ולהגדיר מהן "גבולות הגזרה" שלה, מהם תחומי העיסוק \ הענפים הטכנולוגים הנכללים תחת ההגדרה של אבטחת סייבר ?.

אני מציע לחלק את הענף הראשי באופן גס לארבעה תת-ענפים מרכזיים: 1. **סייבר הגנתי** ,2. **סייבר התקפי** ,3. **אבטחת מידע** ,4. **הגנת הפרטיות**. אולם למרות החלוקה, לפי תפיסתי האישית ולפי תפיסתם של CISO רבים אחרים, בפרדיגמה ההולכת ומתחזקת, כיום בשל מורכבות בניהול ובתחזוקה השוטפת של המערכות, דרישות התקינה והרגולציה לניטור המערכות והפעילות בהן, והן כאשר מבקשים לערוך ביקורת בתחומי מערכות המידע, כבר לא ניתן להפריד את תת-הענף אבטחת המידע מתת-הענפים של הסייבר ההגנתי \ הסייבר ההתקפי מתת-ענף הגנת הפרטיות, **השילוב והתלות בין תת-הענפים** הוא חלק כולל מענף "**אבטחת הסייבר**" כפי שהשתרש בתודעה של מי שעוסק בתחומי טכנולוגיות המידע והציבור בכלל.

מצורפת טבלה המציגה מיון ראשני של תת-ענפים הכלולים בענף אבטחת הסייבר (Cyber Security)

מיפוי תת-ענפים בענף "אבטחת הסייבר" (רשימה חלקית)

ענף	התמחויות משנה
סייבר הגנתי	• **הגנה ואבטחה ברמת תשתיות התקשורת:** תשתיות פיזיות (כבילה) , פרוטוקולי תקשורת, מערכות תקשורת "קלאסיות" (כגון: נתבים, מתגים, מערכות טלפוניה, מערכות תקשורת ברמת ISP או Telecom). • **יישום הגנה ואבטחה במערכות Network & Infrastructure Security**: (NGFW | NAC | IPS-IDS | SASE | DECEPTION | DDOS Protection | Secure Web Gateway | Web Proxy | DNS & WEB Filtering). • **הגנה ואבטחה ברמת מערכות הפעלה:** Digital VAX | AS/400 | UNIX | LINUX | Windows | Mac OS | CHROM OS. • **הגנה ואבטחה ברמת מערכות תשתית לשירותים ,שרתים ומערכות Back Office / Front Office**. • **הגנה על התקני קצה:** שרתים, מחשבי קצה, התקנים ניידים כדוגמת סמארטפונים או טאבלטים הכוללים מ"ה של אפל iOS או מ"ה Android. • **הגנה על התקנים מסוגים שונים בעלי מערכת הפעלה לא סטנדרטית או מערכות הפעלה משובצות – Embedded**. • **הגנה אפליקטיבית:** מערכות אפליקציה \ בסיסי נתונים \ הגנה על מערכות דוא"ל. • **תפעול מאובטח בסביבת ענן ציבורית – DevSecOps.** • **יישום אבטחה בסביבות תקשורת שונות:** WAN / Wireless LAN / Mobile / Data Center / Public Cloud / OT – ICS - SCADA. • **אבטחת מידע בסביבות מחשוב שונות:** רשתות מקומיות , סביבת דאטה סנטר , סביבת ענן ציבורי , סביבת מחשוב תעשייתית. • **סכמות הצפנה ברבדים שונים:** תקשורת נתונים \ אמצעי אחסון \ גיבוי \ בסיסי נתונים \ אפליקציות \ תקשורת ברמת החומרה. • **הגנה על סביבות ענן ציבורי בכל הרבדים:** מהתקן הקצה בדרך אל הענן (CASB), הגנה על גישה חיצונית אל הענן (ברמת ה-Infrastructure), הגנה בתוך סביבת הענן (ברמת ה-Container \ סגמנטציה פנימית בתוך ה - VPC), עמידה בדרישות הרגולציה ובדיקות ברמת ציות (Compliance). • **מערכות אוטומציה ואורקסטרציה לניהול הגנת הסייבר \ סביבת הענן \ סביבת הדאטה סנטר**.
סייבר התקפי	• **בדיקות חוסן לתשתיות תקשורת \ שרתים.** • **בדיקות חוסן לשרתי אפליקציות \ שרתי Data Base.** • **בדיקות חוסן** ברמת הקוד, ברמת מערכת הפעלה, ברמת תשתיות אפליקטיבית , ברמת תשתיות מחשוב , ברמת תשתיות תקשורת , ברמת החומרה, ברמת האבטחה הפיזית. • **חקירת התקפות סייבר ואיסוף ראיות משפטיות (חקירה ברמת זיהוי פלילי) – Digital Forensics.** • **בדיקה ואיתור חולשות** בפרוטוקולי תקשורת \ פרוטוקולי הצפנה \ מערכות הפעלה \ קוד תוכנה \ חומרה. • **מערכות לניתוח וזיהוי אירועים חריגים – Network Analysis & Forensics.**
אבטחת מידע	• **ייעוץ קלאסי בתחום אבטחת מידע:** סקר סיכונים, נהלים \ מסמכי מידניות. • **ייעוץ בליווי פרויקטים:** אפיון למרכזים והגדרת דרישות \ אפיון פרויקטים \ ניהול פרויקטים. • **עמידה בדרישות הרגולציה** – GRC. • **תקינה בניהול אבטחת מידע** כדוגמת: CIPA, FedRAMP , HIPAA / HITEC , PCI-DSS, ISO/IEC 27001. • **תקינה למערכות אבטחת מידע והגנת סייבר:** FIPS 140, NSS Labs , Common Criteria , MITRE , ICSA. • **מתודולוגיות פיתוח תוכנה מאובטחת:** DevSecOps / OWASP / SSDLC / Security By Deign ועוד. • **תחום ה-Data Protection:** גיבויים, רפליקציה של דאטה, הצפנת דאטה, DLP - מניעת זליגת מידע. • **תוכניות המשכיות עסקית (BCP) \ תוכניות התאוששות מאסון (DRP).** • **ניהול מרכז תפעול אבטחת מידע \ רשת** (Network Operations Center / Security Operations Center). • **מודעות עובדים להונאות סייבר והתנהלות תקינה במסגרת מידניות אבטחת מידע ארגונית**. • **תרגול ונהלים לניהול משברי סייבר - Cyber Resilience.** • **תרגול ונהלים לתחקור אירוע סייבר ומתן מענה מידי - Incident Response.** • **ניהול זהויות** – Identity & Access Management. • **מערכות לאיסוף מודיעין סייבר (פנימי או חיצוני), התראה ותגובה.** • **מערכות לזיהוי הונאות כלכליות והתנהגות חריגה של משתמשים במערכות מחשוב.** • **ייעוץ משפטי \ יעוץ לניהול משברי סייבר** - מומחים לניהול משא ומתן עם תוקפים באירועי סייבר.
הגנת הפרטיות	• **תקינה בינלאומית בניהול הגנת הפרטיות** כדוגמת: FERPA , FISMA , CCPA, GDPR. • **תקינה מקומית ישראלית** - תקנות הגנת הפרטיות (אבטחת מידע) של הרשות להגנת הפרטיות (משרד המשפטים). • **מתודולוגיות פיתוח תוכנה מאובטחת בהתאם לדרישות הגנת הפרטיות – Privacy by Design.** • **ייעוץ קלאסי בתחום הגנת הפרטיות**: סקר מיפוי נכנסי מידע , סקר פערים , סקר מאגרי מידע , סקר סיווג מסמכים , סקר סיכונים כללי , נהלים , מסמכי מידניות ארגונית. • **ייעוץ משפטי \ ייעוץ טכנולוגי** – ביקורת ציות ועמידה בדרישות הרגולציה (GRC) על פי שיוך מגזרי: ביטוח, פיננסים, רפואה, מוניציפלי ועוד.

3. מהי פילוסופיה?, מהן הפילוסופיות שיכולות להוות מקור השפעה עבור הפילוסופיה של אבטחת הסייבר ?.

3.1 הגדרה מילונית – פילוסופיה מהי?

אם שואלים את **ד"ר הנרי אונגר**, פילוסוף ישראלי מוכר "פילוסופיה מהי ?" התשובה כנראה תהיה שזה הכול חוץ מאשר המשמעות הלשונית מהמקור היווני הקדום והיא פילוסופיה משמעותה "אהבת החוכמה".

אך אם בכל זאת אני אנסה לפרש את הרצאתו של ד"ר אונגר [30], למיטב הבנתי ופרשנותי לדבריו, פילוסופיה היא לא רעיונות בודדים בפני עצמם, **פילוסופיה היא** סִיסְטֶמָטִיזַצְיָה [31] של חשיבה מעמיקה, חשיבה ביקורתית וללא השפעות של דוֹקְטְרִינַצְיָה [32] מוקדמת כדי לבחון לפי שיטה סיסטמתית ושיטתית מנקודות ראייה שונות ערכים ורעיונות בתחומי המציאות השונים.

ואם נפרש את המשפט לעיל לשפה אנושית ומובנת גם למי שאינו מגיע מתחום הפילוסופיה, התשובה לשאלה תהיה: **פילוסופיה היא** כלי בחינה ביקורתית, ללא דעות וההשפעות קודמות, ע"מ לבחון לעומק רעיונות מופשטים או ממשיים. הדרך שבה מבצעים את הבחינה הביקורתית היא שיטתית ועל פי מתודת עבודה קבועה ומוגדרת.

יש פה פרדוקס, כשל לוגי שמודעים אליו, היות ומיום הולדתנו תפיסת עולמנו שבוייה בפרדיגמות [33]. גם אם אנחנו לא מודעים לזה ברשות היחיד או שאין אנחנו מודים בזה ברשות הרבים, הפרדיגמות הללו "מנווטות" אותנו, כך שתמיד יש השפעה כלשהי על הכרתנו והבנת המציאות שלנו כפי שאנחנו מפרשים אותה באופן סובייקטיבי, וזה משפיע עלינו גם כאשר אנחנו בוחנים רעיונות חדשים או תופעות חדשות בפילוסופיה, בתחומים מדעיים או טכנולוגים.

אם נבחן את גורמי ההשפעה על תודעתנו מחוץ לתחום הפילוסופיה, אפשר לתאר את המציאות בת זמננו כמעין סוג של מלחמה בלתי פוסקת על התודעה שלנו, בתחומי השיווק, הפרסום ,בתחום הכלכלה ההתנהגותית, בתשדירי הבחירות לכנסת ואף פושעי הסייבר שמפעילים עלינו מניפולציות רגשיות כדי שניפול "במלכודת" שהם טומנים לנו. **כולם מנצלים לרעה את התלות שלנו בעולם הדיגיטלי.** תלות אשר מסייעת לכל מי שרוצה **לשנות את תודעתנו ולהשפיע על תפיסת עולמנו, ואף להניע ולהשפיע עלינו לפעול כרצונו** (לרכוש מאתר מסוים, להצביע עבור בבחירות, ללחוץ על לינק ממקור לא מוכר). לפי הערכות בשנים האחרונות בפעילות האנושית שלנו במרחב האינטרנט (מרחב הסייבר) **"80% מההחלטות שלנו נעשות ללא שליטה מודעת".**[34] גם כאשר מדובר בהחלטות החשובות שאנחנו מקבלים בחיים. מערכת השיקולים וקבלת ההחלטות הפנימית שלנו כיצד לפעול הן ממקור רגשי ולא שכלתני או שמקורן היא החלטה רציונלית ותועלתנית. **מערכת ההחלטות שלנו "השתבשה" כתוצאה מהתלות שלנו בעולם הדיגיטלי.** ההחלטות שלנו מונעות מהשפעות חיצוניות חדשות שאנחנו "רוכשים" בגיל מבוגר כדי להתאים את עצמנו לעידן הדיגיטלי או לחלופין מתפיסות שגדלנו והתחנכנו עליהם בבית הורנו מגיל צעיר. לדוגמא עיקר האינטראציה האנושית עברה להודעות מערכות מסרים מיידים (ווצאפ או בעבר SMS) אנחנו כמעט והיום לא מתקשרים לדבר אחד עם השני אלא "שולחים הודעות" בווצאפ, דוגמא נוספת אם משמעמם לילד אז במקום משחק או קריאת ספר, בוא נדחוף לו ליד סמארטפון "שיעביר את הזמן" [35].

---

30 ההרצאה "**פילוסופיה מהי**" – **ד"ר הנרי אונגר** , לינק להרצאה בו מובא ההסבר "מהי פילוסופיה" ומהי היא לא פילוסופיה.

31 **סִיסְטֶמָטִיזַצְיָה (שיטתיות)**: קביעה דייקנית, אַרגון רעיונות ברצף מסודר בהתאם למערכת.

32 דוֹקְטְרִינַצְיָה (בהקשר של שטיפת מוח): היא מאמץ לחנך לדוקטורינות מסוימות שלא באמצעות התבונה וההגיון.

33 **פַּרַדִיגְמָה:** המערך הקולקטיבי של עמדות, ערכים, שיטות, טכניקות, היוצר את הראייה המקובלת בתחום מסוים.

34 **ד"ר לירז מרגלית** פרסמה בשנת 2022 ספר בשם "**עיצוב התודעה – הנדסת ההתנהגות והתחושות שלנו בעידן הדיגיטלי**" בספר היא בוחנת מחקרים רבים המראים כמה קל לגורמים מסחריים שונים להנדס את התודעה שלנו ולהשפיע על האופן שבו אנחנו פועלים, חושבים ומקבלים החלטות ממקום רגשי – אמוציונלי ולא רציונלי, שאינו כולל מחשבה עמוקה על התוצאות לטווח ארוך. הציטוט "**80% מההחלטות שלנו נעשות ללא שליטה מודעת**" נלקח מכתבה שפורסמה בעיתון מעריב, 31.07.2022 ע"י תמר אוריאל-בארי תחת השם "סמנכ"לית הדיגיטל באסתי לאודר ישראל: "תקשיבי ללקוחה!". לינק

35 עיתון הארץ, 03 בפברואר 2021, יגאל באום, "**הילדים במסכים וזו לא אשמתם, לא השארנו להם ברירה**" - לינק

אולם למרות המגבלות התפיסתיות היות והפילוסופיה לא מביטה על המציאות כמו סוציולוג, כמו הפיזיקאי וכמו כל תחום מדעי אחר, **החקירה הפילוסופית מאפשרת לנו חשיבה אנאליטית, פעולת אנליזה קונספטואלית וסיסטמתית**, כלומר הפילוסופיה לוקחת מושגים כגון: שיוויון, חוק, צדק, רשויות, חומר, רוח, מוסר טוב \ רע , יופי ואסתטיקה, חירות, אושר, והפילוסוף פשוט "מפרק" אותם (כמו בתהליך של אנאליזה), לאחר שהוא מגיע ליסודות של המושג, הפילוסוף מנסה לבנות מערכת (סיסטמה), בה נרקמת מערכת זיקות מדויקת בינו לבין מושגים אחרים, **אזי לא ניתן להגדיר רעיון כפילוסופיה או אפילו התחלה של פילוסופיה, עד אשר אין לי יסודות שנותחו לעומק, בוצע מיפוי מה התנאים ההכרחיים או המספיקים ליסודות השונים כדי לבנות פְּרֶדִיקַצְיָה [36] לגבי סיטואציות אפשרויות העשויות להתממש.**

לפי הגדרתו של ד"ר אונגר אין התנגשות בין המדע לבין הפילוסופיה שכן "**הפילוסופיה לא מתמודדת עם המציאות, אלא היא בוראת לנו מציאות אפשרית, ואנחנו צריכים לבחור**", מטרת הפילוסופיה היא לא להחליט עבורנו איך לנהוג או איך לפעול אלא "**העדפה של פילוסופיה היא באמצעות כושר שכנוע**". כושר השכנוע יכול לפעול בשני אופניים: הראשון, **הקוֹהֶרֶנְטִיוּת** [37] ובהירות של מערכת הטיעונים שהוצגה בפנינו. שכנוע עם טיעונים רציונליים בכוח המחשבה של מי שמציג בפנינו את עמדתו. האופן השני הוא **האפליקביליות של הטיעון**, היכולת שלנו להבין את התועלת של הרעיון ואף גם ליישם את הרעיון באופן ממשי.

נקודה למחשבה שממש מתבקשת כבר בשלב זה, האם גם בתחום הפילוסופיה של אבטחת הסייבר תחול אותה "**השרשת רעיונות**", שרשרת יחסים של רעיונות שעברו באופן חלקי או מלא בין פילוסופים והוגי דעה מתקופות שונות ?. באנלוגיה לענף אבטחת הסייבר, רעיונות ותפיסות שהושרשו על ידי אנשי מתודולוגיה או אנשי מקצוע טכנולוגים אל כלל הקהילה המקצועית העוסקת בתחום.

אנקדוטה מעניינת והיא שהמדען והמתמטיקאי **אייזיק ניוטון**, הנחשב כאחד "מהאבות המייסדים" של תחום המדע והמחקר המדעי כפי שהוא מוכר לנו כיום, אמר **"אם הרחקתי ראות יותר מאחרים, אין זאת אלא משום שעמדתי על כתפי ענקים."** [38] , כלומר ניוטון מודה שבזכות מה שהוא למד מקודמיו הוא הצליח לשכלל את הידע שלו ולהתקדם באופן משמעותי מהר יותר. גם בתחומים טכנולוגים כמו בתחומים פילוסופים שונים קיימת "**השרשה**" של: רעיונות, שיטות עבודה, פרדיגמות או אפילו אסכולות (משפחה של רעיונות סביב רעיון מרכזי אחד) בין מומחי טכנולוגיה מתקופות שונות.

בעוד בתחום הפילוסופיה תהליכים הם מאוד איטיים והתפתחות רעיון או תפיסה מסוימת יכולה להימשך כמה מאות שנים, כך שתהליך "השרשה" של רעיונות ומושגים משרת את הפילוסוף שאינו נאלץ לברוא עולם מושגים חדש יש מאיין, ויש לו נקודת התחלה כלשהי להתחיל לפתח את התיאוריה שלו (גם אם בחלק מהמקרים היא תיאוריה מנוגדת, לתיאוריה המושרשת), מאידך בתחומים טכנולוגים בכלל ובתחומים השונים של ענף הסייבר בפרט, התוקף והרלוונטיות של הידע הוא קצר מועד, הטכנולוגיה משתנה בקצב גבוהה (שנים בודדות ובמקרים מסוימים גם חודשים בודדים) וכך גם הרלוונטיות של שיטות העבודה, מתודולוגיות האבטחה וההגנה, סביבת המחשוב והכי חשוב ההתנהגות האנושית משתנה במהירות וגם לה יש השפעה ישירה על הרלוונטיות של האופן בו מיישמים בפועל אבטחה והגנת סייבר.

---

36 **פְּרֶדִיקַצְיָה (Prediction)**: הִשְׁאָה; הנחה, דעה; קישור בין הנושא לנשוא על-ידי ייחוס תכונה | אפשר גם לייחס לזה את ההסבר בהקשר הבא: תחזית \ צפי, חיזוי((פעולה).

37 **קוֹהֶרֶנְטִיוּת:** קישוריות; עקיבות, עקביות: עקביות בין הנאמר לבין המעשה בפועל.

38 מאמר של **ד"ר לביא ביגמן**, משנת 2022 על **אייזק ניוטון** מתוך האתר של מכון דוידסון – מכון ויצמן למדע – לינק.

קיים פרדוקס בתחום אימוץ טכנולוגיות ושיטות עבודה חדשות בענף הסייבר. בעוד הטכנולוגיות בענף הסייבר מתפתחות בקצב מהיר, מאידך הארגונים ואנשי המקצוע השונים, בדגש אלו העובדים בארגונים גדולים וותיקים, כדוגמת: בנקים, חברות ביטוח, ממשלה, מוניציפאלי ועוד, נמצאים בסטגנציה מחשבתית, בקיבעון ובקיפאון תפיסתי מבחינת אימוץ של טרנדים טכנולוגים חדשים, המספקים מענה טוב יותר לדרישות העסקיות בעידן הדיגיטלי. **בסופו של דבר, הגורמים העיקריים שמעכבים זמן רב אימוץ של טכנולוגיות או שיטות עבודה חדשות הם אותם אנשים שעובדים בענף הסייבר**, בשל תהליך ארוך עד שהם מקבלים ומאמצים את הטכנולוגיות ושיטות העבודה החדש כחלק מפרדיגמות ניהול מערך הסייבר שלהן. **<u>כיום התמודדות עם אתגרי אבטחת הסייבר אינה בעיה טכנולוגית אלא בעיית הגורם האנושי</u>.** הסיבות לכך שונות, והם בדרך כלל נובעות בגלל "**שמרנות טכנולוגית**" שמאפיינת אנשים בארגונים מסוימים, אולם קיימים גם אתגרים עסקיים, שיקולי תקציב, שיקולי כ"א, הקצאת זמן לבחון וליישם טכנולוגיות חדשות, חוסר ידע ומודעות שיש פתרונות ודרכי עבודה חדשים , ובסוף גם הפחד הטבעי משינוי ותוצאותיו של השינוי.

נשאלת השאלה האם תהליך "השרשת ידע" אינו גורם שמעכב את התפתחות בתחומי הסייבר השונים, היות ובחלק גדול מהמקרים הפרדיגמות והמתודולוגיות עבודה תקועות הרבה שנים ב "**שלב השמרנות**" , באנלוגיה לשלב "**המדע התקני**" כפי שהגדיר אותה פילוסוף המדע, **תומאס קון** בתיאוריה שלו של התחלפות פרדיגמות במדע [39], בשלב "המדע התקני" למרות שמתגלות חריגות ואנומליות בתיאוריות הנוכחיות, עדין אלו האוחזים והנאחזים בפרדיגמה בוחרים להתעלם מהחריגות של המודל הנוכחי, לבצע תיקונים "אד-הוק" , וכל עוד האפקטיביות של שיטות העבודה אינן עולות בכובד משקלן על החריגות, הם ממשיכים להיאחז בפרדיגמות הנוכחיות.

כפי שמצוטט בספר [40] של תומס קון "**קהילות אנושיות באופן כללי וקהילות מדעיות בפרט נוטות לשמרנות, ולכן לא ממהרות לעשות שינויים רדיקלים**" קון מתאר בספרו שבמקרים מסוימים לשכנע מדען לשנות פרדיגמה אחרי שהוא האמין בה ועבד לפיה הרבה שנים, זה שווה ערך לשכנע אותו להמיר את אמונתו הדתית. השאלה הגדולה שחייבים לשאול בהקשר הזה, **האם יש מקום לתקיעות כזאת בענף הסייבר גם כאשר מדובר על תחומים "טכנו-אנושיים" המשתנים בקצב גבוהה במיוחד**, הרבה יותר מהשינויים שחווה תומאס קון בשנות ה-70 בעת פרסום התיאוריה שלו.

<u>3.1 מהן הפילוסופיות המהותיות שיכולות להוות מקור השפעה עבור הפילוסופיה של אבטחת הסייבר ?</u>

היות ועוד לא התגבשה דיסציפלינה העוסקת באופן אקדמי מסודר בפילוסופיה של אבטחת הסייבר, כדאי לבחון איזה דיסציפלינות אחרות בתחום הפילוסופיה חולקות תחומים חופפים או יכולות לתרום "מניסיונם" עבור "**הפילוסופיה של אבטחת הסייבר**" ומאידך באופן הדדי גם להיתרם ממנה. היות ובמקרה זה אין לי "כתפים של ענקים לעמוד עליהם", קיבלתי על עצמי את המשימה ליצור יש מאיין. מפת השפעות הדדיות, שלמיטב הבנתי יש ביכולתן להשפיע כתרומה של רעיונות \ תיאוריות עבור התחום הפילוסופי החדש.

---

39 הרחבה בנושא אפשר מומלץ לקרוא במאמר "עליתן ונפילתן של פרדיגמות" ע"פ **תומאס קון** , יותם הכהן, מחברת דואלוג - לינק

40 **המבנה של מהפכות מדעיות - The Structure of Scientific Revolutions** הוא ספר העוסק בפילוסופיה של המדע שנכתב על ידי הסוציולוג, הפילוסוף תומאס קון בשנת 1962. הספר ראה אור לראשונה בעברית בשנת 1977, בהוצאת ספרי "סימן קריאה" ,בתרגומו של יהודה מלצר ,ומאוחר יותר, בשנת 2005 הוא יצא מחדש בהוצאת ספרי עליית הגג ובהוצאת ידיעות ספרים. מקור: לינק

שם	בשלות התחום	פילוסופים או הוגי דעה בולטים	תחומים החופפים או התחומים המשפיעים
הפילוסופיה של המדע Philosophy of science	- התחום נחשב תחום בשל, הן מבחינת ההתפתחות האדירה שלו במאה שנה האחרונות, והן מבחינת כמות החוקרים, אנשי האקדמיה והפילוסופים העוסקים בתחום באופן שיטתי בכל העולם. - תחילה ממוסדרת של התחום היא משנות העשרים של המאה העשרים.	**<u>מדענים:</u>** - גלילאו גליליי - אייזק ניוטון - צ'ארלס דרווין - מיכאל פולאניי - אלברט איינשטיין **<u>האבות המייסדים:</u>** - רנה דקארט - דיוויד יום - ג'ון סטיוארט מיל - עמנואל קאנט - פייר דוהם - ארנסט מאך **<u>המאה ה-20 ועד היום:</u>** - קארל פופר - תומס סמואל קון - ברטראנד ראסל - אלפרד נורת' וייטהד - הילרי פטנאם - רודולף קרנפ - אימרה לקטוש - קרל המפל - וילארד קוויין - נלסון גודמן - פול פייראבנד - דיוויד בלור - בארי בארנס - איאן האקינג - ננסי קרטרייט **<u>פילוסופים ישראלים בולטים:</u>** - לודוויק פלק - יוסף אגסי - ישעיהו ליבוביץ - גד פרוידנטל - אלעזר ויריב - זאב בכלר - ימימה בן מנחם	**רקע כללי:** הפילוסופיה של המדע שואפת לענות ולהסביר שאלות כגון טבעם של קביעות ומושגים מדעיים; האופן שבו הם נוצרים; כיצד המדע מסביר, חוזה, ומשתמש בטבע באמצעות טכנולוגיה ;כיצד אפשר להחליט על הדיוק של מידע ;הניסוח והשימוש במתודות מדעיות ;אופני החשיבה שבהם משתמשים על מנת להגיע למסקנות; והמשמעויות של המתודות והמודלים המדעיים לחברה ככלל, ולמדעים עצמם. [41] **התרומות העיקריות:** - ההשפעות ישירות ועקיפות על הפילוסופיה של הטכנולוגיה. - לוגיקה בקבלת החלטות \ הסקת מסקנות. - בחינת אמינות, דיוק ואישוש של מתודות, תיאוריות ושיטות מחקר. - בניית מודלים לתרחישים של ניהול סיכונים בהתבסס על מודלים שמקורם הפילוסופיה של המדע.

41 **פילוסופיה של המדע** – מקור - לינק

שם	בשלות התחום	פילוסופים או הוגי דעה בולטים [42]	תחומים החופפים או התחומים המשפיעים
הפילוסופיה של הטכנולוגיה **Philosophy of Technology**	- התחום נחשב תחום בשל, הן מבחינת ההתפתחות האדירה שלו ב- 50 שנה האחרונות, והן מבחינת כמות החוקרים, אנשי האקדמיה והפילוסופים העוסקים בתחום באופן שיטתי בכל העולם. - במהלך ההיסטוריה היו ניצנים ראשונים של התייחסות לטכנולוגיה כחיקוי של הטבע, ואף התייחסות שטכנולוגיה היא הרחבה של היכולות של הטבע החלו עוד בפילוסופיה היוונית (הרקליטוס, דמוקריטוס, ובמידה מסוימת גם אריסטו) אולם הדיון הראשון המהותי בנושא השפעות הטכנולוגיה על האנושות החלה בימי הביניים כאשר פורסם ב- 1627 לאחר מותו של הפילוסוף והמדינאי האנגלי, **סר פרנסיס בייקון** את יצירתו "ניו אטלנטיס" (1627) בייקון הציג תפיסת עולם אופטימית שבה מוסד בדיוני בשם "בית סלומון" (שלמה) אשר משתמש ביסודות מתחום הפיזיקה וטכנולוגיה להרחבת כוחו של האדם על הטבע - למען שיפור החברה, באמצעות עבודות המשפרות את תנאי החיים.	**<u>האבות המייסדים:</u>** - **פרנסיס בייקון** (ניו-אטלנטיס) - **ארנסט קאפ** (המדע לרשות האנושות כדי להתגבר על אתגרי הטבע) **<u>המאה ה-20 עד היום:</u>** - **ג'ון דיאוי** (טכנו' \ חינוך) - **מרטין היידגר** (השאלה הנוגעת לטכנולוגיה, 1954) - **הרברט מרקוזה** (טכנו' \ מרקסיזם) - **גינטר אנדרס** (טכנו' \ השפעות תקשורת המונים) - **חנה ארנדט** (טכנו' \ פוליטיקה) - **ז'אן בודריאר** (טכנו' \ מדיה \ תרבות \ סוציולוגיה) - **אלברט בורגמן** (פרדיגמת מכשיר) - **פול טי דרייבן** (טכנו' \ אתיקה) - **דונה הראווי** (טכנו' \ פמיניזם) - **ז'אק אלול** (טכנו' \ סוציולוגיה) - **הנס יונאס** ("המכונה שולטת באדם ולא האדם שולט במכונה") - **קרל מיטצ'ם** (טכנו' \ הנדסה) - **דון איידי** (פוסטפנומנולוגיה \ טכנומדע) - **פטר-פול ורביק** (טכנו' \ פילוסופיה \ פנומנולוגיה) - **ניק בוסטרום** (סכנות ה-AI) - **יוסף אגסי** הראשון בעולם שפרסם ספרים ממוקדים בנושא "הפילוסופיה של הטכנולוגיה") **<u>המאה ה-21 (לא פילוסופים אבל משפיעים של ההגות בתחום:</u>** - **נורברט וינר** (מייסד הקיברנטיקה) - **מרשל מקלוהן** (טכנו' \ תקשורת המונים \ סוציולוגיה) - **אלווין טופלר** ("הלם העתיד" [43] , טכנו' \ סוציולוגיה) - **קווין קלי** (טכניום , תרבות טכנו') - **ריימונד (ריי) קורצווייל** (סינגולריות) - **ג'ון קנת גלבריית** ("עידן אי הוודאות") - **מיצ'יו קאקו** (חלל, מדעי המוח) - **ניל פוסטמן** (אנטי-טכנולוגיה) - **ג'ון זרזן** (אנטי-טכנולוגיה) - **ג'רון (ירון) צפל לנייר** (אנטי-טכנולוגיה) - **פיטר דיאמנדיס** (מייסד "אוניברסיטת הסינגולריות" , מייסד ארגון X Prize) - **סטיבן קוטלר** (המדע והטכנולוגיה להטבת האנושות) - **לורנס ס' סמית** ("העולם בשנת 2050" ,טכנולוגיה להצלת כדור הארץ ממשבר ההתחממות הגלובלית) **<u>הוגי דעה ישראלים בולטים בהשפעות הטכנולוגיה</u>** - **דויד פסיג** ("צופן העתיד") - **יובל נוח הררי** (השפעת התפתחות הטכנולוגיה המואצת על האנושות) - **רועי תזנה** ("השולטים בעתיד" - רעיון "מדינות הענן") - **גלית ולנר** (פנומנולוגיה של דון איידי, מ.היידגר , השפעות הטכנו' על האנושות) - **יובל דרור** ("קוד סמוי" – "החצר האחורית" של רשת האינטרנט, הפוליטיקה של הטכנולוגיה) - **לירז מרגלית** (עיצוב התודעה בעידן הדיגיטלי)	**<u>רקע כללי:</u>** הפילוסופיה של הטכנולוגיה היא תת-תחום של הפילוסופיה החוקר את טבעה של הטכנולוגיה. נושאי מחקר ספציפיים כוללים מחקר על תפקידו של ידע סמוי ומפורש ביצירה ושימוש בטכנולוגיה, אופי הפונקציות בחפצים טכנולוגיים, תפקידם של ערכים בעיצוב ואתיקה הקשורה לטכנולוגיה. טכנולוגיה והנדסה יכולות שתיהן לכלול יישום של ידע מדעי. הפילוסופיה של ההנדסה היא תת-תחום מתפתח של הפילוסופיה הרחבה יותר של הטכנולוגיה. [44] **<u>התרומות העיקריות:</u>** - **מלבד הפילוסופיה של הידע, זאת הפילוסופיה עם ההשפעה החזקה ביותר על הפילוסופיה של אבטחת הסייבר.** - גם בתחום אבטחת הסייבר למרות הבידול שלו כתחום נפרד, בסופו של דבר הוא עוסק ברובו בהיבטים הקשורים לטכנולוגיה, לכן בעיות ואתגרים פילוסופים מהפילוסופיה של הטכנולוגיה חלים ברוב המקרים גם על הפילוסופיה של אבטחת הסייבר.

42 **List of philosophers of technology** מקור - לינק

43 **הלם העתיד** (באנגלית: **Future Shock**) הוא ספר שכתב הסוציולוג והעתידן **אלווין טופלר** בשנת 1970, ועוסק במונח פסיכולוגי בשם זה שטבע טופלר. הספר קובע לאור קצב השינויים הטכנולוגיים והחברתיים בעשרות השנים שקדמו לכתיבתו כי העתיד צופן בחובו שינויים רבים בקצב שלא יאפשר לרבים להתמודד עמו מעמדת יציבות, דבר שיגרום למתח נפשי גבוה, בלבול ותחושת אובדן דרך. מקור - לינק

44 **הפילוסופיה של הטכנולוגיה** מקור - לינק

שם	בשלות התחום	פילוסופים או הוגי דעה בולטים	תחומים החופפים או התחומים המשפיעים
הפילוסופיה של המידע Philosophy of Information (PI)	תחום צעיר ולא בשל, נמצא בתחילת דרכו הן מבחינה פילוסופית והן מבחינה אקדמאית. התחום התפתח כדי לענות על אתגרים ושאלות בנושאים של - שימוש בבינה מלאכותית - לוגיקה של מידע - מידע כחלק מהמרחב הקיברנטי - אתיקה בשימוש במידע - חקר שפה הפילוסופיה של המידע מתבססת על "**תורת המידע**" : תורת המידע היא המחקר המדעי של כימות, אחסון ותקשורת של מידע דיגיטלי. התחום הוקם ביסודו על ידי יצירותיהם של הארי ניקוויסט וראלף הארטלי, בשנות ה-20, ו קלוד שאנון בשנות ה-40. התחום נמצא בצומת המחברת תחומים בינהם: תורת ההסתברות, סטטיסטיקה, מדעי המחשב, מכניקה סטטיסטית, ניתוח מידע והנדסת חשמל.	**המאה ה-20 ועד היום:** - **אלן טיורינג** (לוגיקה ופורמליזציה לכתיבת אלגוריתמים) **- בקמינסטר (בקי) פולר** (רעיון "המעצב הכולל", איסוף מידע וניתוחו לפיתוח טכנולוגיות חדשות להטבת האנושות) - **גרגורי בייטסון** (מידע בהקשר של סוציולוגיה ותקשורת המונים) - **בריאן קנטול סמית'** (פרקטיקה ותיאוריה של מדעי המחשב) - **הארי תאודור נייקוויסט** (מתמטיקאי, תורם חשוב לפיתוח תורת האינפורמציה) - **ראלף הארטלי** (מדען שעסק בהעברת מידע באמצעים אלחוטיים) - **קלוד שאנון** ("אבי תורת המידע" , אלגוריתמים לפיצוח הצפנה) - **דונלד מקקרימון מקי** (תורת המידע, מדעי המוח) - **אלברט בורגמן \ מארק פוסטר** (היבטים חברתים ותרבותיים של מידע בתיווך אלקטרוני) - **לוצ'יאנו פלורידי** (אתיקה דיגיטלית)	**<u>רקע כללי:</u>** פילוסופיית המידע (PI) היא ענף בפילוסופיה החוקר נושאים רלוונטיים לעיבוד מידע, מערכת ייצוגית ותודעה, מדעי המחשב , מדעי המידע וטכנולוגיית המידע. זה כולל: את החקירה הביקורתית של הטבע הרעיוני ועקרונות היסוד של המידע, כולל הדינמיקה שלו, ניצולו ומדעים פיתוח ויישום של מתודולוגיות מידע תאורטיות וחישוביות לבעיות פילוסופיות.[45] **<u>התרומות העיקריות:</u>** - לוגיקה בקבלת החלטות ב-AI. - אתיקה בשימוש במידע. - מניפולציות במידע: שיבוש מידע, החסרת מידע, הפצת מידע כוזב. - נתינת משמעות למושגי יסוד המשותפים גם לפילוסופיה של אבטחת הסייבר: מה ניתן להגדיר כמידע?, מה ניתן להגדיר כידע?, מה יכול להיחשב כישות בעולם הדיגיטלי?, האם למערכות מחשב יכולה להיות תודעה?, מה נחשב תודעה דיגיטלית ?, מהו ניסיון בהקשר של למידת מכונה ?, מהו היגיון בהקשר של AI ?, מהי האבולוציה של התפתחות המידע ?.

45 **הפילוסופיה של המידע** – מקור - לינק

שם	בשלות התחום	פילוסופים או הוגי דעה בולטים	תחומים החופפים או התחומים המשפיעים
פילוסופיה של המוסר \ אתיקה \ Ethics \ Moral Philosophy	**"חיים ללא בדיקה עצמית אינם ראויים לאדם"** – אמר הפילוסוף סוקרטס. **פילוסופיה של המוסר** היא אחד תחומי ההגות הראשונים שהעסיקו את האנושות עוד מראשית העת העתיקה וזה ממשיך להעסיק אותנו נכון לגבי ימנו אנו. התחום בשל מכיוון שהוא חלק מכל תוכנית אקדמית העוסקת בתחום המשפט, מדעי הטבע ובחלק גדול ממדעי הרוח. בנוסף הוא נדון תדיר באמצעי התקשורת והמדיה השונים. **האתגר הגדול של תחום האתיקה הוא שמהותו הוא <u>ערכים</u>, שלא כמו במדע המקובל כערך אוניברסלי של האדם, כאשר מדובר על מוסר (החלטות אתיות) קביעת נקודות ההתייחסות לכל החלטה מוסרית תהיה סובייקטיבית** [46] . מחד ההגדרה של מעשה מוסרי או החלטה מוסרית הוא מה שקובע מצפונו של כל אחד ואחד טען הפילוסוף **דיוויד יום**, ומאידך יש לקחת בחשבון כי האדם חי בחברה והוא מושפע ומשפיעה עליה, לכן הכרעה מוסרית תמיד תהיה גם תחת השפעת החברה שבה אנחנו נמצאים או שהייתה אחראית על גיבוש תפיסת עולמנו (רלטיביזם מוסרי). **הערה חשובה לגבי המונחים**: **הפילוסופיה של המוסר** = **אתיקה** = **תורת המידות.** כדי שההבחנה תהיה ברורה **<u>מוסר</u>** הוא אוסף כללי ההתנהגות המקובלים בחברה ובתרבות. מאידך **<u>אתיקה</u>** היא תחום הידע שמציע ביקורת על המוסר, ומציג אוסף של כללי התנהגות שבחלקם הם חלופות לכללי ההתנהגות של המוסר.	**<u>האבות המייסדים העת העתיקה:</u>** - **סוקרטס** (הסגולה הטובה כערך עליון). - **אפלטון** (המידה הטובה). - **אריסטו** ("אתיקה ניקומאכית" , מושג "הטוב העליון", השגת האושר). - **הרמב"ם** (מקור החיוב להתנהגות מוסרית הוא התורה) [47]. **<u>המאות ה-16 עד ה-19:</u>** - **דיויד יום** ("הכשל הנטורליסטי", גישת התועלתנות). - **תומאס הובס** ("לויתן", מושג האגואיזם \ הגישה המטריאליסטית - חומרנות + מכניסטית - הכול תלוי סיבה-תוצאה). - **ג'רמי בנת'ם** (הדוניזם \ גישת התועלתנות \ גישת הנהנתנות). - **ג'ון סטיוארט מיל** (הדוניזם \ מייסד גישת התועלתנות). - **עמנואל קאנט** (התבונה היא מקור המוסר, "מוסר אוטונומי" - האדם הוא הערך העליון). - **ג'ון לוק** – ("האמנה החברתית" , הבסיס המוסרי להגנה על הפרט וקניינו האישי). - **פרידריך וילהלם ניטשה** – (מוביל תחום הספקנות המוסרית, שלילת המוסר הקיים – ניהיליזם). - **ג'ון .ל. מקי** – ("תיאורית השגיאה של המוסר", הספקנות המוסרית, אין ערכים אובייקטיביים). **<u>המאה ה-20 עד ימנו:</u>** - **ג'ון דיואי** (אתיקה פרגמטית). - **ישעיהו ליבוביץ** ("נביא הזעם" \ "המוכיח בשער" של החברה הישראלית, גישה המוסר ההומניסטית (למרות שהוא עצמו לא הגדיר את עצמו כך), "לוחם למען התדמית האנושית של ישראל") - **אסא כשר** (ממעצבי הקוד המוסרי של צה"ל). - **אלעזר וינריב** (מחבר סדרת הספרים "בעיות בפילוסופיה של המוסר"). - **יוסף רז** (מפתח תפיסת של הליברליזם פרפקציוניסטי). - **יורגן הברמאס** (אתיקה של השיח). - **ג'ון בורדלי רולס** (מושג "מסך הבערות" , הספר "תאוריה של צדק" 1971). - **רוברט נוזיק** (עקרון "אי-התוקפנות" , הספר "אנרכיה, מדינה ואוטופיה" 1974).	**<u>רקע כללי:</u>** **אתיקה** או **פילוסופיה מוסרית** היא ענף בפילוסופיה שכולל שיטתיות, הגנה והמלצה על מושגים של התנהגות נכונה ושגויה. האתיקה מבקשת לפתור שאלות של המוסר האנושי על ידי הגדרת מושגים כמו טוב ורע, נכון ולא נכון, צדק ופשע. שלושה תחומי לימוד מרכזיים בתחום האתיקה המוכרים כיום הם: 1. **מטא-אתיקה**, הנוגעת למשמעות התיאורטית ולהתייחסות של הצעות מוסריות, וכיצד ניתן לקבוע את ערכי האמת שלהן (אם ישנם). 2. **אתיקה נורמטיבית**, הנוגעת לאמצעים המעשיים לקביעת דרך פעולה מוסרית. 3. **אתיקה יישומית**, הנוגעת למה שאדם מחויב (או מותר) לעשות במצב מסוים או בתחום פעולה מסוים. [48] ניתן לחלק את הפילוסופיה של המשפט לפסיקה אנליטית ולפסיקה נורמטיבית. **פסיקה אנליטית** שואפת להגדיר מהו חוק ומהו לא על ידי זיהוי המאפיינים המהותיים של המשפט. **פסיקה נורמטיבית** חוקרת הן את הנורמות הלא-משפטיות המעצבות את החוק והן את הנורמות המשפטיות המופקות על ידי החוק ומנחות את פעולת האדם. **<u>התרומות העיקריות:</u>** **אתיקה היא <u>הכרחית ומהותית</u> בחיבור שלה לפילוסופיה של אבטחת הסייבר**, מכמה בחינות: 1. מבחינת נקודות ההתייחסות האתיות הקשורות להגנת הפרטיות: השימוש במידע, הנגישות למידע, שיתוף מידע, סילוף מידע, השמטת מידע, הסתרת מידע ועוד. 2. השפעה ישירה על היחס והשיפוטיות שלנו ביחס לסייבר התקפתי, הן בהקשר לפעולתו של התוקף, והן לגבי אחריותו של המותקף (הצד הנפגע). 3. שימוש בטכנולוגיות של סיבר התקפי בהתמודדות עם פשע וטרור, האם השימוש בה מוסרי ?, האם היא פועלת לטובת האנושות או לרעתה, כדוגמת הצדקות המוסריות בדיעבד לשימוש בכלי NSO על ידי גופי הביטחון הישראלים \ מדינות זרות. [49]

47 סעיף 8.4 במאמר "**הגותו של הרמב"ם על רקע ההגות הכללית והמדעית**" – הקדמה לספר המדע יצחק איציק ואלכסנדר קליין מקור: לינק

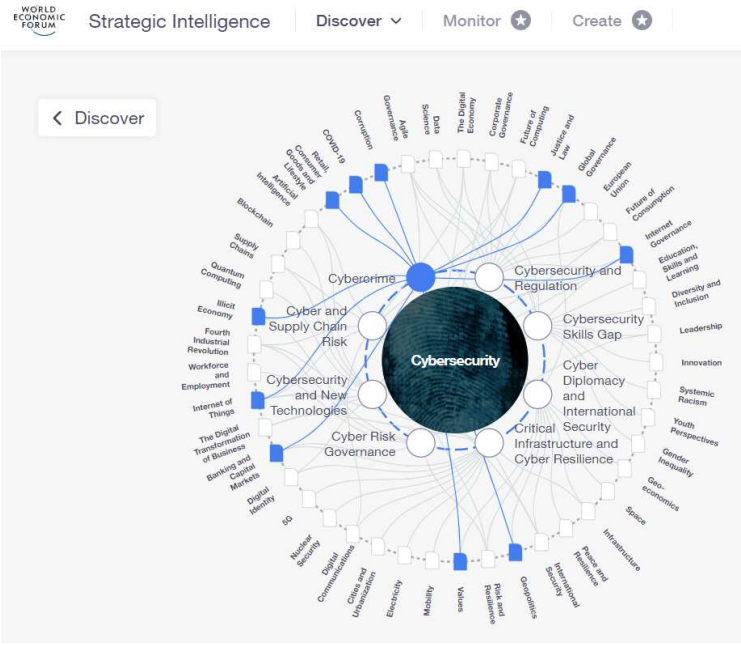
48 **מהי אתיקה ?** – מקור - לינק

3.4 מהן הפילוסופיות הנוספות או תחומים אקדמיים אחרים שיכולים להוות מקור השפעה עבור הפילוסופיה של אבטחת הסייבר ?.

הפורום הכלכלי העולמי (World Economic Forum) יצר מפת חשיבה \ מפת הקשרים דינאמית (או כמו שהם מכנים זאת: **מפות טרנספורמציה - Transformation Map** [50]) המדגימה באופן ויזואלי את המורכבות הגדולה של **ענף הסייבר אשר משפיע ומושפע באופן ישיר ועקיף מעל ל-250 תחומים אחרים.**

לפי המפה תחומי השפעה הראשיים של \ על ענף הסייבר נכון לסוף שנת 2022 הם:

- **Cybercrime** - פשיעת סייבר על רקע כלכלי.
- **Cyber and Supply Chain Risk** – ניהול סיכוני סייבר ובעיות אבטחת מידע בשרשרת האספקה.
- **Cybersecurity and New Technologies** – הקשר בין סייבר ושימוש בטכנולוגיות חדשות (חשיפה לבעיות אבטחת מידע חדשות בעקבות שימוש בטכנולוגיה חדשה).
- **Cyber Risk Governance** – עמידה בדרישות משילות, ניהול סיכונים ורגולציה ממשלתית - GRC (ממשל - Governance, ניהול סיכונים -Risk management, ציות לרגולציה - Compliance).
- **Cybersecurity and Regulation** – עמידה בדרישות רגולציה בינלאומיות.
- **Cybersecurity Skills Gap** – המחסור העולמי בכוח אדם בענף הסייבר והאתגר בגיוס והכשרת מקצועית בכל קשת התפקידים המורכבים בענף הסייבר.
- **Cyber Diplomacy and International Security** – דיפלומטיה בינלאומית בהתמודדות עם אתגרי האירועים הגאו-פוליטיים במרחב הסייבר ומניעה של אי-יציבות ביחסים והידרדרות למלחמה בין מדינות, מלחמות סייבר ברמה הבינלאומית \ ברמת מדינות: מרחב החלל, פגיעה בתשתיות קריטיות לחיי אדם, השפעות כלכליות בינלאומית כתוצאה מהתקפות סייבר.
- **Critical Infrastructure and Cyber Resilience** – פגיעה בחוסן מדינות ובתשתיות לאומיות העלולות לפגוע בתפקוד המדינה עד לרמה של אי יכולת לספק שירותים הכרחיים לתושבי המדינה (חשמל, מים, תחבורה, רופאה).



48 **מהי אתיקה ?** – מקור - לינק

49 **ד"ר תהילה שוורץ-אלטשולר** – מאמר בשם - "**לשרטט גבולות לבחורינו הטובים**" ("גלובס", 12.6.2019). "בטכנולוגיה כשלעצמה אין דבר המחייב לעשות טוב, ומשימת הדור הזה היא לגרום לטכנולוגיה לעבוד לטובת החברה האנושית ולא לשעתק רעות מן העבר וליצור חדשות". מקור - לינק

50 לינק למפה הדינאמית של **הפורום הכלכלי העולמי** – סגמנט "סייבר" – לינק

כפי שמוצג במפה של ה-WEC ענף הסייבר מורכב ביותר, משפיע ומושפע מתחומים שונים, **לכן גם בהקשר הפילוסופי הוא תחום שמשפיע ומשופע ממספר רב של ענפים אחרים בתחום הפילוסופיה**.

במיפוי הבוחן לפי מעגלי קרבה תופעות \ תחומים שונים [51] כמקובל במיפוי טרנדים ומגמות אפשר לחלק את התחומים לשלושה מעגלי השפעה: **המעגל בקשר ישיר**, **המעגל העקיף בקשר קרוב**, **המעגל העקיף בקשר רחוק**.

1. במעגל השפעה בקשר <u>ישיר</u> אפשר לכלול את התחומים (<u>לפי סדר החשיבות שלהם</u>):

- **הפילוסופיה של המידע.**
- **הפילוסופיה של הטכנולוגיה.**
- **הפילוסופיה של המוסר (תורת המידות \ אתיקה).**

2. במעגל ההשפעה <u>העקיף בקשר קרוב</u> אפשר לכלול את התחומים (<u>אין</u> חשיבות לסדר):

- **הפילוסופיה של המדע**: מתודולוגיות עבודה, בחינה ותיקוף ממצאים ותוצאות מחקר.
- **לוגיקה (תורת ההיגיון)**: מתודולוגיה לקבלת החלטות אנושיות או על ידי בינה מלאכותית.
- **הפילוסופיה של הכלכלה**: בחינת השפעות הכלכליות על ענף אבטחת הסייבר.
- **פילוסופיה מדינית \ פילוסופיה פוליטית:** התייחסות המדינה לתושביה בהקשר של פרטיות ושימוש במידע שיש ברשות המדינה על אזרחי (נתיני) המדינה.
- **הפילוסופיה של הסוציולוגיה**: השפעות על תופעות חברתיות על ענף הסייבר.

3. במעגל ההשפעה <u>העקיף בקשר רחוק</u> אפשר לכלול את התחומים (<u>אין</u> חשיבות לסדר):

- **הפילוסופיה של המשפט**: השפעות של ענף הסייבר על ענף המשפט והתאמתו להתפתחות הטכנולוגית המואצת.
- **הפילוסופיה של הנפש**: השפעות של ענף הסייבר על עיצוב תודעתנו ובריאות הנפש.
- **תורת ההכרה (אפיסטמולוגיה):** השפעות ענף הסייבר על תפיסת המציאות שלנו, והאופן בו אנחנו "תופסים" ידיעה למול המציאות.
- **הפילוסופיה של ההיסטוריה (היסטוריוסופיה):** בחינת השפעות של סילוף מידע \ השמטת מידע בהקשר לחקר ההיסטוריה של הטכנולוגיה וההשפעה שלה באופן ישיר או עקיף על האנושות.

<u>4. מהן הבעיות והשאלות המהותיות בהן צריכה לדון הפילוסופיה של אבטחת הסייבר ?.</u>

<u>4.1 מבוא.</u>

השאלות "הבוערות", האתגרים העתידיים של האנושות, הסוגיות הבינתחומיות שבהן תדון הפילוסופיה של אבטחת הסייבר הן בסופו של דבר גם ההצדקה **מדוע התחום הפילוסופי הזה חייב "להיוולד" ולהתפתח**, היות ואין תחום פילוסופי או תחום מחקר אחר שדן **באופן מעמיק ובלתי תלוי** באותם אתגרים המייחדים את ענף אבטחת הסייבר וגם "מציף" את הבעיות שחלק מהן כבר אפשר לצפות מראש כבר היום שיהפכו לבעיות קריטיות בעתיד הקרוב עבור כלל האנושות.

הסתכלות רחבה ככל האפשר וחיבור מולטי-דיסציפלינרי בין תת ענפים ממדעי החיים ותחומים מדעיים וטכנולוגיים שונים תעזור לנסח את השאלות באופן ממוקד וברמת רלוונטיות גבוה. **ענף הסייבר משפיע באופן ישיר על תחומים רבים בהם**: משפט , כלכלה, כלכלה התנהגותית, סוציולוגיה, שיווק ופרסום, פוליטיקה, גאופוליטיקה ויחסים בינלאומיים, שימוש בטכנולוגיה בקשת רחבה, תחום מדעי המחשב בקשת רחבה, שדה הקרב העתידי,

51 שיטה למיפוי הקשרים בין טרנדים \ מגמות \ תחומים שונים ע"פ מתודולוגית מחקר מקובלת בתחום טרנדולוגיה , מקור: עמוד 80 בספר "**הבא – השיטה לחזות טרנדים בעולם משובש**" – **עדי יופה** - 2019

תחבורה וניידות, ערים חכמות, תעשייה ומסחר בינלאומי ועוד.

כזכור הפורום הכלכלי העולמי ביצע מיפוי של 250 תחומים שענף הסייבר משפיע עליהם או מושפע מהם, כך שלמעשה ההתעלמות של האנושות היום מאותן אתגרים של "**המהפכה התעשייתית הרביעית**" **שאנחנו רק בתחילת דרכה**, וענף הסייבר הוא חלק מהותי ובלתי נפרד ממנה, זה שווה ערך להתעלמות של האתגרים שבפניהם האנושות מתמודדת כיום בעקבות המהפכה התעשייתית הראשונה מלפני מעל 200 שנה.
את התפתחות המואצת של הטכנולוגיה אי אפשר לעצור, ולאנושות גם אין אינטרס לעצור אותה, הרי בסך הכול הטכנולוגיה הופכת את החיים שלנו להרבה יותר קלים (ואת האנושות להיות הרבה יותר עצלנית ונצלנית מאשר בעבר) אבל לא מן הנמנע שכבר היום נדון לעומק ונתכנן כיצד הולכים להתמודד בעתיד עם האתגרים שהטכנולוגיה הולכת לזמן לאנושות בתחומים שונים, **אתגרים שחלק מהם אנחנו חווים כבר היום**.

4.2 מי קהל היעד של תחום הפילוסופיה של אבטחת הסייבר ?

קהל היעד הפוטנציאלי של הפילוסופיה של הסייבר הוא נרחב היות והתלות בענף הסייבר היא בלתי נפרדת מתחום הפעילות של אותם גורמים, ולכל גורם המניעים שלו **לחפש תשובות לבעיות ואתגרים שהוא מתמודד איתם או צופה שהוא עתיד להתמודד איתם**. בחלוקה גסה אפשר לחלק את הגורמים באופן הבא:

- **אקדמיה**: בקשת רחב של תחומי מדעי החיים, תחומי מדעי הרוח (פסיכולוגיה, פילוסופיה, היסטוריה), כלכלה, שיווק, מדעי המחשב בקשת רחבה, משפטים, דיפלומטיה ויחסים בינלאומיים, מינהל ציבורי ועוד.
- **גופים בינלאומיים העוסקים בפיקוח על שימוש בטכנולוגיה**: לדוגמא "הפורום הכלכלי העולמי" , פורמים שונים של האו"ם, גופים בינלאומיים המפקחים על שימוש בנשק, גופים בינלאומיים המפקחים על שימוש ב-AI, גופים בינלאומיים המפקחים על שימוש ברשת האינטרנט, ועוד.
- **גופים ממשלתיים מקומיים:** משרד המשפטים (הרשות להגנת הפרטיות, הרשות לאיסור הלבנת הון ומימון טרור), משרד הביטחון (אגף הפיקוח על היצוא הביטחוני), משרד החדשנות (או בשמו המלא: משרד החדשנות, המדע והטכנולוגיה), משרד ראש הממשלה (מערך הסייבר הלאומי), משרד האוצר (המפקח על הבנקים וחברות הביטוח), גופי רגולציה המפקחים על מוסדות הרפואה, תעשייה, משק לשעת חרום, תשתיות לאומיות ועוד.
- **קהילת מקצועיות של העוסקים בתחום הסייבר ונמצאים בין מקבלי ההחלטות:** CISO, DPO, CIO.
- **קהילת מקצועיות העוסקים בטכנולוגיות המידע:** מנתחי מערכות, פיתוח תוכנה, CDO, מנהלי IT, מנהלי תחום תשתיות.

4.3 דוגמה לשאלות "הבוערות" שהפילוסופיה של אבטחת הסייבר חייבת לדון בהם כבר היום (רשימה חלקית של שאלות בעיקר בנושאים שצצו ועלו בשלוש שנים האחרונות):

אתיקה \ משפט:

- **מי אמור לשאת באחריות למול הקורבנות של פשיעת סייבר?** כאשר ארגון הוא קורבן למתקפת סייבר וכתוצאה מאותה התקפה, מידע רגיש הודלף לרשת האינטרנט (או לכל מדיה אחרת של רשות הרבים, לדוגמא פרסום בעיתונות הכתובה), בגלל הדלפת הפרטים לקוחות \ ספקים \ עובדים של החברה נפגעו באופן אישי מחשיפת המידע הרגיש עליהם או צפויים להיות נתונים לסחיטה עתידית בגלל אותו מידע (ראה מקרה חברת נתוני האשראי אקוויפקס [52]) **נשאלת השאלה מי אמור לפצות אותם ?**: האם זה **התוקף ?** (במידה ונתפס והובא לדין, ואם כן תחת איזה סמכות משפטית ? של מדינת הנפגע או של מדינת הפוגע?), האם זה הנפגע \ **החברה המותקפת ?** (כי היא לא שמרה על המידע הרגיש של הלקוחות שלה כמו שהיא היתה מחויבת לעשות כן), האם זאת **המדינה** ? (כי היא לא סיפקה הנחיות \ רגולציה \ פתרונות הגנה נאותים למגזר האזרחי הן כנגד פשיעה כלכלית והן כנגד התקפת סייבר על רקע גאופוליטי).
מי אמור לשאת באחריות משפטית \ פלילית (תלוי במקרה) \ אחריות לפיצוי כספי כלפי מי שנפגע באופן ישיר \ עקיף (כדוגמת בני משפחה) \ פגיעה בציבור ? \ פגיעה בביטחון המדינה ?.

<u>מקרה בוחן:</u> בתקיפה של אתר **אטרף** [53] (אתר ההיכרויות לקהילה הגאה) במהלך שנת 2021 נחשפו **<u>למעלה ממיליון רשומות</u>** משתמשים כולל פרטים אישיים מלאים ותמונות אינטימיות, חלק מחברי האתר שלא רצו להיחשף כמי ששייכים לקהילה הגאה "הוצאו מהארון" בעל כוחם, חלק מחברי האתר הם קצינים בדרגות שונות בצה"ל, משטרה, משרדי ביטחון לאומי (חשיפת שמם עלולה להיות פגיעה בביטחון המדינה), מנהלים בכירים במשרדי ממשלה, אנשים נשואים עם משפחות (שמסתרים את נטיתם המינית), יהודים השייכים לקהילה החרדית, ערבים מוסלמים דתיים ועוד.
כל מי ששמו נחשף בהתקפה הזאת, ממש לא היה מעוניין בחשיפה כזאת, בנוסף היות ומדובר בנושא מהותי בחייו של אדם (נטייתו המינית), חשיפה כזאת עלולה להיות גורם מהותי לסחיטה של הנחשף בעל כורחו [54], במקרים מסוימים גם לגרום לאובדן חיים (התאבדות) [55] כמו מקרה הפריצה ודליפת המידע מהאתר "**אשלי מדיסון**" "אתר הבוגדים-בוגדות" האמריקאי בשנת 2015 בה נגנבו 37 מיליון רשומות מהאתר, כולל פרטים של 170,000 ישראלים שתבעו את האתר בתביעה ייצוגית ובשנת 2020 גם זכו בתביעה כנגד האתר [56].

---

52 ראה מקרה מפורסם בחברת **אקוויפקס** (חברת נתוני האשראי מהגדולות בארה"ב) בו היה קיים חשד שהמנהלים בחברה היסתירו ביודעין במשך כמה ימים ולא דיווחו לבורסה האמריקאית ולרשות המסחר הפדרלית (FTC) על פריצת סייבר חמורה ביותר שבוצעה בשרתי החברה, התקפת סייבר בה נגנבו פרטים אישים ומאוד רגישים של 148 מיליון לקוחות \ אזרחי ארה"ב | כלכליסט , 08.09.2017 , רפאל קאהאן, "**פריצת ענק לחברת מידע אשראי אמריקאית: פרטים רגישים של 143 מיליון צרכנים נגנבו**" – מקור - לינק

53 **הפריצה לאתר אטרף**: התוקפים חשפו פרטים על מיליון משתמשים. קבוצת בלאק שדאו, המקושרת לפי הערכות לאיראן, פרסמה בערוץ הטלגרם שלה היום קובץ ובו **<u>רשומות על למעלה ממיליון משתמשים באתר אטרף</u>** • הקובץ כולל הודעות בין משתמשים, מיקומים אחרונים שלהם, מספרי טלפון ופרטים מזהים, מתוך גלובס, אופיר דור, 02.11.22 מקור - לינק

54 **חצי שנה אחרי הפריצה לאשלי מדיסון**: **ההאקרים סוחטים את מנויי האתר לאחר שההאקרים גנבו מידע אישי על 37 מיליון משתמשים באתר הבגידות, הם החלו לשלוח לחברים באתר דרישות כופר של אלפי דולרים, ואף פנו לבני זוגם**. עברו שישה חודשים מאז שאתר השידוכים לאנשים נשואים נפרץ בידי האקרים וכעת אתר "אשלי מדיסון" עומד במרכזה של שערורייה חדשה: משתמשים באתר בעבר ובהווה ובני זוגם מקבלים מכתבי סחיטה. כמעט מיד עם הפיכת מאגר השמות של האתר לפומבי בידי ההאקרים, החלו בעלי חשבונות באתר לקבל מכתבי סחיטה אנונימיים, אלקטרוניים ופיזיים. המכתבים דרשו מהמשתמשים תשלום בסכומים של אלפי דולרים תחת איום שחברותם באתר תפורסם בפומבי אם יסרבו לשלם.| כלכליסט | 03.03.2016 | שירות כלכליסט – מקור - לינק

55 **לראשונה מאז ההדלפה: שני לקוחות של אתר אשלי מדיסון התאבדו לפי הודעת משטרת קנדה**, שני בני אדם שמו קץ לחייהם לאחר שהודלף כי היו מנויים לאתר הבגידות. כמו כן, בעלי האתר הציעו פרס של חצי מיליון דולר לכל אדם שיספק מידע שיוביל לזיהוי המדליפים... החשש היה שהצעד הזה יוביל להרבה מקרי גירושין ואף להתאבדויות, כפי שאירע היום. האתר כבר ספג תביעה ייצוגית על סך 578 מיליון דולר, ותביעות רבות של מנויים עשויות להגיע. | סוכנות הידיעות | 24.08.2015 | וואלה , מקור - לינק.

56 פרשת דליפת המידע מאתר הבגידות אשלי מדיסון הסתיימה בפשרה של חצי מיליון שקל זאת במסגרת תביעה ייצוגית שהגיש המבקש, **שהשתייך ל-170 אלף הישראלים שהשתמשו בשירותי אתר הבגידות שממנו נגנבו ב-2015 פרטיהם** של 37 מיליון משתמשים בעולם: היום אישר המחוזי מרכז את הפשרה במסגרתה 2 החברות המפעילות את האתר ישלמו את הסכום לקרן מיוחדת, המיועדת להגנת הפרטיות באינטרנט | כלכליסט | ליטל דוברוביצקי | 25.02.2020 | מקור – לינק.

- **האם ה CISO או ה CIO נושא אחריות לרשלנות מקצועית?** האם ארגון שנפגע ממתקפת סייבר יכול מבחינה אתית לתבוע באופן אישי את מנהל אבטחת המידע שלו (CISO) או את מנהל מערכות המידע (CIO) על רשלנות בביצוע תפקידו ?. האם במקרה בו החברה נפגעה כלכלית עד כדי פשיטת רגל עובדי הארגון שאיבדו את מקור פרנסתם יכולים העובדים לתבוע את מנהלי החברה \ הדירקטוריון \ ה-CISO על רשלנות מקצועית ?.

<u>מקרה בוחן:</u>

  - **2017** - **סוזן מולדין** ה CISO (לשעבר) של חברת **אקוויפקס** הואשמה על ידי קהילת הסייבר בכל העולם ברשלנות מקצועית בגלל אי הכשרה מקצועית מתאימה למילוי תפקידה, ונזק עצום נגרם לחברה שלה ולציבור גדול שהמידע האישי שלו הופץ ברבים בגלל פרצת אבטחה פשוטה שסוזן בחרה שלא לטפל בה בשרתי סביבת הייצור של החברה, זאת למרות שיש לאותה פרצה Patch שמטפל ומתקן את אותה פרצת אבטחה שדרכה התוקפים הצליחו לחדור לשרתים. [57]
  - **2022** - **ג'וזף סאליבן**, מנהל אבטחת המידע לשעבר של **אובר** הורשע בהסתרת מידע על פשע פדרלי ושיבוש הליכי משפט בעבור פריצת סייבר לחברה בשנת 2016, לאחר שניסה להגן על פרטי המשתמשים וניהל מו"מ עם התוקפים על מנת להלבין את התשלום שהעבירו להם כתשלום כופר. [58]

- **האם זה אתי לתבוע עובד חברה בגין היותו קורבן להונאת סייבר שהחברה נפגעה ממנה?** האם חברה שנפגעה מהונאת סייבר יכולה לתבוע עובד חברה בגין רשלנות, באם בשל פעולה שעשה בשוגג וללא מודעות, היא היתה הסיבה שבגללה הארגון נפגע בהונאת סייבר ?

<u>מקרה בוחן:</u>

  - **2020** – תביעה של חברה (מעסיק) כנגד עובדת בחברה (בשם) **יעל רייבארך** [59] שבגלל רשלנות שלה החברה נפלה קורבן להונאת סייבר.

57 ראה מקרה מפורסם משנת 2017 בו היה עֵלהום תקשורתי במדיה ובקהילות המקצועיות בענף הסייבר שכלל האשמות חמורות כנגד **סוזן מולדין** ה CISO (לשעבר) של חברת **אקוויפקס** בגין רשלנות מקצועית שלה. המניע להאשמות בגין רשלנות מקצועית היה בשל העובדה שלא היה לה הכשרה אקדמית או מקצועית מתאימה כדי למלא את תפקידה ובכל זאת היא לקחה על עצמה למלא תפקיד של CISO בחברה שאוגרת נתונים רגישים ביותר על אזרחי ארה"ב (בקשות לקבלת אשראי ומשכנתאות) , כזכור המחדל מקצועי שהיא הואשמה בו זה היעדר התקנת תלאי אבטחה בשרתי סביבת הייצור של החברה, מה שאפשר בסופו של דבר לקבוצת תקיפה סינית מימוש בקלות רבה של פרצת אבטחה ידועה בשרתי אפאצ'י (<u>פגיעות אבטחה שיש עבורה תלאי אבטחה שסוגר את הפרצה</u>), בעקבות הפרצה שנמשכה מספר שבועות (ללא שצוות ה NOC\SOC בחברה גילו את הפרצה ולא חשדו בנפח התעבורה הגדול שהודלף משרתי סביבת הייצור אל רשת האינטרנט), בפרצה נגנבו 148 מיליון רשומות מלאות הכוללות את כל פרטי דירוג האשראי של תושבי ארה"ב, <u>התוצאות של הפריצה</u>: מחיר המנייה של החברה התרסק ב 30% , החברה נקנסה ב 7 מיליארד $ בגלל היעדר שקיפות ודיווח לבורסה האמריקאית \ רשות המסחר הפדרלית (FTC) , כאשר היה חשד סביר שהמנהלים הבכירים בחברה היסתרו מספר ימים את הידיעה בציבור על התקפת הסייבר שהם נפלו לה קורבן, זאת כדי למכור את המניות שלהם חברה לפני שהפרשה "מתפוצצת" בתקשורת ומחיר המנייה יפגע. מקור: The Washington Post , 19 ספט' 2017 , Barin Fung מקור - <u>לינק</u>

58 "**שעירים לעזאזל: שני פסקי דין חדשים מטלטלים את תעשיית הסייבר**" **ג'וזף סאליבן**, מנהל אבטחת המידע לשעבר של אובר הורשע בהסתרת מידע על פריצת סייבר לחברה בשנת 2016, לאחר שניסה להגן על פרטי המשתמשים וניהל מו"מ עם התוקפים. גם האקרית שלא גנבה דבר ורק ניסתה להתריע על פרצות בבנק קפיטל וואן הורשעה. לא, זו לא הדרך להילחם בתופעה | מתוך כלכליסט | רפאל קאהאן | 06.10.22. מקור – <u>לינק</u>.

59 מקרה שפורסם ברשת הפייסבוק בתאריך 21 אוק' 2020 על ידי **עידו נאור** (המכונה "האקר סטנדרטי" , שגם נתן עדות מומחה בבית משפט לגבי המקרה) לגבי מקרה בו חברה פרטית תבעה עובדת בשם **יעל רייבארך** (Yael Raeburn) ואף פיטרה אותה מעבודה בחברה ללא תשלום פיצויים (שם החברה התובעת לא פורסם) בגין אשמה שהיא האחראית הישירה לנזק הכספי גדול שנגרם לחברה בגלל הונאת סייבר מסוג BEC (הונאות הידועות בשם "הונאות המנכ"ל" Business Email Compromise), והסיבה שהיא אחראית לנזק הכספי שהם ספגו, זה בגלל שהיא שהתרשלה בתפקידה ולא בדקה את הפרטים שבגללם ההונאה הצליחה. מאידך לטענת העובדת הפעולה בוצעה בתום לב, וכי היא לא קיבלה הכשרה מתאימה מהמעסיק כדי לזהות ולהיזהר בהתאם מהונאות סייבר מסוג זה. אחרי שנתיים דיונים ועדויות התביעה נדחתה על ידי הפרקליטות. מקור – <u>לינק</u>.

- **פגיעה בחיי אדם בעקבות תקיפת סייבר:** מה העונש הראוי אם בשל רשלנות מקצועית בתחום הגנת הסייבר נגרם נזק לחיי אדם או פגיעה חמורה בבריאותם של בני אדם כתוצאה ממתקפת סייבר, כדוגמת: חולה שמחובר לציוד רפואי [60] ,שיבוש תוצאות של בדיקות רפואיות שבגללה מתקבלות החלטות רפואיות שגויות [61], זיהום מי שתיה [62], פיזור חומרים מסוכנים ברשות הרבים כך שנגרמת פגיעה משמעותית בסביבה (בעלי חיים , צמחיה) ולבני אדם באותה סביבה ? [63] ועוד. **באחריות מי לשאת בעונש לאותה רשלנות ?** האם יש לקבוע קורולציה בין חומרת העונש לבין מספר הנפגעים ?, האם יש לשאת באחריות גם אם היה "כמעט" פגיעה בחיי אדם ?, האם האחריות היא של הארגון \ החברה \ הגוף העסקי \ גוף ציבורי – ממשלתי ?, או האם האחריות לרשלנות מקצועית היא של מי שנושא משרה ותפקידו היה לאבטח כראוי את אותם התקנים רגישים, שכן פריצה אליהם עלולה להביא נזק לחיי אדם או לבריאות הציבור, וזוהי אחריות שהוא קיבל על עצמו כאשר הוא התמנה לתפקיד ?.
  מקרה בוחן: 2020 - מתקפת הסייבר על מתקני המים: "איראן ניסתה להעלות את רמת הכלור"

- **אם קיבלת ממני שירות בחינם האם זה מוסרי שאני משתמש במידע שצברתי אודותך <u>כנגדך</u> ?** האם מבחינה מוסרית מותר לחברה מסחרית כדוגמת גוגל, מטא (פייסבוק, ווצאפ, אינסגטרם), אמאזון, אפל ועוד, לעשות שימוש במידע פרטני ואישי שנאסף על לקוחות החברה כדי להפעיל מנגנוני "הנדסת תודעה", לנצל את החולשות של הלקוח כדי לגרום לו לרכוש מהפלטפורמה או לבצע פעולות אחרות בגלל מניעים אמוציונליים ?, האם לחברה יש הצדקה מוסרית לפעול כך שכן האפליקציה או השירות ניתנו בחינם ?.
  כבר למעלה מעשור משפטים כגון "**אם אתה לא משלם, אתה לא הלקוח - אתה המוצר**" ("If you are not paying for it, you're not the customer; you're the product being sold".) נאמרים מעל כל במה, וללא שום התנצלות על ידי מנהלים בכירים בכל הקשת הטכנולוגית כך שגם הלקוח לא יכול להיות כל כך תמים שהוא מקבל מוצר או שירות בחינם ולא משלם עליו באופן כזה או אחר. האם יש חובה מוסרית של החברה להתייחסות שונה כלפי הלקוח והמידע שנאסף אודותיו במידה והוא כן שילם ורכש את האפליקציה \ שירות מהחברה ?.
  מקרה בוחן:
  - הנושא נדון במאות כתבות והתייחסויות הן במדיה הדיגיטלית והן במדיה הכתובה.
  - מצ"ב ספרים מומלצים [64] שכוללים הרבה דוגמאות לשיטות הפעולה של חברות הענק בהפעלת מניפולציות והנדסת התודעה שלנו.
- **האם בטחון המדינה קודם בחשיבותו להפרה ופגיעה בפרטיות של אזרחי המדינה ?** האם זה אתי לחברה פרטית להעביר מידע אישי שהיא אספה על <u>לקוח מסוים</u> לגופי אכיפת חוק ממשלתיים \ביטחוניים בטענה כי זה נדרש לצרכים של ביטחון המדינה ?, האם זה אתי במקרה בו חברה מסחרית בוחרת להפר את האמון שהיא קיבלה מהלקוחות שלה ולמסור מידע על הלקוחות שלה לצד ג' בגלל מניעים אחרים ?, האם זה מוסרי שמערכת אבטחת מידע של יצרן מסוים תשמש ככלי ריגול עבור גורם אחר תמורת תשלום ? האם יש זה הצדקה מוסרית כאשר התמורה היא בביטחון המדינה שלך ?.

---

60 **דוח מבקר המדינה מאי 2022** | משרד הבריאות | **הגנת סייבר על מכשירים רפואיים ואבטחת מידע הנאגר בהם** | מקור – לינק.

61 **האיגוד הישראלי לאונקולוגיה קלינית ורדיותרפיה** | 31.01.2018 | **כך תיראה מתקפת סייבר על מכשור רפואי חיוני בבתי החולים בישראל**, השתלטות מרחוק על מכשירי MRI, שיבוש בזדון של תוצאות CT ולקיחת בדיקות דחופות כ"בנות ערובה". חוקרים באוניברסיטת בן גוריון בנגב חושפים במחקר חדש כיצד תיראה מתקפת סייבר על מכשור הדמיה רפואי | מקור – לינק.

62 YNET | 01.06.2020 | מאמר מערכת | מתקפת הסייבר על מתקני המים: "**איראן ניסתה להעלות את רמת הכלור**" | מקור – לינק.

63 גלובס | 16.05.2018 | יובל אזולאי | **המדינה דורשת ממפעלים בסיכון גבוה להתמגן מהאקרים** המשרד להגנת הסביבה ידרוש כבר בחודשים הקרובים מכ-60 מפעלים שמוגדרים בסיכון גבוה להשקיע מיליונים במיגון מפני תקיפות סייבר • **מפעל שלא ייערך, לא יקבל היתר רעלים** • בכיר במשרד להגנת הסביבה: "בשנה האחרונה אירעו שבעה ניסיונות לתקוף מפעל כימי גדול" , מקור – לינק.

64 **ספרים מומלצים בעברית שעוסקים <u>בהנדסת התודעה למטרות כלכליות</u>**:

- **הארבע** – הדי-אנ-אי הסמוי של אמזון, אפל פייסבוק וגוגל | **סקוט גלווויי** | כתר | 2018
- **קוד סמוי** – כל מה שלא רוצים שתדעו ואתם חייבים לדעת על החיים בעידן הדיגיטלי | **ד"ר יובל דרור** | דביר | 2019
- **עיצוב התודעה** – הנדסת ההתנהגות והתחושות שלנו בעידן הדיגיטל | **ד"ר לירז מרגלית** | פרדס | 2021

<u>מקרי בוחן:</u>

- **2008** – ספר בשם "**מפעל הצללים**" [65] ("The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America") יוצא לאור בארה"ב על ידי העיתונאי והסופר **ג'יימס במפורד** [66] (עיתונאי אמריקאי שנחשב עיון כלפי ישראל), הספר עוסק ביכולות הטכנולוגיות המתקדמות שיש ברשות ה NSA כדי לבצע האזנות סתר לטלפוניה, קווי פקס, תקשורת מחשבים, תקשורת אלחוטית, אותות אלקטרומגנטים, תקשורת מכ"ם, רדאר ועוד). בספר נטען כי יחידת המודיעין 8200 הישראלית, היא למעשה המקבילה של ה-NSA האמריקאית, ויש ברשותה יכולות טכנולוגיות מתקדמות (בחלק מהמקרים מתקדמות יותר ממה שיש ל NSA) לציתות ופיענוח תקשורת אלקטרונית מכל הסוגים, ולא רק שהיא מפתחת טכנולוגיות מתקדמות כאלה היא מפעילה אותן גם כדי לרגל אחרי גופי ביטחון, משרדי ממשלה וחברות פרטיות בארה"ב. בעולם הערבי "תופסים טרמפ" [67] על האשמות חסרות השחר שמופיעות בספר כך **שחברות ההייטק הישראליות הן למעשה חלק מהזרוע הארוכה של קהילת המודיעין הישראלית**, הם מתבססים על כך שבשנת 2006 (שנתיים לפני פרסום הספר) חברת צ'ק פוינט הישראלית הגישה הצעה לרכוש את חברת האבטחה **Sourcefire** האמריקאית (אחרי מספר גלגולים ב 2013 החברה נמכרת לסיסקו האמריקאית). לפי המופיע בספר בגלל שחלק מלקוחות החברה הן משרד ההגנה האמריקאי, הסוכנות לביטחון לאומי (NSA), ועוד גופי ביטחון אחרים בארה"ב, הממשל האמריקאי באמצעות <u>הוועדה להשקעות זרות בארה"ב לא מאשר את הרכישה</u> [68]. **החשש של האמריקאים הוא מריגול ישראלי**, היות וחברת צ'ק פוינט שהוקמה על ידי גיל שוויד ועמיתיו גם הם בוגרי יחידת המודיעין "ההייטקית" 8200, צ'ק פוינט תאפשר לגופי ביון ישראלים מעקב אחרי התקשורת שעוברת במערכות ה-FireWall שהם מוכרים לחברות וארגונים שונים בעולם. בעולם הערבי מופצות שמועות כי לא רק צ'ק פוינט היא חלק "מהחגיגה" **אלא גם חברות הייטק מובילות בתחומן בינהם**: ורינט, קומברס, נייס סיסטם הן הם גם חלק מהזרוע הטכנולוגית הארוכה של גופי הביון הישראלי (ובראשון המוסד) וכי גם הן חלק ממערך היכולות הטכנולוגיות המתקדם של המוסד הישראלי לעקוב אחרי תקשורת אלקטרונית של חברות \מדינות שונות בעולם. בנוסף בספר נטען גם שחברות תקשורת \ טלפוניה אמריקאיות רבות, לרבות ה NSA בעצמה מסתמכות על טכנולוגיה (חומרה\ תוכנה) שמפותחת על ידי חברות הייטק ישראליות, בכך גם הן מסתכנות וחושפות את עצמן לסיכון שהחברות הישראליות יקבלו גישה ללא ידעתן למידע הדיגיטלי שעובר במערכות שלהן , **<u>כמובן שאין בספר שום גיבוי לתזה הזאת, מלבד שבוגרי 8200 הם בכירים בחברות הייטק רבות.</u>**

- **2011** – חשדות שה- **NSA** [69] עושה שימוש במאגרי התמונות של Facebook \ Google (ופלטפורמות חברתיות נוספות) כדי לבצע איסוף מידע מודיעני, מיפוי אזרחים כדי שבעת הצורך יהיה אפשר להשתמש במאגר תמונות הזה ביחד עם מערכת של זיהוי פנוי לצורך איתור וזיהוי פושעים וטרוריסטים. **בהמשך בשנת 2014** – בפעם הראשונה בארה"ב אדם מורשע בדין לאחר שמערכת לזיהוי פנים זיהתה אותו כמבצע הפשע (שוד ברכבת התחתית בשיקגו) [70]

---

65 כתבה של יוסי מלמן | עיתון הארץ | 2008 | הנושאת את השם "**Is Israel's Booming High-tech Industry a Branch of the Mossad?**" Author of 'The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America' says the NSA thinks so | מקור – לינק.

66 ראיון מצולם משנת 2008 עם **ג'יימס במפורד** על הספר. מקור – לינק.

67 דוגמה לפוסט שפורסם בבלוג Ummah – The Online Muslim Community ב 19-10-2008 בו *משתמשים* בפרסום של הספר כדי לטעון שמסוכן *להשתמש* ב Zone-Alarm שנרכשה על ידי צ'ק פוינט היות והיא כלי ריגול ישראלי | מקור – לינק.

68 מופיע גם בערך של **סורספייר** ויקיפדייה תחת הכותרת Financial | מקור – לינק.

69 2011 - **חשדות שעלו מחשיפת מסמכי סנודון ש NSA מחוברת ישירות למאגרי המידע של Facebook כדי לנצל את מאגר התמונות של פייסבוק כמאגר לזיהוי פנים** | מקור ראשון: כיכר השבת, מישאל לוי, 10.06.14, לינק | מקור שני: Natasha Lomas , Tech Crunch, 06.01.2014 , לינק.

70 2014 - **תקדים:** אדם בשיקגו הורשע בדין על סמך תוכנת זיהוי פנים: **פייר מרטין**, גבר בן 35, נשלח למאסר של 22 שנה בכלא בגין מעשי שוד שביצע ברכבת התחתית בשיקגו. הוא הורשע לאחר שתוכנה לזיהוי פנים זיהתה אותו כשודד (חדשות דיגיטל) | כיכר השבת, מישאל לוי, 10.06.14, לינק | הארץ - קפטן אינטרנט, 10.06.14 לינק

- **2017** – ממשלת ארה"ב מפיצה חשדות שפתרון ה-EPP (חבילת הגנה סייבר על תחנת הקצה) של חברת **Kaspersky** [71] משמשת למעקב וריגול על אזרחים אמריקאים בידי שירותי הביטחון הרוסים. גורמי הביטחון הלאומי בארה"ב אף מפרסמים כי לפי המידע שברשותם מערכת אבטחה של חברת קרספרסקי שימשה לגניבת מסמכים רגישים ממשרדי ממשלה אמריקאים. על פי הנחיה של משרד ההגנה האמריקאי נאסר השימוש במערכות של קרספרסקי בכל משרדי הממשלה בארה"ב ובנוסף המלצות לגופים בכל העולם שעובדים מול משרדי הביטחון והממשלה האמריקאים להסיר מיד מערכות של קרספרסקי מתחנות הקצה והשרתים ולהפסיק לאלתר מהשימוש במערכת. בעקבות הלחץ האמריקאי בשנת 2018 התקבלו החלטות במספר מדינות של האיחוד האירופאי להפסיק גם הן את השימוש במוצרי קרספרסקי ברשתות ממשלתיות, **בנוסף ביוני 2018 האיחוד האירופאי הכריז על קרספרסקי "כמערכת זדונית"**. אך ורק **בשנת 2019** לאחר לחץ של בלגיה, גרמניה וצרפת, פורסם מסמך רשמי על ידי האיחוד האירופאי שהנושא נבחן לעומק, ולא נמצאו סמנים המעידים על שימוש לרעה של מערכות קרספרסקי למטרות ריגול עבור גופי ביון רוסיים, כך שהאיסור לעבוד עם מערכות האבטחה של החברה הוסר. למיטב ידיעתי האיסור של משרד ההגנה האמריקאי תקף עד היום [72] ובעקבותיו בגלל שיתוף הפעולה הצמוד עם ארה"ב גם במשרדי הביטחון הישראלים נמנעים מלהשתמש במערכות הגנה על תחנות הקצה של קרספרסקי עד היום.

- **האם זה מוסרי שרשויות החוק במדינה דמוקרטית עוקבות דיגיטלית אחרי פעילות של אזרחים גם כאשר מראש הם לא נחשדים בהפרת החוק** ?.

האם זה לגיטימי למטרות של ביטחון הציבור או בהצדקה של ביטחון המדינה כן לאפשר לרשויות החוק מעקב כזה ? (בדומה לשינוי המדיניות בארה"ב בשנת 2001 לאחר אירועי 9/11), ואם כן באיזה תנאים מגבילים ? אצל מי נמצאים "**האיזונים ובלמים**" של שימוש במערכות המאפשרות מעקב וריגול אחרי פעילות של אזרחים ?, האם זה לגיטימי לאפשר לעקוב אחרי כולם ולא רק אחרי אזרחים מסוימים ? או ממש להיפך זה לגיטימי לאפשר להם לעקוב אך ורק אחרי קומץ של אזרחים שיש חשד שהם מעורבים בפעילות פלילית או כזאת שמסכנת את בטחון הציבור או בטחון המדינה ?. איפה עובר הגבול בין חופש הפרט במדינה דמוקרטית לבין הצורך המבצעי של קהילת הביטחון לאסוף מודיעין כדי לזהות בשלב מוקדם פעילות פלילית או ביטחונית ?.

מקרה בוחן:

- **2020** – חשדות כי משטרת ישראל מנטרת (עוקבת) אחרי פעילות הגישה לאינטרנט של אזרחים [73]
- **2022** – חדשות כי משטרת ישראל מבצעת האזנות סתר והאזנה בטלפונים ניידים של אזרחים ישראלים בעזרת מערכת NSO, כולל עיתונאים, ראשי ערים, מנהגי מחאת "הדגלים השחורים" ובעלי תפקדים במשרדי ממשלה, ללא צו ופיקוח בית המשפט. [74]

---

71 **2017 - גופי ממשלה אמריקאים היעלו חשדות ש Kaspersky מעבירה מידע שהיא אוספת מתחנות הקצה בהן הותקן ה EPP שלהם לגופי ביון רוסים**, למרות שזה הופרך בהמשך על ידי גורמים שונים, טענה זה נתקבע בתודעה כך שבישראל בגופים שעובדים מול משרד הביטחון נאסר באופן מוחלט שימוש במערכת ההגנה לתחנות הקצה של Kaspersky | ZDNET | European Commission "not in EU: No evidence of Kaspersky spying despite 'confirmed malicious' classification 16.04.2019 | possession of any evidence regarding potential issues related to the use of Kaspersky Lab products." | מקור – לינק.

72 **נציבות התקשורת הפדרלית בארה"ב (ה-FCC) הוסיפה את חברת האנטי וירוס הרוסית קספרסקי לרשימת החברות הנחשבות כמסוכנות לביטחון הלאומי של ארה"ב. עד כה כללה הרשימה רק חברות סיניות**. עם כניסת קספרסקי לרשימה תחדל התמיכה הכספית הפדרלית מארה"ב, שסייעה עד כה ברכישת ציוד ושירותים מהחברה. לפי יו"ר ה-FCC, המהלך נועד לחזק את רשתות התקשורת של ארה"ב נגד איומי הביטחון הלאומי, לאחר שהזהירה קודם לכן מפני האפשרות של מתקפות סייבר בעקבות פלישתה של רוסיה לאוקראינה. קספרסקי בתגובה הביעה אכזבה מהחלטת ה-FCC לאסור על השימוש בתמיכה הכספית הפדרלית, והוסיפה כי ההחלטה נבעה משיקולים פוליטיים בלבד. מקור: בלומברג (**טוד שילדס**). law.co.il מזכיר כי הודעת ה-FCC מתווספת להזהרתן האחרונה של גרמניה ואיטליה משימוש במוצרי החברה, עקב החשש שינוצלו לרעה על ידי הממשל הרוסי. | 27.03.2022 | **עו"ד אור כהן** | הפורטל המשפטי לאינטרנט, סייבר וטכנולוגיות המידע | מקור - לינק.

73 **האם המשטרה מנטרת את הפעילות של גולשים באינטרנט? עו"ד יורם הכהן**, מנכ"ל איגוד האינטרנט, אמר בדיון בכנסת כי יש לאיגוד מידע שלפיו המשטרה משתמשת בהגדרות DNS כדי להעביר נתוני גולשים לשרתיה • נציג המשטרה הכחיש את הפרסומים ואמר כי היא פועלת רק באתרים גלויים. | מתוך אנשים ומחשבים 21.12.2020 , מקור – לינק.

74 **דיווח: המשטרה עקבה אחרי ישראלים בעזרת תוכנת NSO שהותקנה בטלפונים ללא פיקוח התוכנה הותקנה מרחוק בטלפונים של ישראלים, האזינה לשיחות הטלפון שלהם וצפתה בהתכתבויות שלהם.** לפי הדיווח שפורסם בכלכליסט ההוראה למעקב ניתנה ללא צו ופיקוח בית משפט. המשטרה: "אין שחר לטענות". בר-לב: "אין פרקטיקה של האזנות סתר, אוודא שלא מתבצע עיגול פינות" | וואלה |18.01.2022 | מקור: לינק | **תחקיר כלכליסט חברת NSO בשירות משטרת ישראל**: פריצות לטלפון של אזרחים ללא פיקוח או בקרה מראשי ערים ועד מנהיגי מחאת הדגלים השחורים - משטרת ישראל משתמשת בתוכנת הריגול פגסוס של NSO כדי לפרוץ מרחוק לטלפונים של אזרחים ישראלים ללא צווי חיפוש או האזנה. המשטרה: "יש פיקוח" | כלכליסט , **תומר גנון**, 18.01.2022 מקור - לינק.

- **אם באופן גלובלי נפסיק להיכנע, וקורבנות של פשיעת סייבר יפסיקו לשלם לתוקפים, האם פשיעת סייבר תמשיך להתקיים ?.**

ברמה התיאורטית אם אף ארגון שנפגע מהתקפת סייבר על רקע כלכלי, לא ייכנע, ולא ישלם דמי סחיטה בגין התקפת כופר שהופעלה כנגדו, האם זה יעצור את ניסיונות הכופר הבאים מתוך ידיעה של התוקפים כי הקורבנות לא ישלמו את דמי הסחיטה ?. האם מתוך הנחה של התוקפים כי הם לא יקבלו תגמול אחרי התקפה מוצלחת, אזי אין להם טעם להמשיך עם התקפות הכופר כלפי קורבנות נוספים, כי "שכר לעמלם" הם לא יקבלו.

מקרה בוחן: כבר מעל עשור שנים יש קריאות של האו"ם [75] וגופים בינלאומיים אחרים להתארגנות מסודרת כדי לעצור את פשיעת הסייבר על כל גווניה, על ידי הקמת כוח ושיתוף פעולה בינלאומי שילחם בתופעה ויצמצם אותה משמעותית. "**פשיעת סייבר היא לא כוח טבע שלא ניתן לעצור אותו**" הוא משפט שנשמע מידי פעם על ידי מי שקורא לשיתוף פעולה בינלאומי שכזה.

אולם ככל הידוע ההצעה להפסיק לשלם ולהיכנע לפשיעת סייבר ברמה גלובלית **בהתחייבות ובאכיפה** של כל המדינות השייכות לאו"ם, זאת הצעה שאף פעם לא הועלתה במסגרת הפרסום של האו"ם או כל גוף בינלאומי אחר, **זאת למרות שבחלק מהמדינות שחברות באו"ם קיימות תקנות או חוקים מקומיים האוסרים על תשלום דמי כופר.** [76] מאידך בחלק ממדינות ה-OECD קיימות פוליסות ביטוח המאפשר תשלום כופר (ולמעשה הן בעצמן תורמות להלבנת הון ומימון טרור) [77]

- **האם זה מוסרי לשלם תשלום לסחיטת סייבר גם כאשר ברור לנו מעל לכל ספק, שיעשה שימוש לרעה בתשלום שהועבר לתוקפים ?** .

האם זה מוסרי לשלם דמי סחיטה של התקפת כופר כדי להציל את המידע של הארגון שלי גם כאשר קיים חשש סביר כי התשלום שלי יממן פעילות טרור כנגד חפים מפשע או ישמש למימון המשך הפעילות של התוקפים ולביצוע של התקפות כופר כנגד ארגונים אחרים?

- **האם זה מוסרי להסתיר את היותי קורבן לתקיפת סייבר כדי לשמור על תדמיתי ?**.

במקרה בו ארגון פרטי נפגע מהתקפת סייבר, אולם הגוף המותקף מצליח להתאושש מהר מאותה התקפת סייבר, ומצליח לחזור למצב פעילות תקין בפרק זמן קצר, נשאלת השאלה האם כדי שתדמיתו של הארגון בפני קהל הלקוחות או בפני התחרות בשוק לא תיפגע, האם זה אתי כלפי הלקוחות \ המגזר העסקי להסתיר את האירוע?. האם זה מוסרי כלפי חברות אחרות באותו סקטור עסקי, שכן אם הארגון מסתיר את המתקפה , אזי הוא מונע שיתוף ידע בקהילה בנוגע לאופי התקיפה (ואולי כיצד מומלץ להתגונן בפניה מראש), מה שעשוי היה לעזור לארגונים אחרים להתגונן ולהתכונן לקראת התקפה זהה, היות שגם הם פוטנציאל להתקפה זהה.

---

75 **Taking action where we can to stop cybercrime** | Yury Fadotov | 2018 | פורסם באתר Arab News מקור – לינק | ובנוסף באתר של האו"ם , מקור- לינק.

76 **מאמר דעה | על המדינה למנוע בכל דרך תשלום כופר להאקרים למרות שיש בידי מדינות כלים משפטיים למנוע תשלום כופר לארגוני פשע בינלאומיים** – בפועל אין בנמצא מדינה שאכן מבצעת אכיפה של החוק על גופים פרטיים ... כיום מרבית מדינות ה OCED נותנות בפועל חסות ואפילו לגיטימציה למתקפות הסייבר. למרות שיש בידי מדינות אלו כלים משפטיים למנוע תשלום כופר לארגוני פשע בינלאומיים – **בפועל אין בנמצא מדינה שאכן מבצעת אכיפה של החוק על גופים פרטיים**. יותר מכך ברבות ממדינות OECD נמכרות פוליסות ביטוח הכוללת החזר על תשלומי כופרה לארגוני פשע בינלאומיים.... המדינה אישרה בפועל פוליסה שמאפשרת לשלם לארגון פשע בינלאומי – דבר האסור או לפחות סותר לכאורה את החוק ואת רוח חוק מאבק בארגוני פשיעה. יותר מכך – חוק איסור הלבנת הון, חוק איסור מימון טרור, חוק הבנקאות וחוק ניירות ערך – חוקים אלה ורוחם עומדת בסתירה מוחלטת להשלמה בשתיקה או בהסכמה לתשלום כופר על ידי חברות פרטיות וציבוריות . | 29.10.21 | **שבתאי שובל** | Israel Defence | מקור – לינק.

77 **הרשות לאיסור הלבנת הון ומימון טרור במשרד המשפטים מפרסמת סקירה רחבה של תחום תשלומי הכופר בעקבות אירועי סייבר, ודרכי הלבנת ההון המופק מהם לתוך ניצול לרעה של המערכת הפיננסית**. הרשות מספקת הצצה לשיטות הפעולה בתחום, נתונים על היקפי התופעה בארץ ובעולם, דרכי הלבנת ההון והשימוש במטבעות קריפטוגרפים, דוגמאות לדיווחים לרשות, חשיפת חקירה כלכלית שביצעה הרשות, בה התחקות אחר כספי הכופר הובילה לאיראן ועשויה להצביע על טיב המתקפה ועוד. הסקירה כוללת "דגלים אדומים" לשימוש הסקטור הפיננסי לזיהוי מקרי תשלום כופר. 15.02.2022, מקור – לינק.

- **אם הונאת סייבר (או תקיפת סייבר) בוצעה מהמחשב שלי, אך היא בוצעה ללא ידעתי, האם אני עדין צריך לשאת באחריות כלפי מי שנפגע מאותה הונאה\תקיפה שבוצעה מהמחשב שלי ?.**
אם המחשב האישי שברשותי ובאחריותי (או כל משאב מחשוב: שרת, התקן IOT, מדפסת, התקן מדיה ועוד) שימש באופן עיוור וללא ידיעתי, כ "מחשב זומבי" ממנו בוצע התקפת סייבר כנגד צד שלישי, **האם מוטלת עלי האחריות (מכל סוג שהיא) בגלל שההתקפה בוצע מהמחשב שלי ?** האם מוטלת עלי אשמה של התרשלות בגלל שלא הייתי מודע לפרצת אבטחה במערכת שלי שבגללה ניצלו את המחשב שלי לרעה על מנת לבצע התקפה כנגד צד ג'. האם מוטלת עלי אשמה בגין התרשלות או אחריות לו ידעתי שקיימת פרצה או בעיית אבטחה אבל לא דאגתי לתקן או לחסום את אותה פרצה ?

מקרה בוחן:

  - **2013 -** ניצול פרצה במקרר חכם דרכו נשלחו כמה מאות אלפי הודעות ספאם, הפרצה בוצע ללא ידיעת הבעלים של המקרר [78]

- **האם זה מוסרי לפרסם פרצת אבטחה, גם אם היא עדין לא תוקנה ?.**
אם גיליתי פרצת אבטחה חמורה במערכת מסוימת, דיווחתי לחברה שבמערכות המידע שלה קיימת פרצה חמורה, אך הם בגלל שיקולים כספיים \ תפעולים \ תדמיתיים בוחרים במודע לא לתקן את הפרצה ולהמשיך "לחיות איתה" מבלי לשנות כלום, האם זה מוסרי לפרסם את הפרצה כדי להזהיר את הציבור ואת הלקוחות של החברה בגין אותה פרצה שקיימת במערכת שלהם ולא תוקנה ?.

מקרה בוחן:

  - **2018 -** חוקרים ישראלים איתרו פרצת אבטחה חמורה במערכות מחשוב של תחנות דלק [79], החברה למרות שהיא קיבלה את כל הפרטים על הפרצה, במשך חצי שנה סירבה להתייחס, ולהגיב כיצד היא מתכננת לטפל בפגיעות שהתגלתה במערכות שלה. אחרי חצי שנה החוקרים החליטו לפרסם ברבים אודות קיומה של הפרצה (בלי לחשוף איך לממש אותה). החברה החליטה לתבוע את החוקרים שפרסמו אודות הפרצה. ככל הידוע החברה בחרה במודע שלא לתקן את הפרצה במאות אלפי תחנות הדלק שלה בעולם בגלל שמבחינתם משיקולים של עלות \ תועלת יותר משתלם מבחינה כספית להישאר עם הפרצה ולקחת סיכון מנוהל שאם הפרצה תמושש, אזי זה יהיה במקרים בודדים, ותוחלת הנזק לא תהיה משמעותית מבחינתם.

- **האם זה אתי מבחינה מקצועית או עסקית כאשר מישהו אחר חושף ברשות הרבים כי במערכות של החברה שלי קימות פרצות אבטחה ?.**
האם קיום של אתרים כגון Shodan [80] ("הגוגל של האתרים הפרוצים") המאפשרים חיפוש קל ומהיר אודות מערכות שסובלות פגיעויות אבטחת מידע הוא לגיטימי ?.

78 **פרצת אבטחה במקרר חכם של חברת LG נוצלה לרעה להפצה של מאות אלפי הודעות ספאם בתוך מספר ימים** | פורסם בתאריך 18.01.2014 ב NBC News לינק | פורסם ב BBC NEWS בתאריך 17.01.2014 | לינק.

79 **חוקרים ישראלים** (בהם , עידו נאור) **איתרו פרצת אבטחה בתחנות דלק**: "האקר יכול לגרום לפיצוץ וחיוב יתר" תקלה בתוכנת הניהול שמותקנת בתחנות דלק רבות בארץ ובעולם הופכת אותן פגיעות למתקפות סייבר: "הלקוח לא יכול לדעת אם התחנה אכן נפרצה", מעריב, **סתיו נמר**, 01.02.2018, מקור - לינק | מתוך IT-News, 07.02.2018 **מאיר עשת** מקור – לינק.

80 **מעבר לשירות שמספק Shodan קיימת רשימה ארוכה של אתרים שמספקים מידע זהה** כגון Wigle, LeaxIX, Censys, NATLAS, ZoomEye, Oneyphe, Hunteri, Ivre.Rocks, BinryEdge, Greaynoise , רשימה שפרסם ברשת לינקדאין **מרטין אברמוב** , 10.10.2022 , לינק.

- **האם זה אתי לפרסם ברבים כלים ושיטות לביצוע התקפות סייבר ?**.

האם קיום של פלטפורמות תקיפה כדוגמת Kali Linux [81] הכוללים מאות כלים לביצוע התקפות סייבר כדוגמת: התקפות Brute Force לפיצוח סיסמאות, התקפות על רשתות אלחוטיות ופיצוח סיסמאות שלהן, כלים להתקפות על תקשורת VOIP, כלים לביצוע פורנזיקה דיגיטלית וגילוי עקבות של שימוש קודם במחשב, כלים לביצוע Reverse Engineering לקוד תוכנה, כלי תוכנה לציתות לרשת, כלים להפעלת פגיעויות שונות – Metasploit, ועוד. נשאלת השאלה, **האם הנגשת כלי ההתקפה והפריצה הללו ברשות הרבים הן צרה צרורה או ברכה ?**, מצד אחד הכלים הללו הן בעיה כי בזכותם התקפות סייבר נגישות ומונגשות לכל מי שחפץ להפוך להיות "פושע סייבר", מאידך הן כלי מעולה והכרחי על מנת להכשיר מומחים אבטחת מידע אתיים (האקרים "כובע לבן") בתחום סייבר התקפי וסייבר הגנתי.

<u>לוגיקה בקבלת החלטות של בינה מלאכותית:</u>

- **האם ניתן להסתמך באופן עיוור על המלצות של מנגנוני AI/ML בקביעה ושינוי של מדיניות אבטחה במערכות הגנה שונות ?**.

אם מערכת ה-AI ממליצה על פעולה מסוימת אך ה-CISO של הארגון חושב שזאת קונפיגורציה או פעולה שלא רצוי לבצע אותה, מי צודק ? **הדעה של מי יותר נחשבת של ה-AI או של ה-CISO האנושי ? למי יש זכות הטלת וטו על החלטה שהתקבלה טרם יישומה ?.** איפה נמצאת נקודת האיזון בקבלת החלטה עצמאית המבוססת על שיקולים רציונליים אנושיים לעומת קבלת ההמלצה של ה-AI באופן עיוור אך ורק בגלל שאנחנו מתקשים לחלוק על "המלצת האפליקציה" שהיא נסמכת על מערכת שיקולים חכמה מבוססת "בינה מלאכותית". מקרים כאלה מוכרים לנו מחיי היום יום , כגון אפליקציית WAZE ששולחת אותנו בדרך לא הגיונית ולמרות זאת אנחנו נוסעים לפי ההנחיות של האפליקציה (למרות שזה נראה לנו טעות) או מקרה אחר בו מערכת AI בבנק לא מאשרת הלוואה ללקוח, למרות שהפקיד בבנק חושב שזאת טעות בשיקולים כך שההלוואה לא אושרה (האם אתם מכירים פקיד בנק שיעז לחלוק על ההמלצות האלגוריתם במערכת האישורים להלוואות ?). אלו הן רק שתי דוגמאות נפוצות לכך שאנחנו "האנושות" נכנענו כברירת מחדל להמלצות של ה-AI, איפה עוברת נקודת האיזון בהפעלת שיקול הדעת האנושי בקבלת החלטות מהותיות באופן עצמאי ?.

- **כיצד ניתן לבחון המלצות לפעולה של מערכות מבוססות בינה מלאכותית כך שהיא תהיה בעלת סיכוי נמוך לשגיאות ?**. האם יש דרך לבחון מערכת AI כזאת שאנחנו מאפשרים לה לקבוע מדיניות הגנת סייבר באופן אוטונומי להימנע מטעויות הסתברותיות : "**שגיאה מסוג I**" (תוצאה חיובית כוזבת - False positive) או "**שגיאה מסוג II**" (תוצאה שלילית כוזבת – False Negative) ?. האם ניתן למנוע טעויות כאלה ?, כיצד ניתן לחקור את הנזק התפעולי \ אבטחתי שנגרם בגלל טעויות אלו ?. אם בני אדם לא מעזים לחלוק על המלצות של מערכת מבוססת AI , האם אלגוריתם שעליו מתבססות ההחלטות במערכת AI יכול לבחון את עצמו כך שהוא יקבל אינדיקציה שהוא קיבל החלטה שגוייה ?.

- **כיצד ניתן לבחון שהמלצות של מערכות מבוססות בינה מלאכותית נקיות וללא כוללת הטיות ברמת הקוד ?** כיצד אפשר לבדוק שבמערכות AI שמקבלות החלטות אין הטיות מכוונות והטיות בלתי מודעות שהוגדרו על ידי צוות המפתחים בבסיס מערכת ההחלטות של האלגוריתם ?, איך מוודאים שאין בקבלת

---

81 **ברשת זמינים מאות רשימות והמלצות של כלי תקיפה אתיים כדוגמת קאלי לינוקס, כולל הנחיות מהיכן להוריד את כלי התקיפה, ובחלק מהמקרים הדרכה מסודרת איך להשתמש בהן באופן אפקטיבי** | מקור 1 – לינק | מקור 2 – לינק.

ההחלטות של ה-AI הטעיות בגלל ניסיון עבר שאינו רלוונטי לנתונים בהווה ? [82] [83]

מקרי בוחן וסיכום מספר וועדות רב-מגזריות שעוסקות בנושא והתקימו בישראל בשנים האחרונות:
(**<u>מקור גלובס</u>**) [84] [85] [86] טכנולוגיות בינה מלאכותית נמצאות בבסיס רוב המהפכות הטכנולוגיות שאנו נמצאים בעיצומן או בפתחן. הטכנולוגיה מתבססת על אלגוריתמים שמנתחים כמויות גדולות של מידע ונתונים, מזהים דפוסים חוזרים, מפיקים מהם תובנות, מתאימים את עצמם לשינויים ופועלים בהתאם. ואולם, הבעיה מתחילה כאשר כלי שמזהה דפוסים המסייעים בקבלת החלטות - מתבסס רק על המציאות הקיימת. **הסכנה היא שהתובנות שמבוססות על אותה מציאות וההמלצות לפעולה שמבוססות עליה, עלולות לשקף גם הטיות לא רצויות**. זאת בניגוד לבני אדם, שמבססים את החלטותיהם לא רק על ניסיון העבר והמטרות שהם רוצים להשיג, אלא גם על ערכים וסדרי עדיפויות. ... על מנת להדגים את הסיכונים שבשימוש לא מבוקר בבינה מלאכותית, תיאר הדוח עשרה מקרי מבחן המבוססים על מקרים אמיתיים שכבר פורסמו בעולם. מקרה אחד מתאר הולכת רגל שנהרגה על ידי מכונית אוטונומית של אובר בעת שחצתה כביש במקום חשוך. ככל הנראה הרכב זיהה כי עומד לפניו מכשול ויכול היה להימנע מלהתנגש בו, אך מכיוון שהמהנדסים הנמיכו את רגישות התוכנה לחסמים המכונית לא זיהתה את האישה כמכשול שמצריך ממנה לעצור, והאישה נהרגה. [87] במקרה נוסף התגלה שכלי לזיהוי פנים של אמזון שגה יותר כשהופעל על אנשים בעלי גוון עור כהה, מאשר בעת שהופעל על אנשים עם גוון עור בהיר.[88] מקרים אלו הוצגו בדוח לצד שמונה מקרים נוספים, שעסקו בין השאר באפליה בסינון מועמדים לעבודה; מניפולציות על תודעה האוכלוסייה האזרחית כמו למשל בעת קמפיין בחירות; חיזוי סיכון ממחלות; חיזוי מסוכנות אסירים ועוד.

- **איך בודקים רלוונטיות של סטטיסטיקה בתחום שמשתנה כל הזמן ?**.
בתחום הסייבר ההגנתי כאשר חוקרים את דרכי הפעולה של התוקפים, היות והאופן שבו מבוצעת התקפות הסייבר משתנות בקצר מהיר, וכמו שמקובל להגיד בתחום החדשנות ש "**הדבר הכי קבוע זה השינוי התמידי**", מכיוון שמערכות AI היא בסופו של דבר אלגוריתם שמתבסס על **ניתוח סטטיסטי של כמות גדולה של מידע מתויג** על פי תבנית מוכרת מסוימת ודפוסים חוזרים שנבחנו בעבר במספר רב של מופעים, אם ניקח בחשבון שעל פי הערכה **בכל יום "משוחררות" למרחב הסייבר מעל ל- 450,000 מוטציות חדשות** של התקפות סייבר מסוגים שונים [89] (חלקן הגדול הוא באמת "שדרוג" של התקפה ידועות, אולם חלק מהן הן התקפות חדשות לחלוטין שאין תבנית זהה להן במערכת החוקים של ה-ML), **נשאלת השאלה כיצד מונעים טעות של מערכת AI שמתבססת על למידת מכונה שהמידע המתויג בה אינו רלוונטי**

---

82 "**טעות במערכת AI לזיהוי פנים שלחה לכלא אדם חף מפשע**", פורסם ב-CNN, 29.04.21 "A false facial recognition match sent this innocent Black man to jail" | מקור -לינק

83 **על הקשר בין בינה מלאכותית, בינה אנושית, אתיקה ומוסר** | **אנחנו לא חייבים לדעת איך אלגוריתמים עובדים בדיוק, אבל יש לנו את הזכות לדעת שהם מפותחים ומופעלים בצורה אתית, שלא מפלה בין משתמשים על בסיס משתנים לא רלוונטיים** | לכאורה, אין קשר בין בינה מלאכותית לאתיקה או מוסר. זו מערכת מחשוב שמקבלת החלטות על בסיס מידע קר וקשה, בלי רגש או שיקולים אנושיים, רק היגיון. אבל מערכות טובות רק כמו האנשים שמפתחים אותן והמידע שמזין להן, ובכמה מקרים בעבר כבר התברר שגם מערכת בינה מלאכותית עלולה לסבול מהטיות ושגיאות שמובילות לתוצאות לא אתיות בעליל. | כלכליסט-טק | **עומר כביר** | 10.03.21 | לינק.

84 **מה עם זכויות האדם והתחרותיות במשק? כך תנסה ישראל להימנע מהסכנות של עתיד הבינה המלאכותית פגיעה באוכלוסיות חלשות, בזכויות אדם ובתחרותיות במשק: בינה מלאכותית יכולה להשפיע על חיינו לרעה** • כך מנסה ועדה בהשתתפות נציגי ממשלה, חוקרים וגופים עסקיים, למנוע זאת - מהטלת האחריות על גופי הממשלה השונים ועד הגדרה מתי יהיה מדובר ברשלנות | 10.12.2019, גלובס, **אורי ברקוביץ'**, מקור - לינק

85 **וועדת משנה של המיזם הלאומי למערכות נבונות בנושא אתיקה ורגולציה של בינה מלאכותית** | דין וחשבון | 2019 | ועדה בראשות **פרופ' קרין נהון**, מדענית מידע בבית הספר לממשל ובבית הספר לתקשורת במרכז הבינתחומי, ולשעבר נשיאת איגוד האינטרנט הישראלי. מקור – לינק.

86 **וועדת בינה מלאכותית ומדע הנתונים** | מרץ 2021 | פורום תל"ם ועדת בדיקה לבחינת הצורך בהתערבות ממשלתית לשם האצת התפתחות תחום הבינה המלאכותית ומדע הנתונים. מקור – לינק.

87 **"אובר: רכב אוטונומי הרג הולכת רגל (איליין הרצברג) , הניסויים נעצרו",** כלכליסט, עומר כביר 19.03.2018 מקור – לינק. | "תיעוד: הרגע בו מכונית אוטונומית של אובר דרסה הולכת רגל" , מערכת וואלה, 22.03.2018 מקור – לינק.

88 **מחקר: טכנולוגיית זיהוי פנים עובדת מצוין - עבור גברים לבנים התוכנות מזהות תצלומים של גברים לבנים ב-99% מהמקרים, אך שיעור הטעות גדל ככל שצבע העור של המצולם כהה יותר.** מרצה מאוניברסיטת יוטה: הגיע הזמן להתייחס לכשלים של הטכנולוגיות הללו. פורסם בעיתון הארץ, מוסף מדע בתאריך 11 פברואר 2018 , מקור 1 (עברית) – לינק | מקור 2: סטיב לור, ניו יורק טיימס, 11 פברואר 2018 (אנגלית) - לינק

89 **מידע לפי גוף המחקר הבלתי תלוי AV-TEST** – מקור – לינק.

להתקפות החדשות ? האם ניתן לבצע "הֲדִירוֹת" (חֲזָרתִיוֹת – כמו שמתבקש בפילוסופיה של המדע כאשר רוצים לבחון אופן ביצוע של ניסוי מדעי) של מסקנה **מהי התקפת סייבר חדשה כאשר התקפות הסייבר כל הזמן משנות את פניהם ?.**

<u>טכנולוגיה:</u>

- **לאן מובילה אותנו הטכנולוגיות החדשות במרחב הסייבר ?** כיצד אפשר לבחון אם טכנולוגיה בטוחה לשימוש בטווח קצר \ בטווח ארוך ? איך בוחנים באופן אובייקטיבי השלכות של טכנולוגיה חדשה ?.

- **כיצד אפשר להגביל שימוש בטכנולוגיה מסוימת כך שהיא לא תשפיע לרעה על האנושות או תנוצל על מנת להשיג מטרות לא נורמטיביות ?**

אם טכנולוגיה מסוימת גורמת או עלולה לגרום לנזק לאחרים, האם אפשר להגביל את השימוש בה ?. לדוגמא:

- האם באופן אובייקטיבי נבחנה ההשפעה של הקמת אלפי Data Center על המערכת האקולוגית בכדור הארץ ?
- האם ניתן למנוע שימוש של קבוצות תקיפה בטכנולוגיות של AI as a Services על מנת לטייב את הונאות הסייבר שלהם ?.
- האם ניתן להגביל שימוש של קבוצות תקיפה במערכות ענן ציבורי כדי לממש בפועל התקפות סייבר מסוג DDOS ?.
- האם האפשרות לשימוש בטכנולוגיות מסוימת כגון Deep Feck צריך להיות זמינה ונגישה לכולם וללא בקרה ?, שכן אפשר להשתמש בטכנולוגיה הזאת לפעילות חיובית בתחום ההוראה או תעשיית הסרטים ומאידך לפעילות שלילית משימוש בהונאות כופר, סחיטה (כמו פורנו-נקמה) ועד ליצירת סכסוך גאופוליטי שעלול לגרום למלחמה עולמית.

היות וכמעט כל טכנולוגיה אפשר לנצל לטובה או לרעה, והיות ולטכנולוגיה אין רצון עצמאי משל עצמה, האם אפשר לסמוך על שיקולים אנושיים באופן בו ישתמשו בטכנולוגיה ?. [90]

- **מי "המבוגר האחראי" כדי לנהל את רשת האינטרנט ?.**

מי צריך לשלוט ולפקח על המתרחש במרחב הסייבר ?, לפי איזה אסכולה צריך להחליט לגבי הפיקוח וקבלת ההחלטות מה לאפשר ומה למנוע במרחב הסייבר ?, **האסכולה הדמוקרטית** או **האסכולה הטכנוקרטית** [91] האם בכלל קיימת זכות לגוף כלשהו להגביל או לקבוע חוקים ותקנות לגבי השימוש במרחב הסייבר ?.

---

90 "כאשר דנים בפילוסופיה של הטכנולוגיה היום (2011) , נזהרים מלומר שאנו יודעים מה האדם רוצה, או שכל אדם יודע מה הוא עצמו רוצה. אנחנו יודעים היום, שאדם מגלה אם הוא רוצה או לא רוצה דברים רבים רק כאשר הם מופיעים בשוק. זאת אומרת, הטכנולוגיה שינתה את הטעם הצרכנים. אנו מוכנים היום להסתכן ולנסות מכונות חדשות כדי לבדוק אם אנו נהנים מן השימוש בהן או לא. **<u>כלומר הטכנולוגיה פיתחה צרכים ורצונות ושינתה את אופי האדם באופן קיצוני</u>**. האם לטוב או לרע? , זו שאלה שקשה לענות עליה. כפי שאמרנו ונחזור ונאמר , **<u>יש טענה אחת שאין חולקין עליה והיא שמכשיר כשלעצמו אינו טוב ואינו רע</u>**, כגון הנשק שבידי השודד שהוא רע, ואותו הנשק שבידי השוטר שהוא טוב. על-כן הנסיבות שעושות מכשיר לטוב או רע. אין הוא עצמו טוב או רע. **<u>על-כן הדעה המסורתית היא שטכנולוגיה אינה טובה או רעה , אלא תלויה באדם שמשתמש בה לטוב או לרע.</u>** היום אנחנו יודעים שאין זה כה פשוט. **<u>הנסיבות והאדם היוצר את המכשיר מכוונים אותנו פעמים רבות הן לטוב והן לרע.</u>** על כן יש סיכון בניסויים טכנולוגים. מקור: **הפילוסופיה של הטכנולוגיה – פרופ' יוסף אגסי** , הוצ' מודן 2011 – עמוד 53.

91 "שתי אסכולות עיקריות קיימות היום בפילוסופיה בכלל, ובפילוסופיה של הטכנולוגיה בפרט. **האחת היא הדמוקרטית**, האומרת שלכל אזרח זכות שווה להביע את העדפותיו ואת ציפיותיו מן המכונה החדשה, ומאחר שהיא תיבנה לפי המחקר שממומן בכספי משלם המיסים, הרי חובה להתחשב בדעותיו. **מן הצד השני הטכנוקרט**, שאין לאיש הפשוט מושג במה מדובר, אפילו בעניין הנוגע לו, לגופו ממש. .... **אלא אפוא שתי התיאוריות הקיימות**: האחת, הדמוקרטית, הטוענת כי צריך להתחשב בהערכותיו ובהעדפותיו של האזרח הפשוט גם אם אינו צודק, כי זו הדרך לחנכו. והשנייה הטוענת כי עד שתחנך את האזרח ייהרס העולם, אלא אם ישלוט בו הטכנאי, הרופא, המהנדס, הפיזיקאי , לשון אחר – בעל הידע" מקור: **הפילוסופיה של הטכנולוגיה – פרופ' יוסף אגסי** , הוצ' מודן 2011 – עמודים 12-11

- **כיצד בונים תהליך של שימור ידע טכנולוגי לאורך שנים בעולם בו טכנולוגיות מתחלפות בקצב מהיר** ?. כיצד ניתן לשמר ידע טכנולוגי המאפשר שימוש ותפעול טכנולוגיות ישנות, כאלה שעדין נמצאות פעילות במגזרים מסוימים (כדוגמה מגזר פיננסי, משרדי ממשלה , המגזר המוניציפאלי) **על מנת לטפל בבעיות ופרצות אבטחת מידע חדשות שמתגלות במערכות "ישנות"** ועדין המערכות הן חלק מהותי ובלתי נפרד בסביבת הייצור של החברה ?. לדוגמא כיצד ניתן לשמר ידע על מנת לתקן פרצות אבטחה חדשות שנתגלו במערכות AS/400 או Digital VAX, בנוסף כיצד ניתן לתקן פרצות אבטחה במערכות שנכתבו בשפות תכנות ישנות מראשית שנות ה-90 כדוגמת קובול או שפת C כאשר אין אנשי מקצוע מומחים זמינים בשוק העבודה שמחזיקים בידע לעשות זאת ?.

- **כיצד מנגישים שימוש בטכנולוגיות חדשות לכלל האוכלוסייה ?** – כיצד דואגים בחברה דמוקרטית למתן הזדמנות שווה לכלל האוכלוסייה, כך שכלל האוכלוסייה תקבל חשיפה והזדמנות שווה לעשות שימוש בטכנולוגיות חדשות ?. כיצד מקדמים אוריינות דיגיטלית בקהילות ובמגזרים "חלשים" מבחינה טכנולוגית או מבחינה סוציואקונומית כך שגם להם יהיו האמצעים לרכוש ולהשתמש בטכנולוגיות החדשות ?. כיצד מקטינים את הפער ההולך ומתעצם בחברה האנושית בין אלו שטכנולוגיה היא חלק מהותי מחייהם לבין אלו שנשארו מחוץ לתמונה \ מחוץ לחברה ?

- **כיצד דואגים להזדמנות שווה לכלל אוכלוסיית העולם להשתמש בטכנולוגיה לרווחתם?** כאשר לפי הערכות רק 52% מאוכלוסיית העולם מחוברת נכון לשנת 2022 לרשת האינטרנט [92], איך דואגים להגיע לאוריינות דיגיטלית של שאר אוכלוסיית העולם כדי שגם היא תוכל להשתמש לטובה בטכנולוגיות החדשות שמציע מרחב הסייבר ?, אם נצא מנקודת מוצא כי טכנולוגיה פותחה כי לשרת לטובה את כלל צורכי האנושות, איך דואגים שכלל האנושות תקבל הזדמנות שווה להשתמש בטכנולוגיה על מנת לשפר את מצבה ותנאי הקיום שלה ?.

- **כיצד ניתן לבחון יעילות של טכנולוגיה בכלל ובתחום אבטחת הסייבר בפרט?** איך בוחנים איזה טכנולוגיה טובה יותר ?, איך בוחנים אמינות ותקפות של המלצות הניתנות על גופים מקצועיים הממליצים על טכנולוגיות של יצרן מסוים על פני יצרן אחר?. לדוגמא המלצות של מי נכונות יותר של: Gartner , IDC , Forrester , LABS-NSS או של MITRE ?, על פי איזה קריטריונים אני כלקוח (כצרכן של המידע המפרסם) יכול לשפוט חוות דעת מקצועיות כאשר מראש אין לי את כל הידע המקצועי להכריע בנושא ?, האם עלי לקבל את ההמלצות שלהם "כתורה מסיני" שאין לחלוק עליה ? [93] . אם המשפטים השנויים במחלוקת והיו מקובלים כפרדיגמה של מנהלי מערכות מידע רבים בתחילת המאה ה-21 "מעולם לא פיטרו מנהל IT בגלל שהוא רכש מערכת אכסון של IBM" (ויש לזה גם וְריאַציוֹת שונות מעולם התוכן של תקשורת נתונים או הגנת סייבר) הם פרדיגמות ותפיסות שאבד עליהן הקלח ?. מהם הקריטריונים החשובים בעת בחינה והשוואה בין פתרונות \ יצרנים שונים ?. **האם <u>אי היכולת</u> להגיע לקריטריונים <u>המקובלים על כל הצדדים הנבחנים</u> הופכת את ההשוואה מראש ללא רלוונטית ?** האם מראש אנחנו בסיטואציה שבה לא ניתן לקבוע בה הכרעה חד משמעית בדומה להשוואה מעולם הספורט כך שלא ניתן להגיע **להכרעה רציונלית** מי שחקן כדורסל יותר טוב לברון ג'יימס או מייקל ג'ורדן [94], כך גם לא יכולה להיות הכרעה רציונלית גם לגבי בחינה של מערכות טכנולוגיות ?

---

92 **מעל 5.5 מיליארד בני אדם מחוברים לרשת האינטרנט** נכון ליום כתיבת המאמר | מקור – לינק.

93 מאמר בשם Gartner, Forrester, IDC & All The Consultants Out There Should Know How PowerPoint Distorts Reality & Undermines Technology Problem-Solving פורסם בפורבס נכתב על ידי **פרופ' סטיב אנדריול** (Steve Andriole) בתאריך 19 אוק' 2020 , מקור – לינק.

94 דוגמאות לדיונים \ וויכוחים רבים (ואין סופיים) ברשת אודות **מי הכדורסלן הטוב ביותר בכל הזמנים ?** באף אחד מהן אין הסכמה על הפרמטרים בהם מבצעים את ההשוואה, מקור 1 - לינק | מקור 2 - לינק

- **כיצד ניתן לבחון את הטענה כי ענף הסייבר נגוע בתפיסות ופרדיגמות דֶּטֶרמִינִיסטִיוֹת [95] ?**.
כיצד ניתן לבחון את האופן שבו אנחנו מנהלים כיום אבטחת מידע ביחס למה שהיה מקובל כמה שנים קודם לכן ?, והאם התפיסות הישנות רלוונטיות לאופן שבו מערכי המחשוב, הרשתות, השרתים ומשתמשי הקצה פועלים כיום?. האם תפיסות ליישום אבטחה מידע ארגונית, שימוש בטכנולוגיות אבטחה מסוימות, הגדרת נהלי עבודה באופן מסוים, הגדרת מדיניות אבטחה, הגדרת רגולציה בתחום, **הן תולדה של פעולות, החלטות, מחשבות, תפיסות שהושרשו מאירועי העבר וממה שהיה מקובל בעבר.**
האם בענף שמשתנה כל הזמן, כך שאנחנו חייבים לבחון ולתקף מחדש את הידע שלנו, שיטות העבודה, מדיניות האבטחה נגועות בגישה דטרמיניסטית וזה פועל לרעתנו ?, **האם נמשיך לפעול כמו שעשו קודמנו בתפקיד כי ככה לימדו אותנו ?**, כי ככה מקובל בענף? כי זה מה שנלמד בהכשרה המקצועית ?, כי אני חסר הידע מקבל "כתורה מסיני" מה שמלמדים אותי בכיתה מבלי להפעיל שיקול דעת עצמאי, מבלי להתנסות בלמידה מתוך "ניסוי ותעיה", מבלי לרכוש ידע בלמידה מפי בעלי דעות מקצועיות שונות (דיון פתוח שבו שומעים יותר מדעה אחת), ובחינה דעתו של מי מהם אני מקבל ומאמץ מבחינה רציונאלית לאחר שקיבלתי הסברים ונימוקים מפורטים למה הדרך שמציעים לי, היא הדרך היותר טובה נכון לרגע זה ?.

- **האם אנחנו משועבדים לטכנולוגיה? ומה גישתנו לטכנולוגיה גישה של אדונים או של עבדים ?**:
האם הטכנולוגיה שולטת בנו ולא אנו שולטים בה (כפי שטוען הפילוסוף **הנס יונאס**), האם החברה האנושית וההתנהגות שלה מעוצבת על השימוש שהיא עושה בטכנולוגיה מסוימת (כפי שטוען הסוציולוג **מרשל מקלוהן** שהיה בין הוגי המושג " **דֶּטֶרמִינִיזְם טכנולוגי**" [96]) **בעוד שהטכנולוגיה היא זאת שמשפיעה על החברה , מאידך החברה אינה משפיעה על ההתפתחות הטכנולוגית עצמה.**
כיצד התלות שלנו בטכנולוגיה מסוימת פוגעת בכישורים האנושיים או המקצועיים שלנו ?, כיצד היא משפיעה על דרכי העבודה שלנו ?, דרכי החשיבה שלנו ?, האם היא פוגעת ביצירתיות שלנו ?.
האם מובילי דעה כגון **ג'רון לנייר** שהיה יזם ומפתח חומרה ותוכנה מהבולטים בעולם בתחום האינטרנט והמציאות המדומה בתחילת שנות ה-90, ועד לפני 10 שנים (כאשר הוא עוד היה פעיל חברתי) היה לאחד הקולות הטכנולוגים הבולטים בעולם שאמר "**טעינו – איבדנו כיוון**" [97] רצינו לעשות טוב אבל למעשה הטכנולוגיה והשימוש שאנחנו עושים בה כיום פועלת לרעת האנושות, **האם אלו דעות שעלינו להקשיב ולבחון אותן יותר ברצינות, מאשר להתעלם מהם ולקרוא למי שמשמיע אותם "הזוי" ולא מחובר למציאות ?.**

- **כיצד אפשר לקדם המצאה וחשיבה על טכנולוגיות חדשות בתחום אבטחת הסייבר ?.**
האם קימות שיטות ודרכי עבודה, שיטות מחקר מתחומים של הפילוסופיה של המדע, כלים ושיטות מתחום חדשנות לפיתוח מוצרים או פיתוח שירותים \ שווקים חדשים שיכולים לסייע לנו לחשוב על דרכי התמודדות, פיתוח שיטות ומתודולוגיות עבודה חדשות, פיתוח טכנולוגיות חדשות או דרכים לשימוש חדש ואחר ממה שהיה מקובל עד היום בטכנולוגיות קימות כדי להתמודד עם האתגרים החדשים בענף הסייבר ?.
איך אפשר לקדם חדשנות \ רעיונאות (Ideation) \ יצירתיות \ חשיבה נונקונפורמיסטית, בענף הסייבר שלמרות התדמית ההייטקיסטית שלו, האנשים העובדים בענף ברובם הם לא ממש Open Mind לצורות חשיבה חדשות שלא מתוך העולם המקובע של מדעי המחשב ?.

---

95 **דֶּטֶרמִינִיזְם** או בעברית כְּרִחָנוּת , היא השקפה פילוסופית לפיה כל מאורע בעולם, פעולות, החלטות או מחשבות אנושיות נקבעים באופן בלעדי על ידי אירועים קודמים. דטרמיניזם עולה בהקשרים רבים, ביניהם המדע ,הדת ופילוסופיה של המוסר. מקור - לינק.

96 **דֶּטֶרמִינִיזְם טכנולוגי** הוא זרם במדעי החברה, הטוען כי התפתחות הטכנולוגיה מעצבת ומובילה את התפתחות החברה ,ערכיה, כישורי האנשים החיים בחברה וצורת המחשבה שלהם. הטכנולוגיה היא שמשפיעה על החברה, ויש לה התפתחות עצמאית שאיננה מושפעת מגורמים חברתיים. מייסד הזרם הוא חוקר התקשורת **מרשל מקלוהן** ,שפיתח את הזרם בהתייחס לעולם התקשורת. הוא, יחד עם חוקר התקשורת **הרולד אדמס איניס ,**קבעו כי הטכנולוגיה היא שמאפשרת לאמצעי תקשורת חדשים להתפתח. הם מתפתחים, ומשפיעים על כלל החברה. דוגמאות לטכנולוגיות ששינו את החברה ואת האופן בה היא חושבת ופועלת : דפוס, טלוויזיה , רשת האינטרנט, טלפון נייד ועוד. מקור: לינק.

97 "**גן העדן של האינטרנט לא עובד עבור הרבה מאוד אנשים**" אחרי 30 שנה שבהן סייע להכניס את האנושות לעידן טכנולוגי חדש, **ג'רון לנייר** (Jaron Lanier) מודה: טעיתי, איבדנו כיוון. בראיון בלעדי למוסף כלכליסט מסביר אחד ממאה האנשים המשפיעים בעולם למה האינטרנט הורג את הכלכלה, גוגל מחסלת את מעמד הביניים, פייסבוק מחבלת בסיכוי להיות אנושי וויקיפדיה מכסחת את היצירתיות. כלכליסט | 10.03.2011 | **אורי פסובסקי** | מקור – לינק.

- **האם בענף הסייבר אפשר לצמצם את הלולאה האין סופית של "פרדוקס החדשנות הטכנולוגית" ?**
פרדוקס החדשנות הטכנולוגית הוא למעשה לולאה שחוזרת על עצמה:
האדם פונה אל הטכנולוגיה כדי למלא מטלות על מה שאינו הוא ← השימוש בטכנולוגיה החדשה מייצר בעיות חדשות לאנושות שלא היו קימות קודם לכן ← האדם פונה אל הטכנולוגיה כדי לפתור את הבעיות החדשות שנוצרו ← ובחזרה לנקודת ההתחלה.

מקרה בוחן: כבר היום אנחנו רואים שימוש בטכנולוגיות חדשות בענף אבטחת הסייבר שמייצרות בעצמן בעיות חדשות, שכדי לפתור אותן צריך לפתח טכנולוגיות חדשות, שגם הן מייצרות בעיות חדשות.
לדוגמא: **המעבר לציוד IIoT [98] בסביבות תעשייה**, בקרים בעלי חיבור תקשורת נתונים במקום בקרים מהדור הישן שלא היו בעלי יכולת זו, קידם משמעותית את היכולת לשיפור והתייעלות תפעולית. היכולת לבצע פרויקט של טרנספורמציה דיגיטלית מקצה לקצה, החל מפס הייצור במפעל ועד ליעד הסופי שבו המוצר צריך להיות מסופק, היכולת הטכנולוגית החדשה שינתה לחלוטין את האופן שבו עלינו לתכנן ולבנות מחדש רשתות תקשורת במפעלים ובסביבות ייצור. חיבור סביבת הייצור התעשייתית, סביבת ה-OT [99] לסביבת ה-IT [100], רשת מערכות המידע של החברה, דרש לפתוח גישה מרשתות "סביבת היצור" הסגורות, רשתות שהיו עד היום מנותקת מרשת האינטרנט, גישה אל רשתות סביבת ה-IT (מערכות CRM או ERP מקומיות) ובחלק גדול מהמקרים גישה ישירה לרשת האינטרנט \ לענן ציבורי כדי לנצל את היכולות המתקדמות לאיסוף מידע בנפחים גדולים (Big Data) וניתוח ה-DATA לתובנות עסקיות בעזרת אלגוריתמים חכמים ומודלים סטטיסטים מתקדמים (AI/ML). בחלק גדול מהמקרים, בעיקר בגלל שיקולים של: עלות, זמינות המערכות, נגישות מכל מקום, שרידות המערכות, שיקולי TTM [101] וזמן פיתוח מהיר, מערכות בסביבת הענן הציבורי הן המקום בו נאסף המידע שזורם הישר מתוך המערכות השונות של סביבת הייצור התעשייתית. **עצם ההכרח העסקי שמחייב אותנו לאחד ולמזג בין רשתות ה-OT לרשתות ה-IT בשילוב של טכנולוגיות חדשות הוא פתח לאתגריים מקצועיים חדשים**, כך שה-CISO ומנהלי תפעול במפעלים ובתעשיות השונות בכל העולם, רק מתחילים ללמוד איך להתמודד עם אתגרים טכנולוגים ותפעוליים אלו.

- **<u>האם ידע זה כוח אך ורק אם חולקים אותו עם אחרים</u> או <u>האם ידע זה כוח אך ורק אם אני שומר אותו לעצמי ? :</u>**
האם כיום כאשר אבטחת סייבר הוא אחד משישה ממדי לחימה (יבשה, ים, אוויר, חלל, ל"א, סייבר) המהווה יתרון צבאי בולט לכל צבא בעולם, האם שיתוף ידע טכנולוגי בתחום הסייבר ההגנתי או ההתקפי עם מדינות אחרות הוא לטובתנו ושומר על האינטרסים של מדינת ישראל או שהוא מסכן אותנו ופוגע בעליונות שלנו מבחינה עליונות טכנולוגית צבאית ? [102], האם ניתן לקבוע מדדים מה הידע שניתן לשתף ?, עם מי מותר לשתף ידע ?, האם ניתן לקבוע מדדים מתי ידע אסטרטגי בתחום הסייבר מאבד את תוקפו או את הרלוונטיות שלו ?, האם שיתוף הידע שמערך הסייבר הלאומי עושה עם גופים מקבילים באירופה ובארה"ב [103] מחזק את האינטרסים הביטחוניים של מדינת ישראל, או שעלול לפגוע באינטרסים הביטחוניים, היות וברגע שאתה משתף מידע עם אחרים, אין לך כבר שליטה מי, איך ומתי זה הוא יכול להשתמש בידע הזה גם כנגדך.
בנוסף נשאלת השאלה, גם היא באופן ההיפותטי לחלוטין, **אם כן יהיה שיתוף מידע כלל עולמי בתחום**

98 **IIoT** = Industrial Internet of Things.
99 **OT** = Operational Technology – טכנולוגיה תפעולית.
100 **IT** = Information Technology – מערכות מידע.
101 **TTM** = Time to Market
102 הרמטכ"ל מודה: "ערכנו השנה מבצעי סייבר התקפיים רבים" בהתייחסות ראשונה לסייבר ההתקפי, **ראל אביב כוכבי כינה את ממד הסייבר "מרחב הלחימה המשמעותי ביותר שהשתנה השנה"** | מתוך אנשים ומחשבים | יוסי הטוני | 10.12.2020| מקור – לינק.
103 **מערך הסייבר הלאומי חתם על הסכמי שיתוף פעולה עם המחלקה לביטחון המולדת בארה"ב** במסגרת ההסכם יחזק ויורחב שיתוף פעולה בין המדינות במטרה לחזק את הגנת הסייבר של המשק והתשתיות הקריטיות, להיאבק באיומים משותפים כגון מתקפות כופרה | מתוך Israel Defence | עמי רוחקס דומבה | 02.03.22 | מקור – לינק.

הסייבר בצידוק ומתוך כוונה ששיתוף פעולה כזה יכול לחסל את פשיעת הסייבר על רקע כלכלי (שגורמת נזקים לכולם, אבל יש גם מדינות בעולם שמרוויחות מזה) **האם נוֹרְמָלִיזַצְיָה כזאת תאפשר מאזן כוחות כך שזה גם יסיים את מלחמות הסייבר על רקע-גיאו פוליטית בין מדינות שונות בעולם?**

מקרה בוחן:

בעבר (עד לפני 12-10 שנים) בין יצרני פתרונות להגנת סייבר התקיימו "**מלחמות יוקרה**" על מנת להוכיח למי יש עליונות טכנולוגית, במסגרת אותן "מלחמות" נפוצו האשמות כלפי חברות מסוימות בתחום יצרני פתרונות "האנטי וירוס" לתחנות הקצה והשרתים, כשאר מרבית ההאשמות כוונו בעיקר אל חברת Kaspersky הרוסית, בכך שהיא "משחררת" ומפיצה במרחב הסייבר וירוסים ורוגלות חדשות שהיא בעצמה פיתחה, זאת על מנת לקבל יתרון טכנולוגי תחרותי ותדמיתי, היות וגוף המחקר שלהם הוא המוביל והראשון בעולם לפרסם שהוא גילה, זיהה ויצר חתימות על מנת לחסום רוגלות חדשות לפני כל יצרני האנטי וירוס האחרים בשוק. **האשמות כאלה כבר לא נשמעות יותר בענף אבטחת הסייבר**, **ראשית** בגלל כמות הרוגלות שנפוצות במרחב הסייבר מידי יום (זה כבר חיסל את הדירוגים המטופשים והמיותרים של "מי מקום ראשון", "מי מקום שני" במשחק "סכום אפס" שהתנהל במשך שנים), **שנית** היות ובמהלך העשור האחרון, הלכו וגדלו מספר שיתופי פעולה הגלובליים והגלויים בין יצרני פתרונות הגנת הסייבר שעד אתמול נחשבו "**מתחרים עוינים**" והיום הם "קולגות" (או "**מתחרים ראויים**" [104]) במלחמה המשותפת שלהם כנגד פשיעת הסייבר על רקע כלכלי, פשיעה ההולכת ומתעצמת מיום ליום.

שניים מהארגונים האלה הם:

- **CTA:** מאז שנת 2014 פועל גוף עצמאי משותף (ללא מטרות רווח) הקרוי "**Cyber Threat Alliance**" [105] (או בקיצור CTA) בהתחלה הוקם כהתארגנות זמנית ומאוחר יותר ב 2017 כהתארגנות קבועה על ידי יצרני פתרונות הגנת הסייבר הגדולים בעולם (Fortinet, McAfee , Palo Alto Network , Symantec) מטרתו להוות פלטפורמה לשיתוף ידע ומודיעין סייבר בזמן אמת, כדי לסכל מתקפות סייבר גלובליות, ולאפשר שיתוף פעולה טכנולוגי, Eco-System בין פתרונות הגנת סייבר שונים. מאוחר יותר הצטרפו עוד כמה עשרות של יצרני פתרונות הגנת סייבר "לברית איומי הסייבר" שמונה כיום 33 יצרנים שונים.
- **GCA:** מאז שנת 2015 פועל גוף גלובלי (ללא מטרות רווח) בשם "**Global Cyber Alliance**" [106] "ברית הסייבר העולמית" (או בקיצור GCA) בגוף זה חברות גופי מחקר בענף הסייבר \ גופי תקינה בענף הסייבר \ יצרנים בענף הסייבר \ גופים כלכליים, אשר מטרתם היא שיתוף ידע טכנולוגי על מנת להילחם ולהירתם למאמץ קולקטיבי למלחמה בפשיעת סייבר. בגוף זה כיום חברות עשרות חברות: גופי בטחון, חברות מסחריות, אקדמיה וגופי מחקר, גופים פיננסים, יצרנים של תוכנה \ חומרה \ פתרונות סייבר בקשת רחבה.

הגישה המקובלת כיום בין החברות הגדולות המפתחות מערכות בענף אבטחת הסייבר, היא גישה האומרת כי לתועלת של כל הנוגעים בדבר (היצרנים עצמם, הלקוחות שלהם, קהילת בעלי האינטרסים בענף הסייבר) עדיף לכולם לשתף ידע לגבי פרצות והתקפות סייבר חדשות, אחרת כולם "יפסידו" במלחמה הן לתוקפי הסייבר הפועלים ממניעים כלכליים והן לטרור סייבר הפועל ממניעים גאו-פוליטיים.

---

104 "**מתחרים ראויים**" (worthy rival) הוא מונח שטבע מוביל הדעה בנושא פיתוח מנהיגות עסקית, **סימון סיניק** (Simon Sinek), היכולות לשתף פעולה עם "מתחרים ראויים" מקדמת ותורמת באופן הדדי של הנוגעים בדבר, לשיפור והצלחה משותפת של כל תחום העיסוק המשותף, מעבר לרווח האישי של כל צד, גם קהל הצרכנים \ המשתמשים נהנים מפירות ההצלחה של שיתוף הפעולה, וזוכים למוצר או שירות משופר. מקור - לינק

105 **The Cyber Threat Alliance (CTA)** is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. | מקור - לינק

106 **The Global Cyber Alliance (GCA)** is a non-profit organization dedicated to making the Internet a safer place by reducing cyber risk. We build programs, tools, and partnerships to sustain a trustworthy Internet to enable social and economic progress for all. GCA is a 501(c)(3) in the U.S. and a non-profit in the U.K. and Belgium. | מקור - לינק

<u>שאלות ואתגרים בתחום הפסיכולוגיה \ סוציולוגיה:</u>

- **מה ההשפעות הפסיכולוגיות של "מרחב הסייבר" עלינו ?**.

כיצד אנחנו רואים את עצמנו כאִינְדִיבִידוּאֶל כחלק ממרחב הסייבר ובאוקיינוס המידע האין סופי ?, האם ניתן להעריך את ההשפעה לרעה או לטובה על הדור הצעיר (דור ה-Z) שהטכנולוגיות במרחב הסייבר זמינות עבורו מגיל ינקות, והטכנולוגיה היא חלק בלתי נפרד מחייו \ חלק בלתי נפרד מגופו ?. האם התלות שלנו בטכנולוגיה היא כל כך גדולה כך שאם היא לא זמינה עבורנו אפילו לפרק של כמה שעות אנחנו מרגישים אבודים בלעדיה ?.

מקרה בוחן:

2021 - תקלה מערכתית שהשביתה את זמינות האפליקציות והשירותים של קבוצת מטא (פייסבוק, אינסגטרם ווצאפ) למשך כמה שעות, גרמה לאפקט פסיכולוגי הכולל תחושות קיצוניות של שעמום, חוסר סבלנות, כעס ובדידות, בקרב צעירים ישראלים [107].

- **מהן ההשפעות הסוציולוגיות של מרחב הסייבר על החברה בכללותה** ?.

האם השימוש בטכנולוגיה קובעת את סדר יומנו, קובעת את האופן שבו אנחנו מנצלים את הזמן שלנו ?. עד כמה מרחב הסייבר בה פועלים הרשתות החברתיות ופלטפורמות לשיתוף תכנים, מגדיל את הקיטוב בין קהילות \ מגזרים \ דתות \ לאומים שונים בחברה האנושית ? או מאידך מרחב הסייבר מגדיר מחדש את האופן שבו בני אדם מתקשרים, מתקשרים ומתחברים אחד עם השני, כך שהוא מאפשר יצירה של "**קהילות מדומיינות**" [108] חדשות, שלא היו יכולות להיווצר אלא בזכות מרחק הסייבר ?.

- **האם השימוש והתלות בטכנולוגיה גורמת לנו להתנוונות של כישורים אנושיים ("כישורים רכים) ?**

האם השימוש בטכנולוגיה פוגעת בהתפתחות של יכולות אישיות ויכולות פיזיות אצל בני האדם ?. האם השימוש בטכנולוגיה של אפליקציות "מסרים מיידים" כדוגמת ווצאפ או SMS פוגעת ביכולת שלנו לאינטרקציה והיכולת ליצור שיח אישי פנים מול פנים מול אדם אחר ?. האם בגלל תלות בטכנולוגיה אנחנו מאבדים יכולות כגון היכולת לכתוב בכתב יד, לנווט באופן עצמאי גם כאשר מדובר ביעד שנתיב ההגעה אליו מוכר לנו היטב, היכולת לקבל החלטות באופן עצמאי ללא התערבות מערכות מבוססות AI, היכולת לזכור בע"פ מספרי טלפון חשובים , ועוד.

- **"המלחמה בפייק ניוז" - הפצת מידע כוזב במרחב הסייבר ומהן ההשפעות החברתיות של שימוש לרעה במידע ?**:

האם ניתן למנוע \ לצמצם \ לאסור על פי חוק הפצה של "מידע מַטְעֶה" (דיס-אינפורמציה) [109] , "מידע מוטעה" (מיס-אינפורמציה) [110], "החסרת מידע" (השמטת מידע סלקטיבית ובאופן מכוון) , "הַסְתָּרַת מידע" (מניעת פרסום של מידע מסוים), שימוש בפלטפורמות חברתיות ובמדיה דיגיטלית שלא נמצאת תחת פיקח, לצורך הפצת שמועות, ספקולציות, תיאוריות קונספירציה וחדשות כזב בפני הציבור הרחב ?.

כיצד מידע מסולף שאינו תואם את המציאות ומפורסם באמצעי המדיה השונים או ברשתות החברתיות, משפיע על אופי החברה ?. האם ניתן למדוד באיזה אופנים ובאיזה רמת עוצמה של אימפקט חברתי "כזב- מידע"

---

107 בתחילת חודש אוקטובר 2021 אירעה **תקלה עולמית בשירותי פייסבוק, אינסגטרם ווצאפ**, בכל העולם היתה השבתה של השירות לכמה שעות, בסקר שערכה בזק בשם "**מנהלים את החיים הדיגיטליים שלנו**" וכלל מדגם מייצג של 3,300 ישראלים, דווח כי בעת התקלה נוער \ מבוגרים מעל גיל 18, חשו בעוצמה תחושות קיצוניות של שעמום, חוסר סבלנות, כעס ובדידות | מקור: לינק.

108 "**קהילות מדומיינות**" - קהילות מדומיינות (באנגלית: Imagined Communities) הוא מושג שטבע **בנדיקט אנדרסון** בספרו בשם זה שיצא לאור ב-1983 ובמהדורה מורחבת ב-1991, בו דן בצמיחת רעיון הלאומיות והתפתחותו לתופעה עולמית. המושג "קהילה מדומיינת" משמש את אנדרסון לתאר קבוצות אנשים גדולות, המאוחדות סביב רעיון מלכד אשר גורם להן לפעול כקהילה, למרות שבפועל הקשר והדמיון בין הפרטים המרכיבים אותן, וקבוצות פרטים בתוכן, מזעריים או לא קיימים כלל. תודעת הקהילה כה חזקה בקבוצות אלה, עד כי יש בכוחה להוציא את אנשיהן למלחמה בשדות קרב רחוקים ולמות למענן, כאילו היה מדובר בהגנה על ביתם הפרטי ומשפחתם | מקור – לינק.

109 **דִיסְאִינְפוֹרְמַצְיָה** - הפצה מכוונת של מידע שקרי ומטעה על ידי צד אחד שנועדה ליצור תמונת מציאות מעוותת אצל היריב.

110 "תעמולה דיגיטלית והאיום על הבחירות" , פרק 3. **מידע מטעה** (דיס־אינפורמציה) **מידע מוטעה** (מיס־אינפורמציה) והפצה מניפולטיבית של מידע פוליטי , המכון הישראלי לדמוקרטיה | מקור – לינק.

משפיע על קיטוב והקצנת עמדות בחברה ?, כיצד זה משפיע על העמדות של הציבור כלפי נושאים מסוימים או כלפי אוכלוסיות שונות בחברה?. האם מדובר בנזק בלתי הפיך המשפיע לרעה ברמת האמון שהאדם רוכש כלפי המדינה, מוסדות הממשלה או אמצעי התקשורת המוסדיים?, האם המאבק למניעת פיק ניוז שהיא "מלחמה פסיכולוגית" על תודעתנו צריכה להיות טכנולוגית, על ידי חינוך הציבור והגדלת המודעות לזהות "כזב-מידע", או מאבק חוקתי – משפטי כנגד מי שמפיץ "כזב-מידע"?.

- **מהן ההשפעות החברתיות והפסיכולוגיות על החברה בגין הפרת הפרטיות ללא הצדקה על ידי גופים מסחריים או גורמי הממשלה ?:**

מה ההשפעות החברתיות והפסיכולוגיות בטווח קצר ובטווח הארוך על החברה כאשר מתגלה ומפורסם ברבים כי חברה מסחרית או גוף ממשלתי עשה שימוש לרעה במידע שהוא אסף אודותנו ולא למטרות מסחריות או למטרות של בטחון אזרחי ובטחון המדינה ?.

מקרה בוחן:

- **2022** - "**פרשת NSO**" - **חברת NSO בשירות משטרת ישראל**: פריצות לטלפון של אזרחים ללא פיקוח או בקרה מראשי ערים ועד מנהיגי מחאת הדגלים השחורים - משטרת ישראל משתמשת בתוכנת הריגול פגסוס של NSO כדי לפרוץ מרחוק לטלפונים של אזרחים ישראלים ללא צווי חיפוש או האזנה. המשטרה: "יש פיקוח מצד היועמ"ש וגורמים משפטיים חוץ ארגוניים" [111]
- **2020 – משטרת ישראל מתעדת תעבורת DNS בגישה אל שרתים הקשורים להפגנות המחאה החברתית בתחילת שנת 2020:** האם המשטרה מנטרת את הפעילות של גולשים באינטרנט? עו"ד יורם הכהן, מנכ"ל איגוד האינטרנט, אמר בדיון בכנסת כי יש לאיגוד מידע שלפיו המשטרה משתמשת בהגדרות DNS כדי להעביר נתוני גולשים לשרתיה. נציג המשטרה הכחיש את הפרסומים ואמר כי היא פועלת רק באתרים גלויים. [112]
- **2018 – פרשת קיימברידג' אנליטיקה** - 100 אלף מסמכים חושפים מעורבות של קיימברידג' אנליטיקה במערכות בחירות בעולם בחשבון הטוויטר האנונימי - שכבר חשף מעורבות במערכות בחירות בברזיל ואיראן - נכתב כי החודש תיחשף מעורבות במערכות בחירות של יותר מ-60 מדינות. המסמכים חושפים כיצד פעל מנגנון להלבנת כספים, ששימשו למימון קמפיין טראמפ.[113]
- **2020 – המשטרה בארה"ב עושה שימוש במצלמות ביטחון במרחב הציבורי לזיהוי מפגינים במחאות "Black Lives Matter":** מפגין ברחוב? חייך למצלמה, המצלמות שחשפו את התנהלות המשטרה ברחובות ארה"ב עם סרטונים שהובילו למחאה משמשות כעת את המשטרה כדי לעקוב אחר המפגינים ולהשתמש במידע כנגדם. [114]

נשאלת השאלה, באיזה אופן משפיעים הפרסומים החושפים בפני אזרחי מדינה במשטר דמוקרטי, כי הם לא באמת מוגנים בפני רשויות החוק, כך שהיא לא תעשה שימוש לרעה בטכנולוגיה או במידע שהאזרחים מסרו למדינה מרצונם, גם במקרים שבהם לא היתה סכנה לביטחון הציבור או לביטחון המדינה ?.
האם קיימת בקרב הציבור תחושה של נרדפות בגין פרסומים אלו ?, האם זה מייצר תחושת חוסר אמון של אזרחי המדינה במשילות ?, אובדן אמון במוסדות המדינה ?, האם יש לזה השלכות חברתיות עתידיות על קיום והמשך הדמוקרטיה במדינת ישראל ?.

---

111 **פרשת NSO** - כלכליסט, **תומר גונן**, 18.01.22, מקור - לינק

112 **משטרת ישראל מתעדת תעבורת DNS -** אנשים ומחשבים, **יהודה קונפורטס**, 21.12.2020, מקור - לינק

113 **פרשת קיימברידג' אנליטיקה -** דה מרקר, **רפאלה גויכמן**, 07.01.2020 , מקור - לינק

114 **המשטרה בארה"ב עושה שימוש במצלמות ביטחון במרחב הציבורי לזיהוי מפגינים -** כלכליסט, **עומר כביר**, 04.06.2020 , מקור - לינק

- **האם אובדן הפרטיות האישית מובילה את האנושות לתחושת כאוס ואובדן אמון שבין האזרח לבין "היררכיות המסורתיות" כגון: מוסדות מדינה, צבא וביטחון פנים, מוסדות מוניציפליים, מוסדות דת, מוסדות פיננסים, מוסדות רפואה, תאגידים ענק פרטיים ?**

שנת 2020 תיזכר בהיסטוריה האנושית כשנה שבה היו הכי הרבה מחאות חברתיות מאז ראשית האנושות, הפגנות חברתיות בכל העולם ובפרק זמן קצר של כמה חודשים , בהם [115]: ארה"ב ("Black Lives Matter" - המחאה החברתית הגדולה ביותר בעולם מאז ראשית האנושות), בלארוס (קץ שלטונו של לוקשנקו), סרביה (הפגנות בגלל המצב כלכלי), בולגריה (שחיטות שלטונית), רוסיה (אלכסי נבלני), איטליה, ארגנטינה , פולין, אירן, תאילנד, הודו, פרו (הנשיא התפטר) , צילה (שינוי חוקה), וכמובן מחאות חברתיות בישראל (אי אמון בממשלה, טיפול במשבר הקורונה, יוקר המחייה [116]) **האם מחאות חברתיות אלו הם למעשה הניצן הראשון המראה כי קיים סדק עמוק באמון שבין האזרח לשלטון בכל נקודה בכדור הארץ ?.**

- **האם מודלים כלכלים ועסקיים חדשים המציעים רמות שונות של פרטיות בשימוש בשירותים שונים הוא אפשרי ?.**

האם מודלים כלכלים של "**תשלום עבור פרטיות**" (**Pay For Privacy**) או מודל "**כלכלת הנתונים האישיים**" (**Privacy Data Economic**) [117] הם מודלים שהציבור יסכים לאמץ ולקבל ?, האם הציבור מוכן לשלם יותר עבור מוצר או שירות הכולל רמת פרטיות גבוהה יותר ?, האם יש הבדל בגישה בין הדורות השונים לבין היחס שלהם לפרטיות בעולם הדיגיטלי \ בעולם הפיזי, האם יש לאנשים הבחנה בין הממד של הפרטיות במרחב הדיגיטלי לבין המרחב הפיזי ?.

<u>חינוך טכנולוגי \ הכשרה מקצועית \ מודעות לסכנות במרחב הסייבר:</u>

- **מאיזה גיל קיימת מודעות אישית לסכנות במרחב הסייבר ?**

זה מראה נפוץ לראות תינוק בגיל שנה וחצי אוחז ב-Tablet או ב-Smartphone ויודע איך להשתמש בו וברמה מסוימת גם מבין איך לתפעל אותו, נשאלה השאלה אם מגיל צעיר ביותר אנחנו חושפים את ילדנו למרחב הסייבר, נשאלת השאלה, **מאיזה גיל צריך ללמד את ילדנו התנהגות זהירה ושימוש נאות במרחב הסייבר ?, ומאיזה גיל מתחילה מודעות לסכנות במרחב הסייבר ?.**

- **מאיזה גיל אפשר לדרוש לשאת באחריות אישית או אחריות פלילית בגין עבירות שבוצעו במרחב הסייבר ?**

האם יש שוני באחריות פלילית לגבי עבירה שבוצעה בעולם הפיזי לבין עבירה שבוצעה במרחב הסייבר ?. הכפשה והוצאת לשון הרע, גניבת מידע, פרסום מידע כוזב, הונאות לשם עשיית רווח שלא כדין, פרסום מידע פוגעני או אישי כלפי מישהו, האם יש הבדל ברמת חומרת העונש או בסוג העונש שיש לגזור על מי שביצע עבירות אלו בעולם הפיזי לבין עבירות במרחב הסייבר ?.

- **קֶרֶדֶבִּילִיוּת מקצועית – מי הוא "מומחה" סייבר ?:**

---

115 **בעולם / גל מחאות חברתיות באירופה**: בסרביה ההפגנות גרמו להקלה בסגר אך המפגינים ממשיכים למחות בבולגריה המפגינים ממשיכים לצאת לרחובות למרות העלייה בתחלואה ומוחים על השחיתות הממשלתית | בבלארוס מסתכנים במאסרים אלימים כדי לסיים את שלטונו של 'הדיקטטור האחרון של אירופה' המכחיש את קיומה של הקורונה ופוסל את מועמדי האופוזיציה בבחירות | מתוך עיתון דבר | אוריאל לוי | 16.07.20 | מקור – לינק.

116 **מחאה חברתית 2020?** , האמון הציבורי במקבלי ההחלטות ובגופים המקצועיים בארץ בהקשר לטיפולם במגפת הקורונה, הוא כיום נמוך מאוד. התחושה הרווחת היום בציבור, כולל בקרב מצביעי מפלגות הקואליציה, היא שאין קברניט לאומי שיודע לנווט כראוי בסערה. גם בקרב אוהדיו המושבעים ראש הממשלה, נתניהו מאבד אהדה במהירות. לא כל שכן הוא דינם של מקבלי ההחלטות המקצועיים ברפואה - ועוד יותר מכך, בכלכלה - המותקפים לא רק על ידי מי שנפגעים מהחלטותיהם, אלא גם על ידי עמיתיהם למקצוע, המטילים ספק בשיקול דעתם המקצועי. לכאורה, אפוא, לפנינו קרקע פורייה לפריצת מחאה עממית רחבה. | פרופ' תמר הרמן , 19 ביולי 2020 , המכון הישראלי לדמוקרטיה , מקור – לינק.

117 מאמר משנת 2017 שמציע אימוץ של מודלים עסקים חדשים בתחום הפרטיות האישית (**PFP - Paying For Privacy** תשלום עבור פרטיות | **PDE - Personal Data Economy** כלכלת הנתונים האישיים) בשימוש במערכות דיגיטליות. מקור – לינק. הרעיון מפורט בהרחבה בספר של פרופ' **Stacy-Ann Elvy** בשם "A Commercial Law of Privacy and Security for the Internet of Things" הרצאה שלה בנושא: מקור – לינק.

איך עושים הבחנה בין מי ששולט ברמה סבירה בטכנולוגיות של סייבר התקפתי \ סייבר הגנתי, לבין מי שטוען שהוא מומחה בכיר בתחום ? **איך קובעים את רמת המומחיות המקצועית? ,** מי מעניק את הקֶרֶדִבִּילִיוּת המקצועית או החברתית להיקרא "מומחה סייבר" ?.

- **שמירה על רלוונטיות הידע המקצועי למול דרישות השוק:**

כיצד שומרים על רלוונטיות מקצועית **בענף שדורש למידה אין סופית**, ענף שדורש חידוש ותיקוף הידע אשר משתנה באופן תדיר ומהיר בגלל שהטכנולוגיה \ היצע הפתרונות \ שיטות העבודה \ דרישות הרגולציה , משתנות כל הזמן.

מקרה בוחן:

מערכות הגנת סייבר משתנות כל הזמן, היצרנים השונים בעיקר בגלל התחרות בשוק חייבים לפרסם "גרסאות ראשיות" (major release) למערכות שלהן (לפחות פעם בשנה "שחרור" של גרסה ראשית חדשה), בחלק מהמקרים בין גרסה לגרסה נוספות מעל לכמה מאות תוספות \ שינויים ושיפורים שקימות אך ורק בגרסה החדשה. בפועל גם אם היה לך ניסיון מקצועי טוב במערכת בגרסתה הנוכחית, כדי לשמור על רלוונטיות של הידע המקצועי במערכת, **אתה נאלץ ללמוד אותה מחדש** בגרסתה החדשה.

נשאלת השאלה **כיצד מטפחים בקרב אנשי המקצוע של ענף הסייבר מחויבות של "למידה לאורך החיים"** (life long learning): רכישת ידע מתמשכת התנדבותית וממוטיבציה עצמית, למטרות אישיות או מקצועיות. למידה מחדש של ידע שכבר קיים אצלנו הוא כורח המציאות כדי לשמור על רלוונטיות מקצועית.

5. מהם הגורמים שיכולים להוות קטליזטור להתפתחות דיסציפלינה פילוסופית עצמאית בתחום אבטחת הסייבר ?.

כיום אנחנו תקועים במצב הדומה לשאלה "מה קדם למה, הביצה או התרנגולת?", מצד אחד ענף הסייבר כבר משפיע על כל תחומי החיים ועל עתיד האנושות באופן ישיר ועקיף, מאידך, אין מודעות עמוקה בקרב הציבור הרחב להשלכות של היעדר חשיבה ותיכנון לתווך ארוך בכל מה שקשור להתפתחות הטכנולוגיה ובפרט בתחומים הקשורים למרחב הסייבר.

בחינת השאלה **מהם הגורמים שיכולים להוות קטליזטור להתפתחות דיסציפלינה פילוסופית עצמאית בתחום אבטחת הסייבר** היא שאלה המחייבת סיעור מוחות ושיתוף פעולה בין כל אותם בעלי אינטרסים פוטנציאלים לקדם את פיתחו של תחום זה. אלום ראשית יש להגדיר מי הם אותם **"בעלי אינטרסים פוטנציאלים"**, כיצד פיתוח התחום הפילוסופי הזה תורם להם, מה הערך שהם מקבלים, ובמה זה יכול לעזור להם או לקדם אותם על מנת להתמודד כבר היום עם שאלות ובעיות שנצטרך לתת עליהם דין וחשבון בעתיד.
לעניות דעתי קיימים מספר נתיבי התפתחות וכיווני פעולה שיכולים לעזור, לקדם ולפתח תחום כזה מול גורמים בעלי אינטרסים כדוגמת: מוסדות אקדמיים, מוסדות בינלאומיים, גופים ממשלתיים ,חברות פרטיות.

- **<u>אקדמיה VS הכשרה מקצועית בהתאם לדרישות שוק העבודה</u>**

  - מבחינה היסטורית האקדמיה במהות שלה היא מקום נהדר לפתח בו תחומים ואפיקי ידע חדשים, אולם אם נבחן את המציאות בעיניים פקוחות [118] , אנחנו כבר בתקופה ארוכה שבה עשרות שנים האוניברסיטאות הגדולות נמצאת "**במלחמת רלוונטיות**" מול המכללות האקדמית הפרטיות, כאשר יש ביניהן תחרות גלויה מי תהיה יותר רלוונטית "ביום שאחרי" סיום התואר. מי מהן מספקת את הערך הגבוהה ביותר לסטודנטים, כך שהתואר האקדמי שהסטודנטים למדו והשקיעו בו את מיטב זמנם וכספם (בחלק מהמקרים מיטב כספם של ההורים שלהם) יהיה יתרון תחרותי אמיתי בהשתלבות מקצועית במקום עבודה, ולא "עוד תעודה לתלות על הקיר בסלון בבית של ההורים הגאים.

  - לעניות דעתי, כדי שכבר בעשור הקרוב האקדמיה תסכים להכניס לתוכניות הלימודים הרלוונטיות, קורסים בתחום הפילוסופיה של אבטחת הסייבר, היא תרצה קודם לכן לבדוק ולבחון מה הרלוונטיות של הקורסים העוסקים בתחום זה לשוק העבודה או לתחומי התמחות ומחקר אחרים. הקושי הגדול במקרה זה הוא איך אפשר להוכיח לאקדמיה או למעסיקים הפוטנציאלים שהתחום הוא תחום הכרחי הן באקדמיה והן בשוק העבודה, כאשר אין מודעות לקיומו של התחום לא מהצד של המעסיקים ולא מהצד של האקדמיה.

  - נקודות אור קטנה אחת בפיתוח התחום הפילוסופי במסגרת אקדמאית כך שאפשר לציינה כבר היום, היא שבחלק מהאוניברסיטאות \ המכלכלות האקדמיות כן קיימת דרישה במסלולי התמחות של מדעי המחשב \ הנדסת מחשבים לקורס שעוסק בנושא "**סוגיות אתיות בראי יישומי הבינה המלאכותית**". זה אומנם קורס שלא עוסק באופן ישיר בתחום אבטחת הסייבר, מאידך הוא כן מתחבר לנושאים שונים הקשורים לתחום "הפילוסופיה של הטכנולוגיה" וזה כבר התחלה טובה. [119]

---

118 אין זה סוד שהאקדמיה בכל העולם נמצאת במשבר רלוונטיות של ממש, והסיבות לכך הן רבות כפי שמפורט בספרים: "**כל שקרי האקדמיה**" (**ד"ר תמר אלמוג, פרופ' עוז אלמוג**) ובספר "**סדקים באקדמיה**" (**פרופ' אמנון רובינשטיין, עו"ד יצחק פשה).** המשבר בתחומים ובמסלולים הטכנולוגים הוא גדול במיוחד היות וקיים פער בין מה שנלמד בתואר לבין דרישות שוק העבודה שהן הרבה יותר מתקדמות. בנוסף קצב השינויים בעולם העבודה הוא הרבה יותר מהיר מהקצב שבו האקדמיה מעדכנת את תוכן הלימודים במסגרת התואר, כך שתחום האקדמי תמיד מפגר אחרי הצרכים של שוק העבודה.

119 במערכת הלמידה המתוקשבת Campus.gov.il במיזם "ישראל דיגיטלית" פעל בעבר קורס ציבורי בשם "**אתיקה בהנדסה בעידן ההייטק**" קורס שעסק במוסר, אתיקה וטכנולוגיה ופותח על ידי **ד"ר נתן פנחס** מהטכניון, הקורס פתח צוהר לדיון אקדמי וציבורי בנושא של אתיקה וטכנולוגיה. הקורס אינו פעיל מאז 01/10/21 לינק.

- למרות שמדינת ישראל מקבלת יחס בעולם כ- "**Start-Up Nation**", אנחנו כישראלים (בעיקר הפוליטיקאים) קצת משקרים לעצמנו, כי גם לנו קשה להודות שבמדינת ישראל אולי אנחנו מצטיינים בלהמציא ולפתח טכנולוגיות חדשות (בעיקר בתחומי הביטחון), אנחנו נחשבים מעין סוג של "אור לגויים" מבחינת חדשנות טכנולוגית, אולם מאידך במציאות אנחנו כמדינה הרבה פחות מוצלחים בכל מה שקשור לאימוץ של טכנולוגיה חדשה הלכה למעשה, גם כאשר מדובר על טכנולוגיות שהיו יכולות לשפר משמעותית את רווחת החיים של אזרחי המדינה.

- ככל שהעמקתי לחקור ולבדוק, האקדמיה בישראל אף פעם לא קידמה באופן רציני קורסים בנושאים של "**<u>הפילוסופיה של הטכנולוגיה</u>**". לראייה בעברית יש רק ספר אחד בלבד [120] שעוסק בתחום, וגם הוא פורסם בשנת 2011.

- בעשור האחרון זה הפך להיות נדיר "לזכות" בקורס שעוסק בתחום "הפילוסופיה של הטכנולוגיה" במסגרת לימודי התואר האקדמי שלך [121]. מאידך זה עוד יותר מאתגר עבור האקדמיה למצוא מרצים שמתאימים ללמד קורס כזה.

- כמקרה בוחן האם האקדמיה כיום מקדמת למידה מעמיקה בנושא של השפעות אבטחת הסייבר על החברה, אם נבחן את תיאור המסלול האקדמי לתואר שני בנושא "מדע, טכנולוגיה וחברה" באוניברסיטת בר אילן [122] (או בכל אוניברסיטה אחרת שהתחום המשולב הזה נלמד כתואר אקדמי), נגלה שמדובר במסלול אקדמי מרתק מבחינת התוכן שלו, אולם גם בו אין ולו קורס אחד בודד שעוסק וממוקד בפילוסופיה של הטכנולוגיה, או קורס שעוסק בהשפעות של "אבטחת הסייבר" על המדע, הטכנולוגיה או החברה, זאת למרות שתוכן של קורסים שעוסקים באופן ישיר בשילוב של הפילוסופיה של טכנולוגיה או הפילוסופיה של אבטחת סייבר, הם בהחלט רלוונטיים ואף הכרחיים כחלק מתוכנית לימודים במסלול כזה.

- ככל הידוע לי במסגרת של קורסים והכשרה מקצועית בין אם היא שייכת בעקיפין לאוניברסיטה כלשהי (כגון "היחידה ללימוד חוץ" , "היחידה ללימודים משלימים" וכדומה) או בקורסים במסגרות מקצועיות פרטיות, אין עניין להכניס תוכן של הפילוסופיה של הטכנולוגיה או הפילוסופיה של אבטחת הסייבר, היות ובקורסים כאלה עוסקים בהכשרה מקצועית בגישה הישראלית המוכרת לכולם כ "גישת התכל'ס", כך שהמיקוד הוא בדרישות הידע של המעסיקים בשוק העבודה כיום, ללא ראייה או חשיבה לדרישות שוק העבודה בעתיד.

- האקדמיה או מוסדות להכשרה מקצועית (חוץ-אקדמית, פרטית) יהיו בעלי אינטרס לשלב קורסים שעוסקים בהיבטים שבהם עוסקת הפילוסופיה של אבטחת הסייבר, אך ורק כאשר תהיה דרישה של המעסיקים כחלק מדרישות ההתמחות המקצועית שהם מצפים שיהיו לבוגרי אוניברסיטה או בוגרי מסלול הכשרה מקצועית כדי להשתלב בשוק העבודה.

---

120 הספר היחידי שיש בעברית בתחום הפילוסופיה של המדע הוא הספר "**הפילוסופיה של הטכנולוגיה**" מאת **פרופ' יוסף אגסי** , שיצא בהוצאה מיוחדת בשנת 2011 , על ידי הוצאת משרד הביטחון \ הוצאת מודן, הספר הוא מעין תקציר עבור ספר מקיף שכתב פרופ' אגסי ופרסום אות באנגלית בלבד , ספר העוסק בחיבור שבין טכנולוגיה ופילוסופיה, 1985 - Dordrecht Kluwer - Technology - Philosophical and Social Aspects

121 במקרים בהם מדובר על קורסים במסגרת של תואר אקדמי העוסקים "<u>במרחב הסייבר</u>" מצאתי אזכור לקורס אחד כזה, שהתקיים לפני מעל עשור באוני' ת"א והוביל אותו ידי **פרופ' איציק בן ישראל**, הקורס עסק בסוגיות הקשורות למרחב הסייבר ובשימוש בטכנולוגיות Big Data ו ML-AI ולא עסק בתחומים הרלוונטיים לנושאים של אבטחת סייבר.

122 לימודים לתואר שני – **מדע, טכנולוגיה וחברה**, אוניברסיטת בר-אילן – מקור - לינק

- יש לקחת בחשבון שמעל עשור שנים הלך הרוח בקרב הסטודנטים בישראל ואני משער שגם בעולם הוא גישה של "הגעתי לעשות תואר" ולא גישה של "הגעתי ללמוד במטרה להרחיב אופקים". המטרה של מרבית הסטודנטים ותפיסת עולמם (ה Mindset שלהם), הוא לסיים את התואר באופן הקל והמהיר ביותר, במטרה לסמן V בקורות חיים. הדרישה לתחומי לימוד ובהם קורסים הדורשים חשיבה מעמיקה, קריאת טקסטים ארוכים, התמודדות עם למידה עצמית, אינטגרציה וחיבור בין מספר תחומי לימוד, הם קורסים ותחומי השכלה שהדרישה אליהם בירידה משמעותית בשנים האחרונות, בתחומים של מדעי הרוח מדובר על ירידה של מעל 50% במספר הנרשמים ללימודים [123]. בנוסף בחלק גדול מהמקרים אין אינטרס למרצים ולסגל ההוראה לפתח קורסים מורכבים כדוגמת קורס שיעסוק בתחומים של הפילוסופיה של אבטחת הסייבר, היות וזה לא תחום ההתמחות שלהם, הם לא מקבלים תגמול על ההשקעה הרבה הנדרשת לפתח קורס כזה, ולבסוף זה גם אינו מקדם את הקריירה שלהם [124]. במצב הנוכחי הן הסטודנטים לא מתעניינים ולא מעוניינים ללמוד קורסים מורכבים כאלה הדורשים מהם להתאמץ מעבר למה שמקובל בקורס ממוצע, ומאידך הן המרצים לא רוצים לפתח קורסים מורכבים כאלה, היות והם לא מתוגמלים על המאמץ הרב בפיתוח קורסים כאלה או בללמד אותם.

- לעניות דעתי, הן באקדמיה והן בהכשרה מקצועית בתחומים של: מדעי המחשב (הנדסת תוכנה, הנדסת חומרה, ניהול מערכות מידע), משפטים (רגולציה, הגנת הפרטיות, דיני עבירות מחשב), ראיית חשבון (ביקורת מערכות מידע, ניהול סיכונים), מסלולי מנהלים במסגרת לימודים של MBA, וכמובן בקורסים מקצועיים להכשרת דירקטורים, הכשרת CISO / DPO, הכשרת CIO / CDO, ועוד. בכל מסלולי לימוד והתמחות אלו, **<u>חייבים</u>** לכלול תוכן לימודי מתוך הסוגיות שעוסקות בהן "הפילוסופיה של אבטחת הסייבר", מדובר **<u>בידע הכרחי</u>** שנדרש לאותם מקצועות על מנת להבין לעומק את סך כל השיקולים שעליהם להתייחס אליהם בעת תהליך קבלת החלטות מושכלות במסגרת עבודתם, זה מקבל תוקף מוגבר יותר כאשר מדובר במקצועות ובתחומים של ניהול בתחום אבטחת הסייבר.

- **<u>גורמים בינלאומיים והאינטרסים המשותפים שלהם לנורמליזציה במרחב הסייבר</u>**

- שלושת האתגרים <u>הגלובליים</u> הגדולים והראשיים העומדים בפני האנושות הם: **האתגר הגרעיני**, **האתגר האקולוגי והאתגר הטכנולוגי**, לגבי שלושת אתגרים מרכזיים אלו, **<u>אין</u> נכון להיום שיתוף פעולה אמיתי** עם כוונות כנות הכולל את כלל 196 המדינות הרשמיות המוכרות בעולם [125]. כל זאת למרות שברור לכולם כי ללא שיתוף פעולה גלובלי כזה אי אפשר לתת מענה אמיתי לאף אחד מהאתגרים והבעיות שכבר משפיעות על כלל האנושות.
יש הטוענים כי קיים אתגר גלובלי נוסף שגם עליו יש לתת את הדעת, אתגר שהוא בהחלט תולדה של התפתחות מואצת ומהירה של המדע והטכנולוגיה, הוא **האתגר הדמוגרפי**, מספר בני האדם החיים בכדור הארץ לאור גידול משמעותי באורך החיים.

123 כתבה בשם: "**על רקע הירידה בהרשמה לחוגים למדעי הרוח, יוקמו תוכניות לימוד רב תחומיות**". ועדה לקידום מדעי הרוח במוסדות להשכלה גבוהה המליצה ליצור מסלול לימודים רב תחומי לתואר ראשון, ועל עידוד הקמת מרכזים בין-תחומיים לתואר שני. בחלק מהחוגים במדעי הרוח ירד מספר התלמידים בלמעלה מ-50%", פורסם באתר עיתון הארץ, אור קשתי, 06.04.2021, לינק.

124 מאמר בשם: **שקט, חוקרים: על קריסת מדעי-הרוח בישראל - מי אשם בירידה החדה בהרשמה למדעי-הרוח: אבו ג'ילדה, נתניהו, חומרנות ישראלית, או הסגל האקדמי?** "דוברי האוניברסיטאות אוהבים להגיד עד כמה ההוראה חשובה; העבודה של אקדמאי מוגדרת כ-50% הוראה ו-50% מחקר, הם נוהגים לומר. אבל שיטת התמריצים האמיתית, קרי, המפתח לקביעות וקידום אקדמיים, כמעט איננה מתחשבת בהוראה. רק במקרים נדירים, בהם יש בין שני מועמדים כמעט-שוויון בתיק המחקר ופער גדול בהוראה, ההוראה יכולה להשפיע. המשמעות פשוטה, וכל אקדמאי מתחיל מקבל את העצה הזו מידידיו: העתיד האקדמי שלך תלוי במחקר ולא בהוראה. אם בזמן שבו תשקיע בהוראה המתחרה שלך יכתוב מאמר או שניים יותר ממך, כבר לא ישנה כמה ההוראה שלך טובה" מקור: אתר מידה, רן ברץ, 23.10.2012, לינק

125 **מדינות חברות באו"ם 193 | סך המדינות רשמיות\מוכרות 196** | מקור: גיל אל עמי | מסע אחר | נכון לספטמבר 2022 | מקור – לינק.

- מובן לכל בעל בינה כי **האתגר הטכנולוגי** אינה תופעת טבע עוצמתית שלאנושות אין יכולת להתמודד מולה אלא רק להגיב לתוצאותיה, **ועל כן** האתגר הטכנולוגי ניתן לפיקוח, ניהול ובקרה מתוך החלטה רצונית של בני האדם במידה והם חולקים ערכים מסוימים משותפים.

אחת הבעיות המרכזיות של האנושות כיום היא שאין תפיסה גלובלית, ועדין לא התקבע בתודעה האנושית באופן נרחב שכדי שהציוויליזציה האנושית תמשיך להתקיים גם בעתיד הרחוק בכדור הארץ, **כבר היום באופן גלובלי ומחייב יש לתת את הדעת על הסוגיות השונות הקשורות בהשפעת השימוש בטכנולוגיה לטובת כלל האנושות.**
הטכנולוגיה הקיימת כיום כבר משנה ועוד תשנה בעתיד באופן עוד יותר קיצוני מהמוכר לנו כיום את כל היבטי החיים שלנו: היחס לתעסוקה (או האי-תעסוקה בעתיד), פתרונות ניידות (תחבורה), מעמדות חדשים ("Super Human" לעומת "אדם רגיל") [126], היחסים שלנו עם המדינה \ השלטון \ "האי-פרטיות" שלנו, ההשפעות מקצה לקצה בכל היבט הקשור לחיינו: חיי המשפחה, יחס לדת, זמן פנוי, אושר, בריאות \ רפואה מותאמת אישית ברמת ה-DNA , יחס ושימוש בכסף, ואפילו כמה זמן נחייה והאם ננצח את המוות. **<u>הכול נכון להיום הם אתגרים ובעיות טכנולוגיות.</u>**

- ענף אבטחת הסייבר משפיע ומושפע באופן ישיר ועקיף ממאות תחומים אחרים, **לא ניתן לשמור על יציבות ונורמליזציה בעולם** מכל הבחינות: גאו-פוליטיות, כלכליות, חברתיות וטכנולוגיות **ללא סדר ופיקוח** על מרחב הסייבר ובתוכו גם ההיבטים הכלולים בענף אבטחת הסייבר.

- קיימים גופים בינלאומיים כדוגמת: GCA ("ברית הסייבר העולמית") , CTA ("ברית איומי הסייבר"), WEF (הפורום הכלכלי העולמי), יחידת הפיקוח בנושא סמים\פשיעה של האו"ם, גופים שונים באיחוד האירופאי אשר מטרתם פיקוח על שימוש במערכות AI (ארגונים כדוגמת AIA [127], AI2 [128]), ועוד. כולם גופים שמקדמים שיתוף פעולה גלובלי **<u>ללא מטרות רווח</u>**, כדי "לנרמל" שיתופי פעולה בינלאומיים בנושאים טכנולוגיים.

- **שאלה חשובה עומדת בפתחנו, האם צריך להמציא את הגלגל מחדש כדי להגדיר רגולציה בינלאומית על מנת לפקח ולמנוע שימוש לרעה בטכנולוגיה באופן כללי, ומניעת שימוש לרעה במרחב הסייבר בפרט ?**.
האם ניתן "להעתיק" הצלחות קודמות מההיסטוריה של הסכמים גלובליים כדוגמת הסכמים בתחומים של הגנה על "קניין רוחני" (IP = Intellectual Property) בינהם: "אמנת פריז" 1883 [129]

---

126 **"Super Human" לעומת "אדם רגיל"** – ההבדל בין בני אדם "רגילים" לבין בני אדם שבהם יש שילוב של טכנולוגיה המחוברת או המושתלת בגופם כך שהיא מעניקה להם "יכולות על" שאין לבני אדם "רגילים".

127 **מנגנון פיקוח על השימוש בבינה מלאכותית באיחוד האירופאי , ה- AI-ACT** | מקור – לינק.
The AI Act is a proposed European law on artificial intelligence (AI) – the first law on AI by a major regulator anywhere. The law assigns applications of AI to three risk categories. First, applications and systems that create an unacceptable risk, such as government-run social scoring of the type used in China, are banned. Second, high-risk applications, such as a CV-scanning tool that ranks job applicants, are subject to specific legal requirements. Lastly, applications not explicitly banned or listed as high-risk are largely left unregulated.

128 **AI2** is a non-profit research institute founded in 2014 with the mission of conducting high-impact AI research and engineering in service of the common good. מקור – לינק.

129 **אמנת פריז 1883** (Paris Convention for the Protection of Industrial Property) - אמנת פריז היא אמנה בינלאומית להגנת קניין רוחני אשר נחתמה ב-20 במרץ 1883 בפריז שבצרפת. האמנה, שחשיבותה רבה ביותר בנושא הקניין הרוחני, היא אחת האמנות הראשונות מסוגה, מדינת ישראל הצטרפה לאמנה בשנת 1950. אמנת פריז מתייחסת לפטנטים, מדגמים, מדגמי תועלת וסימני מסחר – מקור – לינק.

"אמנת ברן" 1886 [130] אמנת TRIPS" 1995 [131] ? כאשר בכל ההסכמים הנ"ל [132] (שגם עודכנו מספר פעמים כדי להתאים למציאות העסקית והטכנולוגית המשתנה) יש שמירה באופן גלובלי על זכויות קניין רוחני הכוללים גם בסיסי נתונים, תוכנות מחשב (כולל קוד מקור), זכויות יוצרים וזכויות מסחר בינלאומי;

כאשר בוחנים הסכמים גלובליים אחרים כדוגמת: הסכמים של ארגון הסחר העולמי, הסכמים כלכליים ופיננסים בינלאומיים, הסכמים ואמנות בינלאומיות להפחתת פליטות גזי חממה ומזהמים לאטמוספירה, הסכמים ואמנות בינלאומיות למניעת תפוצה נשק גרעיני, ואפילו "אמנת ז'נבה" הקובעת חוקים בינלאומיים של משפט בינלאומי וזכויות של שבויי מלחמה. **אפשר לצפות** שכאשר "האנושות" מגיעה להבנה רציונלית כך שלטובת כל הצדדים עדיף לכונן יחסים ולמסד הסכמים אשר יצרו יציבות ונוֹרמָלִיזָצִיָה בעולם מכל הבחינות: גאו-פוליטיות, כלכליות, חברתיות וטכנולוגיות אזי גם שימוש לרעה במרחב הסייבר למטרות של פשיעת סייבר על רקע כלכלי, וטרור סייבר על רקע גאו-פוליטי "אינו גזירה משמים" כך שבהחלט בהחלטה גלובלית בינלאומית אפשר להקטין את התקפות הסייבר, ולבסוף גם לצמצם אותם למינימום.

- אם נסכים לקבל את עמדותיו של **פרופ' ישעיהו ליבוביץ** ז"ל שטען מעל לכל במה ש "בין בני אדם אין ערכים אוניברסליים", ו "ערכים אינם עניין של מסקנות אלא עניין של הכרעות" ו "הכרעות ערכיות אינן פרי הידע שיש לאדם אלא פרי רצייתו, מגמותיו ושאיפותיו." אני משער שגם פרופ' ליבוביץ היה מסכים שלאור הגלובליזציה הנוכחית (החל מסוף מלחמת העולם השנייה ועד היום) גם אם אין לנו כבני אדם ערכים משותפים, והכרעות ערכיות אינן רציונליות, מאידך **למדינות כן יש אינטרסים "עליונים" משותפים** [133] [134] [135] , והאינטרסים הללו (כדוגמאות הסכמים גלובליים שנחתמו בעבר) **הם אלו שיכולים לקדם שיתופי פעולה והסכמים בינלאומיים עד לכדי נוֹרמָלִיזָצִיָה גם במרחב הסייבר**. בשל התלות שלנו בטכנולוגיה, וההשפעה הישירה שלה בכל אספקט המשפיע על מרקם החיים של בני אדם בכל העולם, **אין לנו ברירה** אלא להגיע לאמנות והסכמים גלובליים כאלה.

- לעניות דעתי, במסגרת דיון בתחומים בהם עוסקות הפילוסופיה של הטכנולוגיה והפילוסופיה של אבטחת הסייבר, ובעזרתן יהיה אפשר לפרק ולנתח את האינטרסים המשותפים ביחס לכל הבעיות והאתגרים הגלובליים, ובעזרתם גם להגדיר הבנות הדדיות משותפות כך שיש בהם מקסימום הסכמה לאינטרסים המשותפים (בהנחה שאנחנו לא יכולים להגיע לערכים משותפים בין בני אדם).

---

130 **אמנת ברן 1886** (The Berne Convention for the Protection of Literary and Artistic Works) אמנת ברן להגנת יצירות ספרותיות ואמנותיות, הידועה גם בקיצור כאמנת ברן, היא אמנה בינלאומית המגינה על זכויות יוצרים. האמנה נחתמה לראשונה בעיר ברן שבשווייץ ב-1886 ותוקנה מאז מספר פעמים. נכון לאוקטובר 2007, חתומות עליה 163 מדינות. מקור – לינק.

131 **אמנת 1995 TRIPS** (Trade-Related Aspects of Intellectual Property Rights) הסכם TRIPS של ארגון הסחר העולמי הוא הגנה ושמירה על זכויות הקניין הרוחני מעוגנת בהסכמים בינלאומיים, ייחודו של הסכם TRIPS הוא בהיותו מקיף היבטים רבים ומגוונים של נושא הקניין הרוחני, תוך קביעת סטנדרטים מינימליים שעל המדינות החברות לאמץ בחקיקתן הפנימית. המדינות החברות מתחייבות גם להבטיח את קיומם של אמצעי אכיפה משפטיים כדי לאפשר לבעלי הזכויות לפעול באפקטיביות נגד הפרות של זכויותיהם, ולאפשר ביקורת שיפוטית על כל החלטה מנהלית בקשר לזכויות בקניין רוחני. ישראל, כחברה בארגון הסחר העולמי, מחויבת להסכם ,TRIPs החל משנת 2000. מקור – לינק.

132 **Artificial Intelligence Regulation Across the World** | סמינר מקוון בהובלה של Cornell China Center שנערך ב-27 במאי 2022, חוקרים משפטיים שבסיסם בסין, שוויץ וארצות הברית סקרו את רגולציה של בינה מלאכותית (AI) ברחבי העולם, ויהו קווי דמיון אסטרטגיים והבחנות מקומיות. האירוע ריכז יותר מ-150 משתתפים על פני אזורי זמן לשיחה המתפרשת על קניין רוחני, זכויות נכים ומדדי רגולציה גלובליים.- לינק

133 מתוך דבריו של **פרופ' ישעיהו ליבוביץ** (תשל"ו) - "כל מדינה! – היא מוסד של סיפוק צרכים ואינטרסים אנושיים" –מקור: "יהדות, עם יהודי ומדינת ישראל" עמ' 154.

134 מתוך דבריו של **פרופ' ישעיהו ליבוביץ** (1971) - "שני המישורים של הצרכים שאותם מספקת המדינה אינם למעשה אלא אחד, אם קיימת תודעה לאומית, נעשה קיום העם גם הוא צורך הפרט הרואה עצמו בן העם ההוא. נמצא, שבסיס קיומה והצדקת קיומה של המדינה הם אנתרופוצנטריים* - היא קיימת למען האדם, והיא מודרכת ומכוונת ע"י צרכים ואינטרסים וסיפוקים." מקור: ב"הדרך", מס' 4, סיון תשל"א/מאי 1971 , מקור – לינק.

* **אנתרופוצנטריות** היא השקפה בתחום הפילוסופיה והתאולוגיה הרואה באדם את מרכז או תכלית העולם.

135 "המדינה וממשלתה החוקית הן מוסדות אנושיים, הקיימים ומקויימים למען צרכים אינטרסים אנושיים, למען שלום האדם והעם. ציטוט מתוך הספר: רציתי לשאול אותך פרופ' ליבוביץ ... מכתבים אליו וממנו ,עמ' 417.

- **<u>אגודות פילוסופיות \ מכוני מחקר בחסות אוניברסיטאות</u>**

  - **אגודות פילוסופיות:** ככל הידוע לי בחסות מוסדות האקדמיה בישראל קימות אך ורק שתי אגודות פילוסופיות [136] [137] ,אשר מטרתן לקדם חילופי רעיונות בין פילוסופים בישראל, לעודד פעילות פילוסופית אקדמית, ולייצג את הפילוסופיה כדיסציפלינה. בכנסים השנתיים של אגודות אלו אין התייחסות ישירה לתחומים (או מסלולים ממוקדים) של אבטחת הסייבר \ טכנולוגיה, אלא בהתייחסות של טכנולוגיה וחברה בלבד.

  - **מכוני מחקר:** במסגרת האקדמיה הישראלית קימות מספר מכוני מחקר העוסקים בתחומים של: ביטחון לאומי, טרור, סייבר, פרטיות, אתיקה, אינטרנט. בישראל מספר מכוני מחקר מובילים בתחומם (גם ברמה עולמית) כדוגמת : INSS – המכון למחקרי ביטחון לאומי – אוני' ת"א [138], המכון לחקר האינטרנט – אוני' ת"א [139], המרכז למשפט וטכנולוגיה – אוני' חיפה [140], המכון למדיניות נגד טרור – ICT – אוניברסיטת רייכמן [141] , ICRC – המרכז הרב תחומי לחקר הסייבר על שם בלווטניק – אוני' ת"א [142] ועוד.

  - **האם ניתן לחבר בין אגודות הפילוסופיה הפעולות בישראל לבין מכוני מחקר הפועלים בתחומים הקשורים לאבטחת הסייבר ?**
    - למיטב הבנתי כיום אין "גשר אקדמי" המחבר בין האגודות הפילוסופיות לבין הפעילות של מכוני המחקר השונים העוסקים באופן ישיר או עקיף בתחום אבטחת הסייבר.
    - בנוסף ככל הידוע, אין שיתופי פעולה גלויים בין מכוני מחקר שאינם תחת השתייכות של אותו גוף אוניברסיטאי אחד, ברוב המקרים זה בעיקר שיתופי פעולה עם גופי מחקר מקבילים מחו"ל.
    - סביר להניח שהתוכן הנחקר בפעילות של אותם מכוני מחקר מושפע באופן ישיר על ידי גורמי המימון שלו, וקידום האינטרסים של האקדמיות שתחת חסותן הן פעולות.
    - לעניות דעתי, פיתוח של תחום הפילוסופיה של אבטחת הסייבר יכול להיות כלי מחקר נוסף שיעזור באופן משמעותי לנתח ולהבין תופעות ואירועים בתחומים שבהם עוסקים אותם גופי מחקר, אולם אם לא יהיה אינטרסים של האוניברסיטאות ליצור פעילות המחברת בין תחום הפילוסופיה לבין תחום אבטחת הסייבר במכוני המחקר השונים שנמצאים תחת חסותן של אותן אוניברסיטאות, אזי הסיכוי ששיתופי פעולה כאלה יקרו הוא נמוך ביותר.

---

136 **אגודת הפילוסופיה הישראלית (החדשה)** נוסדה בשנת 1998. מטרות האגודה הן לקדם חילופי רעיונות בין פילוסופים בישראל, לעודד פעילות פילוסופית אקדמית, ולייצג את הפילוסופיה כדיסציפלינה. בהנהלת האגודה חברים ראשי המחלקות של המחלקות לפילוסופיה באוניברסיטאות השונות (בן-גוריון, בר-אילן, הפתוחה, העברית, חיפה, תל אביב) וכן חבר נוסף מכל מחלקה. מדי שנה מארגנת העמותה כנס פילוסופיה ארצי, שבו נערכים הרצאות ודיונים במושבים שונים בסוגיות מעולם הפילוסופיה. הכנס מתקיים מדי שנה באחת מהאוניברסיטאות בישראל. אין לאגודה אתר אינטרנט מסודר מקור | תוכנית כנס שנתי 2022

137 **האגודה הישראלית להיסטוריה, פילוסופיה וסוציולוגיה של המדע** היא עמותה ללא כוונת רווח הפועלת בישראל משנת 2000, מתוך מטרה לקדם מחקר אינטר-דיסציפלינרי על אודות מדע טכנולוגיה וחברה. האגודה פותחת את שעריה לכל מי שמוצא/ת עניין בהבנת ההיבטים ההיסטוריים, הסוציולוגיים, הפילוסופיים והאנתרופולוגיים של המדע והטכנולוגיה. אנו שואפים לבסס ולהרחיב את נראותם והשפעתם של תחומי מחקר אלו בספירה הציבורית ולהוות זירה לפעילות משותפת ולמידה הדדית לחברי האגודה. מקור: לינק | תוכנית כנס שנתי 2022

138 **INSS – המכון למחקרי ביטחון לאומי** – לינק.

139 **IIS - המכון לחקר האינטרנט** - לינק.

140 **המרכז למשפט וטכנולוגיה** – אוני' חיפה – לינק.

141 **ICT - המכון למדיניות נגד טרור** – אוניברסיטת רייכמן – לינק.

142 **ICRC – המרכז הרב תחומי לחקר הסייבר** על שם בלווטניק – אוני' ת"א – לינק.

- **גורמי מחקר מסחריים**
  - קיימים כ- 20 גופי מחקר עצמאיים בינלאומיים אשר עוסקים במתן ייעוץ למנהלים על ידי בחינה השוואתית בין מערכות מחשוב ושירותים שנים בתחום מערכות מידע בכלל ואבטחת סייבר בפרט. מטרתם המוצהרת של אותם גופים, היא לנסות לעשות סדר "בים" המידע שמציף את המנהלים העסקיים על ידי ניסיון לחזות את הכיוונים הטכנולוגים של תחומי טכנולוגיות המידע ובכך לסייע להם לקבל החלטות אסטרטגיות מבוססות נתונים עבור הארגונים שלהם, הגופים המוכרים ביותר בתחום הם: Gartner[143], IDC[144], Forrester Research[145], McKinsey & Company[146], Accenture[147], BCG[148] ועוד.

  - כמי שקורא ועוקב מעל עשור שנים, אחרי הדוחות של החברות המוזכרים לעיל, אני יכול להצביע על אחת הבעיות המרכזיות והמהותיות בדוחות ובסקרים שהחברות הנ"ל מפרסמות. הבעיה המרכזית **שהם מתבססים על "מידע עבר", בעיקר נתונים כלכלים או טכנולוגים שהם אוספים ממקורות שונים,** כדוגמת היקפי מכירות בשנים קודמות לפי מגזרים, מדידת נתח שוק לפי חלוקה למגזרים, היקף אימוץ של טכנולוגיה חדשה במערכות טכנולוגיות דומות, סקרי שביעות רצון של לקוחות לגבי פתרונות \ מערכות \ גרסאות מוצר ישנות, ועוד. את הנתונים האמפרים הללו מנתחים בעזרת מודלים סטטיסטיים שונים ומודלים לזיהוי של תבניות ודפוסים חוזרים ומנסים על בסיסם לנבא את הטרנדים והמגמות העתידיות בתקופת "קצרת-טווח" של 2 עד מקסימום 5 שנים.

  - בעשור שבו אנחנו נמצאים חקר עתידים לטווח קצר המתבסס אך רק על זיהוי "דפוסים חוזרים" שמתבססים על נתונים היסטוריים מאבד את הרלוונטיות ורמת הדיוק של החיזוי בתחום טכנולוגיות המידע, בעיקר **כאשר בענף הסייבר כבר היום משמעות לתכנון מעל ל-3 שנים קדימה**. לאור קצב השינויים הטכנולוגים המאוד מהירים בתחום טכנולוגיות המידע, כמעט שאין היום חברות שמבקשות לבנות ולתכנן תוכניות אסטרטגיות מעבר ל-3 שנים.

  - **בעיה נוספת וחמורה לא פחות** היא שהיצרנים ומי שמפתח את המערכות הנבחנות באותם סקרים \ דירוגים \ המלצות כדי להצליח יותר טוב בדירוג הבא, הם "מנתבים מחדש" את פיתוח המערכות שלהם על פי ההמלצות שכתבו אותם גופי מחקר בדוח האחרון. זה מצב אבסורד שבמקום שהיצרנים יבנו ויפתחו את המוצרים בגרסאות החדשות שלהם **בהתאם לדרישות הלקוחות והשוק המשתנים**, הם מנסים לרצות את גופי המחקר, ומפתחים במקרים רבים יכולות מתקדמות במערכות שלהם ע"פ החזון של אותם גופי מחקר, בסופו של דבר מתגלה כי הלקוח מלכתחילה אינו צריך וגם אינו ביקש את אותן יכולות מתקדמות וחדשות ולכן גם לא מאמץ אותן ומשתמש בהן באופן נרחב בהמשך הזמן.

    במקום שהיצרנים יובילו את התחום שבהם הם מפתחים מערכות, ויבנו את המערכות הטובות ביותר על פי הצרכים והדרישות של הלקוחות ודרישות השווקים או הסקטורים שבהם הן פועלים, למרבה הצער הם במקום זאת "נגררים" אחרי גופי המחקר, ולמעשה הם מובלים על ידם, יש פה פרדוקס שמי שאמור לנבא את הטרנדים והמגמות העתידות למעשה הוא זה שמכתיב ליצרנים איך לפתח את הגרסאות החדשות של המוצרים והמערכות שלהם לשנים הקרובות.

---

143 **Gartner** - לינק

144 **IDC** – International Data Corporation – לינק.

145 **Forrester** - לינק.

146 **McKinney** – לינק.

147 **Accenture** – לינק.

148 **Boston Consulting Group** – לינק.

- החוק הראשון של תחום הטרנדולוגיה בחיזוי טרנדים ומגמות לטווח קצר הוא "**שההתנהגות של האנושות בעבר <u>אינה</u> מעידה דבר על ההתנהגות של האנושות בעתיד**". גופי המחקר המוזכרים לעיל בדוחות שלהם הבוחנים אימוץ טכנולוגי במרבית המקרים מתעלמים מגורמי השפעה שאינם טכנולוגים או כלכליים בתחזיות הטכנולוגיות שלהן. הדבר פוגע מהותית ביכולת של אותם גופים לנבא את התרחשים העתידיים בסבירות ודיוק גבוהים יותר. בדרך כלל הדוחות והתחזיות לא כוללות התייחסות להשפעות כדוגמת: תהליכים סוציולוגיים בחברה אנושית, השפעות חברתיות, השפעות פסיכולוגיות, השפעות של המדיה והתקשורת, בעיות גיאופוליטיות, אתגרים דמוגרפיים, בעיות הנובעות מהמשבר האקולוגי.

מקרה בוחן: האם בסקר השוואת פתרונות שבוחן וממליץ איזה מערכת SASE [149] כדאי לרכוש, נלקחים בחשבון ההשפעות של עבודה מהבית, תופעות חברתיות כגון "ההתפטרות הגדולה", "ההתפטרות השקטה", מחסור בכוח אדם מיומן בענף הסייבר, המעבר למערכי ענן ציבורי וההשפעות שלו על כלל תחום טכנולוגיות המידע, מלחמות גאופוליטיות עד לרמה של פגיעה פיזית מכוונת בתשתיות אינטרנט של מדינות אחרות, המחסור בשבבים, בעיות בשרשרת האספקה העולמית, רגולציה בינלאומית בתחום הגנת הפרטיות ובתחום אבט"מ, דרישת הלקוחות לשקיפות ואחריות תאגידית, השתכללות טכנולוגית של קבוצות התקיפה בפשיעת סייבר על רקע כלכלי ותקיפות סייבר על רקע גאו-פוליטי. **כל אותם גורמים דורשים הבנה מולטי דיסציפלינרית ובחינה של מספר ממדים הקשורים לאימוץ טכנולוגי <u>מעבר</u> להיבטים כלכלים או טכנולוגים.** ואלו היבטים שלא נבחנים באותם סקרים המוזכרים לעיל.

- לעניות דעתי, הפילוסופיה של אבטחת הסייבר יכולה להיות כלי מחקרי מהותי, המאפשר לאותם גופי מחקר לבחון את ההיבטים השונים המהווים את גורמי ההשפעה הישירים והעקיפים של ההמלצות שלהם באופן רחב ועמוק יותר. קידום תחום הפילוסופיה של אבטחת הסייבר הוא בהחלט חייב להיות גם האינטרס המשותף של גופי המחקר העצמאיים ככלי שעוזר להבטיח את אמינות המלצותיהם.

- **קהילה פתוחה (פודקאסטים, בלוגים, אירועים, מדיה)**
  - לצערי כל החיפושים ברשת (באופני חיפוש שונים: philosophy of cyber security או philosophy of information security), במאגרים של מאמרים אקדמיים, מאמרים מסחרים לא מצאתי ולא מסמך אחד אשר מתייחס לנושא המרכזי של מסמך זה פילוסופיה של אבטחת הסייבר.
  - בדרך כלל השימוש במילה "פילוסופיה" היא במשמעות של "תפיסת עולם" או "מנטרות עבודה" ולא במשמעות של פילוסופיה כפי שהגדרתי בתחילתו של מסמך זה.
  - ברשתות החברתיות שנגישות לכלל הציבור בדגש על קהילות פייסבוק, לא הצלחתי לאתר דיונים או קבוצות בהן יש התעניינות בתחום שבו עוסק המאמר.

149 **Secure Access Service Edge (SASE)** – מסגרת לארכיטקטורת הגנת סייבר שמסופקות כשירות ענן, כוללת בתוכה מספר פתרונות הגנת סייבר, אבטחת מידע ותקשורת על מנת לאפשר גישה מאובטחת ומוגנת של עובדי החברה או ספקיה אל משאבי המחשוב (מערכות, יישומים, שירותים) של הארגון ללא מגבלה מה מיקום לקוחות הקצה או ההתקן ממנו הם מתחברים, וללא מגבלה היכן משאבי הרשת נמצאים (ענן ציבורי במודלים שונים, ענן פרטי , רשתות IT או OT מקומיות (On Premise).

6. <u>סיכום – האם לאנושות יש אינטרס לפתח פילוסופיה של אבטחת הסייבר כדיסציפלינה פילוסופית?.</u>

- היום כבר ברור לכולם כי התפתחות תחום אבטחת הסייבר הולכת וגוברת בחשיבותה עבור יחידים, עסקים ומדינות לאום. עם זאת, ההיבטים המשפטיים, האתיים, החברתיים, הסוציולוגים, הכלכליים, הגאופוליטיים והטכנולוגים של אבטחת הסייבר אינם מובנים היטב לשום גורם: ארגוניים גלובליים, אקדמיה, גופים ממשלתיים, גופי ביטחון המדינה, גופי מחקר בינלאומיים, חברות פרטיות ובוודאי שלא ידועות ומובנות בקרב הציבור הרחב.

- אנחנו כבר נמצאים במציאות שבה יש עליה מתמדת בשימושים של מרחב הסייבר, נכון לחודש אפריל 2022 נמצא כי מעל ל-63.1% מהאנושות כבר מחוברת באופן קבוע לרשת האינטרנט (מתוכם 59% הם חברים ברשתות חברתיות) [150], בנוסף מאז הרבעון הראשון של שנת 2020 קצב האימוץ הטכנולוגי של מסחר אלקטרוני ושירותים מתוקשבים נמצאים בצמיחה אקספוננציאלית [151], בנוסף קיימת תלות של 'הדור הדיגיטלי' בטכנולוגיה, כך שההתייחסות שלנו לטכנולוגיה שהיא חלק בלתי נפרד מגופנו (כולל תופעות המזהות כהתמכרות). כיום לא ניתן להתעלם מהתלות שלנו בתחום אבטחת הסייבר על מנת לקיים אורח חיים תקין, הן בגלל פשיעת סייבר על רקע כלכלי והן בגלל טרור קיברנטי שמהווה איום ממשי גם ברמת פגיעה בחיי אדם בודדים ואף פגיעה אוכלוסיות גדולות [152] , בל נשכח מלהזכיר שמספר ההתקפות הסייבר בשנתיים האחרונות נמצאות בעליה חדה ומתמדת כפי שלא חווינו מעולם.

- ארבעת אתגרים ראשיים עומדים בפני האנושות והם: שימוש בטכנולוגיה גרעינית, המשבר האקולוגי, האתגר הטכנולוגי, הבעיה הדמוגרפית הגלובלית. אני סבור שאין מחלוקת לקביעה הנחרצת, כי אם "האנושות" לא תיתן היום את דעתה והתייחסותה כבדת המשקל בנושא "האתגר הטכנולוגי" והשלכותיו באופן גלובלי, לא נוכל להבטיח את עתיד האנושות בעתיד.
ההשפעה של האתגרים הטכנולוגים מורגשת היטב כבר בהווה, במיוחד כאשר בוחנים תחומים של: פשיעה וטרור, שוק העבודה ותקשורת המונים. הדחיפות גבוהה היות וחלק גדול מההשפעות כפי שאנחנו חווים אותן כיום הן בלתי הפיכות, בטווח של 25 שנה מהיום.

- כאשר בוחנים איזה "כלים" יכולים לעזור ולהוות "גשר" על מנת להתחיל להבין עם מה אנחנו בעצם מתמודדים כשאר מדברים על "האתגר הטכנולוגי" בכלל הסוגיות הפילוסופית, האתיות, הגאו-פוליטית, המשפטית , הסוציולוגיות והכלכלית, **אזי** דיסציפלינה של **פילוסופיה של אבטחת הסייבר**, בשילוב עם **הפילוסופיה של הטכנולוגיה** (כמשפיעה עליה), **והפילוסופיה של המידע** (כמושפעת ממנה), יהיה אפשר לקבל סט כלים בעזרתו יהיה ניתן לבחון ואף להציע דרכים לפתרון של חלק מהבעיות המהותיות "באתגר הטכנולוגי" באופן גלובלי ובאופן לוקאלי.

- בזמן כתיבת מאמר דעה זה לא נחה עלי דעתי בשל שאלה אחת מאוד מטרידה שממשיכה להטריד אותי גם עכשיו ללא תשובה ברורה, למה תחום הפילוסופיה של הטכנולוגיה (כמעין "אב רוחני" של

---

150 מתוך דו"ח בשם **Worldwide digital population July 2022** פורסם בתאריך 20 ספט' 2022 באתר Statista "נכון לאפריל 2022, היו יותר מחמישה מיליארד משתמשי אינטרנט ברחבי העולם, שהם 63.1 אחוז מאוכלוסיית העולם. מתוך סך זה, 4.7 מיליארד או 59 אחוז מאוכלוסיית העולם היו משתמשי מדיה חברתית" , מקור – לינק.

151 **ברבעון ראשון של שנת 2020 קצב האימוץ הטכנולוגי של מסחר אלקטרוני ושירותים מתוקשבים במשקי בית בארה"ב הראה צמיחה אקספוננציאלית השווה באחוזים לצמיחה בעשור שקדם לו (2010 ועד 2020)** , הנתונים הם מתוך דוח מרוכז של רשות החדשנות לסיכום שנת 2020, בו הוצג סיכום של מספר דוחות שבוצעו על ידי גופי מחקר שונים בינהם: מקנזי, בנק אוף אמריקה, פורסטר, משרד המסחר האמריקאי, Shaw Spring.

152 **טרור קיברנטי, או "סייבר טרור"** , הוא מונח המתאר פעולות טרור הנעשות באמצעות לוחמת רשת, אם על גבי פלטפורמת רשת האינטרנט ואם על מערכות ממוחשבות אחרות. הגדרת הסייבר טרור – בדומה להגדרת המונח "טרור" – נתקלת בעמימות. מקור – לינק.

הפילוסופיה של אבטחת הסייבר), סובל מהתעלמות מבחינה אקדמאית, מחקרית ומסחרית כפי שתיארתי קודם לכן, זאת למרות שהוא החל דרכו מאז סוף מלחמת העולם השנייה ובאופן מקצועי ואקדמי עוסקים בו מעל 50 שנה. מי שמעוניין ללמוד את התחום באופן אקדמי (לפחות לפי בדיקה שערכתי לגבי האקדמיה בישראל), צפוי לגלות שאין מסגרות אקדמאיות שמתמחות או עוסקות בתחום.

- התמזל מזלי בזמן כתיבת המאמר (חודש נוב' 2022) זכיתי לפנות באופן אישי אל פרופ' יוסף אגסי, כמי שנחשב כפילוסוף הישראלי הראשון ובין הראשונים בעולם שעסקו באופן אקדמי ומעמיק בנושא של הפילוסופיה של הטכנולוגיה, **בשאלה** למה לדעתך הפילוסופיה של הטכנולוגיה לא התפתחה כפי שהתפתח התחום של הפילוסופיה של המדע ?, הפילוסופיה של המדע הוא תחום שנלמד באופן מעמיק במסגרת של מספר דיסציפלינות לימוד באקדמיה (קורס חובה בכל תואר במדעי הטבע או בכל תואר ראשון או שני בפילוסופיה) ואפשר ללמוד את הנושא גם בהרצאות לקהל הרחב שלא במסגרת אקדמית (כדוגמה קורסים והרצאות של ד"ר הנרי אונגר שהזכרתי לעיל). תשובתו של פרופ' אגסי היתה שבימי הבינים מי שעסקו בפיתוח חשיבה מעמיקה שהתפתחה גם למתודולוגיה פילוסופית כפי שאנחנו מכירים היום, היו אותם "בטלנים" בעלי ממון, שיכלו להרשות לעצמם לעסוק בלימודים ובהגות שלהם ולא לעבוד. אם פירשתי נכון את תשובתו של פרופ' אגסי כדי שתחום פילוסופי חדש יתפתח, חובה שתהיה קהילה שתפתח אותו, וזה לא יקרה אם לא יהיה מי שיממן את אותם "בטלנים" שיחקרו את הנושאים לעומק, ידנו ויעסקו בסוגיות ובבעיות שעולות מן הדיונים בתחום, וינסו להציע דרכים שונות להתמודד עם הבעיות שהתחום הפילוסופיה של אבטחת הסייבר עוסקת בהם. האתגר הטכנולוגי וכיוצא בזה גם **האתגרים והבעיות שבהן עוסקת הפילוסופיה של אבטחת הסייבר אינם "כוח עליון" שלא ניתן למנוע אותו** אלא רק להגיב ולטפל במידת האפשר אחרי שהאסון או האירוע מתרחש. ולמרות זאת, כיום אין גוף מרכזי, בינלאומי שמטפל בנושא עם שיתוף פעולה גלובאלי.

- במקרים שכן קיים שיתוף פעולה גלובלי, כדוגמת **תחום המשפט הבין לאומי פומבי** [153], ראינו שכאשר אין ברירה האנושות כן מתגייסת לשיתוף פעולה והתחייבות הדדית וגלובאלית, אולם מאידך נראה כי הדיון האם המשפט הבין לאומי חל במרחב הסייבר אינו מתקיים בזירה המשפטית הבין לאומית, אלא בזירה האקדמית, כך שלמרות יזומות בינלאומיות כמו מסמך "**מדריך טאלין**" [154] [155]

153 **משפט בין-לאומי פומבי** הוא הענף המשפטי העוסק בכללים המסדירים את פעולותיהם של שחקנים בזירה הבין-לאומית, מדינות, ארגונים בין-לאומיים ואף פרטים הנושאים באחריות בין-לאומית. תחום זה מסדיר את היחסים שבין מדינות, את השימוש בכוח ואת המנגנונים הבין-לאומיים ליישוב סכסוכים. מקור – לינק.

154 **מדריך טאלין** - המדריך נכתב בידי 20 מומחי משפט שעבדו בשיתוף פעולה עם **המועצה הבינלאומית של הצלב האדום ועם פיקוד הסייבר האמריקאי**. המומחים הוזמנו על ידי מרכז הגנת הסייבר המשותף בטאלין, בירת אסטוניה אשר התכנסה לטובת יצירת מסמך משפטי בדבר החלת הדין 26 ומכאן שמו. המדריך הינו תוצר הועדה CCDCE על לוחמה קיברנטית. תהליך כתיבת המסמך החל בשנת 2009 אך זה יצא לאור רק בשנת 2013 .מסמך זה הינו הניסיון הראשון לקבוע כיצד יש ליישם את החוק הבינלאומי על מתקפות סייבר. עם זאת יודגש, כי המדריך מסייע למשפטנים בהתמודדות עם הכלת הדין הבינלאומי הקיים למרחב הסייבר אך אינו מהווה מסמך רשמי ומחייב מטעם נאט"ו. המומחים מציינים במבוא כי במצב הקיים, קשה לקבוע באופן מוחלט כי קיימות נורמות של משפט בינלאומי מנהגי בתחום הקיברנטי. המומחים אינם טוענים שקביעת המדריך משקפות את המשפט הבינלאומי הקיים באופן שאינו מעורר מחלוקות, אלא משקפים באמצעות המדריך את הקונצנזוס בקרב המומחים באותה העת . .כמו כן, כתבו 27 המדריך קובע, כי ניתן לפתוח במלחמה קונבנציונלית בשל מתקפה על מערכות מחשב המשתתפים במתקפות מקוונות יכולים להיות מטרה חוקית 28 המומחים כי האקרים כדוגמת 'אנונימוס 'במהלך מלחמה, למרות שהם אזרחים. מקור: **מדיניות התגובה למתקפת טרור סייבר** | **אסף נקש** | המרכז הבינתחומי הרצליה | עמוד 9 , מקור – לינק.

155 **הפעילות במרחב הסייבר בראי המשפט הבין-לאומי** - מרחב הסייבר מאתגר את המשפט הבין-לאומי בכמה היבטים: ראשית, המשפט הבין-לאומי, על כל ענפיו, עוסק בעיקר בהסדרת היחסים הקשורים לגופים מוחשיים (גוף, נכסים, קרקע). לעומתו, מרחב הסייבר אינו מוחשי. כתוצאה מכך מתעוררת השאלה אם הנורמות הקיימות במשפט הבין-לאומי מתאימות למרחב זה, או שיש צורך בעיצוב נורמות חדשות; שנית, המשפט הבין-לאומי מבוסס באופן ספציפי על חלוקה טריטוריאלית: הזירה העולמית מחולקת לשטחי אדמה — מדינות — ודגש רב מושם על חלוקת הסמכויות והזכויות — ריבונות. לעומת זאת, עולם הסייבר הינו במהותו חוצה גבולות; שלישית, המשפט הבין-לאומי מבוסס באופן מסורתי על עליונות המדינות כשחקניות בזירה הבין-לאומית: להן יש זכויות, והן נושאות באחריות. נדמה שבתחום הסייבר המדינות אינן השחקניות המרכזיות. הבדלים אלה מעוררים שאלה בסיסית: האם המשפט הבין־לאומי חל במרחב הסייבר? העיסוק בשאלה זאת מתקיים בעיקר בזירה האקדמית. מדריך טאלין הראשון, **מסמך שניסחה קבוצת אנשי אקדמיה והתפרסם בשנת 2013** ,התמקד בשאלה כיצד ניתן להחיל את המשפט הבין־לאומי על מרחב הסייבר, בראש ובראשונה בהקשר של פעולות המהוות הפרה של האיסור על שימוש בכוח ושל הזכות להגנה עצמית, או פעולות המתרחשות במהלך סכסוך מזוין. **מדריך טאלין השני מ־2017** הרחיב את הדיון בסוגיה זאת לשאלת התחולה של המשפט הבין־ לאומי על פעולות שאינן מגיעות לכדי שימוש בכוח או למצב של סכסוך מזוין בזירה המדינית.

מסמך שמנסה להתמודד עם השאלה ולהציע הצעות ופשרות, כיצד להחיל את המשפט הבינלאומי על מרחב הסייבר, נדמה כי גם כאשר יש פתרונות ותשובות, הן לא מוצאות את דרכן לגוף שיש ביכולתו להביא אותן לידי מימוש. במאמר של **פרופ' יעל רונן** העוסק בנושא "הפעילות במרחב הסייבר בראי המשפט הבין-לאומי" מצוין שבשנת 2015 במסגרת קבוצת מומחים ממשלתיים שהתכנסה באו"ם, הושגה הסכמה לפיה מגילת האו"ם חלה במלואה גם במרחב הסייבר. הקבוצה כללה, בין היתר, מומחים מארצות הברית, בריטניה, רוסיה וסין, שהן השחקניות הראשיות בזירה הבין־לאומית בתחום זה. אולם כמו שאנחנו רואים היום הלכה למעשה, זה ממש לא מפריע לאותן מדינות שחתומות על המסמך להפעיל באין מפריע יחידות צבאיות שעיקר פעילותן היא סייבר התקפי, יחידות צבאיות שפועלות לא בהכרח למטרות של התגוננות (אפשרות הגנה עצמית כפי שבא לידי ביטוי בסעיף 15 במדריך טאלין) אלא למטרות של איסוף מודיעין, ריגול, פגיעה מכוונת בתשתיות של מדיניות שונות (גם לא בזמן מלחמה או סכסוך).

- לסיכום אני חייב להודות שגם לאחר "מסע אדפטיבי" בו ניסיתי להבין טוב יותר את: המורכבות של מרחב הסייבר, המורכבות בתחום אבטחת הסייבר, המורכבות בתחום הפילוסופיה (מדע, טכנולוגיה, מידע, אתיקה), מהם האתגרים הגלובליים של האנושות בדגש על "האתגר הטכנולוגי", מהם התחומים \ האתגרים \ הבעיות שבהן צריכה לעסוק הפילוסופיה של אבטחת הסייבר, ניסיון להבין את המורכבות למי יש אינטרסים (או צריך שיהיה לו כאלה) על מנת להבנות את תחום הפילוסופיה של אבטחת הסייבר, להבין את המורכבות מה צריך לעשות כדי שכן תתגבש דיסציפלינה של הפילוסופיה של אבטחת הסייבר, בסופו של דבר נשארתי עם הרבה יותר שאלות מסובכות שאין לגביהן תשובה ברורה מאשר השאלות שהיו לי בתחילת הדרך.

- באופן אישי כריאליסט אני רוצה להאמין שבסופו של דבר (ונקווה שלא יהיה זה מאוחר מידי) האנושות תבין עד כמה התלות שלה בטכנולוגיה מהותית להמשך קיום האנושות, והתלות בטכנולוגיה כוללת בתוכה גם את התלות במרחב הסייבר (שהיום הוא צורך בסיסי של האנושות כמו מים ומזון) ובתוכו תחום אבטחת הסייבר שמנסה לעמוד באתגר ולמנוע את קריסתו של מרחב הסייבר להיות "תוהו ובוהו", כך שזה הופך אותו לתחום מהותי להמשך קיום הסדר בקרב הציוויליזציה האנושית. **הפילוסופיה של אבטחת הסייבר** יכולה להיות התחלה לבסיס שבו יהיה ניתן לעסוק באותן שאלות קריטיות הרות גורל שמשפיעות וימשיכו להשפיע על כלל האנושות.

אני תמיד שמח לקבל הארות, הערות ורעיונות. גם ביקרות ומחלוקת היא דרך נפלאה בעיני ללמוד ואפשר בעזרתה להרחיב את ידיעותיי, אני מאמין גדול במימרה ש "**ידע הוא כוח, אך ורק אם חלקת אותו עם אחרים**", כך שאני תמיד שמח לשמוע מכל מי שנחשף וקרא, ויש לו מה לשתף איתי. בברכה , הילל קוברובסקי
Hillel@Innovateordie.co.il | (וצאפ) 054-7700919 | LinkedIn: Hillel Kobrovski

תודה לכל מי שהיווה השראה למאמר זה, הם\ן מוזכרים\רות לאורך כל המאמר. תודה מיוחדת למוריי בתחום הפילוסופיה: הפילוסוף והפיזיקאי **פרופ' יוסף אגסי** ו**ד"ר רמי ישראל**, שפתחו בפני ערוץ חשיבה חדש לבחון את "עולם הסייבר" מזווית חשיבה פילוסופית שלא נחשפתי אליה עד לפני שהכרתי אותם.

העיסוק של מדינות בתחולת המשפט הבין-לאומי במרחב הסייבר נותר מצומצם. אחת הסיבות לכך היא שהטכנולוגיה מאפשרת חדירה לתחומים רגישים ,שבהם ממשלות נזהרות מלהתבטא. למרות זאת, יש כיום קונצנזוס שהמשפט הבין-לאומי חל גם על מרחב הסייבר. אחת ההתפתחויות הבולטות בהקשר זה היא ההסכמה שהושגה ב־2015 במסגרת קבוצת מומחים ממשלתיים שהתכנסה באו"ם, לפיה מגילת האו"ם חלה במלואה גם במרחב הסייבר. הקבוצה כללה, בין היתר, מומחים מארצות הברית, בריטניה, רוסיה וסין, שהן השחקניות הראשיות בזירה הבין-לאומית בתחום זה. להסכמה שהושגה ביניהם יש משמעויות שונות ,שכמה מהן יפורטו להלן. | מקור : סייבר מודיעין וביטחון | כרך ב' | גיליון 3 | דצמבר 2018 | **פרופ' יעל רונן** , המרכז האקדמי שערי מדע ומשפט | המסמך המלא – לינק.