תופעת הסייבר – מווייז ועד סטקסנט

הצעה לקורס לתואר שני במב"ל – תש"פ 2020

פרופסור אביתר מתניה

ביה"ס למדע המדינה ממשל ויחב"ל באוניברסיטת ת"א

המקים ולשעבר ראש מערך הסייבר הלאומי (2012 – 2017)

מבוא

אנו עדים לתופעה חדשה: **תופעת הסייבר**. תופעה שהתחילה ממש בסוף המאה הקודמת ושנוצרה מהקישוריות הכמעט טוטאלית של רשתות מחשבים ותקשורת, חיבור האינטרנט לכמעט כל פינה ואדם בעולם, מהירות העיבוד המאפשרת זרימה אדירה של נפחי מידע, הוזלה של רכיבי חישוב וזיכרון והיכולת לאגור מידע ולעבדו בכמויות בלתי נתפסות.

כל אלו הביאו לשינוי של עולם התעשייה, פני הכלכלה, מרקם החיים, ובכלל זה גם איומים חדשים (איום הסייבר), והם משפיעים על מכלול חיינו, כפרטים, כחברה וכמדינה.

ניתן להשוות את השלכותיה של **תופעת הסייבר** להשלכותיה של המהפכה התעשייתית: כשם שהמהפכה התעשייתית שחררה את האדם מכבלי "כוח ידיו", והשפיעה השפעות מרחיקות לכת על האנושות, כך מהפכת הסייבר משחררת את האדם מתלות במרחב הפיסי בלבד, ומעבירה חלק ניכר מהפעילות האנושית למרחב וירטואלי. תוך עשורים בודדים החברות הגדולות בעולם הן חברות מתחום הסייבר-דיגיטל, ולא חברות של העידן התעשייתי, עימותים מתרחשים יותר ויותר בשימוש ברשתות חברתיות ומערכות מיחשוב. וזאת רק ההתחלה: אנו מתקדמים בצעדי ענק לפיתוח של טכנולוגיות בינה מלאכותית מבוססות נתוני עתק, שהיכולת להגיע אליהם, לכרות אותם, לנתח אותם וליצור מהם תובנות שלא נמצאות באף אחת מנקודות הקצה שלהן – יכולת זו היא תוצאה של **תופעת הסייבר** – הקישוריות הטוטלית ויכולת המחשוב.

דא עקא, השפעתה הרוחבית של תופעה זו מחייבת שליטה והבנה לא רק בדיסציפלינות הטכנולוגיות, אלא גם בהיבטים האסטרטגיים שלה. שליטה כזו בתחומים אלו היא קריטית ליכולתם של מנהלים ומקבלי החלטות בעולם הציבורי והביטחוני כאחד להוביל בבטחה את עשייתם ואת ארגוניהם בעידן הפוסט תעשייתי הזה – עידן הסייבר.

המטרות האקדמיות של הקורס

1. הרחבת אופקים בתחומי הדעת של הסייבר שאינם טכנולוגיים גרידא.
2. פיתוח ראייה מערכתית של איום הסייבר והגנת הסייבר בכלל הרמות – הלאומית, המגזרית והארגונית.
3. הענקת כלים להובלה ולהנהגה של פרטים, חברות וממשלות בעידן הסייבר.

המודולים המרכזיים

1. הדואליות של הסייבר – מרחב ותופעה: כלכלה חדשה, השטחה חברתית, איומים חדשים.
2. עצמה בסייבר: הסייבר כמרחב לחימה, תמרון ואש בסייבר, עליונות.
3. הטופולוגיה של הסייבר: סוגי תקיפות והגנה, תקיפות מתקדמות, חולשות, חיסון, ניתוח מקרים.
4. הגנת הסייבר: האבולוציה של האיום, עקרונות ההגנה – שלוש השכבות, מהארגון ועד למדינה.
5. המקרה הישראלי: אסטרטגיה לאומית, החלטות ממשלה, מדיניות ציבורית, הסייבר כמנוף מדיני.
6. סוגיות: דמוקרטיה בעידן הסייבר, המאבק על האמת, בינה מלאכותית וסייבר. לאן הולכים מכאן?

אופן ההעברה

4 ימים מרוכזים של 3 יחידות אקדמיות (שעה וחצי כל יחידה).

הקורס יועבר בעברית. השקפים יהיו חלקם באנגלית וחלקם בעברית (בהתאם לנושא).

אופן ההערכה

מבחן סיום.