סיכום הרצאתו של אל"מ במיל. דרור בן דוד בנושא סייבר, בינה מלאכותית והמעשה המודיעיני

ביום רביעי, ה-20.11.19, התקיימה במרכז למורשת המודיעין הרצאתו של אל"מ במיל. דרור בן דוד בנושא סייבר, בינה מלאכותית, הממשקים ביניהם והקשר שלהם למעשה המודיעיני. בהרצאה נכחו עשרות רבות של משתתפים. במהלך ההרצאה תוארה הגדרת הסייבר; הוצגו ההגדרות השונות לבינה מלאכותית; והוסבר הקשר בין השניים לבין ההשלכות האפשריות על המעשה המודיעיני.

סייבר

הסייבר עוסק בשני מושגים מרכזיים- נגישות וחולשות. נגישות למכשיר היעד (פלאפון, מחשב וכיו"ב של היריב), על מנת להכניס אליו קטע קוד שישרת את צרכי המפעיל. זאת, על ידי ניצול חולשות במכשיר, כך שהפעולה תוכל להיות מבוצעת מבלי שהצד השני יידע.

פעולת סייבר יכולה לשרת צרכים מגוונים. איסוף מודיעין חשאי ומותמם; סייבר להגנה על תשתיות או ישויות מפני התקפות סייבר; וסייבר להשפעה יכול לשמש במסגרת המערכה על התודעה (דוגמה טובה לכך היא בחירות 2016 בארה"ב). סייבר יכול לשמש גם לתקיפות פיזיות, בנקודות החיבור של תשתיות אלקטרוניות עם חומרות פיזיות. יתרונותיו המרכזיים של הסייבר הם מגוונים-

- הסייבר לא מוגבל בטווח. בניגוד לפעולה צבאית קינטית, פעולת סייבר יכולה להיות מבוצעת מכל מקום ולעבר כל מקום.
- הסייבר מבוצע באופן מותמם, כך שבפועל הוא כמעט אנונימי. מאוד קשה לייחס פעולת סייבר מסוימת לגוף או לאדם מסוים.
- לא פעם קשה לזהות שהייתה תקיפה, היות שהפעולה מבוצעת על ידי ניצול חולשות.

הבינה המלאכותית

אין הסכמה מלאה על הגדרת הבינה המלאכותית, ומה בינה לבין הגדרות קרובות כמו למידת מכונה. ישנן מספר הגדרות כלליות שמסבירות מה עושה הבינה המלאכותית-

- פעולה באמצעות מחשב שאם אדם היה עושה היינו טוענים שזו פעולה של אדם אינטליגנטי.
- עיבוד כמויות גדולות של מידע והפקת ידע חדש מתוכו.

- ביצוע פרדיקציות (הערכות) על בסיס מסד הידע הקיים.
- רובוטיקה. לדוגמה- בוט שכותב כתבות עבור העיתון וכיו״ב.

באופן סכמטי אפשר לטעון שיש שתי דרכים מרכזיות שעל בסיסן עובדת הבינה המלאכותית-

א. פידבק- מציגים בפני האלגוריתם דוגמאות רבות ומגוונות של מאורע מסוים, ומסבירים לו מה התוצא הרצוי עבור כל אחד מהמאורעות. האלגוריתם מייצר רשת נוירונים ומשנה אותה אחרי כל דוגמה, עד שהיא משרתת את התהליך הניתוחי בצורה מיטבית.

ב. תמריצים- במקום להציג לאלגוריתם דוגמאות, אפשר לתת לו לרוץ פעמים רבות, כשבכל פעם הוא מקבל החלטות באופן שרירותי על בסיס קומבינטוריקה. עבור כל תוצא, אפשר להגדיר לו האם מדובר בתוצא רצוי או לא. לצורך העניין, רובוט שלומד לשחק משחק. הוא ייבחר את צעדיו באופן שרירותי, ואנחנו נגדיר לו האם המהלך שביצע קידם אותו לעבר המטרה או לא.

בעבר ניסו לבנות רובוט שיודע לפתור משוואות או לחקות פעילות מוטורית על בסיס הגברת יכולות העיבוד. היום, לא מנסים לחקות את הפעולה, אלא מנסים לחקות את שיטת החשיבה ולתרגל מספיק על מנת שיצליח. לא מקודדים, אלא נותנים למערכת ללמוד. למעשה אי אפשר לחזות מה היא תעשה בהינתן סיטואציה מסוימת.

<u>ההשלכות על המעשה המודיעיני</u>

הבינה המלאכותית יחד עם הסייבר ובתוספת מספר מגמות גלובאליות, גוזרות מרחבי השפעה ופעולה אדירים. בשורה התחתונה זה מעצים עשרות מונים את המודיעין לא רק כמוסד לבירור המציאות, אלא גם כאופרטור שמפעיל כוח. איך זה ייראה בפועל?

בשלב הראשון- human-machine teams. הרעיון הוא לבנות סוכני בינה מלאכותית שמסייעים לעוסק במודיעין לבצע את עבודתו. כך למשל, המכונה יכולה לרוץ על מסד מידע ענק, להציף אירועים שהיא חושבת שיכולים להיות מעניינים והאדם יבחן את המאורעות ויסיק מסקנות.

בשלב השני- מדיניות רחבה. אם מדינת ישראל תשכיל להסדיר מדיניות רחבת היקף שכוללת את מערכת הביטחון, האקדמיה והמגזר הפרטי בנושא הבינה המלאכותית, היא יכולה להיות פורצת דרך ולהוביל את התחום ברמה הגלובאלית.