

Generative AI וביטחון לאומי – סיכום כנס

ענבר נוי-פרייפלד, לירן ענתבי, ירדן אסרף | 14 באוגוסט, 2023

ב-30 ביולי 2023 התקיים במכון למחקרי ביטחון לאומי כנס בנושא בינה מלאכותית יוצרת (Generative AI) והשפעתה על הביטחון הלאומי. בינה מלאכותית יוצרת הינו תת-תחום של טכנולוגיות בינה מלאכותית אשר מתייחס ליצור סוגי תוכן כמו טקסט, אודיו ותמונות בשימוש אלגוריתמים של בינה מלאכותית. בכנס נטלו חלק אישים מתעשיית ההייטק, האקדמיה והביטחון, שדנו בהרחבה על אודות השפעתן של ההתפתחויות האחרונות בפיתוח Generative AI, ובכללן הדיפ-פייק, על צה"ל, מעמדה הטכנולוגי של ישראל, התחרות הבין-מעצמתית, וכן רגולציה ותפקיד הממשלה בישראל בהתמודדות עם האיומים הביטחוניים הנובעים ממגמות אלה. מנהל המכון, פרופסור מנואל טרכטנברג, דיבר בפתיחת הכנס על ההבטחה שבהתפתחויות בתחום ה-Generative AI, שהתחדדה וגברה עם הפיתוח וההפצה של Chat GPT. עם זאת, בדבריו הודגש הצורך לפקח על היבטים שליליים של התפתחויות בתחום באמצעות רגולציה. דאגה זו השמיעו בכירים נוספים מתחום הטכנולוגיה, שהשתתפו בכנס. פרופ' טרכטנברג סיכם את דבריו בכך שעל ישראל להיות בחזית פיתוחי טכנולוגיות בינה מלאכותית, ושנוכח גודלה ומגבלותיה של המדינה עליה להעדיף איכות על פני כמות תוך שימור הכוחות הצעירים העוסקים בתחום, שהם נכס שאין לו תחליף.

תובנות מרכזיות

הדוברים בכנס והמשתתפים במושב השיח התייחסו לאתגרים הניצבים בפני ישראל בהקשרי טכנולוגיות בינה מלאכותית והעלו הצעות למדיניות כמענה להם, בפרט ביחס לביטחון הלאומי: התחרות הבין-מעצמתית ומעמדה של ישראל; משמעויות לצה"ל; תפקיד הממשלה; הזירה האזרחית; וסוגיות ביטחוניות לאומיות שאינן תחת אחריותו או אחריותו הבלעדית של צה"ל (כגון מבצעי השפעה).

התחרות בנושא הבינה המלאכותית ומעמדה של ישראל

ישראל מתקשה לעמוד בקצב המרוץ העולמי בכל הקשור להשקעה כספית ופיתוח של פרויקטים בתחום הבינה המלאכותית, ואף נמצאת בתחרות מול שכונותיה ומדינות נוספות במזרח התיכון. לפי נתוני [Global AI Index](#), מרבית המדינות המובילות בעולם עוסקות בפיתוח בינה מלאכותית ולמרבותן גם במידה כזו או אחרת אסטרטגיה בתחום. מרבית התקציב

בישראל מושקע בתשתיות חישוביות בעוד התכנון האסטרטגי והתקצוב של פיתוחי טכנולוגיות בינה מלאכותית נשך מאחור ביחס למדינות אחדות.

איחוד האמירויות היא בין המדינות המובילות באזור המזרח התיכון ובעולם בהשקעת משאבים בפיתוח יכולות בינה מלאכותית. היא השקיעה רבות בפיתוח טכנולוגיות, מחקר אקדמי ומודלים מתחרים ל-Chat GPT. איחוד האמירויות גם נמנית על המדינות המובילות בהטעמת בינה מלאכותית בשירותים הממשלתיים הניתנים לאזרחים ולתושבים. מדינות נוספות באזור – ערב הסעודית ומצרים משקיעות אף הן משקיעות בתחום הבינה המלאכותית. ערב הסעודית מדורגת ראשונה באינדקס של שנת 2023 בתחום האסטרטגיה הממשלתית בתחום. (המובילה העולמית במדרג הכולל, ארצות הברית, מדורגת במקום השמיני). עם זאת, ערב הסעודית סובלת ממצוקת הון אנושי בתחום לעומת איחוד האמירויות, המעניקה ויזות לחוקרים זרים כדי להתגבר על המחסור המקומי. ישראל ירדה השנה שני מקומות בדירוג הכללי באינדקס ועלולה להמשיך להידרדר, בעיקר עקב היעדר מדיניות ותקצוב ממשלתיים מספקים. נושא זה זכה לתשומת לב מחקרית נרחבת בפרסומי המכון בחמש השנים האחרונות.

אחד החסמים המרכזיים בנוגע למעמדה של ישראל בתחום הבינה המלאכותית הוא המחסור בתשתיות, הן מבחינה לאומית והן מבחינת צה"ל. ישראל נמצאת מאחור ביחס למדינות אחרות המשקיעות בקניית חומרה וגיוס מוחות מהאקדמיה. ישראל נשרכת מאחור גם בהתייחסות לאתגרים המשפטיים והמוסריים הנוצרים עקב שימוש בטכנולוגיות בינה מלאכותית ובטיפול בהם ברמה הממשלתית ובכלל.

צה"ל והבינה המלאכותית

בכנס נדון בהרחבה נושא פיתוחן והטמעתן של טכנולוגיות בינה מלאכותית ביחידות צה"ל. נוכח המחסור בתשתיות ובמשאבים צה"ל, ובפרט יחידה 8200, אינם עומדים בחזית הטכנולוגיה ברמה הלאומית, כפי שהורגלנו למשל בתחום הסייבר, אלא נעקף על ידי האקוסיסטם האזרחי. הפיגור נובע בין היתר מהיות צה"ל גוף גדול ובירוקרטי, המתקשה להגיב במהירות לקצב השינויים המהיר בתחום.

אתגרים המגבילים הטמעת בינה מלאכותית בצה"ל בקצב ובעוצמות הנדרשות:

- **ייעול תהליכים ושינוי מבנים** - בעוד שבצה"ל מתנהלת חשיבה במבנים מוכרים, הטמעת בינה מלאכותית דורשת לייעול **ולשנות** תהליכים ומבנים קיימים בעוד יכולת הארגון ואנשיו אשר רגילים למצב הקיים לרכוש מבנים חדשים עלולה להתברר כנמוכה.
- **פער ביחס לעולם ולזירה האזרחית** - בשונה מהמתרחש בתחום הסייבר, צה"ל אינו מוביל בתחום הבינה המלאכותית ביחס לזירה האזרחית וביחס למדינות אחרות בעולם.

הסיבות לכך הן מחסור במשאבים וקושי להתחרות על המשאב האנושי (מכאן נובעת גם השפעה על האקוסיסטם, שכן בשונה מתחום הסייבר, הצבא אינו מכשיר אנשי מקצוע בעלי ידע בתחום הבינה המלאכותית, הרלוונטי לאזרחות).

- **סכנות באימוץ בינה מלאכותית** - למרות המאמץ לאמץ ולהטמיע טכנולוגיות בינה מלאכותית בשורות צה"ל במהירות, ברי כי הישענות נרחבת עליהן, בהיותן טכנולוגיות מחשוב, עלולה ליצור אתגרים של תלות ופרצות אפשריות לתקיפה על ידי יריבים. לכן יש לאמץ רגולציות ואסטרטגיה הולמת. צה"ל פועל בהקשר זה בזהירות הנדרשת, אך קצב האימוץ וההטמעה איטי.
- **שינוי ארגוני וקושי למדוד תועלת** - צה"ל נוטה בדרך כלל לבחון הטמעה של טכנולוגיות בארגון הקיים באמצעות מדידת יעילותן הפוטנציאלית. אולם עקב השינויים המשמעותיים הגלומים בהטמעת טכנולוגיות בינה המלאכותית, יש צורך בשינוי ארגוני נרחב יותר על מנת להפיק ממנה תועלת מקסימלית, מה שלעיתים קרובות מעורר התנגדות וחסמים ומקשה על הצגה או מדידה מתאימה של הפוטנציאל.
- **מידור ומחסור בשיתוף לרוחב מערכת הביטחון** - מאפיינים אלה של המערכת באים לידי ביטוי בפיתוח מערכות דומות בארגונים שונים ובהיעדר שיתוף תובנות לגבי תהליכים והטמעה, וכן בחוסר יכולת של בעלי תפקידים לנוע לרוחב הארגונים במובן מסלול קריירה והמשמעויות של העברת ידע בין ארגונים. פוליטיקה בין-ארגונית, מידור וביטחון מידע מקשים מאוד גם על שיתוף ידע עם גורמים אזרחיים ועם האקדמיה. במקומות מסוימים במערכת, כגון באמ"ן הודגמו מודלים המאפשרים פתרון של חלק מבעיות אלה, אך הם לא מיושמים בהרחבה.

הממשלה ובינה מלאכותית

תפקידם של מקבלי ההחלטות ומשרדים ממשלתיים בנוגע למדיניות ישראלית בתחום הבינה המלאכותית:

- **ניכר צורך בשיתוף פעולה** משמעותי יותר מאשר כיום בין תעשיות ביטחוניות, אזרחיות והממשל, בכל הנוגע לניסוח ויישום מדיניות לאומית לגבי לבינה מלאכותית.
- **הכרה ממשלתית בפוטנציאל הטכנולוגיה לשימוש אזרחי** - לבינה מלאכותית פוטנציאל לתת מענה כמעט בכל תחומי החיים. ישראל היא אומנם מהמובילות ביישומים בתחום היבטחוני, אולם הפוטנציאל נרחב בהרבה ואינו מנוצל. היעדר תשתית ומדיניות מתאימה מותיר את משרד הביטחון המוביל המרכזי של התחום (מבחינת תקציבים וניהול) והפער מול תחומי החיים האחרים הולך וגדל. כך עלולה ישראל, על פי מדדים בינלאומיים שונים, להישאר מאחור גם בזירה זו, שכן הפער יגיע

לכדי מצב שמשדד הביטחון אינו יכול לצמצמו או לכסות עליו. לכן, על הממשלה לשנות מהותית את סדר העדיפויות בנושא ולהקצות לו מינויים ותקציב הולמים.

- **מינוי בעלי תפקידים** – למרות השחיקה במעמדה בשנים האחרונות, ישראל עדיין מן המובילות הטכנולוגיות בתחום. יחד עם זאת גם במימוש הקיים, ניכר חוסר תיאום בין הגורמים הרלוונטיים השונים, ולכן יש צורך לרכז את קידום הנושא על ידי הממשלה. כפי שבאיחוד האמירויות מכהן שר הבינה מלאכותית, גם בישראל יש צורך להכיר בחשיבות הנושא ולקדם מינויים ממשלתיים שיספקו מענה להיבטים רחבים של ביטחון לאומי.

- **מאיצי פיתוח** – אחת ההצעות שעלו במהלך הכנס הייתה לפתח מעין "פרויקט מנהטן" בתחום הבינה המלאכותית בארץ – לא רק על מנת לנסח מסמכי מדיניות, אלא לגייס מומחים ולאפשר להם לבחון יחדיו אפשרויות לפיתוח ולשימוש בבינה מלאכותית.

- **שיתופי פעולה** – יש לבחון ולהשקיע בקידום שיתוף הפעולה עם איחוד האמירויות, מעבר למה שמתקיים כיום, תוך חיזוק "הסכמי אברהם" והיחסים בין המדינות. ניתן למשל ללמוד מיצירת מודלים של שפה באמירויות, כפי שנוצרו בערבית, משום שעניין העברית מהווה כיום אחד החסמים המרכזיים להטמעת בינה מלאכותית בשירותי ממשלה לאזרחים.

- **הטמעת בינה מלאכותית במשרדי ממשלה** – נושא ההטמעה זוכה בתקציב מצומצם. לכן עלתה בדיונים שנערכו בכנס החשיבות של תיעדוף התקציב על פי סדר עדיפויות לאומי של הפרויקטים בין המשרדים השונים. (הוזכר כי הקצאה של כשני מיליארד ש"ח לנושא ידרוש שינוי תיעדוף בתקציב הלאומי.) כן הודגשו הקושי לגייס כוח אדם מתאים, החשיבות של בחינת פרויקטים מעמיקה ותיעדופם, ובנוסף צורך להשקיע משאבים בשיתוף פעולה עם האוניברסיטאות.

- **משפט ורגולציה** – היבט זה של התאמה לבינה המלאכותית הוצג בכנס כמשתרך מאחור. עלתה המלצה לייצר פתרונות, גם אם יהיו בלתי מושלמים, וליישם תוך למידה, חיכוך עם השטח ושינוי. המלצה נוספת הייתה לשפר את שיתוף הפעולה עם מדינות אחרות שהתקדמו בנושא, כדי לקדם למידה מהן.

השפעות על שוק העבודה

השפעות אחריות של הבינה המלאכותית בהווה ובעתיד, בעיקר על שוק העבודה נדונו בכנס ממספר כיוונים.

- **בינה מלאכותית לכל עובד** – לנוכח חסמים שונים וביניהם בירוקרטיה ושמרנות, על מנת להטמיע במידה נרחבת את הבינה המלאכותית בשוק העבודה וכדי שכוח

העבודה ייערך להתמודדות עם האתגר, יש לקדם הכשרה בתחום הן בארגונים עצמם והן בבתי הספר וביחידות צבאיות.

- **ביקורתיות ואחריות בשימוש בבינה מלאכותית** - הן בעלי תפקידים ונושאי משרות והן "האדם הפשוט" או כל עובד/ת במשק, זקוקים כיום לחשיפה נרחבת יותר לאתגרים הגלומים בשימוש בבינה מלאכותית. בקרב נושאי המשרות מדובר ביכולת להפעיל ביקורתיות ולפעול באחריות, ובקרב האזרחים מדובר באוריינות טכנולוגית, שתשפיע על שוק העבודה וגם על חיי היום יום. בין הדוגמאות שניתנו במהלך הדיונים בכנס: ביקורתיות כלפי תשובות שמקבלים מכלים דוגמת Chat GPT או התמודדות עם סרטוני דיפ פייק.

- **הסבות מקצועיות** - קיים חשש שמהפכת הבינה המלאכותית תייתר מקצועות מסוימים, ולכן יש להיערך להסבת בעלי מקצועות אלה לתחומים אחרים. חוסר היערכות עלול לגרום אבטלה גבוהה, בעוד הסבות מקצועיות על חשבון המדינה לאפיקי תעסוקה רלוונטיים לעידן החדש עשויות להגביר פריון.

אתגרים ביטחוניים ובינה מלאכותית

בכנס נדונו בהרחבה אתגרים ביטחוניים הקשורים לבינה מלאכותית בכלל ויוצרת בפרט.

- **דיפ-פייק ומבצעי תודעה** - אחד האתגרים שצוינו הוא היכולת לייצר באמצעות כלי בינה מלאכותית יוצרת טקסט, תמונה ווידאו מזויפים במסגרת מבצעי השפעה. מכאן צורך דחוף בטיפול לאומי שישלב חקיקה ורגולציה, וכן חינוך לביקורתיות של האזרחים לצד היכרות עם התופעה. בנוסף נדרשת הסדרת היחסים עם החברות הטכנולוגיות המובילות בתחום, לשיתוף מידע משמעותי.

- **משאבי האנוש כצוואר בקבוק מתהדק** - אחד האתגרים המשמעותיים בהקשר הביטחוני הוא משאבי האנוש כצוואר בקבוק, לצד התשתיות הלאומיות החסרות. ניכר כי מעמדה הנשחק של ישראל בתחום הבינה המלאכותית ביחס למדינות אחרות עלול להוות אתגר משמעותי בזירה הביטחונית, שישראל הייתה רגילה להסתמך בה על עליונות טכנולוגית. לאתגר זה יש להידרש ברמה הלאומית, לא ברמת משרד הביטחון והצבא בלבד. העוסקים בתחום משתייכים לקבוצה איכותית, שמניעה לעיסוק בבינה מלאכותית ולשיתוף פעולה עם משרד הביטחון או עבודה במערכת הביטחונית כוללים תחושת שליחות וזהות אינטרסים. מניעים אלה עלולים להיפגע עקב המשבר החברתי-פוליטי הפוקד את מדינת ישראל בימים אלה. גם בארצות הברית, למשל, נרשם קושי להוציא לפועל פרויקטים עקב חוסר שיתוף פעולה מצד כוח אדם מיומן בתחום.

סיכום

את הכנס סיכום מנהל המכון, אלוף (מיל') תמיר הימן, שהתייחס בתחילת דבריו לתשתיות בתחום הבינה המלאכותית וציין כי קיימת חולשה ישראלית בתחום, מה שדורש תכנון ארוך טווח ויציבות שלטונית - סוגיות חלשות במנגנון הישראלי. האלוף הימן טען כי צה"ל אינו מוביל בישראל את תחום הבינה המלאכותית כשם שהוא מוביל בסייבר, וכי נדרשת בהקשר זה התערבות לאומית שכן הבעיה אינה ניתנת לפתרון על ידי הצבא לבדו. על סמך תובנות שהוצגו בכנס, האלוף הימן הדגיש שנדרש גיבוש אסטרטגיה ממשלתית ותכנית לאומית, שיקדמו את תחום הבינה המלאכותית בישראל לשלב הבא.

בפני ישראל עומדים בהקשר זה מספר אתגרים: הראשון הוא בתחום הכלכלי-חברתי - השינויים וההתקדמות בתחום בינה מלאכותית יוצרת מהירים מקצב החינוך והרגולציה, ולכן עלולים להעמיק את השסעים הכלכליים והחברתיים הקיימים. השני הוא בתחום הביטחוני והוא נוגע למעמד היורד של ישראל בתחום הטכנולוגי ובה בעת לסיכון שברשות איראן יהיו יכולות טכנולוגיות מתקדמות. טכנולוגיות בינה מלאכותית עלולות לחולל שיבושים ניכרים במערכות שצה"ל עתיד לבסס עליהן את יכולות הלחימה שלו, בדגש על מערכות חצי-מאוישות ביבשה. השלישי הוא נושא התודעה. באמצעות מבצעי השפעה זרה הכוללים דיפ-פייק ניתן ליצור נרטיב שקרי, כשהצרכן אינו יכול לזהות מיהו יוצר הנרטיב ואת השקר עצמו. יכולות בינה מלאכותית אלו עלולות להיות מנוצלות להעמקת הקיטוב הקיים בחברה הישראלית.

דברי הסיכום נחתמו בהמלצה לכוון מדיניות ממשלתית נרחבת, שתכוון למיצוי הפוטנציאל שבטכנולוגיות הבינה המלאכותית מחד גיסא, ותמפה את האיומים הגלומים בהן ותציע דרכים להתמודד עימם מאידך גיסא.

עורכי הפרסום: ענת קורץ ואלדד שביט