

תקציר מנהלים

בינה מלאכותית וחיבורה עבור הביטחון הלאומי של ישראל

בינה מלאכותית היא שם כולל למערכות מחשב מבוססות נתונים, שמסוגלות להפיק ידע ותובנות חדשים באמצעות יכולות כמו הבנה, הנמקה ותפיסה – שעד כה נתפסו כיכולות הייחודיות לבני אנוש.

הבינה המלאכותית מאפשרת לממש יכולות אלה במגוון יישומים ביעילות יחסית, במחיר סביר ובקנה מידה רחב. האוטומציה של יכולות אנושיות אלה יוצרת הזדמנויות חדשות ומשפיעה על תחומים רבים, וביניהם באופן בולט על הביטחון הלאומי. מטרת חיבור זה היא להציג את הנושא המורכב של בינה מלאכותית לציבור בכלל ולמקבלי החלטות בפרט, ולאור תיאור וניתוח של האתגרים וההזדמנויות הגלומים בו – להמליץ על מדיניות רצויה לישראל בתחום.

עבור ישראל מהווה הבינה המלאכותית תחום טכנולוגי בעל חשיבות מכרעת, הן משום שכיום היא אחת המדינות המובילות בעולם בפיתוח והן לנוכח האתגרים המרובים שהיא ניצבת בפניהם, ואשר לטכנולוגיה זו יש פוטנציאל לסייע בהתמודדות עימם. זאת נוסף על העובדה שישראל (כמעט) חסרה משאבים טבעיים, וחוסנה הכלכלי נסמך במידה רבה על תעשיית ההיי־טק.

חשיבות הנושא אף גוברת, משום שמקובל להעריך כי לבינה מלאכותית תהא יכולת להגביר את קצב הצמיחה הכלכלית, למצוא מזור למחלות ולשפר את מערכות הבריאות, לשפר את יעילות התחבורה ואת בטיחותה, לעודד יעילות אנרגטית ולשפר את הבנת תופעות האקלים, ואולי אף להוביל ליציבות מבוססת שלום בזירה הבינלאומית, בין היתר באמצעות הרתעה. מכיוון שכך, על מקבלי ההחלטות בישראל להכיר את התחום לעומקו, לבחון את ההזדמנויות והאתגרים הטמונים בו ועל בסיס המסקנות לגבש מדיניות הולמת ולדאוג להוצאתה לפועל בקצב שיאפשר התמודדות עם התרחשויות אזוריות ובינלאומיות, וכל זאת בהתחשב בתחרות המואצת בתחום זה בזירה הבינלאומית.

תחומים שונים של בינה מלאכותית ויישומיה הביטחוניים

בינה מלאכותית כוללת מספר רב של תת-תחומים, ביניהם למידת מכונה, למידה עמוקה, ראייה ממוחשבת, עיבוד שפה טבעית, וכן מספר טכנולוגיות נלוות בעלות השפעה הדדית ביניהן כגון האינטרנט של הדברים (חפיצים שונים, המאופיינים ביכולות דיגיטליות של חיבור לרשת האינטרנט ויכולת לשדר ולקבל מידע ולסייע בביצוע פעולות מסוימות) וטכנולוגיות דו-שימושיות, המשמשות הן בזירה האזרחית והן בזירה הביטחונית. תחומים אלו ונוספים מהווים יסודות ליישומים מגוונים בתחומי חיים שונים לרבות מסחר, רפואה, אקדמיה ותחבורה, וכן בתחום הביטחוני. בתחום הביטחוני מאפשרות טכנולוגיות בינה מלאכותית יישומים מגוונים ובהם בתחום המודיעין, למשל מערכות המסוגלות לסקור כמויות עתק של נתוני וידאו ולזהות בהם מטרות; יישומים לוגיסטיים המאפשרים טיוב וחיסכון במשאבים; נהיגה אוטונומית, אשר גם לה פוטנציאל בתחום הביטחוני, כמו זה הקיים בתחום האזרחי ואף מעבר לו; מערכות נשק אוטונומיות המאפשרות שיפור דיוק וצמצום סיכון ללוחמים המשתמשים בהן; מערכות תכנון ותמיכה בקבלת החלטות וסימולציות, המאפשרות לשפר ולקצר תהליכי תכנון וקבלת החלטות בשלבים שלפני ביצוע משימות, על בסיס כמויות נתונים אדירות שלא ניתן היה לנתח קודם לכן; מערכות פיקוד ושליטה המאפשרות להתמודד עם נתוני עתק – ביג דאטה (Big Data) ממקורות שונים, תוך הצלבתם וניתוחם בזמן אמת של ביצוע משימות, ולשפר את התוצאות באמצעות הכוונה ושינויים בהחלטות במעגל מתמשך; לוחמת סייבר והגנת סייבר וספקטרום אלקטרומגנטי, שהן בין התחומים המובילים כיום בשימוש בבינה מלאכותית, לצורכי התקפה ולצורכי הגנה, בהתמודדות עם כמויות נתונים וקצבים שעולים על היכולת האנושית; חיזוי, התרעה ומניעה או ניהול של מצבי אסון, ובתוך כך יכולת להשתמש במאגרי מידע עצומים או בחיישנים שונים במטרה לבצע קיבוץ (אגרגציה) של מידע, שיוביל לתובנות שלא ניתן היה להגיע אליהן באמצעים אחרים.

מעבר לכל אלה קיימות טכנולוגיות נוספות הנדרשות לפיתוח ושימוש בבינה מלאכותית. למשל, נתוני עתק נדרשים על מנת לאמן יישומי בינה מלאכותית. לאחר האימון היישומים מסוגלים לבצע פעולה אוטונומית על מקבצים של נתונים חדשים שהם לא נחשפו אליהם קודם לכן. דוגמאות נוספות הן טכנולוגיות שמהוות תשתית להפעלת יישומי בינה מלאכותית כמו מחשוב ענן, מחשוב-על ומחשוב קוונטי, או רשתות דור חמישי, שנדרשות להעברה מהירה דיה של נתונים ולצורך שיפור ביצועי מערכות מבוססות בינה מלאכותית.

כמו כן, קיימות טכנולוגיות הנתמכות על ידי בינה מלאכותית. למשל, טכנולוגיות "נחילים" המשמשות להפעלה בשיתוף פעולה מתקדם של מערכות שונות או טכנולוגיות

ויישומים בתחום אינטראקציות אדם-מכונה וכן ממשק מוח-מכונה, שנועדו לקצר את פרק הזמן בין קבלת המידע על ידי אדם ולסייע בקבלת ההחלטה ובהעברתה חזרה למכונה.

יכולות ויישומים אלו מחדדים את הקשר ההדוק בין טכנולוגיית בינה מלאכותית לביטחון לאומי בכלל, ולביטחון הלאומי בישראל בפרט. זאת על פי תפיסת הביטחון הלאומי של ישראל על היבטיה הנרחבים – גם אלה שמעבר למובנים הצבאיים – וכן על פי 'אסטרטגיית צה"ל' (2015). על כן, קיים פוטנציאל רב לשימור ולשיפור הביטחון הלאומי של ישראל באמצעות ניהול נכון של תחום הבינה המלאכותית בארץ. לכך חשיבות רבה אף יותר אל מול התחרות הבינלאומית ההולכת וגוברת בתחום.

מרוץ חימוש ותחרות טכנולוגית בין מעצמות על הובלה בבינה המלאכותית

ניכר כי בצד ההתפתחות התעשייתית והטכנולוגית, מנהיגיהן של מדינות רבות ובהן גם המעצמות המובילות בעולם מבחינה טכנולוגית וכלכלית השכילו להבין מאז 2014 לערך את חשיבותה של הבינה המלאכותית עבור עוצמתן של המדינות שבראשן הם עומדים. סין, ארצות הברית וחלק ממדינות האיחוד האירופי, למשל, כבר בנו תוכניות לאומיות בתחום והן מקצות לו משאבים ותשומת לב ניהולית, על מנת לדחוף את מדינותיהם קדימה. מרבית האסטרטגיות מדגישות את חשיבותו של התחום כמנוע צמיחה כלכלי, ויותר מכך עבור הביטחון הלאומי, ובתוכו גם יישומים צבאיים.

אחד התחומים המתפתחים במסגרת מרוץ החימוש הזה הוא מערכות נשק אוטונומיות המסוגלות לאתר, לזהות ולתקוף מטרה ללא מעורבות אנושית, כאשר ארצות הברית היא המובילה בתחום זה, לצד תחום ה"נחילים". ואולם, סין אינה ניצבת מן הצד והיא מובילה בתחומים אחרים רבים, בין היתר בזכות הניהול הריכוזי שבה והעובדה שהממשל שולט גם בחברות האזרחיות. על כך נוספת העובדה שסין מובילה במאגרי המידע שלה על אוכלוסייתה, שאותם גיבשה לאורך תקופה ממושכת. איסוף המידע התאפשר בשל אי-התחשבות בזכויות אדם ובזכות אזרח לפרטיות. מנגד, מסיבות אלו ממש סין מתקשה לגייס מומחים וחברות, החוששים מגניבה של אלגוריתמים ומהשלכות מוסריות של השימוש בטכנולוגיה שהם יפתחו. אחרי סין וארצות הברית ניצבים בפיגור יחסי האיחוד האירופי, בריטניה ורוסיה.

יתר על כן, מלבד מרוץ החימוש והתחרות הכלכלית, בינה מלאכותית עשויה להשפיע בדרכים נוספות על הזירה הבינלאומית, ויש להביא זאת בחשבון בעת גיבוש מדיניות בתחום. בין ההשפעות האפשריות ניתן למנות: סיכונים הקשורים לבטיחות בינה מלאכותית, השפעת לוואי על תחומי חימוש אחרים – ביניהם נשק גרעיני – וסיכון ל"מלחמת יתר", וכן השפעה על יחסי עוצמה וסיכוי או סיכון ליצירתו של סדר עולמי חדש, הגדלת הפער בין מדינות מתפתחות ומפותחות, או לחלופין – שיפור איכות החיים

והיציבות בזירה הבינלאומית באמצעות הרתעה. על אודות חלק מנושאים אלה ניתן ללמוד ממקרי מבחן היסטוריים של מרוצי חימוש, ובהם גם המקרה החדש יחסית של מערכות נשק אוטונומיות, המלמד כי קצב ההגבלה של טכנולוגיות חדשניות על ידי המשפט הבינלאומי הוא איטי למדי. ההתפתחות הטכנולוגית בתחום עתידה להציב בפני מקבלי ההחלטות במדינות השונות אתגרים מוסריים ומשפטיים, רגולטוריים ואחרים, שהסיכוי לפתרונם מבעוד מועד, באמצעות ערכאות בינלאומיות ושיתוף פעולה בין מדינות, הוא קלוש.

אתגרים בתחום הבינה המלאכותית והמלצות להתמודדות עימם

בצל האתגרים הנובעים מן התחרות הבינלאומית ולמרות היתרונות הרבים וההזדמנויות, טכנולוגיית הבינה המלאכותית טומנת בחובה אתגרים מגוונים לישראל, שעבורם נדרשת התייחסותם של מקבלי ההחלטות בתחום. ביניהם ניתן למנות:

אתגרים טכניים – כוללים אתגרים בפיתוח; קושי בהתאמה של טכנולוגיה אזרחית לשימוש צבאי; סטנדרטיזציה; אתגרים בתחום החומרה והאנרגיה; חוסר בנתונים גולמיים (דאטה); קושי להסביר את תוצאות פעולתה של מערכת בינה מלאכותית בשל היותה "קופסה שחורה".

אתגרים ארגוניים – כוללים צורך בתקציבים ייעודיים; השקעה וניהול של משאבי אנוש; התמודדות עם היותה של ישראל מדינה קטנה בעלת משאבים מוגבלים.

אתגרים בשימוש – כוללים קשיים בהתאמת הקצב של הסביבה או בני האדם המשתמשים במערכות אלו ליכולותיהן הגבוהות; קושי של המערכות להסתגל לסביבות חדשות שבהן לא אומנו; אתגרים בתחום הבטיחות והאמינות של המערכות; אתגרים מוסריים; הטיית הנובעות מן המידע; וכן השימוש במערכות אלו לייצור "מידע כוזב" הנראה מהימן.

אתגרים ביטחוניים ומדיניים – כוללים את מרוץ החימוש הבינלאומי; קושי להסכים על משטרי בקרת נשק בתחום ולהחילם; תלות שתיווצר במערכות אלו, לצד פגיעותן למתקפות סייבר או למניפולציות אחרות. לקטגוריה זו שייכים גם אתגרים "רכים" שהשפעתם אומנם ניכרת על הביטחון הלאומי, לעיתים דרך תחומים עקיפים. בין אלה: סוגיות מוסריות ומשפטיות; השפעה על שוק העבודה והתעסוקה; פוטנציאל לאי-שוויון קיצוני בחלוקת המשאבים בחברה, העלול לערער את היציבות השלטונית. מכל אלה עולות המלצות למדיניות עבור ישראל, שתכליתן לשמר ואף להגביר את יכולותיה בתחום הבינה המלאכותית, להטמיע אותן לשימוש בקרב גורמי הביטחון השונים וכן להיערך להתמודדות עם אתגרי השימוש בטכנולוגיה זו, כדוגמת השימוש

שעושים בה אויביה של ישראל, או לחלופין בהקשרו של מרוץ החימוש בתחום בזירה הבינלאומית. עיקרן:

- **המלצות ארגוניות:** צורך לנסח אסטרטגיה לאומית לבינה מלאכותית ולהקים גוף שיאפשר את ניהולה ברמה הלאומית, מתוך הבנה של חשיבות ודחיפות הטיפול הלאומי בתחום זה. זאת לצד כינונה של תוכנית רב-שנתית בתחום הבינה המלאכותית; יצירה וחיוזוק של מודלים מבניים במערכת הביטחון, שיאפשרו תגובתיות וגמישות בתחום; יצירת גופים, שיטות פעולה ומכלולי עבודה משותפים לאנשי המקצוע העוסקים בתחום בארגוני הביטחון השונים, ולגורמים אחרים בעלי השפעה על ביטחונה הלאומי של המדינה.
- **מחקר ופיתוח:** יש לבחון שילוב מידי של בינה מלאכותית בתחומים טכנולוגיים ביטחוניים, שבהם לישראל יש כבר עכשיו יתרון יחסי (למשל תחום המל"טים), על מנת לייצר מכפיל כוח על בסיס ידע והשקעות קיימים; מומלץ להשקיע במחקרי עומק במערכת הביטחון ולהימנע מהסתמכות בלעדית על האקדמיה בתחום זה; יש לתעדף מחקר ופיתוח של בינה מלאכותית בתחומים המוגדרים כעשויים לספק יתרון מתמשך; מומלץ לקדם פיתוחים ביטחוניים על בסיס טכנולוגיות בינה מלאכותית אזרחית קיימות וכן פיתוח יכולות נגד של בינה מלאכותית להגנה והתקפה; ועוד.
- **תקצוב ויצירת תשתיות לאומיות:** בין היתר, יש ליצור פתרון מקיף למחסור הבולט בתשתיות לאומיות בתחום הבינה המלאכותית; להקצות תקציב ייעודי מתמשך לתחזוקה בכל הקשור לתחום; וכן להגדיר תחומי מחקר למימון בתקציב ממשלתי.
- **תחום משאבי אנוש:** נדרש לבחון ניהול משאבי אנוש ברמה הכלל-מערכתית, בשונה מהרמה הפנים-ארגונית שבה הוא מתנהל כיום; יש לבחון השתלבות של מערכת הביטחון בהכשרות קיימות וביצירת הכשרות חדשות; יש להכשיר כוח אדם לא-טכנולוגי להיכרות עם התחום, עם יכולותיו ועם מגבלותיו.
- **מוסר, חקיקה, תקינה ונוהלי בטיחות:** מומלץ להקים ולבסס יכולת ליצירת תקנים ופיקוח על בטיחות בבינה מלאכותית; לפתח נורמות ועקרונות לבטיחות ולאחריות בשימוש בבינה מלאכותית במערכת הביטחון; להגדיר קוד אתי למערכת הביטחון בהקשר של בינה מלאכותית, ובמיוחד בהקשר של צוותי אדם-מכונה; יש להגדיר סיווג ותקינה של מערכות בינה מלאכותית למטרות של שילוביות, בטיחות והיכולת לנהל דיון משותף בין גופים וארגונים שונים, כמו גם תהליכים סדורים אל מול התעשיות; הגדרת תקינה בקשר למחקר בתחום אדם-מכונה.
- **שיתוף ידע:** ההמלצה העיקרית היא להגביר את שיתוף הידע במערכת הביטחון של ישראל באמצעות יצירת מנגנונים קבועים, במטרה למנוע כפילות ולהוביל ליצירת פתרונות מותאמים, הנדרשים עקב מגבלת תקציב וכוח אדם בתחום. יש לבסס תהליכי שיתוף ידע מתמשכים עם מערכות נוספות.

• **היבטים בינלאומיים, דיפלומטיים ומודיעניים:** יש לעקוב באורח סדור ברמה הלאומית אחר המתרחש במערכת הבינלאומית בתחום, כדי להתאים את המדיניות ולשמר את היתרון הקיים בתחום; לפעול לחיזוק המחקר המשותף ושיתופי פעולה נוספים בין ישראל לבין מדינות אחרות; ולבחון אם, כיצד ואילו יישומי בינה מלאכותית צריכה המדינה להגביל באמצעות אמנות.

לסיכום, ישראל נדרשת לגבש מדיניות בתחום הבינה המלאכותית, על מנת לגרוף הישגים משמעותיים בתחום ולא להשאיר תחום חשוב כל כך ורווי אתגרים לפעילותם של כוחות השוק בלבד. לאור קצב הפיתוח המהיר והתחרות הבינלאומית קיימת חשיבות למהירות קבלת ההחלטות בנושא, לכמות המשאבים שתוקצה לשם ביצוען ולאופן הפיקוח והניהול של המשימות המרובות השייכות לתחום. טיפול בכל הנושאים הללו יחד עשוי לחולל השפעה מכרעת על עוצמתה העתידית של ישראל, בכלל זאת על כלכלתה ועל יכולתה לשמר ולשפר את הביטחון הלאומי שלה.