

פרק 11

אתגרים

לצד ההתפתחות הטכנולוגית המהירה בתחום הבינה המלאכותית, עולה גם שורת אתגרים מגוונים בזירות שונות – זירת הפיתוח הטכני, זירת הארגון, זירת השימוש והזירה הביטחונית-מדינית. הדיון באתגרים נדרש על מנת לבחון דרכי התמודדות אפשריות עימם, במסגרת מדיניות סדורה.

אתגרים טכניים	אתגרים בשימוש	אתגרים ארגוניים	אתגרים ביטחוניים ומדיניים
פיתוח	התאמת קצב	תקציבים ייעודיים	מוסר בלחימה
התאמה של טכנולוגיה אזרחית לשימוש צבאי	קושי בהסתגלות	משאבי אנוש	חוק ומשפט
סטנדרטיזציה	בטיחות ואמינות	אתגר הקוטן	תלות
חומרה ואנרגיה	תוצאות בלתי צפויות	יחסם של בכירים לנושא	בינה מלאכותית בידי "הצד השני"
אתגרים בהטמעה	אדם מחוץ לחוג או בתוך החוג	פוליטיקה והתנגדות לשינויים ארגוניים	מרוץ החימוש
קביעת תצורה	מוסר	הקשר עם התעשייה האזרחית	בקרת נשק
דאטה	הטיות	חוסר אמון ופערים בין התחום האזרחי לביטחוני	לוחמת סייבר
"הקופסה השחורה" – הסברתיות	מידע כוזב – האתגר המבצעי		נשק גרעיני
			מלחמת יתר
			מידע כוזב
			שוק העבודה והתעסוקה
			אישוויון קיצוני בחלוקת המשאבים בחברה

אתגרים טכניים

אתגרי פיתוח

מערכת היחסים בעבר בין הצבא, התעשייה והאקדמיה התנהלה כשהצבא מוביל בפיתוח טכנולוגי, והטכנולוגיות שפיתח אומצו על ידי חברות מסחריות והאקדמיה. בשנים האחרונות חל היפוך: חברות מסחריות הן המבצעות את עיקר הפיתוח, ואילו הצבא מאמץ את הטכנולוגיה תוך התאמתה לצרכיו.²⁵⁰ כך נוצר קושי בפיתוח טכנולוגי ביטחוני איכותי, כאשר הידע המקצועי אינו נמצא בהכרח בתוך הצבא. בעוד שבתחום הבינה המלאכותית חברות אזוריות נשענות על אנשי אקדמיה בכירים או על גוף אקדמי מוביל, מערכת הביטחון מאותגרת בכל הקשור לפיתוח ידע או למוצרים מבוססי בינה מלאכותית. זאת ועוד, ניכר כי מערכת הביטחון כמעט אינה עוסקת במחקר ופיתוח עצמאיים, שמייצרים תשתית ליכולות ייחודיות עתידיות החיוניות להשגת יתרון יחסי. עם זאת, מערכת הביטחון נמצאת כיום בתהליך של ניסיון להדביק את הפער מול התעשייה האזרחית.

התאמה של טכנולוגיה אזרחית לשימוש צבאי

קיים אתגר בהתאמה של טכנולוגיה אזרחית לשימוש צבאי בשל הצרכים השונים, שמובילים לכך שהאלגוריתם יספק פתרון שונה כתוצאה מאימון עבור צרכים שונים.²⁵¹ הקושי בהתאמה נובע בין היתר גם מאתגר code-to-product – המעבר משורות קוד מבוססות מחקר תאורטי למוצר שניתן לשימוש בשטח. העיסוק האקדמי והתעשייתי בבינה מלאכותית בא לידי ביטוי בנטייה להשקעה במחקר ולא בייצור. במקרים רבים, גם כשהמחקרים מתקדמים מאוד הם אינם ישימים עבור גופי ביטחון – בין מטעמים טכניים דוגמת כוח עיבוד ובין משום שהם נלקחים מבעיות הקשורות לעולם האזרחי, שלא תמיד עולות בקנה אחד עם הצורך הביטחוני.

סטנדרטיזציה

סטנדרטיזציה בתחום הביצועים והבטיחות שונה בשוק האזרחי מזו המקובלת בזירה הביטחונית. לכך מתווספת העובדה שמחקרים מצביעים על החרפה בכשלים של מערכות בינה מלאכותית בסביבות מורכבות, מחוץ למעבדה, מה שמגביר את הקושי של המגזרים לעבוד זה עם זה.²⁵² מדובר במקור לבעייתיות ולעיכובים בשילוב פיתוחים שמקורם אזרחי בתחומים ביטחוניים.

חומרה ואנרגיה

מערכות בינה מלאכותית מצריכות יכולות מחשוב ועיבוד אדירות, ולשם כך נדרשים קירור ואספקת חשמל. גורמים מעטים מצליחים לעמוד בצריכת האנרגיה הדרושה

לשרתים מהסוג הזה, הן מבחינת יכולת האספקה והן מבחינת העלויות. גוגל למשל מתמודדת עם קושי זה בעזרת מערכות בינה מלאכותית המסייעות לה לצמצם את צריכת האנרגיה של מרכזי הדאטה בכ-30 אחוזים.²⁵³ בפייסבוק מנסים להתמודד עם הסוגיה באמצעות הקמת מרכז דאטה בקרבת הקוטב הצפוני, בצפון שוודיה, כדי לרתום את האקלים הטבעי של האזור לקירור הנחוץ למרכזים.²⁵⁴ עם זאת, ההתייעלות בתחום זה היא עדיין שולית ביחס להתפתחויות בתחומים אחרים הקשורים לבינה מלאכותית, וגורמים שאינם חברות הענק שהוזכרו, כולל מדינות, מתקשים להתמודד עם האתגר. מעבר לכך קיים אתגר כללי הקשור לצורך בחומרה חזקה דיה, שתאפשר את יכולת העיבוד הנדרשת ליישומים מתקדמים. כיום אין בישראל מספיק שרתים ואין תשתית לאומית בתחום הבינה המלאכותית. זאת בשונה מתחומי מחשוב ומדע אחרים, שבהם השקעה רבה בתשתיות לאומיות אפשרה הובלה בינלאומית בתחום.

אתגרים בהטמעה

'מערכות מורשת' הוא הכינוי המקובל למערכות צבאיות יקרות האמורות לשרת את גופי הביטחון בטווח הארוך, שכן תקופת החיים שלהן ממושכת והחלפתן אינה תכופה, למשל מטוסים וטנקים. הטמעה של בינה מלאכותית במערכות כאלו היא אתגר, שכן קצב השינויים בתחום הבינה המלאכותית הוא מהיר ודינמי, בעוד מערכות מורשת הן לרוב פלטפורמות המשרתות באופן דומה למדי במשך שנים.

קביעת תצורה

קצב השינוי המהיר מאתגר את המערכת הביטחונית הבירוקרטית גם בסוגיות של קביעת תצורה, שאליה מורגלת המערכת הביטחונית. בפיתוח מערכות ומוצרים חדשים במערכת הביטחון נבחנות מספר אפשרויות לשימוש, וזו המועדפת נבחרת כתצורה הקבועה של המערכת. לאחר מכן תצורה זו מופצת עם הוראות השימוש. בינה מלאכותית משתנה כל הזמן ומקשה על קביעת תצורה כזו. בכך היא עתידה לאתגר את מערכת הביטחון בנוגע לקבלת החלטה אם המוצר שברשותם טוב דיו להפצה לצרכנים בגופי הביטחון השונים.

דאטה (נתונים)

דאטה (נתונים) היא אבן היסוד לפיתוח בינה מלאכותית איכותית, שכן היא מאפשרת לאמן את האלגוריתמים ומכינה אותם לפעולה אוטונומית. יש אף המתייחסים אל הדאטה כאל "הנפט של העידן החדש". היעדר דאטה מספקת מציב אתגר ליכולתה של מערכת הביטחון להשתמש בבינה מלאכותית. למשל, בתחום הביטחוני שבמסגרתו רווח השימוש בחיישנים מזה מספר שנים, הדאטה לרוב נמחקה מעת לעת, עקב חוסר במקום אחסון ועלויות גבוהות שלו בעבר. נוסף על כך, מידע שנאסף לאורך השנים

לא תמיד יתאים לעיבוד במסגרת בינה מלאכותית, ויש צורך "לנקות" אותו ולארגנו מחדש כדי להתאימו לשימוש זה.

סודיות ומידור מהווים אתגר נוסף לגופי ביטחון: ניתוקם מרשתות חיצוניות ומטכנולוגיית ענן לא מאפשר שימוש במרכזי דאטה של גורמים אחרים, בין אזרחיים ובין ביטחוניים אחרים, לפעמים אפילו באותו ארגון עצמו. על כן הגופים נאלצים לפעול במסגרת יכולות ספציפיות המבוססות על יכולות החומרה ומאגרי הנתונים הפנימיים שלהם. במערכת הביטחון יש חוסר בשיתוף לא רק של דאטה אלא גם של אלגוריתמים או תוצאות שהושגו על ידם עבור גורמים שונים, משום חשש מחשיפה של דאטה באמצעות הנדסה הפוכה (Reverse engineering).

יתר על כן, בעולם המודיעיני והמבצעי לעיתים יש מיעוט דאטה, שאינו מאפשר לאמן אלגוריתמים חיוניים לפתור בעיות. אם יש למשל תמונה אחת או תמונות אחדות בעלות חשיבות אסטרטגית, אין די בכך לאימון האלגוריתם כראוי לפעולה באותו נושא או תופעה.

מעבר לכך, עיקר המידע נאסף בעיתות שגרה ואינו מתאר את הסטטיסטיקה המשתנה בעיתות חירום או בקרב. אין גם מאגרי מידע המייצגים מציאות מבצעית עתידית, ולכן אימון המערכות נעשה על סמך תרחישי שגרה או חירום ידועים מהעבר. אתגר זה משול "התכוננות למלחמה הקודמת", בעוד הזירה המבצעית אינה צפויה ומרבה להשתנות.

אתגר נוסף בתחום המידע הוא קושי של ארגונים ביטחוניים להסתמך על מוצרי מדף, שכן יש להם בעיות ייחודיות לגופי ביטחון ומודיעין, שדורשות איסוף וניתוח ייעודי של נתונים שלא קיימים באזרחות.

"הקופסה השחורה" – הסברתיות

אחד המאפיינים הבולטים של מערכות הבינה המלאכותית הוא היותן "קופסאות שחורות" שאינן מסוגלות להסביר את התהליכים שהביאו אותן לקבל החלטה מסוימת.²⁵⁵ בתחום הביטחון הלאומי יש משמעות חשובה לשקיפות במערכות מסוג זה, שכן לרוב קיים יותר מפתרון אחד לבעיה וחיוני לבחון את השיקולים שבדרך.²⁵⁶ לכן קיים חשש מפני הסתמכות מוחלטת על מערכות בינה מלאכותית בקבלת החלטות, מבלי שהובנה הדרך אליהן. שאלה מרכזית בהקשר זה היא אם המכונה והאדם חולקים את אותה הבנה לגבי המטרה והמגבלות בביצועה.²⁵⁷

כהמשך ישיר לכך, קיים חשש מחוסר אמון במערכות. בעיות האמון מקשות על הטמעה של מערכות בינה מלאכותית גם בתחומים שבהם להשלכות עשויה להיות עלות גבוהה.²⁵⁸ גם אם ניתן יהיה להסביר אלגוריתם, לא יהיה זה פתרון מושלם, מה גם שהסברתיות מחקרית אינה דומה בהכרח להסברתיות מבצעית. סף השקיפות

הדרוש לכל משתמש ותחום הוא שונה, ואין הכרח ששקיפות מלאה אכן תתרום באותה מידה לכל התחומים.²⁵⁹ כמו כן, לא בכל יישום אפשר להשתמש בפתרונות הסברתיות, משום שביישומים שנדרשים לפעול בקבועי זמן קצרים מאוד, לעיתים מעל לקצה גבול היכולת האנושית, לא ניתן להציב אדם בחוג ההפעלה של המערכת, אשר ינתח את הנתונים ההסברתיים.

חשוב לזכור כי המטרה ביצירת הסברתיות היא שיפור הביצועים, תוך הכרה בכך שאינם מושלמים. ברם גם כיום, כאשר ההחלטות הן של בני אדם, מתרחשות טעויות שהשלכותיהן עשויות להיות כבדות משקל. אם המכונה תטעה פחות מבחינה סטטיסטית ותשפר את הביצועים, ייתכן כי חרף אתגר ההסברתיות מוטב להסתמך עליה, מלבד מאשר בתחומים שבהם תתקבל החלטה עקרונית להימנע מכך, למשל מסיבות מוסריות או משפטיות.

אתגרים ארגוניים

תקציבים ייעודיים

לשם פיתוח והטמעה של מערכות בינה מלאכותית דרושה השקעה כלכלית רבה בכוח מחשוב ובמערכות תומכות, וכן לצורכי אבטחה של דאטה, תשתיות ואנשים.²⁶⁰ בימינו, לחברות המסחריות הגדולות תקציבים גדולים אף מעל לתקציביהן של מדינות מסוימות, וגופים צבאיים ומדיניים מתקשים להתחרות בכך ולהשיג את התקציב הנדרש לפיתוח ולהטמעה. זו אחת הסיבות לכך שהעיסוק בבינה מלאכותית בגופי הביטחון כיום הוא מועט ביחס לעיסוק בנושאים טכנולוגיים אחרים כגון סייבר, והתקציב אינו מספק. לעיתים הסיבה לכך היא שמוערך כי ניתן יהיה להסתמך על פיתוחים אזרחיים עתידיים. כמו כן, בארגונים ביטחוניים ומדיניים רלוונטיים התחום אינו מתוקצב כראוי או אינו מתוקצב כלל, בשל ראשוניותו והקושי של המערכת להשתנות ולהתאים את עצמה.

משאבי אנוש

קיים קושי לגייס ולשמר כוח אדם מיומן שיוכל לפתח, להתאים ולהטמיע את המערכות בגופי הצבא והמדינה, עקב התחרות הקשה מול התנאים שמציע המגזר הפרטי.²⁶¹ כמו כן, בשל סגירות של ארגוני ביטחון – סודיות ומידור – לא מתקיים מעבר של כוח אדם טכנולוגי בין ארגוני הביטחון השונים באופן שוטף, ולכן קשה לעיתים ליצור מסלולי קריירה שישמרו כוח אדם איכותי בתחום זה בשירות המדינה. לאור העובדה שמדובר בתחום צר יחסית, לאור היותה של ישראל מדינה קטנה עם משאבי אנוש מוגבלים ונוכח הקושי להתחרות על כוח האדם מול התנאים שמציעות חברות אזרחיות, מדובר באתגר כבד משקל בעל חשיבות מכרעת.

אתגר הקוטן

האקוסיסטם הישראלי מושפע לעיתים קרובות לטובה מכך שישראל היא מדינה קטנה יחסית, בין היתר בגלל הקרבה הפיזית בין מוקדי קבלת החלטות לבין מוקדי הפיתוח, והקשר הישיר או הקרבה היחסית בין מקבלי החלטות לבין מפתחים או חברות. המודל הייחודי של גיוס החובה לצבא ושירות המילואים ומעבר כוח אדם לתעשיות האזרחיות משפיעים לטובה על תחומים טכנולוגיים. עם זאת, בישראל יש להתמודד עם קשיי השקעה ותקצוב עקב התוצר המקומי הגולמי (תמ"ג) הקטן ביחס למדינות מתחרות. משום כך מתבקשים פיזור מאמצים וחלוקה של אלה הכשירים בתחומים טכנולוגיים למגוון הצרכים המשקיים והביטחוניים. יתר על כן, כניסתן של חברות ענק לישראל, אשר פותחות בה מרכזי פיתוח בתחום הבינה המלאכותית, הגם שהיא בעלת חשיבות רבה למשק, מייצרת אתגרים בנושא משאבי אנוש משום שהוא מהווה כיום את אחד מצווארי הבקבוק בתחום, כפי שתואר בהרחבה בסעיף שעסק בנושא זה.

יחסם של בכירים לנושא

בקרב מקבלי ההחלטות חסרה היכרות עם יכולות הבינה המלאכותית או הבנת משמעות שילובה בתחומים ביטחוניים. קיים גם קושי, בין היתר בקרב מפקדים ובכירים, לפעול על פי ניתוחים שמקורם במערכת בינה מלאכותית. מדובר בעיקר בגורמים ותיקים השייכים לשדרת מקבלי החלטות ואשר נדרשים לאשר תוכניות ורכש, או לחלופין לקבל החלטות חשובות בתחומים אחרים. גם גורמי שטח בדרגות נמוכות יחסית, שלרוב אינם בעלי רקע סטטיסטי ומתמטי, מתקשים לסמוך על מערכות בינה מלאכותית ולהתבסס עליהן בניהול מבצעים או פעילויות אחרות, למרות שרובם בעלי זיקה טכנולוגיות רבה יחסית מזו של דור הבכירים.

פוליטיקה והתנגדות לשינויים ארגוניים

שינוי טכנולוגי מביא עימו לעיתים שינויים באופי ובהגדרת תפקידים, מה שאינו מעודד אהדה לבינה מלאכותית בקרב חברי ארגוני הביטחון, שמטבעם הם גדולים ובירוקרטיים. כמו כן, לעיתים הטמעת הבינה המלאכותית איננה מביאה תועלת מיידית, ועל כן ניכרת התנגדות להטמעתה ולשימוש בה.²⁶² חלק מההתנגדות נובע מסיבות פוליטיות – שינוי עתידי בתקנים או במשרות. התנגדויות מסוג זה מזכירות התנגדויות היסטוריות שעלו בעקבות מיכון או מחשוב.

הקשר עם התעשייה האזרחית

האופי הארגוני של מערכת הביטחון על גורמיה השונים מאתגר את הקשר עם התעשייה האזרחית, שכאמור הוא חיוני לפיתוח הבינה המלאכותית. למשל, בעבודה מול הצבא

תהליכי הרכישה וההתקשרות מורכבים וממושכים, בעוד קצב העבודה בשוק האזרחי מהיר מאוד.²⁶³ המערכת הביטחונית הבירוקרטית אינה מורגלת בעבודה מול חברות מסחריות אזרחיות, במיוחד חברות הזנק. לאלו יש טכנולוגיה מבטיחה אך הן חסרות תשתיות מנהלתיות שיאפשרו להן לעבוד עם המערכת הבירוקרטית הביטחונית. זאת ועוד, חברות הזנק רבות אינן מבשילות לכדי חברות בעלות קיום מתמשך, וגופי ביטחון מתקשים להתקשר איתן עקב חוסר ביטחון בהמשכיות לאורך זמן.

חוסר אמון ופערים בין התחום האזרחי לביטחוני

יש חברות החוששות משיתוף פעולה עם גורמי ביטחון מטעמים אתיים או מתוך חשש להתנגדות של עובדיהן לנושא (הבעיה בישראל פחותה מאשר בארצות הברית, למשל). כמו כן, חברות המפתחות מוצר חדשני נוטות לחשוש מהתקשרות עם גופי ביטחון עקב דילמות של קניין רוחני.²⁶⁴ חשש נוסף נובע מהגדרתו של המוצר כביטחוני והחלת רגולציה בתחום היצוא הביטחוני, שתקשה על מכירות בחו"ל. במערכת הביטחון קיים חשש הפוך: עבודה עם חברות מסחריות עשויה להביא לזליגת ידע, אלגוריתמים ומידע, כתוצאה מחשיפה או מסחור של מוצר שנוצר בעבודה משותפת.

אתגרים בשימוש

בטיחות ואמינות

מערכות בינה מלאכותית וחלק ניכר מן הטכנולוגיות שהן מתבססות עליהן הן חדשות וחדשניות, ובחלק מן המקרים קיים קושי רב להסביר את אופן פעולתן. מכאן הקושי להתאים למערכות סטנדרטים של בטיחות ווידוא אמינות לפני כניסתן לשימוש. במקביל עשוי להתעורר קושי לתרגל או להטמיע את השימוש במערכות כך שיתאפשר מימוש יתרונות של מהירות וראשוניות, שלא על חשבון בטיחות והוכחת אמינות. הקושי אף יגדל במערכות שפעולתן משתנה ומתפתחת, ומצריכה בדיקות חוזרות. הצורך לאזן בין אופיין של מערכות מסוג זה והצורך לפעול במהירות אל מול סטנדרטים המקובלים כיום בתחום הביטחוני עשוי לאתגר את המערכת, מרמת מקבלי ההחלטות ועד רמת המפקדים בשטח.

קושי בהסתגלות

מערכות בינה מלאכותית מתקשות כיום להסתגל לסביבות חדשות (Domain Adaptability),²⁶⁵ מאפיין שהוא חיוני לזירה הביטחונית הדינמית, בייחוד בשדה הקרב. אתגר זה בא לידי ביטוי גם בצורך לאמן את המערכות לסביבה המתאימה (כאשר לעיתים חסרים נתונים בתחום). הדבר מושפע גם מיכולת מוגבלת של המשתמשים עצמם להפיק מהן את התוצאות הרצויות.

התאמת הקצב

יכולתן של מערכות בינה מלאכותית לפעול ולהגיב במהירות רבה יכולה להוות יתרון, אך קיים חשש ששינוי הקצב בשדה הקרב יגרום חוסר יציבות, בייחוד אם הקצב יעלה על זה של יכולת המפעיל להבין אירועים ולשלוט בהם, ברמה האופרטיבית.²⁶⁶ בעיה נוספת עלולה להתרחש במקרה שקצב פעולת המערכות יעלה על הקצב של מערכת הביטחון לקלוט אירועים, לנתחם ולבחור את הדרכים הנכונות להגיב עליהם, מבחינה אסטרטגית (אתגר זה עשוי להשפיע גם על היבטים בינלאומיים דוגמת 'מלחמת יתר').

תוצאות בלתי צפויות

מערכות בינה מלאכותית מייצרות לעיתים תוצאות לא צפויות ולא קונוונציונליות, כפי שהוזכר באתגר ההסברתיות. אפשרות זו עשויה להוות יתרון בשדה הקרב, בעיקר בתחומים של ניתוח מודיעין או של היכולת להפתיע את הצד האחר. ברם, היא גם עלולה להביא לסיכון ולביצוע שגיאות חמורות הנובעות מהנחות של המערכת, שהן שונות מאלו של אדם בעל שיקול דעת.²⁶⁷ נוסף על כך, קיים חשש מחוב טכני (Technical Debt) – פער בין קצב ההתפתחות הטכנית לבין הבנה מספקת של אופן הפעולה, הסיכונים ודרכי הבקרה שדרושות להתמודדות עם התפתחות טכנית זו.²⁶⁸ בהקשר של בינה מלאכותית וביטחון לאומי, מדובר בשימוש מהיר מדי של צבאות במערכות מבוססות בינה מלאכותית בלי להבין בצורה מקיפה. גם אם הסיכון הכרוך בשימוש במערכת מבוססת בינה מלאכותית אינדיווידואלית נראה מזער, לאינטראקציה שלה עם מערכת יריבה שאומנה על בסיס דאטה שונה עשויות להיות השלכות חמורות, במיוחד אם יחל מרוץ חימוש בתחום.²⁶⁹ זאת ועוד, אתגר ההסברתיות מקשה על תכנון מראש של דרכי הפעולה האפשריות להתמודדות עם אירועים ביטחוניים שונים, ועל הכנת "מקרים ותגובות" בהתאם.

אדם מחוץ להפעלה או בתוכו

אתגר נוסף הוא מחיר השארת אדם בחוג ההפעלה, אל מול הבעיות המוסריות והמשפטיות של הוצאתו. חשיבות שמירת האדם בחוג ההפעלה ופיקוח או מעורבות בהחלטות של המערכת, מסיבות מוסריות, בטיחותיות ומשפטיות, היא נושא הקשור לדיון במערכות אוטונומיות חמושות (ואחרות). עם זאת, שמירתו של האדם כגורם חשוב בקבלת ההחלטות של המערכת עשויה להאט את פעולתה. אתגר משמעותי ייווצר אם מדינות מסוימות יחליטו לשמור אדם בחוג ההפעלה, בעוד אחרות או גורמים לא-מדינתיים ישתמשו בהן ללא אדם בחוג.²⁷⁰

הטיות

נהוג לומר ש"מערכת בינה מלאכותית היא טובה כמו הנתונים שהיא מקבלת". כאשר הנתונים ששימשו לאימון המכונה אינם מגוונים מספיק, עשויה להיווצר הטיות.²⁷¹ אולם נטען שגם כאשר "הדאטה מושלמת" היא למעשה משקפת את ההטיות החברתיות, למשל בהקשר של מגדר והבדלים אתניים.²⁷² אשר לפן המבצעי, מידע מוטא (בשווג או בזדון) עשוי להשפיע על פעולת מערכות ובתוכן מערכות מודיעיניות, מערכות תומכות קבלת החלטות וכמובן מערכות נשק אוטונומיות. לכן נדרשת תשומת לב מיוחדת למערכות שעשויות להשפיע על החלטות הרוח גורל, ולא רק עליהן. כמו כן, בהקשר הביטחוני יש להבחין בין הטיות הנובעות ממחסור בנתונים מגוונים, שאותה ניתן ואף רצוי לפתור, לבין הטיות שיבוצעו באופן זדוני, תוך ניצול נקודות תורפה במערכת על ידי האויב ליצירת הונאה מכוונת.²⁷³

מוסר

העיסוק בפן המוסרי של השימוש בבינה מלאכותית מעלה שאלות לגבי תהליך קבלת ההחלטות של המערכות והשיקולים הערכיים המובאים בחשבון. כאמור, ההחלטות של המערכות עשויות לבטא הטיות ואפליה של קבוצות בחברה. ברם, עיקר הבעיות מתגלעות כאשר מדובר בסוגיות בעלות פוטנציאל להשפיע על חיי אדם. על כן יש צורך במעורבות אנושית מסוימת, בעיקר בעת שימוש במערכות המפעילות כוח קטלני.

מידע כוזב – האתגר המבצעי

באמצעות בינה מלאכותית ניתן לייצר מידע כוזב (Fake News), שיראה אמין ויקשה על הנחשף אליו לזהות את הזיוף. אתגר זה, שיש לו משמעויות מבצעיות, ייסקר בהמשך בהרחבה גם בהקשרים המדיניים. בהקשר המבצעי מידע כוזב עשוי להטות מודיעין או ליצור חסמים בהפעלת הכוח, והערכה שהוא קיים עלולה לעורר חוסר אמון של גורמים במטה ובשטח במידע שיקבלו. מבצעי הונאה כאלו של הצד האחר עלולים ליצור קושי גם עבור מערכת הביטחון להנחות אזרחים בנוגע לפעולות נחוצות בשעת חירום, או להעביר מידע אמין ומהימן בשעת חירום לאזרחים ולכוחות. מערכת הביטחון עלולה גם להיתקל בקושי למנוע העברת מידע כוזב, שעלול להוביל לפגיעה בחיילים ובאזרחים.

אתגרים ביטחוניים ומדיניים

מוסר בלחימה

קשה ואולי אף בלתי אפשרי לחזות ולתכנן מראש כל החלטה שבינה מלאכותית או כלי אוטונומי יידרשו לה בכל אחד מתחומי החיים. האתגר הזה אינו תכנותי

בלבד אלא במיוחד מוסרי, ובפרט ביחס למצבים וסוגיות שאין לגביהם קונצנזוס. גם במקרים של קונצנזוס, החלטות של בינה מלאכותית יהיו תלויות תרבות. למרות שהאתגר המרכזי בהקשר זה הוא שימוש במערכות נשק אוטונומיות המסוגלות ליטול חיי אדם, גם בתחומים אזרחיים תהיה לשימוש במערכות אוטונומיות השפעה בעלת השלכות מוסריות, שיש להביאה בחשבון.

כיום ניטש ויכוח בין שתי קבוצות מרכזיות בכל הקשור לבינה מלאכותית, לאוטונומיות ולמוסריות. קבוצה אחת סבורה כי ניתן במידה רבה לתכנת מערכות מבוססות בינה מלאכותית דוגמת מערכות רובוטיות לפעול בצורה טובה יותר מאשר בני אדם במספר רב של תחומים, משום שכלים אלו מסוגלים לקבל החלטות בצורה מהירה ומדויקת שאינה מוטה על ידי עייפות, פחד או תכונות פיזיולוגיות ורגשיות אחרות של בני אדם. יש אף מי שסבור כי ניתן באמצעים שונים לחשב תאוריות אתיות על בסיס שיקולים של הנאה וסבל.²⁷⁴ בכך למעשה יוכלו מערכות אלו להפעיל, בדרכן שלהן, שיקולים מוסריים בבואן להחליט בנוגע לביצוע פעולה.

הקבוצה השנייה שוללת את יכולתן של מכונות לקבל החלטות בתחום המוסר וסבורה שגם בעתיד, מערכות אלו לא יוכלו לקבל החלטות מוסריות. נטען שבהיעדר רגשות אנושיים ויכולת להעריך ולהבין רגשות לא תתאפשר קבלת החלטה מוסרית הולמת, לעומת זו המתקבלת על ידי בני אנוש, המקדישים התייחסות מוסרית לפעולותיהם. נטען גם כי תכנות, מקיף ככל שיהיה, לא יוכל להקיף את כל הממדים של השיקול האתי, שכן גם אם יכלול חישוב של הנאה וסבל, יתקשה לכלול שיקולים של צדק או הקרבת הפרט למען הכלל.

בכל מקרה, לא ניתן להתעלם מכך שבינה מלאכותית ומערכות אוטונומיות המבוססות עליה מפותחות כיום במהירות וממלאות מגוון משימות במגוון תחומי חיים. מערכות אלו מחייבות את בני האדם, לראשונה בהיסטוריה האנושית, לחשב בצורה מתמטית ולקבל החלטות חד-ערכיות בנוגע לתחומים שהיו מבוססים על קבלת החלטות אישיות של בני אדם שונים במקומות שונים בעולם, על בסיס חינוך, ערכים ותרבות. על כן, האנושות עשויה להידרש לגיבוש מערכת ערכים אחידה על בסיס חשיבה משותפת של פילוסופים בני תרבויות שונות ומשפטנים ממדינות שונות, על מנת לאפשר את המשך ההתפתחות והקדמה בעולמנו. הכורח הזה הוא הזדמנות לשיתוף פעולה בינלאומי, אך מנגד, על בסיס המתרחש כיום בתחום האוטונומיות החמושה והקושי הבינלאומי לקבל החלטות בתחום, נראה שהזדמנות זו תישאר בגדר אתגר. אתגר זה יעמוד גם בפני ישראל בבואה להרחיב את השימוש בבינה מלאכותית לתחומים שונים, ובעיקר לביטחון הלאומי.

חוק ומשפט

אתגר מרכזי לעולם המשפט הוא האחריות לתוצאות השימוש בבינה מלאכותית אוטונומית, או היכולת לתת דין וחשבון משפטי (Accountability). בעוד שבאופן מסורתי, בעליה של מכונה או מפעילה הוא האחראי לתוצאות השימוש בה, קשה לבסס אחריות כאשר פעולות הן תוצאה של למידה עצמונית ופעולה אוטונומית, בייחוד במקרה של גרימת נזק בלתי מכוון לרכוש, אפליה פסולה או פגיעה בנפש.²⁷⁵ נזק הנגרם עקב תקלה במערכת אוטונומית יכול להתרחש למשל בכביש, בסביבת עבודה או כתוצאה מאבחון שגוי בתחום הרפואה. במקרים אלה לא יהיה ברור על מי נופלת האחריות: על היצרן, על המתכנת או אולי על מי שרכש או הפעיל את המכונה. הבעיה מתעצמת בשדה הקרב, שם שגיהא של מערכות נשק אוטונומיות, למשל, עלולה לגרום הרס רב ופגיעה באזרחים – גם בלי שאדם התכוון לכך או יכול לשאת באחריות לכך.²⁷⁶ הקושי בביסוס החבות המשפטית עלול להקשות על החברה האנושית לפעול מבחינה משפטית נגד מדינות החורגות מגבולות החוק הבינלאומי, שכן אלו יוכלו להפעיל מערכות אוטונומיות ולגרום נזק רב מבלי להתמודד עם ההשלכות של מעשיהן. מצב זה עלול לעודד פעולות חסרות אחריות, ולערער את יציבות המערכת הבינלאומית ואת הביטחון הלאומי.

תלות

ככל שנשים מבטחנו בבינה מלאכותית, התלות עלולה לסכן את הביטחון הלאומי כתוצאה מתקלות בחומרה (למשל, הפסקות חשמל או קושי בקירור חוות שרתים חיוניות), כשלי תוכנה או מתקפות מכוונות. אם כמות גדולה של כלים ביטחוניים תהיה תלויה בפעולתה של בינה מלאכותית, פגיעה בה עלולה להשבית את המערכת כולה. על כן חיוני להבטיח שלצד יכולות מתקדמות המחוברות למערכות בינה מלאכותית יתוחזקו גם יכולות מנותקות ממנה – מערכות נשק, כלי רכב ואמצעי תקשורת. כלומר: יש להקפיד על יתירות באמצעות מגוון טכנולוגיות. צורך זה עשוי ליצור אתגר תקציבי ממשלי, וכן לייצר אסימטריה ביחס ליריבים שיחליטו להסתמך על בינה מלאכותית בתחומים שבהם ישראל תבחר להימנע מכך, ומסיבה זו.

בינה מלאכותית בדי "הצד השני"

סוגיה זו מתקשרת באופן כללי לאתגר של בינה מלאכותית בדי "הצד האדום", דהיינו מדינות או ארגונים יריבים. התפשטות הבינה המלאכותית עשויה לאפשר למדינות קטנות ולשחקנים לא־מדינתיים להשפיע באופן לא פרופורציונלי על שדה הקרב, אם יצליחו לנצל את הטכנולוגיה בקנה מידה רחב.²⁷⁷ אתגר זה נוגע במיוחד למדינות וארגונים שהתנהלותם שונה מאלו של מדינות דמוקרטיות ליברליות. למשל, איראן

משקיעה רבות בבינה מלאכותית ומסוגלת לבצע מהלכים מהירים בתחום הטכנולוגי, בגלל היותה מדינה אוטוריטרית השולטת הן בתעשייה, הן באקדמיה והן בצבא באופן מוחלט. בין היתר איראן משקיעה רבות בתחום מבחינה אקדמית, ובשנת 2018 הייתה המדינה הראשונה במזרח התיכון (והתשיעית בעולם) בדירוג מספר הפרסומים בתחום, זאת מתוך 152 מדינות שדורגו. במדרג זה נמצאת ישראל במקום ה-46 בלבד.²⁷⁸ בסוף שנת 2019 קרא נשיא איראן חסן רוחאני לשיתוף פעולה עם מדינות מוסלמיות אחרות, במטרה לשפר את טכנולוגיית הבינה המלאכותית. בציטוט מדברי רוחאני נאמר ש"כלכלה דיגיטלית היא העתיד של הכלכלה העולמית, וצמיחה בתחום תושג על ידי שיתוף פעולה".²⁷⁹ ישראל אמורה להיות מוטרדת מהאפשרות שקריאתו זו תיענה בחיוב על ידי מדינות מוסלמיות נוספות, שחלקן אינן אוהדות את ישראל. בהקשר זה יש לזכור כי לרוב ישראל מתמודדת עם מדינות שאינן דמוקרטיות – ליברליות באופיין, והדבר עשוי להוביל לכך שהן יחליטו להשתמש במערכות בינה מלאכותית באופן שונה מאוד – למשל מבחינה מוסרית ובכל מה שקשור לדין הבינלאומי – מהאופן שבו ישראל תעשה בהן שימוש (בהגבלה עצמית).

מרוץ החימוש

מרוץ החימוש בפיתוח בינה מלאכותית בולט בין ארצות הברית לסין, הנאבקות על הבכורה. במזרח התיכון בולטות ישראל ואיראן. המרוץ עשוי לערער את הסדר העולמי ולשנות את מאזן הכוחות הקיים אם סין תשיג את ארצות הברית, וכן להשפיע על יחסים בין מדינות. אפשר שישאל תיאלץ לבחור עם איזה צד לשתף פעולה – החלטה שיהיו לה השלכות ביטחוניות וכלכליות.

בקרת נשק

התפתחויות טכנולוגיות דוגמת מערכות נשק אוטונומיות, המבוססות על בינה מלאכותית, מעוררות דיונים בערכאות בינלאומית לגבי האופן שבו הן עלולות לערער את היציבות בעולם ולפגוע בזכויות אדם. סוגיה זו חורגת מעיסוק אתי גרידא. מדינות בעלות יתרון יחסי בתחום – ארצות הברית וישראל, למשל – אינן מעוניינות להגביל את עצמן, משיקולים ביטחוניים וכלכליים כאחד. יתר על כן, בעבר תחום בקרת הנשק התמקד בעיקר בבקרת מערכות ותפוצתן, וכיום הדגש מושם יותר ויותר על בקרת רכיבים. יש הסבורים ששינוי זה יהיה משמעותי בהגבלת מדינות למכור או לרכוש יכולות טכנולוגיות מסוימות, כולל התוכנות שבבסיס יישומי בינה מלאכותית. הדבר עשוי להוביל לצמצום האינטרס לפתח טכנולוגיות כאלו בשל צמצום התמריץ המסחרי, או להאיץ מדינות מסוימות לפתח אותן לצורכיהן "כנגד כל הסיכויים".

לוחמת סייבר

מערכות בינה מלאכותית מרחיבות את הפרצה שיכולה להיות מנוצלת על ידי יריבים. ראשית, הן מגדילות את כמות ה"דברים שניתן לפרוץ אליהם" ("hackable things"), בהם גם מערכות שפריצה אליהן תביא לתוצאה קטלנית. חשש זה גובר אם כל המערכות בארגון חולקות את אותה נקודת תורפה.²⁸⁰ שנית, "גניבת" מערכות בינה מלאכותית עשויה להיות קלה יחסית, מכיוון שהן מבוססות כמעט בלעדית על תוכנה שניתן להשתמש בה מייד לאחר הגניבה (בשונה למשל מגניבת תוכנית של מטוס). יתר על כן, למערכות אלה שימוש כפול: את חלקן ניתן להשיג באופן מסחרי ולהתאימן לשימושים ביטחוניים.²⁸¹ שלישית, מערכות בינה מלאכותית יוכלו לשמש לגילוי נקודות תורפה ווקטורים חדשים לתקיפה.²⁸² יריבים יוכלו להכניס טעויות מכוונות לקטגוריזציה של המערכת כך שיכולת הזיהוי שלה, החיונית לקבלת ההחלטות, תיפגם.²⁸³ כמו כן קיים חשש שמערכות בינה מלאכותית יסירו את מחסומי הכניסה של שחקנים יחידים ושל ארגונים לא-מדינתיים למרחב הסייבר. גם אם אינם מסוגלים לפתח תוכנות מורכבות משלהם למתקפת סייבר, הם יוכלו להתאים קוד שפותח על ידי אחרים.²⁸⁴

נשק גרעיני

שימוש במערכות מבוססות בינה מלאכותית בתחומים של קבלת החלטות או בתחומי מודיעין או פיקוד ושליטה עשוי להיות בעל השפעה על הפעלה של חימושים ובתוכם גם נשק גרעיני, בין שהנשק יחובר למערכות אלו ישירות ובין כתוצאה עקיפה של קבלת החלטות. מעבר לכך, קיים חשש שמערכות בינה מלאכותית יגבירו את הסיכוי לשימוש בנשק גרעיני גם אם לא יהיו מחוברות ישירות למשגרי נשק גרעיני. זאת בשל שינוי במאזן הכוחות, שעד כה הבטיח יציבות (יחסית) על בסיס הרתעה הדדית.

מלחמת יתר

ייתכן שאופיין של מערכות בינה מלאכותית וקצב קבלת ההחלטות המהיר שהן מאפשרות, לצד התגובתיות של מערכות נשק, יגרמו מלחמת יתר (HyperWar). כלומר, קצב האירועים יהיה כה מהיר, שהמפעיל או האסטרטג לא יצליח להבין את האירועים ולשלוט בהם, וכך קבלת ההחלטות האנושית כמעט לא תשפיע על התהליך. תגובות מיידיות בעימות הן בעלות פוטנציאל הרסני, למרות שבחלק מן המקרים ובמערכות מסוימות הן עשויות לסייע לייצר הרתעה.

מידע כוזב

בינה מלאכותית מספקת מנגנונים ליצירת תעמולה מותאמת במדויק לקהלים מסוימים ולהרחבת הפצתה. הדבר הופך בעייתי כאשר מדובר במידע כוזב, ואז תוכן שקרי

מופץ בצורה ממוקדת מאוד כך שהשפעתו עשויה להיות נרחבת. כמו כן, במקרה של דמוקרטיה שבהן התקשורת והאינטרנט פתוחים, הדבר עשוי להוות כלי שרת בידי גורמים זרים, שעלולים לנסות להשפיע על תהליכים דמוקרטיים תוך שימוש בכלי הפצה יעילים מאוד.

מצד שני, מערכות בינה מלאכותית יכולות לשמש גם אמצעים לזיהוי ולסינון של תוכן שקרי. הבעיה היא שלרוב היכולת ליצור ולהפיץ מידע כוזב באמצעותה עולה על יכולתם של הכלים לזיהוי מידע כזה,²⁸⁵ מאחר שדרושות דוגמאות רבות לאימון האלגוריתם לזיהוי המידע הכוזב.

דוגמה לשימוש מסוג זה היא בוטים – ישויות שמקדמות באופן מלאכותי תוכן שיכול לבצע מניפולציה על האופן שבו סדר היום מעוצב, שכן הם מכתיבים חשיפה נרחבת – מה שעשוי להתפס כמצביע על אמינות. השימוש בבוטים היה נפוץ מאוד במערכת הבחירות לנשיאות ארצות הברית ב-2016, אז למעלה ממחצית מהתעבורה ברשת הייתה שייכת לבוטים, שהפיצו מידע כוזב על מועמדים.²⁸⁶

דוגמה נוספת היא "Deep Fakes". מדובר בסרטונים מזויפים שמנצלים מערכי נתונים קיימים של וידאו וקול כדי לייצר תוכן מזויף שנראה אמין מאוד. למעשה, סרטונים מסוג זה מאתגרים את הבנת המושג 'אמת' ושוחקים אמון בתוכן ובאמינות של עובדות אמפיריות שנמדדות באמצעות החושים.²⁸⁷ ישראל, שהיא דמוקרטיה בעלת תקשורת פתוחה, ניצבת בהקשר זה בפני אתגר ביטחוני ומדיני כאחד.

שוק העבודה והתעסוקה

בעקבות מהפכות טכנולוגיות ניכרת נטייה לשינויים משמעותיים בעולם התעסוקה. חוקרים רבים סבורים כי האנושות נמצאת על סף מהפכה תעשייתית חדשה, עקב פיתוח בינה מלאכותית וטכנולוגיות האינטרנט של הדברים.²⁸⁸ מהפכה זו תהיה המהפכה התעשייתית הרביעית, לאחר שהראשונה החלה באמצע המאה ה-18, עם כניסתה של אוטומציה מעשה ידי אדם לתהליכים תעשייתיים; השנייה התחוללה במאה ה-19 עקב מעבר לתהליכי ייצור המוני והשלישית התחוללה במחצית השנייה של המאה ה-20, עם כניסתם של מחשבים לעולם התעשייתי. הפיתוחים של המהפכה הרביעית צפויים לייצר מקומות עבודה חדשים, כפי שקרה במהפכות הקודמות, להגביר את היעילות בתעשייה ובתחום השירותים, וכך להעלות את ההיצע ולהוריד את המחירים. הורדת המחירים תוביל מצידה לעלייה בצריכה הפרטית, מה שיוסיף להניע את צמיחת הכלכלה העולמית.²⁸⁹

מנגד, שינויים אלו צפויים להביא להיעלמותם של מקצועות רבים משוק העבודה. בעוד מהפכות קודמות הובילו בעיקר להיעלמותם של מקצועות רבים שדרשו עבודת כפיים, המהפכה הנוכחית עשויה להעלים או לייתר מקצועות בתחומי הידע והמידע,

שאותם יוכלו להחליף מערכות בינה מלאכותית. שוק העבודה יעשה גמיש יותר ויסתמך על כישורי העובדים ועל יכולתם להסתגל למציאות המשתנה, יותר מאשר על הידע המקצועי שלהם.²⁹⁰ מצב זה יוצר אתגר למדינות המפותחות, הנדרשות לשנות את גישתן להשכלה ותעסוקה ולייצר מערכות שיאפשרו למידה והתפתחות לאורך החיים. כן יהיה צורך להתאים את המערכות התומכות במדינה ואת חוקי ההעסקה למציאות המשתנה, על מנת לתמוך בשכבות שונות באוכלוסייה ובצורכיהן.

מבט לעתיד המעט רחוק יותר מעלה שאלות בנוגע לעתידו של עולם התעסוקה, כאשר צפוי כי גם מקצועות שונים, ביניהם כתיבת ספרים וביצוע ניתוחים כירורגיים, יבוצעו בצורה טובה יותר על ידי תוכנת בינה מלאכותית מאשר על ידי אדם, עד שנת 2053.²⁹¹ מצב מסוג זה יציב את מרבית האנושות בפני משבר תעסוקתי חמור, שאפשר כי יאלץ אותה לכוון סדר חברתי שאינו סובב את תעסוקה. לחלופין עשויים להיווצר מקצועות חדשים לחלוטין וצורות עבודה שאינן דורשות מאפיינים מסורתיים של שוק העבודה כיום, ובכלל זה נוכחות פיזית.

אוטונומיות בשוק העבודה מציבה אתגרים עקיפים לביטחון הלאומי. ראשית, הפיכת תעשיות לאוטונומיות גורמת להיותן מטרה למתקפות ולפריצות מצד מדינות מתחרות. מכיוון שכלכלת מדינות תישען יותר ויותר על מערכות ממוחשבות, יהיה עליהן להתמקד בפיתוח אמצעי הגנה שיבטיחו את אמינות התעשיות וביטחונן. שנית, אם המדינות לא יצליחו לייצר עבודה לרבים שיאבדו את משרותיהם, יהיה עליהן להבטיח רווחה באמצעים אחרים. במדינות מסוימות דוגמת פינלנד מתקיים דיון בנוגע לקצבת קיום בסיסית, שנדרשת כדי להבטיח את הביטחון האזרחי-כלכלי של האזרחים, שחלקם אינם מועסקים, בין היתר בגלל השפעות הקדמה והאוטומציה.²⁹² יהיה צורך בהרחבת דיון זה למדינות נוספות, ככל שהאוטונומיות תצמצם תחומי תעסוקה מסוימים. דיון חשוב נוסף בתחום זה מתייחס לגביית "מס הכנסה מרובוטים", המתחילים להחליף עובדים בתחומים שונים.²⁹³ שינויים כאלה יידרשו על מנת לייצב את החברה מבחינה כלכלית וחברתית.

אי־שוויון קיצוני בחלוקת המשאבים בחברה

הגלובליזציה וההתקדמות הטכנולוגית מרחיבים פערים הן במדינות והן ברמה הגלובלית.²⁹⁴ מכיוון שהחברה המודרנית מושתתת על חלוקת הרווחים על פי תרומה יחסית, הישחקותם של מקצועות רבים עלולה להותיר רבים בלי יכולת לתרום לכלכלה. בעוד הכלכלה תוסיף לצמוח, ייתכן כי פחות ופחות אנשים יזכו ליהנות מחלוקת רווחיה.²⁹⁵ גם הגישה לטכנולוגיה עצמה עלולה להתאפיין באי־שוויון. מדינה המחזיקה ראשונה בבינה מלאכותית מתקדמת תזכה ל"יתרון ראשוני" על פני מדינות אחרות במגוון תחומים, לרבות כלכלה וביטחון. כך גם יחידים שתהיה להם גישה לטכנולוגיות

בינה מלאכותית מתקדמות יזכו ליתרון. אי־שוויון יתרחב גם בכל הנוגע לגישה לטיפול בריאות, ביטחון אישי, איכות חיים ויכולת קידום עצמי.²⁹⁶ בהקשר זה צפוי שעסקים מעוטי משאבים יהיו בלתי תחרותיים, שכן הם לא יוכלו להתחרות ביכולות הבינה המלאכותית של בעלי העסקים הגדולים. כך ייווצרו מונופולים עסקיים. כבר כיום מדינות שוקלות להגביל את החברות הטכנולוגיות הגדולות,²⁹⁷ עקב הבנת הסיכונים הטמונים באותם מונופולים. מדובר בבעיה מורכבת, שמאפייניה השונים ימשיכו להתבהר וידרשו מענה ככל שתתקדם ההתפתחות הטכנולוגית.