

ביקורת ספרים

AI, Automation, And War - The rise of military-tech complex / Anthony King, Princeton University Press

יוסי גולדברג

בעל תואר ראשון במתמטיקה ומדעי המחשב מאוניברסיטת בר אילן, בעל ניסיון של 25 שנים בתכנות מחשבים וניהול צוותי פיתוח בפרויקטים בתחומי התקשורת, תשתיות תוכנה וסייבר, וכן בעל ידע עצמאי בהיסטוריה צבאית. לאחרונה מתעניין בשימושים של בינה מלאכותית כחלק מפיתוח תוכנה

בעשור האחרון עובר עולם המחשבים מהפכה של ממש. תוכנות מבוססות בינה מלאכותית מציגות יכולות מתקדמות שרק לפני שנים מעטות נחשבו בלתי אפשריות, ואף עוקפות את המין האנושי בכמה תחומים. המהפכה הזאת, אשר אנחנו נמצאים במהלכה, משפיעה על כמעט כל תחום ומשנה את דרכי העבודה והרגלי החיים. הבינה המלאכותית מעוררות שאלות רבות כגון איזה תחומי תעסוקה יוחלפו על ידי מחשבים או רובוטים, האם אמנות שנוצרה על ידי בינה מלאכותית תהיה שווה ערך לאמנות שיצרו אנשים, והאם מדינה שאין לה יכולות בינה מלאכותית תצליח לשרוד בשנים הבאות?

בספר שלפנינו המחבר רוצה לבדוק כיצד המהפכה הזאת, שיש שמשווים אותה לגילוי האש על ידי פרומתאוס, משפיעה על הצבא. הוא רוצה לבדוק שתי טענות שמושמעות במחקר ובדיונים ציבוריים - האם הבינה המלאכותית תנהל את המלחמה הבאה ותקבל החלטות אסטרטגיות כמו פתיחה במלחמה, או ניהול קרב, והאם נראה בעתיד הקרוב כלי נשק אוטונומיים המופעלים על ידי מחשבים ללא התערבות אנושית? הוא מביא את ספרם של קיסינג'ר, שמידט והוטנלוך מ־2021, שבו קראו למקבלי ההחלטות להטיל מגבלות על הבינה המלאכותית כדי שלא נגיע

למצב בו מחשב יכול להחליט לפתות במלחמה ללא התערבות אנושית (Kissinger, Schmidt, & Huttenlocher, 2021).

כדי לבדוק את השאלות הללו הכותב סוקר את ההישגים של הבינה המלאכותית, הן בתעשייה האזרחית הן בשימושים הצבאיים שלה כיום, כדי לראות האם היא בדרכה להשתלט על הצבא. מטבע הדברים הוא בוחן רק את אופן השימוש של הצבאות המערביים, בעיקר ארצות הברית, בריטניה וישראל. עקב כך יש סימן שאלה בנוגע ליכולות הבינה המלאכותית של צבאות סין ורוסיה שהספר אינו מתייחס אליהם, אולם לדעתי סביר להניח כי לנוכח היכולות של התעשייה האזרחית שלהם, שאין שונות במהותן מהיכולות בתעשייה האזרחית המערבית, אין פריצת דרך בשימושים צבאיים שלהם לעומת צבאות המערב.

הספר מראה כי כיום השימושים העיקריים של הבינה המלאכותית הם ניתוח ועיבוד מאגרי ענק של נתונים לצורך הפקת מודיעין מדויק בזמן קצר; עזרה בניתוח שדה הקרב; ותכנון צבאי ויכולות סייבר התקפיות והגנתיות. לדבריו, ערפל הקרב שדיבר עליו קרל פון קלאוזביץ בא לידי ביטוי כיום בעודף מידע, ורק בעזרת בינה מלאכותית אפשר לפזרו. המשותף לכל השימושים הללו - הם באים לעזור למפקד ולמקבל ההחלטות, אבל לא להחליפו. הבנה זאת מתיישבת עם השימוש של בינה מלאכותית בתעשייה האזרחית היום, כאשר ה-AI הם כלי עזר ולא תחליף. לדוגמה מודלי השפה החדשים (Chat Gpt ודומיו) יודעים לכתוב קוד לזיהוי שגיאות בקוד קיים באופן שאולי מייתר את הצורך במתכנתים, אולם כרגע רואים שהתוכנות האלו רק מיעלות את עבודת המתכנתים אך לא מחליפות אותם. לדוגמה חברה אמריקנית שהחליטה לפני כמה חודשים להחליף את המתכנתים שלה בבינה מלאכותית, ולאחרונה פרסמה כי היא חוזרת בה ומגייסת מתכנתים אנושיים בחזרה.

הכותב מציין, באופן נכון, כי הלוגיקה שבונה את הבינה המלאכותית מורכבת מאלגוריתמים הסתברותיים, ללא הבנה של הקשר, וכי הם תלויים לחלוטין בנתונים שסופקו להם על ידי המפתחים לצורך האימון שלהם. לנוכח עבודה זאת, טוען הכותב כי הבינה המלאכותית לא תתאים לקבל החלטות אסטרטגיות מכיוון שקשה להשיג מאגר נתונים מספיק גדול כדי לאמן מודל על החלטות כאלה. הוא אף מאפיין נכון כי בניגוד לתעשייה האזרחית, בשימושים צבאיים יש אויב המנסה למצוא את החולשות בבינה המלאכותית ולגרום לה לטעות, ולכן יהיה קשה להסתמך עליה בלעדית. לדעתי הוא נוגע פה בנקודה נכונה - הרבה יכולות מחשוב יצאו לשימוש ללא מחשבה מספיקה על הגנה בטיחות - לדוגמה כאשר פרטוקול הרשת IP

התפרסם, הוא נכנס לשימוש בכל העולם במהירות מרבית ללא מחשבה על הגנה מפני התחזות והעתקת מידע לא מאושרת, והיה צורך לפתח כלים רבים שיגנו על הרשת (כמו firewall, vpn ועוד רבים). כבר היום יש דוגמאות כיצד ניתן לנצל בקלות חולשות של בינה מלאכותית, ואי אפשר לסמוך עליה ללא פיקוח אנושי.

בספר סוקר הכותב את התחומים שכיום משתמשים בבינה מלאכותית - תכנון, מציאת מטרות ומבצעי סייבר, ומנסה ללמוד מהם על יכולות הבינה המלאכותית. הפרויקטים שהוא סוקר הם לדוגמה מודל שמנסה לנבא תוצאות קרב לפני נתוני הצבאות המשתתפים, ומודל אחר שמנבא תוצאות קרב אויר אוויר. שני אלה יכולים לעזור במשחקי מלחמה ובבדיקת תוכניות קרב. פרויקט Maven של הצבא האמריקני שפיתחה חברת גוגל, משתמש בבינה מלאכותית כדי לנתח סרטי וידאו ולהפיק בצורה מהירה מטרות ומודיעין ממספר רב של סרטים; פרויקט אחר שהצבא האמריקאי מקדם בעזרת כלי בינה מלאכותית הוא יכולת לנבא איפה יניח האויב מטעני צד. הכותב מביא גם דוגמה מהצבא הבריטי שם השתמשו במודל בינה מלאכותית על מנת למצוא ביעילות חולי קורונה בליברפול בזמן המגפה.

פרויקט אחר מנסה לנבא איפה יניח האויב מטעני צד; מציאת חולי קורונה בליברפול על ידי הצבא הבריטי. גם במבצע "שומר החומות" שערכה ישראל (מאי 2021) הוא מוצא דוגמה לשימוש בבינה מלאכותית - הוא מצטט את הרמטכ"ל דאז, רא"ל אביב כוכבי, שאמר כי בעזרת תוכנה מבוססת בינה מלאכותית שפיתחו בצה"ל, ומייצרת מטרות מתוך כמויות מידע גדולות, היה הצבא מסוגל לייצר 100 מטרות לתקיפה בכל יום, לעומת 50-100 מטרות חדשות בשנה. המחבר מצטט גם את מפקד 8200 לשעבר, תא"ל יוסי שריאל, שטען כי צוות של אנשים ותוכנות יהיו מסוגלים לתת לצבא 80 אלף מטרות לפני המלחמה ו-1,500 מטרות חדשות מדי יום במהלכה, וכי הוא מעריך שצוותים כאלה ידעו גם לזהות טרוריסטים פוטנציאליים.

המשותף כמעט לכל הדוגמאות שהספר מציין הוא שהם פותחו לפני שמודלי בינה מלאכותית ג'נרטיביים נוצרו, ולפני שהחל השימוש הרחב בהם. הדבר מובן מכיוון שלוקח זמן מרגע שטכנולוגיה חדשה יוצאת ועד שהיא מבשילה לכדי שימושים צבאיים, וכנראה שתידרש בדיקה נוספת בעתיד הקרוב לראות אם כלים ג'נרטיביים יהיו מוגבלים או שיפתחו יכולות חדשות שעוקפות את המגבלות שיש כיום לבינה המלאכותית.

חלק מהספר מוקדש לאופן הבנייה של כלי הבינה המלאכותית ואיך הוא משפיע על התעשייה האזרחית ועל הצבא עצמו. הכותב טוען שכיום עולה תעשייה חדשה

- הקומלפקס הצבאי־טק (או דיפנס־טק). מכיוון שאין לצבא ולגופי הביטחון את האנשים והתקציבים לפתח בינה מלאכותית בעצמם, הם נדרשים לרכוש את הכלים הללו מחברות אזרחיות. בניגוד לרכש כלי נשק "מסורתיים", הבינה המלאכותית דורשת מעורבות עמוקה של המפתחים לאורך חיי הפרויקט, והדבר מביא לאתגרים חדשים ולא מוכרים. הדיפנס־טק שונה מהתעשייה הצבאית בהרכב האנשים - הבינה המלאכותית מפותחת בעמק הסיליקון עם חברות בעלות מאפיינים דומים ואידיאולוגיה אנטי־מלחמתית לרוב. הדבר מסכן את השימוש הצבאי בפרויקטים אלה, מכיוון שהחברות יכולות יום אחד להפסיק את הפרויקט משיקולים כלכליים או אידיאולוגיים. לדוגמה פרויקט Maven שפיתחה גוגל עבור צבא ארצות הברית, ובעקבות מחאות של עובדים החליטה להפסיקו. דוגמה טרייה לכך ראינו לפני כמה שבועות, כאשר מיקרוסופט הקפיאה את השימוש של יחידת 8200 בשירותי הענן שלה, וכנראה גרמה לבעיות עיכובים בפרויקטים מסוימים.

הכותב מראה כי בשנים האחרונות יש שינוי בהתייחסות של הממסד הביטחוני האמריקני לבעיות מסוג זה, וניסיון להגברת השליטה של הצבא על הפרויקטים כדי למנוע מצבים כאלה. על רקע זה הוא מציין לטובה את ישראל שבה הקשר בין המגזר הטכנולוגי לממסד הצבאי הוא הדוק ביותר על רקע איומים המידיים, הרקע האתני המשותף ושירות החובה בצבא, ולכן הדיפנס־טק הישראלי רואה באופן שווה עם הממסד הביטחוני את הצורך בפיתוח משותף. לדוגמה פרויקט משואה של אלביט שבה החברה נהנית מקשר ישיר ללקוח, המאפשר פיתוח שמתאים לצה"ל ולאתגרים הספציפיים שלו. כמו כן, צה"ל סומך על אלביט לשיתוף פעולה גם בזמן מלחמה או עימות מוגבל, שיכולים לעורר בעיות אתיות או מוסריות. לקורא הישראלי תתעורר פה השאלה האם לנוכח חוסר הסכמות בחברה בעת האחרונה, והוויכוח הפוליטי העז וערעור על הלגיטימיות של פעולות הממשלה, נראה בעתיד סירובים של חברות אזרחיות לעבוד עם הצבא והממסד הביטחוני בכלל.

נקודה נוספת שהכותב מעלה היא הכוח הרב, לעיתים ברמת מדינות, שחברות כאלה צוברות. הוא חושב שיכול להיות שהקומפלקס הנ"ל מערער את ההגדרה של מדינה כפי שהגדיר אותה מקס וובר (מונופול על הפעלת כוח) ויהיה צריך לראות איך מתמודדים עם חברות אזרחיות שמחזיקות בכוח שווה ערך למדינה. לדוגמה המקרה של חברת סטרלינק של אילון מאסק, המאפשרת תקשורת לוויינית לאוקראינה אחרי שרוסיה השביתה את התקשורת שם, ובהחלטה אחת של מייסדה סגרה את התקשורת לכל הצבא שלהם.

אספקט נוסף הוא צורך בשילוב המפתחים בעת השימוש במודל - דבר המשותף לפרויקטים רבים מבוססי תוכנה, אך בבינה מלאכותית הצורך גובר עקב הצורך בכוונון המודל לפני הנתונים בשטח והבעיות המשתנות, ולכן ניתן לראות כיום צוותי טכנולוגיה אזרחיים שנמצאים במפקדות מבצעיות ומשתתפים בפועל בזמן פעילות. הכותב מתאר בפירוט את ההקמה והפעילות של הגוף שהיה אחראי לאיתור המיקום של גנרל ולרי גרסימוב מפקד הצבא הרוסי באוקראינה במאי 2022, ומראה שהקבוצה הזאת הייתה מורכבת מאנשי צבא שהיו אחראים לצד המבצעי, ומאזרחים שהיו נוכחים במפקדות ואחראים לפיתוח התוכנה, טיובה ופתרון בעיות בזמן אמת ככל שקרו. לטענתו אנו רואים שינוי בהרכב המפקדות וככל שהבינה המלאכותית תוטמע בצבאות - יותר אזרחים יהיו נוכחים שם ושותפים לפעילות הצבאית. השיתוף מוביל לשאלות כמו איזו אחריות ניתן להטיל על המפתחים של הבינה המלאכותית? האם הם נחשבים כמפעילים כוח צבאי על אף שאינם חיילים? האם אפשר לסמוך עליהם כמו על חיילים? הספר משאיר את השאלות אלו פתוחות ולא נותן להם תשובות.

השאלה בנוגע לשיתוף של המפתחים באופן השימוש הצבאי בכלי הנשק שהם מפתחים אינה חדשה, ולאחרונה הוצגה באופן ברור ומודגש בסרט אופנהיימר על פיתוח פצצת האטום האמריקנית. במהלך כל הפיתוח קבעו המדענים את רוב ההחלטות ואת דרכי הביצוע, כאשר האחראי מטעם הצבא עומד ברקע, אולם ברגע שהושלם הפיתוח השתלט הצבא על הפרויקט וההחלטות על הנשק הופקעו למעשה מידי המדענים - דבר שגרם להם לתסכול רב ולתחושה שהנשק שפיתחו יוכל לשמש במקומות שלא היו רוצים שישתמשו בו, וכי הם חסרי אונים בקשר לזה.

בניגוד לאטום, או לשאר הנשק שאנו מכירים, מכיוון שמפתחי הבינה המלאכותית מעורבים עמוקות גם בזמן השימוש נותרת יכולת השפעתם גבוהה, אולם לדעתי ברגע שהתעשייה תתייצב ותתבגר יהיה פחות צורך בשיתוף פעולה הדוק עם המפתחים, ולכן יכולת האמברגו שלהם תפחת ותידמה לשאר התעשייה הצבאית: אפשר לראות את התהליך הזה בטכנולוגיות מבוססות תוכנה אחרות - כמו למשל מערכות הפעלה, שכיום לאחר כ-20 שנים יציבות ולא נדרשת מומחיות ברמה גבוהה לתפעולם. בשל כך הידע לשימוש מצוי אצל מספר רב של אנשים, וגם הצבאות יכולות לתת רמה של תמיכה ושימוש פנימיים ללא צורך בתלות בחברות האזרחיות בזמן אמת.

בסיכום הספר טוען המחבר כי בחמש השנים הקרובות לפחות אנחנו לא צפויים

לראות בינה מלאכותית לוקחת על עצמה את ההחלטות בשדה הקרב, והמלחמה לא בדרך להיפך למלחמה אוטומטית שמופעלת על ידי כלי בינה מלאכותית. יתרה מכך, היא איננה "תרופת קסם" וכראיה לדבר הוא מביא את מתקפת 7 באוקטובר 2023, שבה ברגע שנטרלו בחמאס את המצלמות והחיישנים בגבול עזה הם פגע במידע, ולכן האלגוריתם מבוסס בינה מלאכותית לא יכול להפיק מטרות חדשות בזמן אמת ולא היה בו שימוש בזמן שהכי נדרש.

במבט לעתיד, הוא צופה כי הקרב הימי ישתנה עקב היכולת של כלי בינה מלאכותית לנתח מידע ממספר רב של חיישנים, לעקוב אחרי כלי השייט בזמן אמת ולרכוש מטרות באמצעות בינה מלאכותית, ובשל פיתוח טילים מהירים ארוכי טווח יש סיכוי שכלי השייט יהפכו לפגיעים הרבה יותר מהמצב היום.

תחום המחשוב, ללא ספק, עובר מהפכה בשנים האחרונות שהתגברה בעקבות יציאת כלי בינה מלאכותית ג'נרטיבית. העדכונים והחידושים צצים בתדירות שבועית, חברות הטכנולוגיה המובילות בעולם משקיעות הון רב בפיתוח ובטיוב המודלים ושוקי עבודה רבים מתמודדים עם השאלה איך להפיק את המיטב מהכלים החדשים. סביר להניח שהצבאות יגבירו אף הם את השימוש, ויהיה מעניין לראות בתוך כמה שנים האם הניתוח של הספר על תחומי השימוש על ההשפעה על המערכת הצבאית בכללותה הייתה מדויקת או לא.

מקורות

King, A. (n.d.). AI, automation, and war: The rise of the military-tech complex. Princeton University Press.

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). The age of AI: And our human future. Little, Brown and Company.