כך עובדת הבינה המלאכותית בשירות אירגוני הטרור

written by אלי קלוטשטיין | 07.11.2024

בינה מלאכותית (Artificial Intilligence, AI) היא אחד החידושים המיוחדים והמתקדמים של העשור האחרון. היא נמצאת בכל תחומי חיינו, ומשמשת לשלל מטרות. יודעי דבר חוזים שככל שתתפתח הטכנולוגיה הזאת, היא עשויה לפתוח אפשרויות חדשות בפני האנושות ולסייע לה בתחומים רבים.

יש לבינה המלאכותית תפקיד חשוב ומהותי בשנים האחרונות בממד הביטחוני. בישראל היא משמשת לצרכים צבאיים רבים, ומסייעת לכוחות הביטחון להילחם בטרור. כך למשל, לפי דיווחים עזרה טכנולוגיה של בינה מלאכותית לצה"ל לזהות מטרות של חמאס בעזה ולתקוף אותן. יישום אחר של בינה מלאכותית הוא היכולת שלה לסייע למלחמה במימון הטרור ובטרור כלכלי. ביחידה 8200 של צה"ל, יחידת מודיעין האותות ("סיגינט") המרכזית של הצבא, יש מרכז בינה מלאכותית. במבצע שומר החומות, סיפר מפקד המרכז, אפשרה טכנולוגיה מתקדמת לסרוק מאגרי מידע עצומים ולברור מהם מידע שבזכותו הצליח צה"ל לזהות פעילי טרור. ניתן רק לדמיין אילו עוד שימושים יש לכלים מתקדמים כאלה בצה"ל ובמערכת הביטחון כולה, אולם אין ספק שהכלים הללו קיימים ומתפתחים כל הזמן.

אלא שבמקביל, ההתפתחויות המהירות של הבינה המלאכותית יכולות לשמש גם את אויבינו, לצד מחבלים ופעילי טרור בעולם כולו, פושעים בינלאומיים, כנופיות סמים ועוד. היישומים החדשים משדרגים את הפעילות של קבוצות כאלה, ומאפשרים להן לייעל את מימוש מזימותיהן.

מנהלת קבוצת המודיעין הפתוח SITE, ריטה כץ, הבהירה כי בינה מלאכותית משמשת מגוון רחב של קבוצות שליליות, מאל-קאעידה ועד רשתות נאו-נאציות. "קשה להבין עד כמה בינה מלאכותית היא מתנה לטרוריסטים ולקהילות קיצוניות", היא ציינה.

גם גורמי ביטחון מודיעין שותפים לדעה הזאת. מייק בורגס, מנהל ארגון המודיעין הביטחוני באוסטרליה, הזהיר כי "בינה מלאכותית ככל הנראה תהפוך מאמצי הקצנה למהירים וקלים יותר". גוף מיוחד שהקים האו"ם לצורך בקרה על טרור וטכנולוגיה דיווח כי רשתות קיצוניות החלו להשתמש בכלים מתקדמים של בינה מלאכותית לצורך הפצת תעמולה, עיוות הנרטיב של אירועים בעולם האמיתי והשפעה על דעת הקהל ביחס לפעילותם ונגד ממשלות. בין היתר, משמשים הכלים הללו גם לגיוס ממוקד ומוצלח יותר של פעילי טרור, סייענים ותאים רדומים.

ככל שמתפתחות היכולות של הבינה המלאכותית, כך היא מעמידה לרשות המחבלים שימושים

אחרים. כך למשל, אם פעם הוגבלה הטכנולוגיה לשימוש בהודעות טקסט פשוטות, כיום יש לה אפשרות ליצור תמונות, סרטונים או קובצי שמע באיכות כמעט-אמיתית. כל אלה נמצאים גם בשימוש של גורמים שליליים. תארו לעצמכם פעולת פישינג שכוללת הודעה קולית המחקה את קולו של אדם קרוב, המתחנן לקבל כסף. רבים בוודאי ייפלו בפח כזה, וספק אם הרשויות מסוגלות לסכל הונאות מעין אלה בקנה מידה גדול.

ואכן, לא בטוח שישראל גם יודעת להתמודד עם היקף התפוצה של הבינה המלאכותית והשימוש בה. ביוני שעבר זמן נצחי במושגי ההתקדמות של בינה מלאכותית הזהיר מבקר המדינה מתניהו אנגלמן כי "הבינה המלאכותית עשויה להביא לכדי התקדמות טכנולוגית רחבת היקף בתחומים רבים, אך לצידה קיימים גם סיכונים רבים, ובהם 'פייק ניוז' ושימוש על ידי גורמי טרור ופשיעה". המבקר הוסיף כי יבחן את ההיערכות של הממשלה בישראל, ובין היתר יבדוק "כיצד מגינה הממשלה על אזרחיה ועל עצמה על ידי הגבלת השימוש בטכנולוגיות בינה מלאכותית שעלולות לגרום להשפעות שליליות ולחשוף את הציבור לסכנות".

סדנת טרור ו-AI

באופן מסורתי, פעילי טרור ידעו בעשורים האחרונים להסתגל במהירות לטכנולוגיות מתקדמות, לנצל אותן למזימותיהם ולהשתמש בפיתוחים חדשים ביעילות ובקטלניות. באופן פרטני, מחבלים הוכיחו בעבר את נחישותם לנצל את הרשת לקידום מטרותיהם.

למודלים מתקדמים עם יכולות למידה עמוקה כגון ChatGPT נבנים גם כללים שמונעים ממשתמשים להסתייע בהם כדי ללמוד כיצד להתחמק מרצח. ענקיות טכנולוגיה כמו מייקרוסופט הצהירו כי יפתחו אמות מידה לשימוש "אחראי" בבינה מלאכותית, תוך התבססות על עקרונות כגון הוגנות, אמינות וביטחון, פרטיות, שקיפות או אחריותיות. אולם הכללים הללו לא מושלמים, יש בהם פרצות, ומחבלים בעלי ידע וכישורים טכנולוגיים בוודאי יבינו במהירות כיצד לעקוף אותם ולהתגבר עליהם.

הנה כמה דוגמות לאופן שבו השתמשו ארגוני טרור בטכנולוגיות מתקדמות של בינה מלאכותית בשנים האחרונות: דאעש שידר סרטון ובו ישב קריין חדשות שחגג את המתקפה ברוסיה על אולם המופעים במרץ האחרון, שבו נרצחו 140 בני אדם בידי מחבלים של ארגון הטרור. הסרטון נראה אמיתי, אך למעשה היה תוצר של תוכנה המסתייעת בבינה מלאכותית.

תעמולה היא אכן אחד השימושים המרכזיים של בינה מלאכותית בידי פעילי טרור. הרי כל מה שדרוש לשם כך הוא מחשב, יצירתיות וכישרון, הבנה בסיסית של כמה תוכנות מתקדמות, והזדהות עמוקה עם הערכים שמבקש המשתמש לקדם. ואכן, ארגוני הטרור מבינים את הפוטנציאל שיש בהפצת הידע של השימוש בכלים אלה בקרב תומכיהם. גורמים המזוהים עם אל-קאעידה פרסמו בפברואר את קיומה של סדנה ברשת המלמדת את השימוש בכלים טכנולוגיים מתקדמים כאלה. מאוחר יותר הפיצה אותה קבוצה גם חוברת בת עשרות עמודים,

מעין מדריך לאדם ההדיוט, לשימוש ב"כלים מודיעיניים מלאכותיים".

אפילו בזירה המקומית נראה כבר שימוש בתוכנות של בינה מלאכותית לצורך המלחמה של מחבלי חמאס בישראל. בתחילת המלחמה הפיק חמאס תמונות מזויפות של תקיפות לכאורה שביצעה ישראל בעזה, או סרטונים שבהם מופיעות משפחות של עזתים, לכאורה, סורקות את הריסות בתיהן המופצצות והכול במטרה לייצר אהדה לחמאס, ובמקביל לפגוע בתמיכה בישראל ובצה"ל. בסרטים אחרים נראו טנקים ישראליים עוברים דרך שכונות ברצועה.

ארגון הטרור העזתי יוצר באמצעות תוכנית של בינה מלאכותית גרפיקות מתוחכמות כדי לדרבן פלסטינים חדורי אידיאולוגיה לבצע פיגועים בשמו, ובמיוחד בשטחי יהודה ושומרון. תומכי הארגון מפרסמים בטלגרם וברשתות החברתיות קריאות לפגיעה בישראל ותעמולה בעד חמאס בתפוצה רחבה, תוך שימוש בבוטים המונעים על ידי טכנולוגיה חדישה כזו, במטרה לשלהב את ההמונים לצאת לרחובות.

גם חיזבאללה, לפי דיווחים, מנצל יישומים של בינה מלאכותית. הוא משתמש כנראה בבינה מלאכותית בכטב"מים המתקדמים שהוא משגר לעבר ישראל. שנית, חיזבאללה מפעיל שיטות לוחמה פסיכולוגית, קרבות השפעה ותעמולה ברשתות החברתיות ובאינטרנט כבר שנים רבות, וסביר להניח שבשנים האחרונות הוא נעזר לשם כך גם בבינה מלאכותית.

כלי נשק אוטונומיים

ככלל, ניתן אולי להציע חלוקה של יישומי בינה מלאכותית בשימוש הטרור לכלים "רכים" ו"קשים". הראשון מבין הכלים הרכים, שכבר הוזכר לעיל, הוא הפצת תעמולה. בינה מלאכותית מציעה שלל אפשרויות ליצירת תוכן והפצתו במהירות וביעילות גבוהות מאי פעם, ומאפשר למשתמשים "לשחק" על הרגשות של קהל היעד שלהם באמצעות ויזואליה, מוזיקת רקע ומסרים ממוקדים. לא רק שניתן לברוא תוכן מתקדם, אשר נראה אמיתי ומושקע, אלא שישנה אפשרות גם להקים משתמשים מזויפים ("בוטים") ברשתות החברתיות כדי לקדם אותו במספרים גדולים. השימוש בבוטים מקשה גם על חברות שמפעילות את הרשתות הללו לזהות את הפצת התעמולה ולבלום אותה.

אגב, תעמולה אינה מוכרחה להיות הפצת מידע ואידיאולוגיה בזכות הארגון. היא יכולה, למשל, להיות פרסום מידע כוזב, שפוגע באויב, מחליש את המורל של אזרחיו ומטעה את מפקדי היריב. תופעת ה"דיפ פייק", כמו שהיא מכונה, מאפשרת למשל "להדביק" פרצופים על דמויות, להשמיע קולות מדויקים של אדם מסוים ולהשתמש בכך כדי לדבר לכאורה בשמו.

כך למשל, גורמים המזוהים עם רוסיה פרסמו סרטון לכאורה של נשיא אוקראינה, וולודימיר זלנסקי, כשהוא מפציר בלוחמיו להניח את נשקם. פרצופו של זלנסקי מודבק על הדמות המדברת, וקולו נשמע בסרטון אך הגוף שמופיע בסרט נותר סטטי במשך כולו, מה שמעיד על הזיוף. עם זאת, חשבו על לוחמים בשדה הקרב, קבוצה גדולה שלהם מצטופפת סביב מכשיר

טלפון זמין אחד בשעת מנוחה יקרה: האם יבחינו בדקויות הקטנות? כיצד ישפיע עליהם סרטון כזה? כיצד יגיבו בישראל אם חמאס יעשה שימוש בסרטון כזה כדי "לצלם" חטופים ולדובב אותם למענו?

חשוב גם להדגיש את ההשפעה השלילית שיכולה להיות לקמפיינים כאלה על קהל יעד פרטני: ילדים ובני נוער. הללו מבלים חלק ניכר מזמנם ברשת, ובשל גילם הצעיר יכולים להוות מטרה קלה יחסית לאינדוקטרינציה קיצונית.

דרך אחרת לנצל את האפשרויות שמציגה הבינה המלאכותית היא לצורך גיוס פעילים לחוליות טרור. בוטים, שמופעלים בעזרת טכנולוגיה מתקדמת, יכולים לתקשר עם מגויסים פוטנציאליים, לספק להם מידע שנפתר במיוחד לפי האופי שלהם ולבחון את התאמתם לארגון. באפגניסטן, למשל, אנשי מחוז ח'וראסאן של דאעש ניסו להשתמש בקשרים שיצרו באינטרנט עם צעירים אירופים כדי לנסות לשכנע אותם להצטרף לשורות הארגון ולבצע מתקפות בארצות מוצאם.

תוכנות של בינה מלאכותית יכולות גם לשמש לגיוס כספים. מחקר ישראלי מצא כי פלטפורמות מתקדמות הגיבו לבקשות של החוקרים לסייע להם במשימה של "גיוס כספים למדינה האסלאמית", וסיפקו לחוקרים הוראות מפורטות כיצד לנהל קמפיין לגיוס כספים, ומה בדיוק כדאי לומר ברשתות החברתיות כדי להצליח בקמפיין.

לצד זאת, הטכנולוגיה החדישה הזאת גם מאפשרת לפעילי טרור להשתמש בכלים "קשים" יותר. הכוונה, למשל, ליכולת העברת מסרים מוצפנים ונסתרים, או לדליית מידע מסווג באמצעים מתוחכמים. יתרה מכך, כפי שאמרה שרת הפנים הבריטית, הכלים החדישים יכולים לשמש פעילי טרור לתכנון בפועל של מתקפות טרור יעילות וקטלניות יותר. דוגמה אחת היא היכולת להשתמש בסימולטורים לתכנון נתיבי טיסה של כלי טיס בלתי מאוישים, שיכולים לפגוע בלב האויב.

בכלל, השימוש בכטב"מים או בכלים אוטונומיים אחרים הולך ומתפתח במהירות בעזרת בינה מלאכותית. באופן כזה יכולים מחבלים לא לסכן את חייהם, ובכל זאת לפגוע בבטן הרכה של האויב ולבצע מתקפות יעילות יותר. כבר לפני שנים אחדות דן האו"ם בסכנה שנשקפת מהכיוון הזה, ולדברי מומחים כלי נשק אוטונומיים שמקבלים החלטות על ירי בשבריר שנייה, תוך הסתמכות על מידע שמגיע מהחיישנים שלהם, הופכים נפוצים בשדה הקרב יותר ויותר. יש באפשרות המפעילים של הכלים הללו להסתייע בבינה מלאכותית כדי לתכנן מסלול, לנווט, לבצע זיהוי מתקדם של המטרה ועוד. אחד החששות הגדולים של מומחים נגד טרור הוא משימוש עתידי של מחבלים ברכבים אוטונומיים עמוסים בחומרי נפץ, שינהגו למטרה ו"יתאבדו" עליה בדומה לשימוש שצה"ל עשה בנגמ"שים ישנים בעזה. לפי הדיווח, דאעש פועל לפתח רכבים כאלה.

שימוש "כבד" אחר של בינה מלאכותית הוא לצורך שיגור מתקפות סייבר מתוחכמות, כאלה שבני אדם יתקשו לבצע בפרק זמן קצר בכוחות עצמם. מתקפות כאלה יכולות לגרום נזק בפני עצמן, אך הן גם יכולות להוות מעין "מכה מקדימה", אמצעי לריכוך האויב ולבלבולו לפני ביצוע מתקפות עם כלי נשק פיזיים.

מזכ"ל האו"ם, אנטוניו גוטרש, הזהיר זמן קצר לאחר פרוץ מגפת הקורונה מהאפשרות שפעילי טרור יחקו את "ההצלחה" שלה, וישתמשו בכלי בינה מלאכותית, במקביל לפיתוחים ביו-טכנולוגיים, כדי לייצר נגיפים קטלניים נגד קבוצות אוכלוסייה פרטניות תוך התאמת הנגיף לגנטיקה של אותן קבוצות, כדי להפוך אותו לקטלני יותר. מדובר אומנם באתגר לא פשוט, אך לפחות בתיאוריה מדובר באפשרות ממשית.

עוקפים את העיצומים

האיש שדעתו מכרעת בכל הקשור לענייני ביטחון ברפובליקה האסלאמית של איראן, המנהיג העליון עלי ח'מינאי, נחשף כבר ליתרונות של הדבר החם בעולם הטכנולוגיה. חמ'ינאי, שכבר ראה דבר אחד או שניים בחייו, סימן את תחום הבינה המלאכותית כמטרה הבאה של ארצו.

"עלינו להתמחות בכל הרבדים של טכנולוגיית בינה מלאכותית לפני שגוף רגלוטורי בינלאומי כמו סבא"א יוקם ויכריח אותנו לבקש רשות (להשתמש בטכנולוגיה כזאת א"ק) בעניינים מסוימים לא יתנו לנו רשות", אמר ח'מינאי לפני כחודש, בנאום שעלה לאתר האינטרנט האישי שלו. "כיום בינה מלאכותית מתקדמת בקצב מדהים. מדהים להיווכח בתוצאות של הטכנולוגיה הזאת בעולם, וכמה מהר היא מתקדמת. המחלקות השונות שלנו ביטחוניות או צבאיות משתמשות בבינה מלאכותית, אבל אסור לנו לטעות בשל כך. כשזה מגיע לבינה מלאכותית, אין יתרון בלהיות משתמש-קצה", הוסיף המנהיג העליון. ייתכן שאזכורה של סבא"א לא נעשה במקרה: בעיני ח'מינאי, כך נראה, קידום יכולות של בינה מלאכותיות עשוי להיות נשק שובר-שוויון, בדומה לפצצה גרעינית.

דבריו של ח'מינאי הם חלק ממהלך גדול יותר של איראן לקידום טכנולוגיות של בינה מלאכותית, שהחל כבר בימיו של הנשיא האיראני הקודם, איבראהים ראיסי המנוח. בין היתר דיברו אז האיראנים על טכנולוגיות של מטבעות דיגיטליים שישתלבו בשוק המקומי מה שכמובן גם יעזור להם לעקוף את העיצומים שהטילו מדינות המערב על הכלכלה האיראנית.

ביולי האחרון חנכה טהרן את הקמתו של ארגון הבינה המלאכותית הלאומי, מתוך שאיפה למצב את הרפובליקה האסלאמית ברשימת עשר המדינות המובילות בעולם בטכנולוגיה כזו, ובפרט בתחומי ממשל, כלכלה דיגיטלית ויזמות. לשם כך הגו האיראנית מסמך אסטרטגיה מפורט לבינה מלאכותית, שכעת יחל יישומו.

כבר כיום, לפי דיווחים, נעזרת טהרן בטכנולוגיות דומות כדי לעקוב אחרי נשים במדינה ולדכא את זכויותיהן. במקביל טען הארגון המפתח את ChatGPT, OpenAI, כי ארגונים איראניים השתמשו בתוכנית כדי להשפיע על דעת הקהל האמריקנית לקראת הבחירות לנשיאות בארה"ב.

מרגע שאיראן תגיע למומחיות בשימוש בבינה המלאכותית, היא צפויה בוודאי לבחון את כל היישומים האפשריים שלו בתחומים שרלוונטיים לה ביטחון, טילאות, מבצעי השפעה ואפילו גרעין. ואכן, מדע הגרעין צפוי לקבל דחיפה משמעותית מפיתוחים של בינה מלאכותית, שיסייעו

לקידומו מאוד.

יתרה מכך, סביר להניח שאיראן תחלוק כל ידע ופיתוחים המבוססים על בינה מלאכותית שתשיג עם ארגוני השלוחה שלה ברחבי המזרח התיכון, בדומה ליתר אמצעי הלחימה שהעבירה לחות'ים או לחיזבאללה. משמעות הדבר היא שחמאס, למשל, יהיה מצויד בידע להשתמש בתוכנות מתקדמות באופן הטוב ביותר, וזהו אתגר לא פשוט לישראל.

מצידה, הממשלה בירושלים צריכה לבחון כיצד לנצל את הכלים שנמצאים בארסנל הבימה המלאכותית שלה תחום שישראל נחשבת בו מהמובילות בעולם לא רק לצורך התקפה, אלא גם לסיכול טרור משמעותי. כאמור, לפחות מבחינה פוטנציאלית יש לכך יישומים רבים לקידום טרור, וצריך להיערך למנוע את מימושם.

בחודש ספטמבר, למשל, פורסם כי ישראל תחתום עם עוד עשרות מדינות על אמנה בינלאומית המסדירה את השימוש בבינה מלאכותית, תוך הגנה על זכויות אדם ומוסדות דמוקרטיים, ובהקפדה על שקיפות, פרטיות ושוויון. עם זאת, מסיבות מובנות, האמנה הזאת לא מכסה את השימוש של טכנולוגיות כאלה בתחומי ביטחון לאומי שאם כן הייתה עוסקת בכך, סביר מאוד להניח שישראל לא הייתה חותמת עליה.

לכן, במבט צופה פני עתיד, ותוך שימת לב לעניין הטרור, ישראל נדרשת לבחון אפשרויות לקידום רגולציה של התמודדות עם יישומי בינה מלאכותית המסייעים לטרור, אך כאלה שלא יגבילו את השימוש של מערכת הביטחון בכלים דומים. במקביל, היא יכולה לבדוק כיצד ניתן יהיה להקים קבוצות עבודה ייעודיות עם בעלות בריתה בעולם נגד התארגנויות טרור מסוכנות, ולחלוק מודיעין וידע במקרים פרטניים שבהם נדרש לעשות כן כדי למנוע אובדן חיי אדם של חפים מפשע.

בה בעת, ישראל צריכה לפעול כדי לשמור על היתרון האיכותי שלה בתחום הבינה המלאכותית. עליה גם לבחון אילו חידושים היא יכולה לנצל לצרכיה השונים, ולהכשיר את הדור הבא של המומחים כדי שידעו לסייע לכוחות הביטחון להשתמש ביישומים האלה בהתקפה, בהגנה ובשמירה על העם היהודי בארצו.

התפרסם במקור ראשון, בתאריך 07.11.2024.

הדעות המובעות בפרסומי מכון משגב הן על דעת המחברים בלבד.