



המכון לחקר
המתודולוגיה
של המודיעין

27 ביולי 2023



גזית



המרכז למורשת המודיעין

ChatGPT: משמעויות למודיעין

דקל כהן ונפתלי אבדרהם – חוקרים במכון "גזית", חטיבת המחקר באמ"ן

מבוא

בשנה האחרונה נחשף העולם למוצר בשם ChatGPT שעורר עניין רב באקדמיה, בעולם הטכנולוגי, בעיתונות ובציבור בכלל. ChatGPT הינו תוכנת מחשב, המאפשרת למשתמש לקיים "שיחה" (צ'אט) מתמשכת בצורה של שאלות (הנקראות prompts) ותשובות השומרות על הקשר של שיחה. השיחה יכולה להיות בכל נושא שהוא – החל משאלת שאלות אינפורמטיביות הדומות לשאלות במנועי חיפוש, דרך בקשות והנחיות (למשל – כתוב לי שיר בנושא פריחת הדובדבן) ועד לשאלות "חשיבה" או "דעה" (למשל – מה הסיכויים של ארסנל לזכות באליפות השנה?). ChatGPT יכול לכתוב טקסטים כתגובה לשאלה או בקשה של המשתמש, לכתוב קטעי קוד של תוכנה, לייצר גרפים וטבלאות, לבצע משימות באינטרנט, ועוד.

ChatGPT (ובאופן כללי יותר "מודלי שפה גדולים"), מבשר מהפכה עצומה בגישה שלנו לדאטה. כשם שמהפיכת הסמארטפון, שהחלה לפני כ-15 שנה, הציפה את העולם במידע ויזואלי של תמונות וסרטונים, ושינתה לחלוטין את השימוש שלנו במדיום הויזואלי ואת כלל העולם סביבנו (יוטיוב, אינסטגרם, טיקטוק), כך אנו מעריכים שמודלי השפה הגדולים יהוו מהפכה בדרך שבה אנו צורכים, מעבדים ומייצרים תוכן – טקסטואלי, ויזואלי או מקצועי. כמו שקשה היה לנבא את המצאת האינסטגרם, כך קשה לנבא כיום איך בדיוק ChatGPT ישנה את העולם. אבל מדובר ללא ספק בטכנולוגיה בעלת פוטנציאל עצום שתביא לשינויים עמוקים בכל שטחי החיים.

בהתאם לכך, סביר כי עולם המודיעין, שעיסוקו באיסוף, עיבוד וניתוח דאטה, ישתנה לבלי הכר עם הכנסת הטכנולוגיה הזו לשימוש העוסקים במודיעין. כבר היום מדעני נתונים יודעים לתת לחוקרים כלים המשנים את העשייה המודיעינית. החוקר היום נגיש להרבה יותר מידע מבעבר,

הוא אינו מוגבל על ידי פערי שפה, והטכנולוגיה מאפשרת לו לעכל ולנתח כמויות גדולות של נתונים. מודל השפה הגדול יעשה את כל זה ויותר: הוא יבצע "דמוקרטיזציה" של הטכנולוגיה, ויאפשר לכל חוקר למצות את הדאטה בדרכים שהיום רק אנשי מקצוע יודעים, וגם בדרכים חדשות שכיום אנחנו עוד לא מדמיינים.

אגף המודיעין צריך לאמץ בצורה מהירה ועמוקה את הטכנולוגיה החדשה ולהטמיע אותה בעבודה של כלל אנשי החיל. מעבר להמלצה בסיסית של הנגשת ועידוד כלל אנשי החיל להשתמש ב-ChatGPT ובכלים דומים המונגשים באינטרנט כבר היום, על מנת להיחשף לטכנולוגיה ועל מנת למצות את הפוטנציאל האדיר שבמידע הגלוי, אנו ממליצים לקדם הטמעה של הטכנולוגיה ברשת הפנימית והתאמה שלה לעבודה על המידע המסווג. זוהי משימה הדורשת משאבים (כספיים וטכנולוגיים) רבים, אבל בעינינו היא משימה בעלת חשיבות לאומית.

מעבר לכך, אנו ממליצים להשקיע במחקר שימציא יישומים המתבססים על הטכנולוגיה (באנלוגיה – כמו להמציא את "אינסטגרם" שהתבסס על יכולת הוידאו של הסמארטפון). בפרט אנו סבורים כי בעולמות המחקר, הממשק הייחודי והמהפכני של צ'אט יכול להביא לשינוי מהותי בתו"ל העבודה של החוקר. הוא יאפשר לחוקר לתחקר את המידע המודיעיני בצורה של שיחה, לבקש אלטרנטיבות, להטיל ספק, ובאופן כללי להוות סוג של קמ"ן עזר לכל חוקר. למודל השפה יהיו הטיות שונות מלאדם, והוא יוכל להיות מוכוון להטיות שונות על פי המידע שנזין לו. כך אפשר למשל לדמות איך הצד השני רואה את העולם, או לייצר שני צדדים ולהציב אותם אחד מול השני או לאתר סתירות בין קורפוסים שונים של חומרים.

רקע

ChatGPT הוא מוצר שפותח על ידי חברת OpenAI העוסקת בפיתוח מוצרי בינה מלאכותית ונמצאת כיום בבעלות חלקית של מיקרוסופט. ChatGPT הוא מוצר צ'אט, כלומר תוכנה המאפשרת למשתמש לנהל שיחה מתמשכת בצורה של שאלות ותשובות השומרות על הקשר של שיחה. השיחה יכולה להיות בכל נושא שהוא – החל משאלות שאלות אינפורמטיביות הדומות לשאלות במנועי חיפוש (למשל – מה ההגדרה של בינה מלאכותית? מתי נכחדו הדינוזאורים?),

דרך בקשות והנחיות (למשל – כתוב לי בבקשה את היתרונות והחסרונות של רכישת רכב חשמלי, כתוב לי תוכנה שמבצעת שאילתא בשפת SQL) ועד לשאלות "חשיבה" או "דעה" (למשל – איך כדאי לאוקראינה לפעול נגד רוסיה?). כתגובה לשאלה או בקשה של המשתמש, ChatGPT יכול לכתוב טקסטים, לכתוב קטעי קוד של תוכנה, לייצר גרפים וטבלאות, לבצע משימות באינטרנט, ועוד.

ChatGPT הוא מוצר המתבסס על אלגוריתם שנקרא Generative Pre-trained Transformer (GPT) הוצג לראשונה ב-2018, והוא שייך למשפחה של אלגוריתמים הנקראים Large Language Models, ובעברית – "מודלי שפה גדולים". אלגוריתמים אלו הם תוצאה של ההתפתחויות שקרו בשנים האחרונות בתחום ה-NLP (Natural Language Processing) או "עיבוד שפה טבעית", שהם שלב במהפכה הגדולה יותר של הבינה המלאכותית, שנשענת על טכנולוגיה שנקראת Deep Learning או Deep Neural Networks – רשתות נוירונים עמוקות. ChatGPT הוא המוצר המפורסם ביותר, שתפס הכי הרבה כותרות, אבל אלגוריתמים דומים ל-GPT מפותחים על ידי גורמים רבים בתעשייה ובאקדמיה, ובפרט על ידי ענקיות הטכנולוגיה – גוגל, IBM מטה (פייסבוק) וכו'.

באופן כללי, אלגוריתמים ממשפחת ה-LLM הם אלגוריתמים המיישמים מודל סטטיסטי של שפה טבעית. בצורה פשוטה ניתן לתאר זאת כך: הדבר הבסיסי שמודל סטטיסטי של שפה טבעית יודע לעשות הוא לנבא בצורה טובה מה תהיה המילה הבאה ברצף של מילים. כלומר, בהינתן רצף של מילים במשפט, המודל יודע לומר מה המילה הסבירה ביותר כדי להמשיך את המשפט בצורה "טבעית" ו"נכונה" מבחינה סטטיסטית. לדוגמה, אם ניקח משפט כמו "עומד לרדת גשם, לכן כדאי שאקח מטריה", המילה מטריה היא המשך סביר לתחילת המשפט, הרבה יותר מאשר המילה "קיר" או "אומנות" או המון מילים אחרות. כמובן שיש עוד מילים סבירות להשלמת אותו משפט, כמו "אוטובוס" או "מונית", אבל הרעיון הבסיסי הוא שהאלגוריתם יודע לבחור מילה סבירה. איך יודעים מה היא מילה "סבירה"? האלגוריתם "קרא" כמויות עצומות של טקסטים (לדוגמה – כל וויקיפדיה מהווה כ-3% מכלל הטקסט שהוזן לאלגוריתם), וכך הוא יכול לחזות מה המילה הסבירה הבאה, על סמך הטקסטים שהוזנו לו.

Next Word Prediction – ניבוי המילה הבאה – הוא הבסיס ליכולות המאוד מרשימות של ChatGPT. היכולת הבסיסית הזו מאפשרת למוצר לענות על שאלה, מכיוון שהוא יכול לנבא בצורה טובה מה סביר שתהיה תשובה לאותה שאלה. היכולת הזו מאפשרת למוצר להבין הנחיות, לנהל שיחה, לבצע משימות וכו'. עם זאת, העובדה שמדובר במודל סטטיסטי טומנת בתוכה מגבלות: יכולת בדיקת העובדות של האלגוריתם כיום מוגבלת יחסית. למשל, המשפט "נשיא ארה"ב הוא דונלד טראמפ" הוא משפט בעל סבירות סטטיסטית גבוהה (כי זה משפט שנכתב בעבר פעמים רבות), אבל הוא כרגע לא נכון. בנוסף, האלגוריתם ייטה לתת תשובות "משעממות" וצפויות, כי זה מה ששכיח, ויתקשה לתת תשובה "מעניינת" או "מפתיעה" שמופיעה לעיתים נדירות בטקסט.

מה ChatGPT יכול לעשות?

מלבד היכולת הבסיסית של ניבוי המילה הבאה, ChatGPT תוכנן לבצע משימות נוספות בתחום ה-NLP. לדוגמה, זיהוי וחילוץ ישויות (שמות של אנשים, ארגונים וכד') מתוך טקסט, סיכום אוטומטי של טקסט, סווג טקסט לקטגוריות, הסקת מסקנות מטקסט, סווג האם משפטים מסכימים או לא, זיהוי סנטימנט בטקסט (האם הוא מצדד בכיוון מסוים או מתנגד לו) ועוד. באופן מסורתי לכל אחת מהמשימות האלו מפותח אלגוריתם ייעודי, אבל מכיוון ש-ChatGPT הוא מודל כל כך חזק, הוא מסוגל לבצע גם את המשימות האלו, אם כי לרוב לא באותה רמה גבוהה של ביצוע כמו אלגוריתמים ייעודיים (כמו ההבדל בין אולר שוויצרי לסכין שף). בנוסף, גרסאות מתקדמות יותר של המוצר יוכלו גם לבצע משימות של עיבוד, ייצור ועריכת תמונות (כמו למשל – הבנה מה יש בתמונה, ציור תמונה על פי דרישה, שינוי תוכן של תמונה), ולאחרונה נוספות יכולות בתחומים נוספים כמו וידאו ואודיו.

להלן מספר דוגמאות לשימוש אפשרי ב-ChatGPT:

- א. סיכום טקסט: לנסח שאלה כמו "סכם בבקשה את הטקסט הבא", ולתת קטע טקסט.
- ב. לייצר הערכה: לנסח שאלה כמו "בהינתן המידע הבא, אנא הערך מה הסיכוי ל-", ולהזין קטע טקסט עם המידע שמעניין אותנו.

ג. להציע אלטרנטיבות לפעולה: "בהינתן הסיטואציה הבאה, מה הן דרכי הפעולה האפשריות?"

ד. לכתוב תוכנה בשפה מסוימת שמבצעת פעולה מסוימת (למשל – שאילתא למאגר נתונים בשפת SQL).

את כל הדוגמאות הנ"ל, ועוד רבות אחרות, ניתן להריץ מול הצ'אט, בצורה של שיחה ארוכה. האלגוריתם זוכר את תחילת השיחה ויודע להגיב להתפתחויות של השיחה, לתת תשובות משתנות על פי ההקשר, וכד'.

כאן המקום להזכיר את הניסוי שביצעו איתי ברון ותהילה אלטשולר על הערכת מודיעין, שדימה את התקופה הקודמת למלחמת יום הכיפורים.¹ בניסוי זה השיחה התנהלה בצורה שבה המשתמש תיאר לאלגוריתם את ההקשר הכללי ואת המידע המודיעיני, שהשתנה והתעדכן לאורך השיחה, ובשלבים שונים של השיחה המשתמש שאל את האלגוריתם מה לדעתו הסבירות לפתיחת מלחמה. הניסוי יועד להראות בעיקר שהאלגוריתם פחות נתון להטיות קוגניטיביות, כגון "חשיבת יחד" (group thinking) ומכאן בעל ערך כרכיב בתהליכי הערכה.

מהאמור לעיל נובע שאין תשובה פשוטה לשאלה "מה ChatGPT יכול לעשות?", וזאת מכיוון שזהו אלגוריתם צ'אט כללי, שניתן בעצם לבקש ממנו לעשות כל דבר שניתן לדמיין במסגרת של צ'אט. יתרה מכך, לאחרונה נוצר "מקצוע" חדש – "הלוחש לצ'אט" – מקצוע של ניסוח שאילתות כלומר משפטים שגורמים לאלגוריתם להגיב אליהם (המונח הטכני הוא prompt engineering) אותם "לוחשים" מכירים היטב את המוצר ויודעים להפיק ממנו את המיטב במובן של ניסוח נכון של השיחה, הימנעות מתשובות מוטות וכד'.

מה ChatGPT לא יכול לעשות?

הוזכר לעיל ש-ChatGPT הוא אלגוריתם סטטיסטי, והתשובות שלו, כלומר התגובות שלו לטקסט של המשתמש, לא בהכרח נכונות מבחינה עובדתית, אלא רק סבירות במובן הסטטיסטי. דוגמה

¹ ראו בגיליון זה וכן בפרסום מורחב: <https://www.intelligence-research.org.il/post/GPT-and-intelligence>

משעשעת היא העובדה ש-ChatGPT יכול לצטט מאמרים שאינם קיימים (אבל לדייק בנוסח ההפניה לכתב עת אקדמי), או לצטט בצורה שגויה ממאמרים קיימים. דוגמה נוספת היא הכשלון של המוצר בחידון טריוויה של עיתון הארץ ("20 שאלות"). ChatGPT נתן תשובות ארוכות ומנומקות, אבל שגויות לחלוטין. מצד שני ChatGPT מסוגל להצליח בצורה מפתיעה במבחני רישוי לרפואה או לעריכת דין, ולזהות בצורה טובה מחלות על פי סימפטומים.

הבעיה של Fact Checking היא הבעיה העיקרית היום בשימוש ב-ChatGPT לצרכים מודיעיניים ולצרכים דומים (כמו כתיבה אקדמית וכד'). מפתחי המוצר (וגם מפתחים של מוצרים דומים) מודעים לבעיית חוסר הדיוק, ולכן הם משלבים בגרסאות מתקדמות ועתידיות של המוצר מודולים נוספים של Fact checking. לדוגמה, שילוב של חיפוש במאגרי נתונים עדכניים (למשל – שערי מטבע עדכניים או לוחות זמנים של טיסות וכד'), חיפוש במאגרי נתונים אמינים (למשל מאגרים מדינתיים), יכולות כמותיות ספציפיות (כמו למשל שימוש בכלים ייעודיים לביצוע חישובים), תיקוני שגיאות בקוד של תוכנה, ועוד ועוד. לכן, סביר להניח שבעתיד הקרוב בעיית הנכונות העובדתית תקבל מענה יעיל, והמוצר יתגבר על "מחלת ילדות" זו.

עד כמה שהיכולות הטקסטואליות של ChatGPT מרשימות, הטענה כיום היא ש-ChatGPT אינו עומד במבחן של "בינה מלאכותית כללית" (Artificial General Intelligence – AGI). בעוד ש"בינה מלאכותית" היא מונח כללי המתאר יכולות טכנולוגיות המדמות יכולות המיוחסות לבני אדם (כגון זיהוי פרצופים או הבנת פקודה קולית), AGI היא יכולת בינה מלאכותית השווה או עולה על יכולת של אדם, כלומר בינת מכונה המסוגלת לבצע כל פעולה מחשבתית או אינטלקטואלית שאדם מסוגל לבצע. הדרישות מבינה מלאכותית כללית הן הסקת מסקנות, שימוש באסטרטגיה, פתרון חידות, שימוש בשיקול דעת בתנאי אי ודאות, צבירת ידע, תכנון, לימוד, תקשורת בשפה טבעית ועוד. ChatGPT מראה התקדמות מרשימה מאד במספר גדול מהסעיפים האלה, בייחוד בגרסת GPT4 (שיצאה במרץ 2023), אבל הדרך ליעד של AGI עוד ארוכה מאד לדעת רוב החוקרים.

במכתב פומבי שפורסם לאחרונה בחתימת יותר מ-1000 מומחי בינה מלאכותית ומנהלי חברות טכנולוגיה, הם קראו לעצור את פיתוח של כלים כמו ChatGPT.² הם הביעו חשש, בין היתר, מחוסר הדיוק העובדתי שבו דנו לעיל, מאובדן מקומות עבודה, ומכך שכלים כמו ChatGPT מסוגלים להפיק טקסטים ברמת תחכום ויצירתיות אנושיים ובכך להכחיד מקצועות כמו סופרים, משוררים ועיתונאים. חשש דומה עולה באקדמיה מכך שתלמידים יגישו עבודות שנכתבו על ידי ChatGPT. חששות עמוקים יותר הובעו על ידי חוקרים כמו יובל נח הררי שדיבר על היכולת של כלי בינה מלאכותית לעוות את המידע שאנו צורכים ומכאן את עצם הבנת המציאות שלנו. מן הצד שני נטען שכל מהפיכה טכנולוגית יוצרת התנגדות דומה – חשש מאובדן מקומות עבודה, חשש משימוש לרעה וכו' – ושאינן הבדל מהותי בין המהפיכה הזו למהפיכות קודמות.

האם ChatGPT יחולל מהפיכה, ואיך היא תיראה?

רבים טוענים כי ChatGPT יחולל מהפיכה ענקית, אולי אפילו "בסדר גודל של המהפכה התעשייתית". קשה כמובן לתאר מה יקרה בעתיד, אבל ניתן להסתכל על מהפיכה אחרת שהחלה לפני כ-15 שנה, ואנחנו עדיין בעיצומה, ואולי להקיש ממנה. מדובר על מהפיכת התמונה והוידאו. ב-2007 חברת אפל הציגה לעולם את האייפון, ולראשונה בהיסטוריה, לכל אחד מאיתנו הייתה בכיס מצלמה, המחוברת למחשב, שמחובר באופן רציף לאינטרנט. גם לפני המצאת האייפון אנשים צילמו – תמונות סטילס ווידאו, של עצמם, של המשפחה, בטיולים, וערכו סרטי וידאו ביתיים, אבל מאז האייפון כולנו הפכנו לצלמים ועורכי וידאו אובססיביים. הדבר הזה הוליד מהפיכה חברתית וכלכלית ענקית. היום, 15 שנה אחרי כן, יש בעולם יוטיוב, אינסטגרם, טיקטוק, נוצרו תופעות כמו "משפיעני רשת" ועוד דברים ששינו לחלוטין את החברה, הכלכלה, ואפילו את המוחות שלנו. הילדים שלנו צופים בוידאו במכשיר הנייד שלהם בכל שעות היממה, והעולם שלהם שונה לחלוטין מהעולם שאנחנו גדלנו בו. ניתן רק לדמיין איך הייתה נראית מגפת הקורונה

<https://www.themarket.com/wallstreet/2023-03-29/ty-article/.premium/00000187-2bfc-ded8-ade7-2fbffa3010000>

ללא המהפכה הזו. כמובן שמהפיכת התמונה והוידאו היא רק חלק מהמהפכה הגדולה יותר שהביא האיפון, שכוללת את הקישוריות והחיבור המתמיד של אנשים לאינטרנט ולאנשים אחרים.

מלבד השינויים החברתיים והכלכליים שגרמה מהפיכת התמונה והוידאו, המצאת האיפון הובילה גם למהפכה מדעית וטכנולוגית – למהפכת הבינה המלאכותית. ברגע שכולם התחילו לצלם תמונות ולהעלות אותן לאינטרנט, התחילו להיווצר מאגרי תמונות ענקיים, זמינים לכל אחד. בעקבות זאת, ב-2008 הוכרזה באוניברסיטת סטנפורד תחרות בשם ImageNet שהזמינה חברות וחוקרים לפתח אלגוריתם שיוכל "להבין תמונות". מאגר התחרות הכיל כ-15 מיליון תמונות, ב-20,000 קטגוריות, והאתגר בתחרות היה לפתח אלגוריתם שיוכל לסווג נכונה "מה יש בתמונה?" – פיל, או חתול, או אונייה וכד'. מאות חוקרים וחברות ניסו את כוחם בתחרות, עד שב-2012 הופיע אלגוריתם בשם AlexNet ש"שבר" את התחרות והביס את כל האלגוריתמים האחרים. זה היה האלגוריתם הראשון שהציג רשת נוירונים עמוקה (Deep Neural Network), וכך נולדה מהפיכת הבינה המלאכותית. היום, יותר מ-10 שנים אחרי AlexNet, ניתן לומר שה"בעיה" של הבנת תמונה ע"י מחשב כבר פתורה. דבר זה הוליד כמובן את כל היכולות שאנחנו מכירים היום בתחום התמונה והוידאו, החל מזיהוי פנים, דרך פענוח תמונות רפואיות ועד לרכבים אוטונומיים. ב-2017, חמש שנים אחרי AlexNet, פרסמה גוגל רשת נוירונים בשם "טרנספורמר", שעשתה לתחום עיבוד השפה את מה ש-AlexNet עשה לתחום התמונה. והיום, 5 שנים מאוחר יותר, יש לנו את ChatGPT. ניתן אם כן לומר, שהאיפון היה אחד מהגורמים הקריטיים שהובילו למהפכת הבינה המלאכותית, ו-ChatGPT הוא סוג של "נכד" של האיפון. האיפון היווה רק טכנולוגיה – חיבור של מצלמה עם מחשב ואינטרנט – אבל על בסיס הטכנולוגיה זו נולדו דברים ששינו את העולם. האם זה מה שיקרה בזכות ChatGPT? סביר להניח ש-ChatGPT ישנה לחלוטין את הדרך שבה אנחנו צורכים, מעבדים ומייצרים תוכן. כשם שלפני האיפון היו צלמים ועורכי וידאו, גם היום ישנם אנשי מקצוע וכלים שמאפשרים לעבד ולייצר תוכן בדרכים מתוחכמות יותר מאי פעם. אבל הדרך שבה ChatGPT מנגיש את היכולות הללו לכל אחד, עשויה להיות דומה לדרך שבה האיפון הנגיש את עולם התמונה והוידאו לכל אחד. קשה לדמיין

מה בדיוק יקרה, אבל אולי בעוד כמה שנים נראה תופעות בסדר גודל של אינסטגרם וטיקטוק שיווצרו בזכות ChatGPT, ואולי נחווה שינויים בסדרי גודל דומים בחברה, בכלכלה, במדע ובטכנולוגיה. כבר היום יש מבול של סטארטאפים ויוזמות קוד פתוח שעושים שימוש ב-LLMs, אבל קשה לדעת לאן כל זה יוביל. מה שבטוח הוא שעלינו לאמץ את הטכנולוגיה הזו כמה שיותר מהר, ולנסות להיות אלו שימציאו את ה"אינסטגרם" הבא.

מה אפשר לעשות עם מודלי שפה גדולים בעולמות המודיעין?

נחלק את התשובה לשאלה הזו לשלושה חלקים:

- א – מה ניתן לעשות עם מוצרים כמו ChatGPT המונגשים באינטרנט לקהל הרחב
- ב – מה תאורטית ניתן לעשות עם מודלי שפה גדולים, בהנחה שניתן להשתמש בהם על מידע מודיעיני
- ג – מה כדאי לעשות כבר היום.

מה ניתן לעשות עם מוצרים כמו ChatGPT המונגשים באינטרנט לקהל הרחב? נתחיל בשימושים הפרקטיים/טכניים של ChatGPT. כאמור, ChatGPT הינו מודל שפה חזק מאד, המסוגל לבצע משימות עיבוד שפה רבות "בחינם" ולחסוך המון עבודה ייעודית. ניתן להשתמש במוצר על מנת לבצע משימות טכניות כגון קיבוץ נתונים לטבלאות, חיבור דו"חות, הצגת גרפים ועוד המון משימות ידניות שדורשות עבודה סזיפית ידנית.

המוצר גם יכול לקצר המון זמן עבודה בפיתוח קוד (מיקרוסופט פיתחה מוצר מבוסס LLM לשיפור ויעול פיתוח קוד, הנקרא copilot, ומהווה חלק מפורטפוליו מוצרי ה-AI שלה). ניתן אף להשתמש ביכולות המובנות של ChatGPT ליצירת מאגרים לאימון של אלגוריתמים ייעודיים. כפי שנאמר לעיל – ניתן לבצע אינספור משימות בעזרת ChatGPT, זה תלוי ביצירתיות ובמיומנות של המשתמש, בפיתוחים וביכולות החדשות המונגשות בגרסאות המעודכנות (כמו Fact checking או יכולות ייעודיות), ותחת ההבנה שמדובר במידע אינטרנטי ובמודל סטטיסטי שדורש בקרה אנושית על התוצר הסופי.

מה תאורטית ניתן לעשות עם מודלי שפה גדולים, בהנחה שניתן להשתמש בהם על מידע מודיעיני?

תחילה נבין את המגבלות בשימוש ב-ChatGPT לעבודה על מידע ייעודי או מסווג. כאמור, ChatGPT הינו מוצר אינטרנטי. המוצר עצמו שומר את המידע שהמשתמשים הזינו לתוכו ומתעד את השיחות שבוצעו, ואלו משמשות לטיוב ושיפור האלגוריתם. מכך ברור שאי אפשר להזין לאלגוריתם מידע רגיש מכל סוג. כלומר, אם גוף כלשהו רוצה לעשות שימוש במוצר כמו ChatGPT על מידע רגיש, אותו גוף יצטרך מודל שפה פנימי וייעודי.

אחת התכונות של אלגוריתמים לומדים, כמו מודלי שפה סטטיסטיים, היא שהם בעצם משקפים את האופי (הסטטיסטיקה) של המידע שאותו הם למדו לתאר. המשמעות היא שהמודל "מוטה", באופן טבעי, לשפה שהזינו לתוכו (לכן האלגוריתמים האלה חלשים בשפות שאינן אנגלית), ולאופי הטקסטים שהזינו לתוכו. במונח "אופי הטקסט" הכוונה היא למשל להבדלים בין כתבת עיתון, ספרות יפה, מאמר מדעי, ציוץ בטוויטר, תמלול של שיחת טלפון, טבלת אקסל וכד'. כלומר, אם לדוגמה ניקח אלגוריתם שאומן על מאמרים מדעיים ונשתמש בו כדי לבצע משימות עיבוד שפה על ציוצים בטוויטר, סביר להניח שהוא יהיה גרוע בזה.

המשמעות היא, שעל מנת ליהנות מהיכולות של מודל שפה גדול על מידע ייעודי ורגיש יש צורך לייצר אלגוריתם ייעודי שיתאים לצרכי המשתמש. יש להבין עם זאת שעל מנת לייצר מודל שפה גדול יש צורך במשאבים גדולים מאד. ראשית, יש צורך בכמויות עצומות של טקסט, שזה בד"כ הרבה יותר מסך המידע הייעודי הקיים בארגון (כאמור, וויקיפדיה כולה הייתה רק 3% מסך הטקסט שהשתמשו בו כדי לאמן את GPT3). שנית, יש צורך ביכולות חישוב גדולות מאד, ושלישית, יש צורך בצוות גדול מאד של מומחים, ובידע טכני שלא חשוף כולו לציבור.

עם זאת, בימים אלה מתפרסמים חדשות לבקרים מודלי שפה גדולים חנימיים (כנראה פחות חזקים משל החברות הגדולות), שניתן להשתמש בהם כנקודת פתיחה לייצור מודל שפה ייעודי שהותאם לדאטה ייעודי. כלומר, כמו בכל עולם הבינה המלאכותית בשנים האחרונות,

העולם הולך לכיוון של קוד פתוח ודמוקרטיזציה של הידע והיכולות, כך שלא ירחק היום וכל ארגון בעל המשאבים והיכולות המתאימים יוכל לייצר אלגוריתם ייעודי עבור עצמו.

ניתן לנתח את הפוטנציאל של השימוש בכלי כמו ChatGPT לפי חלקי העבודה המודיעינית: איסוף, עיבוד ומיצוי, ומחקר.

איסוף: האיסוף המודיעיני מתבצע על ידי הגעה למידע הקיים במקורות. בתחום זה אין תועלת נראית לעין בשימוש במודל שפה גדול, פרט אולי לאפשרות לשימוש במודל כזה על מנת לייעל את הסינון של המידע לפני שמביאים אותו, אם יש צורך כזה. היתרון המשמעותי של מודל שפה גדול הוא דווקא בשיפור דרמטי של יכולת האיסוף מהאינטרנט. בעצם אין מדובר על "איסוף" מכיוון שהמידע כבר קיים באינטרנט ונגיש לכל אחד, אבל הכוונה היא לייעל את החיפוש והסינון של אינסוף המידע שקיים היום באינטרנט ושלא נעשה בו שימוש, בגלל הקושי לסנן ולברור את המידע המעניין. ChatGPT יכול לסכם אתרים, למצות מידע, לתרגם, ולעשות פעולות רבות מאד שינגישו לחוקרים מידע אינטרנטי שהם בכלל לא רואים היום.

עיבוד ומיצוי: תחילה ננסה לחדד ולהבהיר נקודה חשובה לגבי השימוש ב-ChatGPT כמקור מידע. כאמור, ניתן לנהל שיחה עם ChatGPT ולקבל תשובות, גם לשאלות "עובדתיות", כמו מתי נכחדו הדינוזאורים וכד'. עם זאת, חשוב להבין ש-ChatGPT יכול לתת תשובות אך ורק על סמך המידע שהוזן לתוכו בזמן האימון שלו. כלומר, אם בשום מקום בטקסטים שהוזנו לתוכו לא כתוב על הדינוזאורים אז הוא לא יידע לענות נכון. חשוב להבין, שהטקסטים מוזנים ל-ChatGPT בשלב האימון, שלצורך העניין, בגרסה 3GPT בוצע בשנת 2020. כלומר, אם לדוגמה נשאל את המנוע מי זכה במונדיאל בשנת 2022 לא נוכל לקבל את התשובה הנכונה. בניגוד לכך, מנועי חיפוש (כמו גוגל), מאנדקסים באופן תמידי את כל הדפים באינטרנט, והם מסוגלים למצוא מידע עדכני, נכון לזמן האינדוקס (שיכול להיות ממש היום בבוקר). כלומר, על מנת להשתמש במוצר כמו ChatGPT כדי לענות על שאלות מודיעיניות על סמך מידע עדכני, יש צורך לשלב בין שתי היכולות – מודל שפה ומנוע חיפוש. השילוב הזה יכול תאורטית להתבצע בשתי דרכים: האחת, היא להמשיך ולאמן את מודל השפה על כל המידע העדכני, ובפועל "לאנדקס" את כל המידע הקיים,

והכי עדכני, דרך המודל. הגישה הזו כנראה לא סבירה מבחינה טכנולוגית, מכיוון שאימון של המודל היא פעולה מסובכת, יקרה (בזמן ובכסף), וטומנת בחובה מורכבויות אלגוריתמיות. הגישה האחרת, שכרגע מוצעת על ידי מיקרוסופט בשירות Bing Chat, בעצם משתמשת במנוע חיפוש שמביא מידע עדכני, ומאפשרת הזנה של תוצאות החיפוש לתוך מודל השפה לטובת עיבוד וניתוח. מודל כמו Bing Chat יכול לחולל מהפכה משמעותית במקצועות העיבוד והמיצוי של המידע המודיעיני, מהפכה שתייעל ותפשט מאד את עבודת המיצוי ותאפשר למצות עשרות מונים יותר מידע מהקיים היום, בעזרת יכולות כמו סיכום מסמכים, תרגום, המרת טקסט לטבלאות, ייצור גרפים, ושאר היכולות המובנות ב-ChatGPT.

מחקר: גם בתחום המחקר כלי צ'אט יכול לחולל מהפכה בעבודת החוקר. בהנחה שבעיות הנכונות העובדתית והשילוב עם מנוע חיפוש תפתרנה, הממשק הייחודי והמהפכני של צ'אט יכול להביא לשינוי מהותי בתו"ל העבודה של החוקר. הממשק של צ'אט מאפשר לחוקר לתחקר את המידע המודיעיני בצורה של שיחה. החוקר יכול לשאול שאלות, לבקש מהמודל להציע אלטרנטיבות, לבחון אפשרויות מתחרות, להציע דפ"אות, להטיל ספק, לבחון את תקפות הנחות היסוד שלו ובאופן כללי להוות סוג של קמ"ן עזר לכל חוקר. למודל שפה יש הטיות שונות מלאדם, והוא יכול להיות מוכווון להטיות שונות על פי המידע שנזין לו. כך אפשר למשל לדמות איך הצד השני רואה את העולם, או לייצר שני צדדים ולהציב אותם אחד מול השני. במתארים שונים המודל יכול גם לייצג פרספקטיבות שונות או לאתר סתירות בין חומרים שונים.

בראייה מחקרית, יש לתוכנה יתרונות על כל כוח עזר מחקרי אנושי במהירות העצומה שבה היא מבצעת את המשימות המוטלות עליה ובעתיד גם באמינות, בכך שהיא איננה מושפעת מההטיות האנושיות המוכרות הפוגעות באיכות המחקר המודיעיני, בכך שהיא ורסטילית לחלוטין, כך שניתן להשתמש בה בעת ובעונה אחת בכל תחום מחקר, ומעל הכול בכך שהיא איננה מוגבלת מאילוצים אנושיים אחרים, כך שהיא מסוגלת לחזור ולבצע אותה משימה מדי יום בלי להישחק. למשל, היא מסוגלת לבדוק מדי יום האם הנחות היסוד המחקריות עודן תקפות ולא תהסס לקבוע שהן אינן תקפות, בעוד שחוקר אנושי עלול להתעייף ולא לבדוק זאת שוב ושוב, וגם יהסס לקבוע שהנחת היסוד שלו, שעליה ביסס את הערכותיו מזה זמן, איננה תקפה.

סיכום: מה כדאי לעשות כבר היום?

מוצר כמו ChatGPT מאפשר דמוקרטיזציה של טכנולוגיה. הממשק הפשוט והמהפכני שלו מאפשר לכל אדם, מכל רקע, גישה ליכולות וטכנולוגיות שעד היום היו זמינות רק ליודעי ח"ן. במילים אחרות, בעולם שבו ChatGPT הוא כלי בשימוש יומיומי, כל חוקר יכול לבצע משימות כמו סיכום אוטומטי של מסמכים, חילוץ וזיהוי ישויות, סידור נתונים לגרפים וטבלאות, ועוד המון משימות שהיום צריך "איש דאטה" או עוזר מחקר כדי לבצע אותן, ובכלל כדי לדעת שהן קיימות. ChatGPT יכול להיות "חוקר דאטה" פרטי, לשימוש של כל חוקר מודיעין. זו עשויה התרומה המשמעותית ביותר של כלי כמו ChatGPT בשירות המודיעין.

הדבר הפשוט והמיידני לביצוע הוא חשיפה והנגשה של ChatGPT ומוצרים דומים לכלל אנשי המודיעין. חשוב מאד שהחוקרים בפרט, אבל גם כל שאר אנשי החיל והמפקדים בכלל, יכירו את הכלים האלה, ישתמשו בהם ברמה היומיומית, ויפתחו מיומנות בשימוש בהם, כולל הבנת היכולות והמגבלות שהוזכרו לעיל. כדאי שאנשי המודיעין יספרו על רעיונות שעלו להם באשר לאופן השימוש בכלי, ישתפו בחוויות של הצלחות וכשלונות, ויטמיעו את השימוש במשימות טכניות וסיזיפיות כמו שהוזכרו לעיל (במגבלות החשיפה של מידע כמובן). חשוב שאנשים טכניים (מפתחים, אנשי דאטה וכד') יכירו את הכלים האלה לעומק, כולל הרקע הטכני/מדעי שלהם. מומלץ לגופים הטכנולוגיים באמ"ן לתכנן שימוש ב-ChatGPT במסגרת מיצוי האינטרנט. מומלץ לחשוב על כלי זה כמערכת איסוף, הכוללת זחלנים האוספים מידע, ומודל שפה גדול המשמש למיצוי אוטומטי. כדאי למפות אילו סוגי מידע רוצים לאסוף, בדגש על מקורות מידע שלא ממוצים כיום בגלל מגבלות שפה ונפחים, ולתכנן מערכת המנצלת את יכולות העיבוד המובנות ב-ChatGPT לטובת מיצוי והנגשת המידע.

בנוסף, מומלץ לגופים הטכנולוגיים באמ"ן להתחיל כבר היום בהיערכות לבניית מודל שפה גדול המאומן על המידע הייעודי של אמ"ן. ההיערכות הזו כוללת אימוץ של מודלי שפה חנימיים ובניית תשתית פיזית ואלגוריתמית להתאמה של מודל שאומן "בחוף", לידע ייעודי. התשתית הפיזית כוללת שרתי חישוב, דאטה-בייסים ותשתיות תומכות (כולל אנשי מקצוע רלוונטיים),

והתשתית האלגוריתמית כוללת חוקרים ומדענים שיפתחו את השיטות להתאמה של מודל שפה.
ניתן כבר היום להתחיל את המחקר – להגדיר ניסויים, פרוטוקולים לאימון, מאגרי מידע
לואלידציה, ועוד.