המכון לחקר המתודולוגיה של המודיעין

המרכז למורשת המודיעין

בינה מלאכותית בתחום הויזינט

נועם (רון) ברמן[1]

אוקטובר 2020

בסוף אפריל 2020 פרסמה סוכנות המודיעין הגיאו-מרחבית (NGA-National Geospatial intelligence Agency) מסמך הדן במגמת השימוש בחומר מלוויינים מסחריים ובפיתוחים טכנולוגיים, ובהתאם בהתמודדות עם כמות חומר חזותי בנפח עצום. נראה כי ארצות הברית, הנחשבת למעצמה המובילה בתחום מחקר הויזינט, מעלה כעת את הטענה כי עליה לעשות מאמץ מירבי על מנת להשיג עליונות מחקרית וטכנולוגית בתחום.[2] מסמך זה מבקש לדון באתגרים בשילוב הבינה המלאכותית במחקר החזותי.

עידן הבינה החזותית- שילוב המערכות האוטומטיות במחקר הויזינטי

מהפכת המידע בעידן הקיברנטי האיצה את שילובן של מערכות AI (Artificial intelligence) במחקר המודיעין. עידן זה של אוטומציה לא פסח על העולם החזותי וכולל: שילוב סנסורים ופיתוחם, ניתוח אלגוריתמים למתן תמונה מדויקת כבר ברמת הפקת חומר הגלם וריבוי אמצעי איסוף וצילום כמו גם השימוש בנתונים ממקורות מסחריים. כל אלו מאפשרים כיסוי ויזינטי כמעט רציף, סיוע באיתור מגמות ובזיהוי שלהן וקפיצה משמעותית במתן תמונת מודיעין מקיפה ומהירה. במקביל, אלה מצריכים מערכות היכולות להתמודד עם כמות מידע רחב.[3]

עידן זה הנשען, בין היתר, על "Big Data", מתאפיין בשפע בלתי נדלה של נתונים ומתבסס על שיטות ניתוחיות כגון "Machine learning", קרי תת קבוצה של בינה מלאכותית אשר עושה שימוש בשיטות סטטיסטיות על מנת לאפשר למערכות ממוחשבות ללמוד ולהתאים את תהליכיהן מבלי שתוכנתו לכך במפורש. יחד עם זאת, אפיון תצורה של אובייקט מסוים (לצורך העניין גג של מבנה) לא יכול להיות אחיד כאשר מדובר בשטחים נרחבים או באזורים גיאוגרפים שונים עם אפיונים משתנים (למשל בניה שונה, צפיפות משתנה וכיו"ב). לפיכך, שודרגו מערכות בתחום המחקר הויזינטי לכדי שיטת ה-" Deep learning" ("למידת עומק"), שהיא תת סוג של "למידת מכונה", אשר מנסה לחקות תהליכי למידה של

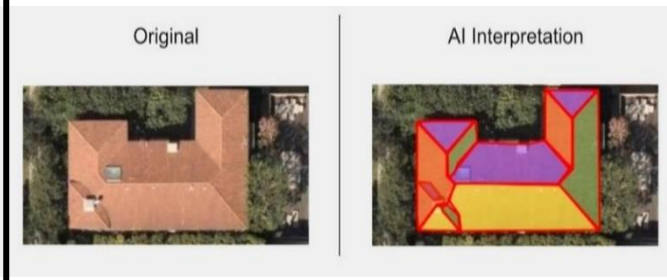
[1] חוקרת ומפענחת חזותית, לשעבר בקהילת המודיעין, ובעלת תואר שני בקרימינולוגיה מחקרית.

[2] Boyed, A. (April 29, 2020). The world is changing—from commercially available GEOINT to COVID-19—so the National Geospatial-Intelligence Agency released a list of tech challenges the agency needs help to overcome. Nextgov. Retrieved June 7, 2020, from: https://bit.ly/2GXr5mM

[3] IDF- Israel Defense Forces. (2017). The IDF see artificial intelligence as the key to modern day survival. Retrieved May 10, 2020, from: https://bit.ly/36YraBw

מוח אנושי. מערכות אלו מתבססות על חומר גלם מגוון וצוברות מידע באופן מתמיד, שעל בסיסו הן יודעות לעבד, לאבחן ולנתח באופן מהיר ואיכותי על רצף מתפתח אוטומטית. כלומר, אלגוריתם למידה עמוק יכול לסייע לזהות אובייקטים בתנאים דינאמיים.

שימוש ב"למידת עומק" לאבחון גג בתצלום אוויר. המחשה של תהליך סיווג התמונה ואפיון הצורה על מנת "ללמד" את המערכת לאתר זאת באתרים דומים. נדלה מאתר NC.AI בתאריך 4.8.20 : קישור



המחשת היכולת של בינה חזותית לאפיין ולפרש מבניות של גג בשימוש בלמידת עומק בהתאם להגדרת המטרה (במקרה הנוכחי מצג סולארי). נדלה מאתר Cisionבתאריך 7.9.20 : קישור

האוטומציה בתחום החזותי מהווה חלק בלתי נפרד מתפיסת ההפעלה של ארגונים מדיניים וביטחוניים בעולם, ובכלל זה בישראל. דוגמאות לכך ניתן לראות בזירה הבינלאומית - החל מפיתוחים של כלים לפענוח אוטומטי לצד השקעה נרחבת של סוכנות ה-NGA באוטומציה החזותית; עבור דרך מתן מענקי פיתוח בתחומים השונים[4]; וכלה בסוכנות הטכנולוגיה של משרד ההגנה האמריקאי DARPA (Defense Advanced Research Projects Agency) ומקבילתה בתחום המודיעין IARPA (Intelligence Advanced Research Projects Activity) אשר שמות את פיתוח ה-AI ולמידת המכונה בראש מעיניהן.[5]

במהלך השנה האחרונה מתנהל ב-IARPA פרויקט ארוך טווח לפיתוח מערכת אוטומטית "לתפירת" הדמאות לוויין מרחבי העולם לכדי תמונה שלמה לאיתור פעילות אנתרופוגנית (השפעת פעילות האדם על הטבע) ושינויי בנייה לשימוש סוכנויות ביון אמריקאיות. המערכת עתידה לאפשר מיזוג נתונים הנאספים באופן ייעודי יחד עם נתונים מסנסורים שונים, ולהתאימם לדפוסי מזג אוויר ולגורמים סביבתיים אחרים העלולים להשפיע על איכות התמונה[6]. ניכר כי פרויקט מסוג זה הוא בעל פוטנציאל רחב היקף באופן גלובלי.

קפיצת מדרגה נוספת בתחום החוזי-האוטומטי ניתן לראות בניסוי שבוצע באוגוסט 2020 במסגרת תכנית צבאית אמריקאית בשם Project Convergence, שנועדה לבחון שילוב יכולות הגנתיות והתקפיות תוך שימוש בנכסים חזותיים מהחלל. בשלב ראשון, נאסף מידע חזותי מלווייני צבאיים ומסחריים כאחד אשר הועבר לתחנת עיבוד קרקעית, שם הוא נותח באמצעות תוכנת בינה מלאכותית בשם Prometheus במטרה לאתר אנומליות ומטרות פוטנציאליות. לאחר שלב זה, תוכנה אחרת (SHOT) קיבלה את פלט הממצאים ועל פיו סיווגה את מאפייני המטרות ותעדפה את כלי הנשק

[4] Wratchford, S. (2019). NGA talks strategy, AAA at Geospatial Gateway Forum in St. Louis: NGA-The National Geospatial-Intelligence Agency. Retrieved May 7, 2020, from: https://bit.ly/34SghP5
[5] DARPA- Defense Advanced Research Projects Agency. (n,d). AI Next Campaign. Retrieved August 16, 2020, from: https://bit.ly/34Mbfnf
[6] Corrigan, J. (April 16, 2019). IARPA is Investing in AI That Constantly Analyzes Worldwide Satellite Images. Nextgov. Retrieved September 8, 2020, from: https://bit.ly/3lG5bUe

המתאימים לתקיפה. משם התוצר עבר לאישור מפעיל אנושי לפני תקיפה. אם בעבר מידע שכזה חולק בין אנליסטים שונים, כעת כללי המשחק שונו לחלוטין ודומה שהפרויקט הוא עדות לשינוי רחב היקף.[7]

בישראל ניצבים בחוד החנית פרויקטים של אוטומציה חזותית במערך החוזי והמיפוי ויחידות אחרות בצה"ל.[8] ביוני 2020 פורסם מאמר על אודות מערכת צה"לית אוטומטית לייצור מטרות בגזרה הצפונית, אשר מייעלת את ייצור המטרות בכ-50% אחוז. מערכת זו מתבססת על פי הכתוב על שילוב אמצעים משלל מקורות איסוף- חזותיים, תקשורתיים ואחרים, כאשר נראה שעל אף הפיתוח הטכנולוגי המקצועי והיכולת להבחין בין מגוון סוגים של מידע, חשיבותה של ה"עין האנושית" במעגל עדיין ניכרת.[9]

"בינה חזותית" - אתגרים וכיצד להתמודד עימם

ההתפתחויות הטכנולוגיות שאפיינו את העשור האחרון ובכלל זה- ניקוי התמונה וחידודה, עיבוד חומר הגלם, זמינות המידע החזותי והיקפו, המהפכה במרחב הקיברנטי ופיתוחי הבינה המלאכותית במרחב המודיעיני בכללותו - הביאו לשינוי בהפקת המודיעין החזותי. כדי להתמודד עם כמות מידע חזותי כה מגוון יש הכרח בפיתוח טכנולוגיה לפענוח רב סנסורי סינרגטי אוטומטי. יחד עם זאת, כמות המידע העצומה מהווה אליה וקוץ בה. בפיתוח מערכות מסוג זה, הן המפתחים והן חוקרי המודיעין נדרשים לנתח ולדלל כמות נרחבת של מידע מאמצעים שונים (וידאו, לוויינים מבצעיים או מסחריים, תצלומי אוויר על סוגיו וכו'). בנוסף, עליהם להפיק את התובנות הנכונות, תוך מזעור טעויות שונות בתהליך הפיתוח, כאשר באותה עת מידע מתווסף משלל אמצעים באופן בלתי פוסק. לאתגרים אלו מתווספים גם אתגרים הקשורים באחוז דיוק הממצאים, צורך באנשים בעלי ידע תכנותי וטכנולוגי מתקדם, שיתופי פעולה, התמודדות עם מצגי שווא ועוד.[10]

בהתאם לכך מתייחסת DARPA לבינה המלאכותית כבשורה בכול הקשור לעולם המחקר ביטחוני, ואף מבהירה כי השאיפה היא להתייחס למחשב כאל שותף לעבודה ולא ככלי, זאת לצד הדגשת פגיעותן הגדולה של מערכות אלו למניפולציות ולכשלים (לוחמת סייבר, שגיאות וכו').[11] קבוצת האתגרים הבולטים, אותם הדגישה גם סוכנות ה-NGA, קשורה למאגר הנתונים ולניתוחם בהיבט האבטחתי מרמת האיסוף ועד רמת הפענוח והתוצר. פגיעה בקוד התוכנה של המערכת עלולה להוביל לסיווג תמונה באופן שגוי, כך שתוכנת הויזינט לא תזהה כראוי את מה שהיא מאתרת, ובכך תגרום לכשלים מחקריים

---

[7] Sydney J. Freedberg JR. (August 5,2020). Army Tests New All Domain Kill Chain: From Space To AI Retrieved September 10, 2020, from: https://bit.ly/30YbOJD

[8] אתר צה"ל (2009). "המצה השמורה של צה"ל- כך שינתה המערכת של 3060 את פני ניתוח המודיעין בשטח". אוחזר ב- 07.06.20 מתוך https://bit.ly/3iPmNuP

[9] זייתון, י. (8 ליוני , 2020). ה"מכונה" להשמדת אויב: זינוק של 50% בייצור המטרות באמ"ן, **Ynet**. אוחזר ב- 09.06.20 מ: https://bit.ly/30WLX4L

[10] IDF- Israel Defense Forces. (2017). The IDF see artificial intelligence as the key to modern day survival. Retrieved May 10, 2020, from https://bit.ly/2SPsA9f

[11] DARPA- Defense Advanced Research Projects Agency. (n,d). AI Next Campaign. Retrieved August 16, 2020, from: https://bit.ly/34Mbfnf

ומבצעיים .[12] לפיכך, מייחסת DARPA חשיבות להשקעה בטכנולוגיה אוטומטית לתיקון טעויות באופן נרחב.

לפי ה-NGA על מנת לקיים קוהרנטיות במערכת "בינה חזותית" המבוססת על מאגר נתונים רחב יש להתמודד עם הכשלים ולהעניק מענה מהיר ומדויק. על המידע להיות שלם ככל הניתן, כאשר חייבת להישמר האפשרות לחזור ולבחון את המידע בכול מקרה לגופו. בראש ובראשונה, יש להתייחס לאופן בו המידע מסווג. כלומר, בעת תהליך המיון לקטגוריות, יש לסווג את הממצאים השונים לפי הערכים שנקבעו (לצורך העניין קטגוריה של רכבים, קטגוריה של רכבים של ארגון מסוים וכדומה). בהתאם, על המערכת להבחין אוטומטית בין תצפיות של אותו אובייקט לבין תצפיות של אובייקט דומה. זאת, על מנת לאמת את הדיוק של איתור הממצא חזותי. כדי להשלים את התמונה המודיעינית, יש לשלב בין נתונים ממקורות חזותיים מגוונים (כגון: הדמאות לוויין, תצלומים או כל מידע מבוסס פיקסלים) לבין מידע ממקורות אחרים (כגון: איכון, מידע סיגינטי ועוד), וכך להגיע לרמת זיהוי אובייקטים באחוז דיוק מקסימלי.

לצד אלו, חשובה היכולת לזהות באופן אוטומטי את המקור ואת שיטת העברת הנתונים, על מנת להעריך את רמת הסיכון של המידע ומהימנותו. זאת, בעיקר לאור השימוש הנרחב במקורות ושירותים מסחריים וציבוריים, שמטבעם חשופים יותר למניפולציות. למעשה, יש צורך להגן על המידע הנאסף משינויים זדוניים לצד שגיאות מערכת הנוצרות בתוכנה עצמה, ומכאן שדבר קשור בדבר, כאשר טעות הנובעת מכוונת זדון, משגיאות מערכת או משגיאות אנוש יכולה לגרור אחריה טעויות נוספות. יתרה מכך, על המערכת לאפשר לחוקרים לאתר אובייקטים ושינויים בתמונה עם תיאור מועט או חסר, על מנת להעריך תנועה או שינויים בתכונות (לדוגמה: תזוזה של אובייקט תחת רשת הסוואה) באופן מידי,[13] וניכר כי היבט זה חיוני בפן המבצעי.

היבטים אילו של מערכת הבינה המלאכותית החזותית בנויים זה על זה כשתי וערב ומכאן מתחזקת החיוניות של שימור האפשרות לחזור ולבחון כל שלב ושלב לגופו תוך אבחון אחוזי הדיוק של כל שלב, ולכאורה לאפשר למערכת להסביר את החלטותיה. על מנת לפתח מערכת כה מורכבת מצד אחד, וכה רגישה לפגיעות מצד שני, יש צורך בפיתוח נרחב ובלתי פוסק. לכן, אין זה מפתיע כי בשנים האחרונות ארגונים רבים כדוגמת צה"ל[14] וה-NGA [15] הרחיבו את שיתופי הפעולה עם חברות הייטק, עם אנשי אקדמיה ועוד.

כחלק ממגמת שיתוף הפעולה ההולך וגדל בין ה-NGA ומחלקות מודיעיניות שונות לבין המגזר הפרטי והאקדמיה, נוצר צורך להשתמש בקוד תוכנה פתוח לפיתוח פלטפורמה ייחודית המאפשרת למשתמשים מקהילת המודיעין, ממשרד ההגנה, מהאקדמיה ומההייטק, גישה לסביבת שיתוף נתונים בלתי מסווגת בעלת ממשק ידידותי. מכאן נובע שעל אף ששיתוף הפעולה עצמו מהווה אתגר באבטחת

---

[12] Katz, B. (April 2020). The Intelligence Edge: Opportunities and Challenges from Emerging Technologies For U.S. Intelligence. Center for Strategic and International Studies (CSIS). Retrieved July 16, 2020, from: https://bit.ly/2FlwmUA

[13] Boyed, A. (April 29, 2020). The world is changing—from commercially available GEOINT to COVID-19—so the National Geospatial-Intelligence Agency released a list of tech challenges the agency needs help to overcome. Nextgov. Retrieved June 7, 2020, from: https://bit.ly/3jWAB8c

[14] Cohen, S. (September 26, 2019). Startrek, Stargate and the Israeli Army's Other AI Projects. Haaretz. Retrieved June 7, 2020, from: https://bit.ly/2GSGtkD

[15] NGA- The National Geospatial-Intelligence Agency. (2017). NGA awards four contracts to enhance artificial intelligence and automation. Retrieved May 7, 2020, from: https://bit.ly/2GTguZY

המידע באופן טבעי מעצם שינוי גבולות המידור, ומעצם החשיפה לשיבושים שונים (נוזקות, שגיאות, מודיעין מסכל, "Deep fake" ועוד), לא מן הנמנע, כי דווקא בשיתוף פעולה כזה טמון הפתרון לתיקון טעויות ובעיות האבטחה השונות. בהקשר זה יצוין כי בינואר 2020 הונחו ב- IARPA לקיים תחרות (נושאת פרס של 5 מיליון דולר) לעידוד מציאת דרך טכנולוגית להתמודד עם "Deep fake" (שינוי מידע חזותי באופן קשה לאיתור), ובכך לעודד תחרות בין המחלקות השונות למציאת פתרון ופרויקטים אוטומטיים בתחום.[16]

סיכום ומשמעויות

מהפכת המידע במרחב הקיברנטי וההתפתחות המואצת של הבינה המלאכותית יצרו יכולות טכנולוגיות מגוונות המרחיבות את אפשרויות הפעולה של עולם האיסוף החזותי. פיתוחים אלו מסייעים במגוון פעולות כגון זיהוי עצמים, איתור מגמות בשטח, הנגשת המידע בזמן אמת ועוד, וכתוצאה מכך מתחוללת קפיצת מדרגה משמעותית במתן מענה מודיעין התרעתי ומחקרי. על אף שמכונה אינה מהווה תחליף מלא ליכולות אנוש, ניכר כי השקעה בפיתוח ויישום מערכות סריקה משולבות בזמן אמת הם הכרחיים כדי להבטיח יתרון אסטרטגי. מערכות מחקר הויזינט האוטומטיות, לצד קצב איסוף המידע ההולך וגדל, מחייבים פיתוח טכנולוגיות ושיטות מחקר באופן בלתי פוסק. שלא כמו בסוכנות המודיעין הגיאו-מרחבית האמריקנית, המערך החזותי בצה"ל מתבסס בעיקרו על מתגייסים צעירים, אשר יש צורך להופכם באופן מהיר למתכנתים מקצועיים ברמה גבוהה על ידי הכשרה. מכאן עולה שיש חשיבות רבה לשילוב כוח אדם מקצועי ואזרחי מגוון, ולפיתוח מגמות מקצועיות רלוונטיות כבר בבתי הספר התיכוניים.

אחד האתגרים הבולטים של הבינה המלאכותית הוא אמינות המידע ומניעת טעויות נגררות. ההתמודדות עם אתגר זה צריכה לשלב יכולות מתחומי ה-"Big Data" וה-"Deep learning", כמו גם הגדרת הצורך והמאפיינים תוך הגדרת המטרה (קרי, השמת הדגש על אופן הגדרת המטרה, הצרכים המשימתיים והסיווג כבר בשלב התכנות של המערכת). שילוב זה, יחד עם כוח אנושי מקצועי מגוון (חוקרים, מפענחים, אנשי טכנולוגיה, אנשי הייטק וכיו"ב), ועם מערכת בחינת כשלים, מהווים נדבך חשוב בכול רמות הניתוח עד להפקת התוצר הסופי. המפתח הוא כמות מרבית של שיטות, של חומרים, של אלגוריתמים, של חישובים ועוד, לצד ביקורת אנושית ומשנה זהירות. נהיר כי לצד צמיחת המערכות הטכנולוגיות, הייעול ברמת הזיהוי והאיתור של עצמים, של אובייקטים ושל מטרות, שיפור רמת הדיוק והגידול בכמות המידע הנאסף, תגדל גם כמות הזיופים והחומר הזדוני, כמו גם היכולת להימנע מגילוי. לפיכך, מערך הפיתוח מחד גיסא, ומערך הביקורת מאידך גיסא, צריך יהיה להשתנות באופן תדיר. עניין זה הוא קריטי וחשיבותו מתעצמת בחלוף הזמן, ועל כן יש להתייחס לנושא זה כעיקרי בפיתוח מתודולוגיה ומערכות ויזינט, ולשים עליו את הדגש.

נוכח התופעה של "Deep Fake" בהקשר החזותי שלה, יש הכרח לפתח "טכנולוגיה מסכלת", קרי כזו הבוחנת את התוצרים ואת תהליכי העיבוד של המערכת הויזינטית משלב האיסוף ועד שלב הסיווג והתוצר. במקביל, יש להריץ בדיקות ואנליזות שונות באופן מתמיד ושיטתי, ובהתאם להשקיע בפיתוח

[16] Keller, J. (January 8, 2020). U.S. intelligence researchers eye $5 million program to encourage new technologies in detecting deepfakes. Militaryaerospace. Retrieved August 11, 2020, from: https://bit.ly/3iYfvFm

ושיתופי פעולה נרחבים. לצד זאת, קיימת חשיבות לשמר את מיומנויות מחקר הויזינט טרום עידן "האינטליגנציה החזותית". זאת, מעצם היותם של חלק מכלים אלו מנותקים מרשת המידע רוב הזמן, ולפיכך פחות חשופים למניפולציות חיצוניות (אלא בעיקר להפרעות מתנאי האקלים וכדומה). יתרה מזאת, יש להתמקד ברמת האיסוף תוך השמת דגש על "טהרת המידע" (כלומר, להשקיע את מירב המאמץ בניקוי חומר הגלם, בניתוח אמינותו ובשיפורה, משום שכפי שצוין לעיל, חומר הגלם חשוף למניפולציות קשות לאיתור). בה בעת, וכפועל יוצא, יש לשים את הדגש דווקא על הכשרת כוח האדם לקבלת ההחלטות תוך שימוש מתמיד ברפרנס (בתחום המחקר החזותי הכוונה לעזר חזותי אחר של האזור הנבדק או הפריט המאופיין וכדומה המשמש ככלי השוואתי).

נקודה זו הנוגעת לחומר הגלם היא קריטית בחשיבותה, ולפיכך יש להתייחס בחשדנות מרובה למידע חזותי המתקבל, גם אם מדובר על כזה המועבר "ישירות" מסנסורים של בעלי ברית (מדינה אחרת למשל). זאת, משום שחומר זה עלול להיות "נגוע" ב- Deep Fake, ברמה כה טובה שלכלים המצויים בצד המקבל, טובים ככל שיהיו (מה גם שיש להניח כי גם ליריב יכולות דומות), לא תהיה היכולת לזקק את החומר המתקבל לכדי תמונה אמינה. כמו כן, לא מן הנמנע שפרויקט "התפירה" של IARPA אשר הוצג לעיל כולל בתוכו עיקרון טכנולוגי לפתרון, שכן בעצם התפירה קיימים חפיפה מסוימת ושילוב רב סנסורים, ולפיכך לכאורה נוצר "חומר גלם חדש", שבעצם היותו רב רבדי פחות חשוף ל- Deep Fake.