ISRAEL INTELLIGENCE HERITAGE & COMMEMORATION CENTER (IICC)

The Institute for the Research of the Methodolgy of Intelligence

סיכום כנס מודיעין - סייבר, דיגיטל ובינה מלאכותית

2 בדצמבר, 2020

בחסות:

FORTINET vmware DATA

כנס מקוון בנושא מודיעין - סייבר, דיגיטל ובינה מלאכותית

המכון לחקר המתודולוגיה של המודיעין (המרכז למורשת המודיעין) בשיתוף עם ישראל דיפנס ומחלקת הסייבר של אוניברסיטת בן-גוריון קיימו ב-2 בדצמבר 2020 כנס מקוון בנושא "מודיעין – סייבר, דיגיטל ובינה מלאכותית". מטרת הכנס הייתה לסקור את ההתפתחויות האחרונות בתחומים אלו ולהבין כיצד טכנולוגיות אלו משפיעות על העשייה המודיעינית ועל יחסי אדם-מכונה במודיעין.

את הכנס הנחה ראש המכון לחקר המתודולוגיה של המודיעין, תא"ל (מיל.) יוסי קופרווסר, והשתתפו בו פרופ' יובל אלוביץ – ראש תחום סייבר, מחלקה להנדסת מערכות מידע, אוניברסיטת בן-גוריון; עמיר רפפורט – מייסד ועורך ראשי, ישראל דיפנס וסייברטק; אל"מ (מיל.) איתי שפירא – לשעבר בכיר בחטיבת המחקר באמ"ן ומוביל תחום אסטרטגיית הדאטא וראש סקטור ביטחון ב-Deloitte; פרופ' ברכה שפירא – סגנית דיקן, המחלקה להנדסת מערכות תוכנה ומידע, אוניברסיטת בן גוריון; אבי יושעי – מנהל טכנולוגיות ראשי, VMware; ד"ר אהוד (אודי) ערן – עמית מחקר בכיר במכון לחקר המתודולוגיה של המודיעין ומרצה בכיר ליחסים בינלאומיים באוניברסיטת חיפה; דרק מנקי – סמנכ"ל מודיעין אבטחת מידע ושיתופי פעולה גלובליים לאיומים בחברת "פורטינט"; פרופ' ליאור רוקח – ראש המחלקה להנדסת תוכנה ומערכת מידע באוניברסיטת בן גוריון; ד"ר שי הרשקוביץ – עמית מחקר בכיר במכון לחקר המתודולוגיה של המודיעין, ראש תחום "ידע" בספרק ביונד ; וד"ר ויקטור מקרנקוב – בוגר אוניברסיטת בן גוריון, שם ביצע את עבודת הדוקטורט במחלקה להנדסת מערכות מידע.

<u>קיצורים:</u>

בינה מלאכותית-AI (Artificial Intelligence)

למידת מכונה –ML (Machine Learning)

מסד נתונים –DB (Data Base).

סיכום הכנס נכתב ע"י ניקול נגבי, עוזרת מחקר במכון לחקר המתודולוגיה של המודיעין

הבינה המלאכותית ומעגל המודיעין
– אל"מ (מיל.) איתי שפירא

ההרצאה עוסקת בשינוי ובשימור של מעגל המודיעין הקלאסי, שמפריד בין השלבים השונים של העשייה המודיעינית, אשר נתפס כלא רלוונטי, נוכח השלכות האפשרויות הנגזרות מהביג דאטה ובהשפעת הבינה המלאכותית.

מעגל המודיעין הקלאסי כבעל גבולות ברורים: הפרדיגמה המסורתית של המודיעין במערב היא גישה מדעית, תעשייתית (מעשה המודיעין כפס יצור) ואינדוקטיביסטית (הדוגלת בהסקה מן הפרט אל הכלל). גישה זו נועדה להגיע לחקר האמת ומפרידה באופן ברור בין התפקודים השונים במערכת המודיעין. בבסיס רעיון מעגל המודיעין עומדת הפרדה בין אכוונה של המאמץ המודיעיני, איסוף המידע, מחקר, והפצה. מאחורי כל מרכיב כזה עומדים תוצר, ארגון ותהליך שונים. יתרה מכך, קיימות הפרדות נוספות כגון דיסציפלינות איסופיות ומחקריות.

הבינה המלאכותית כמטשטשת את ההפרדה במעגל המודיעיני: הבינה המלאכותית היא "טכנולוגיה משבשת" של מעגל המודיעין בכך שהיא לא מפרידה בין המרכיבים השונים במעגל ולכן מטשטשת את הגבולות במעגל המודיעיני הקלאסי.

לטענת שפירא, אחד התוצרים הנדרשים מהמודיעין האסטרטגי שהוא זיהוי תפניות בתחילת התהוותן, הינו בעל פוטנציאל למיצוי ה-AI. ניתן לעשות זאת ע"י זיהוי אנומליות (חריגות) ב-DB גדולים. בישראל כבר החלו לקדם את תפיסת ה"מודיעין הרב-תחומי" ומכאן שיכולות ה-AI מתאימות ליצירת החיבורים הרצויים בין המרכיבים השונים של מעגל המודיעין. בראייתו, בעתיד נראה תוצרים מודיעיניים חדשים מתוך השילוביות שהטכנולוגיות החדשות מאפשרות.

ביג דאטא בינה מלאכותית ומודיעין אסטרטגי
– ד"ר אהוד (אודי) ערן

עד היום, AI ו-BD הם בעלי השפעה על המודיעין הטקטי והמסכל. המודיעין האסטרטגי לעומת זאת (המודיעין שמסופק למקבלי ההחלטות, בעיקר בכל הנוגע לתעלומות, קרי להתפתחויות עתידיות טרם מיצה את הפוטנציאל הטמון בטכנולוגיות אלו.

על אף ההבטחה הגדולה, למהפכה של המודיעין ע"י המכונות, אנחנו עדיין נמצאים בפרדיגמה של אדם-מכונה. זאת מכיוון שלא קיים עדיין מענה טכנולוגי לדמיון ולאינטואיציה של האדם ולכן אי אפשר להסתמך באופן מלא על טכנולוגיה בתחום המודיעין האסטרטגי. כלומר, ההפתעות האסטרטגיות עוסקות בהתפתחות של מציאות חדשה ולרוב בלתי מוכרת ומערכות סטטיסטיות אשר משמשות את ה-AI ו-הML מתבססות על "אירועי עבר" ולכן לא יכולות להשיג תובנה מסוג זה. לכן, בנסיבות האלו

אנחנו עדים לניצול מוגבל של מערכות אלה במודיעין האסטרטגי.

מכאן, שעיקר המיצוי של טכנולוגיות אלו צריך להתמקד בחיזוק של יתרונות החוקר האסטרטגי (באמצעות ה-AI) דוגמת מומחיות תוכן בזירה ספציפית אשר מובילה לאינטואיציה חזקה, שיפור אופן שאילת השאלות, מיסוד תהליך הדמיון ותיקון ההטיות במחקר האסטרטגי. בנוסף, ניתן לייעל את שלבי העבודה של המודיעין האסטרטגי ע"י פירוק נוסף של העשייה המודיעינית למרכיבים קטנים אף יותר (למשל ניתוח טקסט, כתיבת טיוטות ראשוניות וכד') והקצאה של משימות ספציפיות אלו לטיפול של המכונות.

השימוש בטכנולוגיות חדשניות במסגרת המעשה המודיעיני האסטרטגי טומן בחובו סיכונים רבים. לדוגמה, "הטיית האוטומציה" לעיתים גורמת לחוקר להסתמך יותר מדי על תהליכי האוטומציה בשל העומס הקוגניטיבי בו הוא מצוי במסגרת עבודתו. דוגמה נוספת לכך היא התחזקות הטיות מסוימות במסגרת השימוש במודלים של בינה מלאכותית מכיוון שהם מבוססים על נתונים שקיימת בהם הטיה. מכאן שיש לבצע בקרה הדוקה על תהליכי האוטומציה אשר תמנע את הנזקים של סכנות מסוג זה.

בסופו של דבר, סיכם ערן, העולם הטכנולוגי מאפשר ידיעה מקיפה יותר על העולם והתפקיד שלנו כבני האדם הוא לזכור כי המטרה היא לשפר את התבונה האנושית.

דמותו של איש המחקר המודיעיני העתידי ברקע של טכנולוגיות מפציעות – *ד"ר שי הרשקוביץ*

הטכנולוגיות החדישות שנמצאות כעת בתפוצה רחבה מובילות להגדרה מחדש של תפקיד המודיעין בביטחון לאומי כתוצאה ממגוון של תהליכים. סנסורים מייצרים ואוספים מידע בהיקפים חסרי תקדים (בדגש על Internet of things). בינה מלאכותית מאפשרת לאסוף ולעבד מידע בממדים עצומים (Big Data). רובוטיקה מאפשרת לייצר בצורה אוטומטית תוצרי ומבצעי מודיעין. מציאות וירטואלית (VR) מדמה סביבות פעולה רגישות לצורך אימון לקראת מבצע. ולבסוף, הדפסה תלת ממדית וביולוגיה סינטטית מייצרות איומים מסוג חדש לקהילת המודיעין.

כל אלו מעמידים את איש המודיעין מול מספר אתגרים: אובדן האקסקלוסיביות של אנשי המודיעין בשל אובדן הבלעדיות על המידע; מגוון רחב של מקורות/סוגי מידע; מותו של רעיון הציי"ח ומעגל המודיעין; התפקיד המשתנה של בני אדם בעידן של טכנולוגיות מפציעות.

מיפוי של השיח הדיכוטומי על עתיד המודיעין בהשפעת הטכנולוגיות המפציעות: קיימת דיכוטומיה ביחס לתפקידו של האדם במעשה המודיעיני בסביבה של טכנולוגיות חדשניות. הפסימיסטים מזהירים מהשתלטות המכונות על מקצוע שבטבעו הוא אנושי ואשר עוסק בנושאים של דיני נפשות.

מנגד, האופטימיסטים מצהירים כי ע"י שימוש ב-AI ניתן להתגבר על החסרונות (צווארי הבקבוק הקוגניטיביים) של בני האדם במסגרת המעשה המודיעיני. שני המחנות הם טוטאליים מדי בגישתם, בעיקר בעקבות אי הבנה של טכנולוגיות אלו והפוטנציאל והמגבלות שלהן.

כיום קיים צונאמי של מידע שמגיע לאנליסט בהשוואה לעבר ובינה מלאכותית מאפשרת להתמודד אתו. ולכן, גישה דיכוטומית זו לא מאפשרת לאדם ולמכונה לנצל את הפוטנציאל שלהם. גישה הנכונה צריכה להיות גישה שמשלבת בין אדם למכונה. הקדימות לאדם או למכונה יינתנו בהתאם לאופי המשימה והיכולות הקוגניטיביות הנדרשות.

<u>קווים לדמותו של האנליסט העתידי :</u>

1. מחובר למכונות ומסוגל לעבוד איתן.
2. משתף פעולה עם מכונות, אקוסיסטם והציבור.
3. בעל דמיון, יכולת של סיפור סיפורים והנגשה חזותית ומילולית.
4. ביקורתי כלפי עצמו, המכונה והשותפים.
5. מומחה תוכן שמתעלה מעבר לאיסוף העובדות.
6. אוצר תבונות של המכונה ומנגיש אותן כסיפור.

<u>הסברים לזיהוי אנומליות</u>
– פרופ' ברכה שפירא

גורמים זדוניים ברשת יוצרים אנומליות, כלומר חריגות בדאטא. ה-AI וה-ML מסוגלים לגלות את קיומן של האנומליות האלו ב-BD ולאתר אותן על סמך הקשרים החבויים שהן יוצרות.

כיום, קיים חיווי על זיהוי האירועים האנומליים ע"י ה-ML נמסר לצוות האופרטיבי. עם זאת, ללא הסבר לסיבות שבגללן זוהו אירועים אלו ע"י ה-ML, לצוותים האופרטיביים יהיה קשה להגיב בצורה המיטבית. על מנת לפתור קושי זה, התפתח תחום ה-Explainable AI. תחום זה פיתח מודלים שונים שמאפשרים הסבר של התוצאות ומתן המלצות על זיהוי האנומליות שנותחו במסגרת עבודת ה-ML. כלומר, מודלי ה-explainable AI השונים מסבירים את התוצאות של ה-ML למשתמשים במקרים של זיהוי אנומליות. כמו כן, מודלים אלו מסוגלים לשפר את המודלים של זיהוי האנומליות ומעוררים מוטיבציה למשתמשים לתת אמון ב-AI במסגרת התהליכים לזיהוי אנומליות.

המחקר של פרופ' שפירא מתמקד ביצירת הסברים לשיטת זיהוי האנומליות באמצעות ML הידועה

בשם "Unsupervised". שיטה זו מאפשרת זיהוי חריגות מהנתונים שקיימים ברשותנו ללא סיווג מוקדם של הנתונים לנורמלי או חריג. אלגוריתם ל-ML יכול להצביע על הימצאותה של אנומליה על פי שגיאה בשחזור של הפלט מן הקלט. ההסברים במחקרה של שפירא מתבססים על הסבר של דוגמה אחת של אנומליה ע"י שיטת SHAP. שיטה זו, מאפשרת לספק הסברים לאנומליות מתוך הסתכלות על הקומבינציה של התכונות שהובילו להחלטה של המודל והסבר על התכונות שהובילו להחלטה שלו.

למידת מכונה אוטומטית
– פרופ' ליאור רוקח

למידת מכונה היא טכנולוגיה אשר משמשת ארגונים רבים אשר מתמודדים במהלך עבודתם עם ביג דאטא. השימוש בטכנולוגיה זו מחייב את הארגונים לבצע תיקוף ותיקון (training & debugging) של המודלים על פיהם עובד ה- ML, תהליכים אשר כיום מצריכים את עבודתם של מומחי ה-ML. מומחים אלו אינם רבים ולכן נוצר צורך להעביר חלק מתהליכים אלו של תיקוף ותיקון, תהליך של אוטומטיזציה. מעבר לפן של כוח האדם, אוטומטיזציה זאת מאפשרת למומחי התוכן ליצור או לכל הפחות לבחון בעצמם פתרונות מבוססי ML.

פרויקט D3M (Data-Driven Discovery of Models) בשיתוף עם DARPA:

הרעיון העומד מאחורי פרויקט זה הוא להיעזר בדאטא שמגיע מניסויים קודמים על מנת לתכנן באופן מהיר יותר פתרונות (מודלים) בבעיות חדשות. הפרויקט מנסה לקחת את התהליך שאותו עושה ה-ML, לפרק אותו למרכיבים (פרימיטיביים) וכך ליצור פתרונות אוטומטיים ע"י הרכבה של כלל המרכיבים. ע"פ הערכת DARPA, פתרונות מהסוג הזה צפויים להראות ירידה משמעותית מאוד בעלות ובמשך של הפרויקטים. בישראל, פותחה ע"י יחידת התקשוב מערכת Federer – מערכת autoML אשר נמצאת בענן הצה"לי. מערכת זו משמשת עשרות משתמשים צה"ליים שיכולים להפעילה ללא הבנה מוקדמת ב-ML. המערכת מאפשרת מגוון של ביצועים דוגמת: השלמת נתונים מבצעיים; ניטור תקלות של מערכות IT; המלצות למיונים ועוד.

שימוש ברשת נוירונים מלאכותית (RNN) לניתוח משמעויות מרומזות מטקסט
– ד"ר ויקטור מקרנקוב

הלחימה כיום היא בסגנון של לוחמה היברידית שכוללת פגיעה באוכלוסייה מסוימת גם בהיבטים של כלכלה, תודעה, דיפלומטיה, התערבות בבחירות ועוד. בנוסף, התקשורת מצד המנהיגים נהייתה

בלתי-אמצעית אל מול הציבור של המדינה והיריבים. באופן דומה גם ארגונים לוחמניים וארגוני טרור אימצו שיטה זו על מנת להטריד את אזרחי מדינת האויב, לדוגמה דאע"ש וחמאס. לעיתים, דרך פעולה זו, שבאה להשפיע על אוכלוסייה מסוימת, נעשית באמצעות מסרים בסאבטקסט (מרומזים) במדיה ובתקשורת ומכאן עולה החשיבות בהבנת מסרים אלו ע"י בינה מלאכותית. ישראל היא מדינה שעלולה להיות רגישה לניסיונות להתססת החברה דרך מסרים העוברים בתקשורת.

במחקר שנעשה נבדקו היכולות של רשתות נוירונים מלאכותיות ((RNN ללמוד מתוך טקסט ייצוגים סמנטיים שמאפשרים הבנה של מסרים מרומזים. לדוגמה, נמצא באמצעות מחקר זה כי חברות חדשות, שכביכול אמורות להיות ניטרליות, התבררו מתוך המודל כנוטות לאחד הצדדים בקונפליקט הישראלי-פלסטיני על סמך למידה מהייצוגים הסמנטיים שבטקסט. מחקר דומה נעשה על יצירות ספרות בעלות אופי דו-משמעי.

Adversarial Playbook Heat Maps

– דרק מנקי

מנקי סקר בהרצאתו את ההתפתחות האחרונה בתחום מודיעין האיומים אשר מתבטאת בשימוש במודלים של ML ו-AI לצורך יצירה של מודיעין איומים מתקדם לגורמי מודיעין וביטחון ולחברות ציבוריות ומסחריות לצורך הגנה על הרשתות שלהם.

קיימות פלטפורמות בדרגות קושי שונות להתקפת סייבר במסגרת ה- Pyramid of Painדוגמת כתובות IP, שמות דומיין, כלים וכו'. מרבית הפלטפורמות משתנות תדיר ולכן המודל מתמקד דווקא ב-TTPs (הכלים, הטקטיקות והפרוצדורות בהם משתמשים התוקפים) שמשתנה בתדירות נמוכה יותר. מודלים שמשתמשים ב-ML ו-AI במסגרת הגנה מפני התקפות (דוגמת - Adversarial Playbook Heat maps) מאפשרים תגובתיות גבוהה לאיומים הרבים בפלטפורמות השונות שהוצגו לעיל. בנוסף, מודלים אלו מאפשרים מיפוי הפעילות של היריבים ברשת וחיווי חי על כך. מיפוי זה מאפשר להגנת הרשת להגיב בצורה אסטרטגית וכן לזהות שעומדת להיות תקיפה לפני שהיא יוצאת לפועל וכך למנוע אותה.

תפיסת הגנת הסייבר בעבודה מרחוק

– אבי יושעי

המציאות החדשה של תקופת הקורונה אילצה ארגונים מסחריים ואף ביטחוניים לעבור לשיטת העבודה מרחוק תוך כדי שינוי המודלים העסקיים. מצב זה של עבודה מכל מכשיר ומכל מקום גורם לאתגרים קשים בתחום אבטחת המידע.

<u>בנוסף, שלושת האזורים שקיבלו תאוצה בתקופה האחרונה הם:</u>

1. עבודה מכל מקום ומכל מכשיר.

2. היכולת לצרוך שירותים ומערכות משירותי ענן.

3. היכולת לקבל אנליטיקות ושירותים מאותם עננים.

תפיסת אבטחת המידע עד היום היא של ריבוי יצרנים, טכנולוגיות וכלים שונים להגנה על הנכסים הארגוניים ברשת. תפיסה זו לא הצליחה ואנחנו ממשיכים לראות בפועל התקפות חוזרות ונשנות והצלחות מצד האקרים. בנוסף, בעידן הנוכחי נדרש לשנות את הגישה כלפי אבטחת המידע בשל המעבר לעבודה מבוזרת. לכן, התפיסה הנכונה לראייתו היא לספק יכולות אבטחה מובנות, כדי להגן על כל שכבה ברשת, גם באפליקציות וגם בדאטא. קיימים מספר אזורים שבהם נדרשת הגנה, וצריכה להיות מערכת הגנה ייעודית לכל אזור וביניהן קורלציה וסינרגיה. כלומר, החידוש בתפיסה זו הוא העדכון של שאר מערכות ההגנה ברשת בזמן חדירה של נוזקות או התקפות, דבר אשר יוצר מערכת הגנה מובנית שמאפשרת את העבודה המבוזרת של הארגון.