"מלאכים בשמי ברלין" - שאלות מודיעיניות חדשות בעולם רווי נתונים

מאת מ' - סגן מנהל בית הספר למודיעין של שירות הביטחון הכללי

"Ask what, don't ask why"

אבן יסוד בחשיבה המודיעינית המודרנית היא "שיטת/דפוס הפעולה" (Modus Operandi). ארגוני מודיעין משקיעים מאמצים ומשאבים רבים למחקר דפוס הפעולה של היריבים, לאיתורו ולאפיונו, כשהמוטיבציה המרכזית היא להגיע ליכולת איסוף מידע על פעילות היריב ולנטרו בדרך שתאפשר גילוי סימנים מעידים להתרחשותם של אלמנטים מדפוס פעולה זה ועל ידי כך לזהות את כוונותיו של היריב ולהתמודד עימן.

מודיעין האותות ("סיגינט") אשר התפתח במאה השנים האחרונות, פעל אף הוא בתוך המסגרת החשיבתית המודיעינית של אבן יסוד זו. ארגוני מודיעין ניטרו ואספו מידע על אודות הפעילות התקשורתית של יריביהם, ניתחו וחקרו כיצד בא דפוס הפעולה של יריביהם לידי ביטוי בחתימות התקשורתיות של פעילותם, ובנו מנגנונים לזיהוי הסימנים המעידים מתוך הפעילות התקשורתית. עם התפתחות העולם התקשורתי ב־15 השנים האחרונות, התמודדו ארגוני מודיעין עם כמות הולכת וגדלה של אותות מאמצעים רבים ומגוונים ומסוגים שונים של חתימות דיגיטליות המאפיינות פעילות תקשורתית. ארגוני המודיעין השונים השכילו לאמץ ולפתח טכנולוגיות לניתוח קשרים ולאפיון התנהגות תקשורתית אשר הרחיבו את יכולתם לזהות ולנטר את פעילות יריביהם ולמצוא באמצעותם סימנים מעידים לפעילות של היריב. ועדיין, קו המחשבה המוביל בפעילות זו היה ביצוע מחקרים ואיסוף נתונים שיאפשרו לאפיין את דפוס הפעולה של היריב, לאתר את הסימנים המעידים להופעת דפוס הפעולה, לחזור ולנתח את דפוס

הפעולה וחוזר חלילה, תוך השקעת אנרגיה ארגונית ואינטלקטואלית רבה באפיון דפוס הפעולה של היריב.

אם אמשיל את העולם המודיעיני לעולם המסחרי והפרסומי, ניתן לדמות את קו המחשבה המודיעיני הקלסי לשיטות המחקר והמיקוד הפרסומיים במחצית השנייה של המאה הקודמת. כאשר הושקעו משאבים עצומים - כספיים, ארגוניים ומחשבתיים - במחקר ובניתוח השווקים, ההעדפות והטעמים של הצרכנים הפוטנציאליים, וכל זאת כדי להביא אליהם פרסום אפקטיבי שיוביל לצריכה.

מעבר לשינויים שחלו בטכנולוגיה ובפרדיגמות הניתוח של הפעילות האנושית, גם יריביהם של ארגוני המודיעין עברו שינוי. אם בעבר עסקו גופי המודיעין ביריבים הפועלים כארגונים, בין אם מדינתיים ובין אם ארגוני טרור ופשיעה, בשנים האחרונות עובר חלק גדול מהקשב של ארגוני המודיעין ליריבים רשתיים ונטולי היררכיה, המייצרים קשרים שלא על בסיס מבנים ארגוניים קבועים מראש ומניעים את הפעילות באמצעי השראה והפצה ולא באמצעי הנחיה והפעלה - "עולם שטוח" של יריבים המגיע עד כדי התמודדות עם יחידים המהווים גורמי איום וסיכון ואשר פועלים באופן עצמאי. שינויים אלה באופי היריבים מחייבים את ארגוני המודיעין לשנות את תפיסות היסוד שלהם ובמקום לחפש את מודל הפעילות של היריב, לנסות ולאתר סימנים מעידים מסוגים אחרים. סימנים כאלה יכולים להיות שינוי התנהגות, החלפת חזות, עלייה או ירידה בנפח הפעילות, יצירת קשרים חדשים, נגיעה ברכזות (Hubs) של מארגי קשרים ועוד. ארגוני המודיעין נאלצים לשנות את תפיסות האיסוף שלהם ולאסוף נתונים רבים מאוד תוך הצבת סנסורים רלוונטיים לאיסוף נתונים אלה ושימוש בנתונים, וכן לשנות את סוג השאלות שהם שואלים על המידע הנאסף.

עולם הביג דאטה נולד מהתלכדותן של כמה התפתחויות טכנולוגיות מקבילות – הגדלת היכולת לייצר ולאסוף כמות גדולה של מידע על ידי סנסורים חזקים ומגוונים, הגדלת נפח אחסנת הנתונים ומזעורו (או העברתו ל'ענן'), הגדלת כמות המידע בעולם בשל השימוש ההולך וגובר בטכנולוגיות המייצרות חתימות דיגיטליות בפעילות אנושית יומיומית והתחזקות כוח החישוב באופן המאפשר התמודדות עם כמויות עצומות של מידע וניתוחן בפרק זמן קצר ובמקביל.

עולם הביג דאטה מייצר שינוי בדפוסי חשיבה, שינוי שאינו רק כמותי אלא איכותי ומשנה פרדיגמה. עולם זה מייצר שאלות, מחקרים והזדמנויות עסקיות מסדר חדש. בספרם Big Data מאפיינים Mayer-Schoenberger ו־Cukier את השינויים הפרדיגמטיים המרכזיים שמייצר עולם הביג דאטה על דרכי החשיבה המקובלות.[1] עיקרון מרכזי שהם מציבים הוא "שאל מה אל תשאל למה?" ("Ask what don't ask why") ומשמעותו היא כי בעולם של נתוני עתק אין טעם ואין צורך לנסות לחקור ולאפיין את מודל הפעילות של מושא המחקר אלא להפעיל חיזוי מבוסס נתונים, וזאת באמצעות אלגוריתמים המזהים מתאמים ולא בהכרח תלויות. רוצה לומר, גם אם לא נוכל להסביר את מודל הפעילות של מושא הבחינה וגם אם לא נוכל להוכיח כי תופעה מסוימת נובעת

1 Viktor Mayer-Schoenberger & Kenneth Cukier (2013). *Big Data- A revolution that will transform how we live, work, and think. Boston New York 2013.*

מחברתה, די לנו כי האלגוריתם יגלה מתאם בין שתי התופעות כדי שנוכל להשתמש בקשר זה באופן אפקטיבי.

ענקיות הקמעונאות המקוונת, ובראשן חברת 'אמזון', ובעקבותיהן כל זירות הסחר המקוון, מנצלות את המידע העצום שברשותן על אודות רכישותיהם של לקוחותיהן כדי לייצר הצעות רכישה מכוונת התנהגות צרכנית, גם במקומות שבהם הלקוח עצמו אינו מודע לזיקה בין רכישותיו, המוצרים שבהם צפה, הזמן ששהה בכל עמוד מוצר, מידת העניין שלו בתמונות המוצר או בתכונותיו וכיוצא באלה, לבין הצעות הרכישה שיוצגו לפניו על ידי האתר. לעיתים, נוכל להסביר את הקשר והמתאם בין התנהגויות צרכניות שונות. לדוגמה, אדם המתחיל להתעניין במושבי תינוק בגודל NewBorn לרכב, יש להניח כי יהיה מעוניין לקנות חיתולים לתינוק וכדאי לכוון אליו (To target him) פרסום למוצרים כאלה.

שאלות מודיעיניות בעידן הביג דאטה

ניתן לומר כי ארגוני מודיעין עושים היום שימוש רב, עמוק ואפקטיבי בטכנולוגיות ובמתודות בתחום הביג דאטה בכמה תחומי עניין ואל מול כמה שאלות עיקריות. הם מאמצים את השיטות לאיסוף נתונים, לניתוח ולמיצוים לצורך הגעה אל המידע הממוקד המעיד על פעולות היריב ועל כוונותיו - "איתור מחט בערמת מחטים". ארגוני מודיעין פועלים לאיתור איומים והזדמנויות מול יריביהם בתווך הסייברי, ומטבע הדברים בתווך זה חלק גדול מן העיסוק הוא בשיטות הנוגעות לעולם הביג דאטה. בין השאר עוסקים הארגונים בתחומים אלה בניתוח תעבורת נתונים עצומה, ובניסיון לאתר אנומליות המעידות על פוטנציאל תקיפה סייברי, כמו גם איתור תבניות התנהגויות רשתיות שמטרתן זיהוי סימנים מעידים לפעילות סייברית ואיתור נקודות חולשה של היריבים.

ההבדל בין העולם העסקי לעולם המודיעיני: מוקד העניין שיעסיק תאגיד או חברה, יהיה המוצר שאותו הם מייצרים, או הרעיון שאותו הם מבקשים לשווק, אך את ארגון המודיעין יעניין המוטיב האידיאולוגי או הנפשי

מעבר לתווך הסייבר עצמו כזירת התגוששות ואיסוף הדדיים בין ארגונים ויריביהם, גם הפעילות הסייברית מהווה כר נרחב לאיסוף מידע עצום בהיקפו על אודות פעילותם של יחידים וקבוצות וצורות ההתקשרות ביניהם. גם בתחום זה עוסקים רבות ארגוני מודיעין, אשר פועלים בשיטות דומות לאלו הנהוגות בעולם העסקי-אזרחי לצרכים מסחריים ושיווקיים. אם ארגונים עסקיים מתעניינים במידת העניין במוצר מסוים, או בזיהוי צורך שניתן לספקו על ידי שיווק ממוקד, כך גם ארגוני מודיעין מנטרים פעילות ושיח רשתיים ומנסים לזהות את מידת העניין והעיסוק בתחום המהווה פוטנציאל איום או הזדמנויות הנוגעים לתחומי העניין של ארגוני מודיעין אלה וכן מנסים לאתר מתוך ים המידע את היחידים והקבוצות שבהם נמצא פוטנציאל הנזק והאיום, או את ההזדמנות לשפר את יכולות האיסוף והתקיפה של ארגוני המודיעין.

ארגוני מודיעין מתעניינים מטבע הדברים בשאלות המעסיקות גם ארגונים עסקיים, כאשר רק מוקד השאלה שונה. ארגון עסקי שואל את עצמו 'מה חושב הציבור על המוצר שלי?' 'מה מעמדו של המוצר שלי אל מול מוצרים מתחרים?' 'כיצד אזהה צורך חדש ומתהווה וכיצד אוכל להיכנס לשוק בנקודה שבה המוצר שלי יענה על צורך קיים?' ארגונים עסקיים פועלים לקבל תשובות לשאלות אלה בשיטות שונות של ניתוח ביג דאטה החל מניתוח נתוני המכירות והצריכה כפי שנמצאים במאגרי המידע שלהם ושל שותפיהם, דרך ניטור השיח הרשתי והפעלת מתודות מתחומי Opinion mining, Brand Monitoring ו־Sentiment analysis. חברות רבות מספקות שירותים כאלה לחברות ותאגידים בקשת של מוצרים מסוגים שונים.

גם ארגוני מודיעין עשויים לעשות שימוש במתודות כאלה, כשהשאלות הנשאלות על ידם הן מסדר דומה, וההבדל הוא רק במוקד העניין. בעוד מוקד העניין שיעסיק תאגיד או חברה יהיה המוצר שאותו הם מייצרים, או הרעיון שאותו הם מבקשים לשווק, את ארגון המודיעין יעניין המוטיב האידיאולוגי/דתי/נפשי שיכול להביא לפעילות טרור או התעניינות באמצעי לחימה מסוימים או כל נושא אחר הנמצא במרחב ההתעניינות של הארגון.

שאלות מודיעיניות מסדר חדש

עם זאת, כמדומני שישנו תחום רחב שבו לארגוני המודיעין יתרון מובנה על תאגידים וחברות עסקיים, יתרון שיכול לייצר הזדמנויות מודיעיניות ומחקריות חדשות ויצירתיות, ולאפשר לארגוני המודיעין לשאול שאלות מחקריות חדשות, מסדר שונה, שיוכלו להרחיב את תמונת עולמם ואת מסד הידע שעל בסיסו יאפשרו למקבלי החלטות לנהל סיכונים ולקיים תהליכי קבלת החלטות טובים יותר. כדי לנסות ולגרות את המחשבה על שאלות מודיעיניות חדשות שניתן לענות עליהן בכלים ושיטות של מיצוי ביג דאטה, אנסה לתאר מציאות דמיונית המשלבת מציאות פוליטית-חברתית היסטורית עם מציאות טכנולוגית עכשווית.

נכניס עצמנו לסביבת מציאות מדומה. אנחנו בשנת 1983 בעיצומה של המלחמה הקרה, בסביבה גיאו־פוליטית מקוטבת בין הגוש המזרחי בהנהגת ברית המועצות למערב בהנהגת ארצות הברית. אנו בברלין החצויה בין מזרח ומערב. חלקה המזרחי של העיר שייך לרפובליקה הדמוקרטית הגרמנית - DDR (גרמניה המזרחית), ואילו חלקה המערבי של העיר הוא מובלעת השייכת לרפובליקה הפדרלית הגרמנית - BRD (גרמניה המערבית). בליבה של העיר ניצבת חומה שהמעבר העיקרי בה בין מזרח למערב[2] הוא ב־Check point Charlie. בשני חלקי העיר פועלים שני ארגוני מודיעין יריבים - בצידה המערבי של העיר פועל בין השאר ה־BfV, שירות הביון הפנימי האמון על איומי חתרנות אידיאולוגיים (כגון ניאו־נאצים וקומוניסטים) ועל סיכול ריגול מצד הגוש המזרחי. בצידה האחר של העיר פועל ה"שטאזי" המשמש גם כסוכנות ביון החוץ וגם כארגון מודיעין וביטחון הפנים האמון על פיקוח על האוכלוסייה וריגול נגדי.

במציאות הדמיונית שלנו, הטכנולוגיה ומאפייני התקשורת הם של שנת 2018. אזרחי שתי

2 המבקש לחוש את רוח התקופה יוכל לגעת בה באמצעות קריאת כמה ספרים מסוגות שונות ובאמצעות צפייה בכמה סרטים וסדרות טלוויזיה שיצאו בשנים האחרונות. בין השאר ניתן להמליץ על הספר "ילדי השטאזי" מאת דייוויד יאנג (מתרגם: אילן פן) 2015, הסרט "חיים של אחרים" (Das Leben der Anderen) והסדרה Duetschland 83.

המדינות ותושביהן עושים שימוש בטלפונים סלולריים חכמים, לרובם ככולם חשבונות דוא"ל ופרופילים פעילים ברשתות החברתיות השונות. תושבי המדינות עושים שימוש במכשירים המחוברים לרשת האינטרנט ומייצרים חתימות דיגיטליות שונות, כגון טלוויזיות חכמות, שעונים חכמים, צמידי כושר, מכוניות חכמות, תגי זיהוי דיגיטליים וביומטריים ועוד ועוד. במציאות בדיונית זו, לשני הארגונים נגישות בלתי מוגבלת לכלל הנתונים והאותות שנוצרים בעיר ברלין ובאזורי הגבול בין שתי המדינות.

עתה, לאחר שתיארנו את המציאות הדמיונית שבתוכה אנחנו פועלים, נכניס עצמנו לנעליהם של אנשי המחקר בשני ארגוני הביון היריבים, וננסה לחשוב אילו שאלות חדשות נוכל לשאול על מושאי העניין שלנו, אשר יעשירו את הבנתנו המודיעינית וירחיבו את יכולות הפעולה שלנו לעמוד בייעוד הארגון.

ראש אגף הגנת המדינה מתעמולה וחתרנות אימפריאליסטיים ב"שטאזי" כינס את אנשיו וביקש לבצע מחקר אשר יבדוק את מאפייני תרבות הפנאי של תושבי מזרח ברלין, תוך חלוקה לפי חתך גיל ומאפייני תעסוקה, בדגש על ניתוח מדויק יותר של מאפייני הבילוי של עובדי המערכת הממשלתית. אנשי האלגוריתמיקה של ה"שטאזי" ניגשו לעבודה ובנו מחקר המנתח את מאפייני הבילוי הללו בשיטות של מחקר נתוני עתק – ניתוח של כלל נתוני המיקום של הטלפונים הסלולריים השייכים לתושבי העיר המזרחית, או משמשים אותם, תוך פילוח לאורך זמן של ימים בשבוע ושעות ביממה המאפיינים את גרף השינוי בין שעות עבודה לבין שעות וימי בילוי. הניתוח כלל בדיקה השוואתית בין מיקומי הטלפונים הסלולריים לבין הפעילות של בעליהם ברשתות החברתיות, תוך ניתוח של מאפייני התכנים שהועלו ברשתות – תמונות, פוסטים וטקסטים ואיתור מילים המתאימות לפעילות בילוי בניגוד לאלו המתאימות לפעילות ביתית.

ניתוח נוסף שנעשה על ידי מחלקת המחקר ב"שטאזי" היה של ההתקשרויות בין האזרחים, והימצאותם יחד בקרבת מקום עם חבריהם וקשריהם, המתאם או אי־המתאם ביניהם בין שעות העבודה לבין שעות הבילויים, וזאת כדי לבחון האם האזרחים נוטים לבלות יותר עם בני משפחותיהם, עם חבריהם לעבודה או אולי דווקא עם מעגלים אחרים המרחיקים אותם מחבריהם לעבודה.

בעקבות ממצאי המחקר שבוצע ב"שטאזי", שינו באגף הגנת המדינה את מאפייני הכיסוי שבוצע עד היום, והוחלט לגייס מודיעים חדשים באזורי בילוי בלתי מוכרים שהתגלו כפופולריים בסופי השבוע בקרב אזרחי העיר המזרחית בגילים 25–35. אך עם זאת נשמעה צפירת הרגעה במסדרונות האגף כאשר התברר כי עובדי מדינה נטו לבלות בבתיהם גם בשעות הפנאי ולא נסחפו בגל של בילויים בלתי מבוקרים על ידי המדינה. למסקנה זו הגיעה מחלקת המחקר מתוך העובדה כי טלפונים חכמים של עובדי המדינה נטו להישאר בקרבת מקום למכשירים אחרים המחוברים לחשבונותיהם של בעלי הטלפונים כגון הטלוויזיות החכמות ומכשירי ה־PC שלהם.

מעברה השני של החומה, ביקש ראש מחלקת ברלין ב־BfV, מהאלגוריתמיקאים במחלקתו לבנות תמונת מודיעין מבוססת נתונים שתנתח את כל המזרח גרמנים אשר הצליחו להבריח את הגבול או שניסו לעשות כן במהלך שלוש השנים הקודמות. ראש המחלקה ביקש שהמחקר ייתן תשובה

לשתי שאלות: האם עריקה מן המזרח למערב היא דרך פעולה של המודיעין המזרח גרמני כדי להכניס מרגלים למערב? האם ניתן לאתר מבעוד מועד מועמדים פוטנציאליים לעריקה, כדי לעודד אותם לעשות כן ולבנות פלטפורמות שיאפשרו להם להגיע למערב?

מסקנות מחקרם של אנשי השירות המערב גרמני היו כי עריקים וכאלו שניסו לערוק, מאופיינים בכך שצריכת המדיה שלהם כללה הרבה יותר גלישה באתרים מערביים, כאשר ניתן להבחין בגרף עולה של צריכת מדיה כזו, על חשבון ירידה במינון ההיחשפות לתכנים הרשמיים של המשטר המזרח גרמני. כמו כן גילו אנשי המחקר כי ניתן לזהות נקודה על ציר הזמן בשינוי באופי צריכת התכנים שבה מתחילות להופיע התקרבויות גיאוגרפיות של המועמד לעריקה אל החומה והגבול עם מערב גרמניה. על בסיס ממצאי המחקר הזה, בנו אנשי הטכנולוגיה של השירות המערב גרמני מנגנון חיפוש של כלל צריכת המדיה הדיגיטלית במזרח לאיתור משתמשים המייצרים גרף דומה ויצירת התרעה (Alert) בהתלכדות הצירים לנקודה המתאימה, ומנגנון אוטומטי אשר שלח הודעת טקסט לכל מי שעלה בהתרעה כזו. ההודעה הועברה בדרך התקשרות חשאית כדי לנסות ולסייע בעריקה פוטנציאלית. ובמקביל, ייבחנו קשריו כל עריק פוטנציאלי כזה עם המודיעין המזרח גרמני, כדי לוודא שאינו מרגל מזרח גרמני המיועד להחדרה למערב.

מה ניתן ללמוד מכך?

עד כאן עולמנו הדמיוני, ומכאן יוכל כל אחד מן הקוראים לקחת את עולמו המודיעיני ולנסות להשליך את הרעיונות הללו על המציאות בת זמננו. כמדומני שאין צורך אלא בהפעלת הדמיון והיצירתיות המודיעינית כדי לחשוב ולבנות שאלות חדשות מסדר חדש, כאלה שלא נשאלו עד היום, שאלות שעולם נתוני העתק מאפשר לנו לתת עליהן תשובות בעלות ערך שיכול להעשיר את הידע על אודות היריבים ולהרחיב את יכולתם של ארגוני מודיעין לתת כלים בידי מקבלי ההחלטות, הן לניהול המערך המודיעיני והן לניהול סיכונים תוך הערכת האיומים וההזדמנויות באופן המשקף טוב יותר את המציאות.

המפתח ליצירת מחקרים רלוונטיים בשיטות וכלים של ביג דאטה בעולם המודיעין הוא המודעות לאפשרות לשאול שאלות חדשות; ההבנה כי נתוני העתק אינם מייצרים רק הבדל כמותי שמאפשר מענה על שאלות ישנות בכלים חדשים, אלא מייצרים מציאות חדשה שבתוכה ניתן לשאול שאלות חדשות לגמרי שהמענה עליהן ייתן בידי אנשי המודיעין תמונת מציאות משוכללת ומשקפת יותר של היריב ושל הסביבה שבתוכה הוא פועל. כמדומני שהדרך להשתמש במפתח זה היא על ידי יצירת שיתופי פעולה חדשים בין אנשי מחקר מודיעיני קלסי לבין אנשי ביג דאטה, אלגוריתמיקאים ואנליסטים בתחומי כריית המידע, תוך הפריה הדדית ויצירת רעיונות משותפים.