



תוכנות נגד טרור

תוכנות מתוחכמות יכולות לעלות על עקבותיהם של טרוריסטים ושל סייעניהם גם כאשר אלה משבשים את שמותיהם או מתחזים לאנשים אחרים

דביר בן־אהרון

מקורות המימון המערביים של הטרור הבינלאומי קשה מאוד לעצור. הסיבה: את הכספים אוספים מהפזורה המוסלמית באמצעות "מוסדות צדקה" ו"קרנות צדקה" ומזרימים אותם לארגוני הטרור באמצעות חשבונות בנק מוסווים בבנקים מערביים מכובדים. מהסיבה הזאת קשה מאוד ליישם את החלטת מועצת הביטחון מה־28 בספטמבר 2001, המחייבת כל מדינה החברה באו"ם להקפיא את נכסיהם של ארגונים המוגדרים כטרוריסטיים.

מהרגע שבו הוחלט להילחם בטרור גם באמצעות ייבוש מקורותיו הכספיים, היה ברור שאין די בעבודת מודיעין קלאסית של בילוש ועיקוב, אלא יש צורך בפתרון טכנולוגי מתקדם שיסייע לגלות כל רשומה במערכות המחשוב של הבנקים, המתייחסת ליחידים או לארגונים, ששמותיהם או מספריהם דומים לשמות ולמספרים המצויים ברשימות השחורות. הצורך הזה הוא קריטי, משום שהתברר שריבוי התעתיקים של שמות – ובמיוחד של שמות ערביים – מקשה מאוד לעקוב אחר הפקדות חשודות ותנועות של הון. נניח שיודעים כי מטיף כלשהו במסגד בניו־ג'רסי בשם מחמט עלי יוסוף רמדאן מגייס תרומות לחיזבאללה בקרב באי המסגד שלו. אולם אם

שתפעולו עולה מאות מיליוני דולרים. מאחורי מבצע טרור דוגמת שיגור טילי כתף לעבר מטוס "ארקיע" בקניה עומד מערך לוגיסטי גדול ויקר מאוד שצריך לממן לא רק את רכישת הטילים ואת הברחתם, אלא גם את אימון

חיסול הטרור באמצעות ייבוש מקורות המימון שלו הרבה פחות טוב מפשיטה של יחידת עילית על יעד זה או אחר, אבל יעילותו היא רבה ולטווח ארוך

הטרוריסטים, את דירות המסתור שלהם, את אמצעי ההובלה שלהם וכן תשלום נדיב. לעשרות הסייענים שמאפשרים לאנשי השטח עצמם לנוע ממקום למקום בלי להיחשף.

לטרוריסטים הבינלאומיים יש שני מקורות מימון מרכזיים: מדינות תומכות טרור דוגמת איראן, סוריה וערב הסעודית ואיסוף תרומות בפזורה המוסלמית הגדולה שמתגוררת במדינות המערב. את המקור הראשון ניתן לייבש רק באמצעות לחץ בינלאומי תקיף. למרבה האירוניה, דווקא את

שירותי מודיעין יודעים כבר זמן רב כי יש שתי דרכים להילחם בטרור: הדרך האחת היא לרדוף אחר הטרוריסטים ומפקדיהם ולחסלם בזה אחר זה או לעוצרם; הדרך השנייה היא לייבש את מקורות המימון שלהם. הדרך הראשונה, שאותה אנו – הישראלים – מכירים היטב היא יעילה מאוד, אך לטווח קצר בלבד. לכל טרוריסט עצור או מחוסל – יהיה בכיר ככל שיהיה – קמים במהירות רבה יורשים שממשיכים את דרכו. התוצאה היא שבעקבות כל מבצע צבאי ל"חיסול תשתיות הטרור" משתרר שקט לזמן קצר בלבד, עד אשר התשתיות משתקמות וחוזרות לפעול.

הדרך השנייה לחיסול הטרור – ייבוש מקורות המימון – היא פחות הרואית ומצטלמת הרבה פחות טוב מפשיטה של יחידת עילית על יעד זה או אחר, אבל יעילותה היא רבה ולטווח ארוך. חשוב להבין שטרור – ובמיוחד טרור בינלאומי דוגמת זה של אירגון אל־קאעידה, של החיזבאללה ושל החמאס – הוא "קונצרן" ענקי

מנהל פרויקטים בחברת תוכנה



במחשב של הבנק הוא יופיע כמחמד עלי יוסף, הרי סביר להניח שהתרעה של האף-בי-איי לא תיקלט, והכספים ימשיכו לזרום באין מפריע לחיזבאללה. כאן מסייעת התוכנה SSA-NAME3 לחיפוש ולהתאמת מידע של חברת SPL Software. מדובר בתוכנה המאפשרת לעסוק בזיהוי נתונים, לבצע חיפוש והתאמה ומיועדות לארגונים, לגופים ולמוסדות הפועלים בתחומים של איתור חשודים, ביצוע חקירות הונאה ומעקב אחר גופים העוסקים בהלבנת הון, כאשר יש צורך לעבוד מול רשימות שחורות ולהצליב נתונים על פעילויות.

תוכנה כזאת יכולה למצוא, להתאים, לחלק לקבוצות ולבדוק שמות, כתובות או פרטים מזהים אחרים על אנשים, על חברות, על מקומות או על חפצים - בין אם מדובר בחיפוש המתבצע online או בחיפוש אצווה (Offline). התוכנה מסוגלת להתגבר על אי-התאמות או על סתירות באיות ובהגיוי, על רצפים של מילים כמו גם על שמות זרים, על קיצורים ועל מילים חסרות.

תוכנה אחרת יכולה לאתר פעילות בנקאית חשודה באמצעות זיהוי תבניות פעילות חריגות. התוכנה הזאת - של חברת Crystaliz - מנתחת כמויות אדירות של מידע ומזהה נתונים חריגים הסוטים מפעילות "נורמלית" בתחום הרלוונטי.

התוכנה הזאת עוררה עניין רב מצד סוכנות המו"פ הפדרלית של ארה"ב (DARPA), המתכוונת לפתח כלי יעיל להתרעה מראש על פעילות טרוריסטית. הכוונה היא שהתוכנה תוכל, למשל, לחפש תבניות חריגות בדואר אלקטרוני, בהזמנות של כרטיסי טיסה או בהזמנה של חומרי גלם, העלולים לשמש לייצור חומרי חבלה. אם התוכנה תתפקד כהלכה, היא תוכל להבחין בין רכישת דשנים שגרתית לצרכים חקלאיים לבין רכישת דשנים לצורכי טרור.

תוכנה חשובה נוספת למלחמה בטרור מאפשרת זיהוי ביומטרי של

חשודים. וכך זה עובד: לכל אדם יש מאפיינים ביולוגיים הייחודיים רק לו: די-אן-אי, טביעות אצבעות, מבנה של קשתית העין, קול, תווי פנים. מפעל ביטחוני כלשהו יכול לבנות לעצמו מאגר של צילומי רשתית של כל עובדיו, וכל עובד יכול להיכנס לאותו מפעל רק לאחר שהתבונן לתוך עינית, והתוכנה הייחודית וידאה שהרשתית שלו מצויה

ייחודי. ברגע שאדם מגיע לנמל-תעופה, מושווים פניו למאגר הנתונים של החשודים. יתרונה העצום של התוכנה הזאת הוא בכך שלא ניתן "לעבוד" עליה באמצעות תספורות, זקנים, משקפיים, פאות וכו'. התוכנה הזאת אינה "מתרשמת" מכל האביזרים האלה: היא ממירה את תווי הפנים נטו לנתונים מספריים, ומשווה את רצף המספרים



במאגר הנתונים של המחשב. יתרונה של שיטת הזיהוי הזאת הוא בכך שלא ניתן להונות אותה. לעומת זאת סינון עובדים באמצעות תעודות כניסה חשוף לאי-ספור הונאות והתחזויות.

לחלופין אפשר להכין מאגר נתונים גדול של חשודים בטרור. את צילומי הרשתית של חשודים בטרור ניתן אומנם להשיג רק לאחר מעצרו, אך תמונות שלהם ניתן להשיג הרבה לפני כן. צריך איפוא להקים מאגר גדול ככל האפשר של חשודים בטרור, שאליו ניתן להשוות את פניהם של אנשים במקומות ציבוריים המועדים לפיגועים - למשל נמל-תעופה.

תוכנה של חברת Viisage עושה בדיוק את זה: היא ממירה את תווי הפנים של כל אדם למערך מספרים

לרצפים שאגורים אצלה. בתוכנה הזאת טמון פוטנציאל להפוך ל"אח גדול" נוסח ג'ורג' אורוול, ולכן היא מעוררת התנגדות רבה בקרב ארגונים לזכויות אדם. כבר היום ישנם אזורים עירוניים רבים - גם בישראל - המפוקחים 24 שעות ביממה באמצעות מצלמות במעגל סגור. כל מה שצריך לעשות הוא לחבר מצלמות כאלה למאגר נתונים של חשודים (בטרור ובפלילים) ובדרך זו ניתן יהיה "לשלוף" מהרחוב באופן מיידי כל "פרצוף חשוד" - למשל של אסירים בחופשה ש"שכחו" לחזור לבית הסוהר בתום חופשתם ושל טרוריסטים מוכרים.

