מבט על, גיליון 464, 8 בספטמבר 2013

מזימות במדרון אחורי – 'דארקנט' כמגרש משחקים לטרור

יותם רוזנר, אביעד מנדלבאום, שון לונדון ויורם שווייצר

ביום שישי ה-2 באוגוסט 2013, פרסמה מחלקת המדינה של ארצות הברית אזהרת מטיילים שלאחריה נסגרו, בצעד תקדימי, למעלה מעשרים שגרירויות. כצפוי, בעקבות ההתרעה האמריקאית הורו מדינות מערביות נוספות כמו בריטניה, צרפת וגרמניה, לסגור מתקני שגרירויות שונים. כמה ימים לאחר אזהרת המסע וסגירת השגרירויות, פורסם כי הסיבה להתרעה נבעה מניטור שיחה מרובת משתתפים שכללה נבחרת של מנהיגי ארגוני טרור, ובראשם מנהיג אל-קאעדה המרכזי, איימן אל-זוואהירי, עם מנהיגי ארגונים השותפים לו. בהדרגה נמסר מפי גורמי מודיעין אנונימיים, כי המידע המדובר נתפש ברשותו של בלדר אל-קאעדה, שהחזיק הקלטות מהשיחה המדוברת. חלק מהשיחות נמשכו כמה דקות ונועדו להעברה ברשת, והקלטה נוספת באורך שבע שעות של השיח בכללותו. באמצעות המעקב אחר הבלדר הצליחה ארצות הברית לגלות את השיח שככל הנראה התנהל במרחב קיברנטי המכונה לפרקים "הרשת העמוקה", "הרשת השחורה" או דארקנט.

המערכה הגלובאלית נגד הטרור פגעה קשות בתשתיות הפיסיות של אל-קאעדה, אולם במקום להיחשף העמיק ארגון אל-קאעדה את פעילותו במרחב הקיברנטי. פעילי הארגון למדו לנצל את טכנולוגיית האינטרנט לצרכיהם על ידי שימוש ברשתות מוכרות לצורך הפצת תכנים לגיוס, הדרכה ותיאום פעולות טרור. בסוף שנות התשעים פעלו ברשת בסך הכול עשרות בודדות של אתרים, המקושרים עם קבוצות טרור, ואולם בשנת 2005 תועדו כבר למעלה מ-4000 אתרים כאלה.

לרשת האינטרנט צד גלוי וחבוי. הצד הגלוי מכיל אתרים שניתן למצוא באמצעות חיפוש רגיל; הצד החבוי, המכונה "רשת אפלה" או "דארקנט" (Darknet) מכיל אתרים או רשתות אתרים אשר אינם נגישים באמצעות שיטוט רגיל. כך, אתרים אלו משמשים פלטפורמה לגולשים שהאנונימיות חיונית להם, שכן לצד מעטה ההגנה מפני גולשים לא מורשים, אתרי דארקנט כוללים לרוב גם חומות הצפנה מפני ניטור.

המרחבים האפלים של דארקנט אפשרו לארגון אל-קאעדה להתאים עצמו למגבלות שהטילה עליו המערכה הבינלאומית המתנהלת נגדו ולפעול ביתר שאת כרשת טרור וירטואלית. במחקר שפורסם ב-2011 דווח, כי ישנם למעלה מ-50,000 אתרים ו-300 פורומים לארגוני טרור בדארקנט. יתר על כן, מזה כעשור מדווחים מקורות גלויים, כי בעוד שפעילי הג'יהאד הגלובאלי מנצלים את מרחבי הדארקנט גם למטרות שצוינו לעיל, הרשת בעיקרה מהווה פלטפורמה לתקשורת ישירה בין מנהיגי ופעילי הארגון. לפיכך, החדשות על כך שבדארקנט התנהלה שיחת בכירים של הארגון אינן מפתיעות, כאשר למעשה מנכ"ל "קונצרן הטרור של אל קאעדה", אל זוואהירי, מנצל את הטכנולוגיה העומדת לרשותו, כדי לתקשר באופן סדיר עם "מנהליו" הבכירים.

גולשי דארקנט רבים משתמשים בתוכנת TOR (The Onion Router) הניתנת להורדה בחינם באינטרנט ומספקת לגולשים מעטה אלמוניות. כפי שמצוין בדף הבית של TOR, הרשת מונעת ניטור של תכנים וחוסמת את איתור מיקומו הפיסי של הגולש, ובנוסף מאפשרת גלישה לתכנים המוגנים על ידי צנזורים אינטרנטיים. מעבר לכך, TOR אף מונעת זיהוי של מנהלי אתרים שאינם מעוניינים בחשיפה.

ביוני האחרון דיווח אופיר דויד מחברת "סייברהאט" על פריצה לדפדפני מוזילה-פיירפוקס מגרסאות 17 ו-22 שהביאה לחשיפת משתמשיהן. לאחר גילוי זה, אישרו מנהלי מוזילה, כי אכן אירעה פריצה לדפדפנים אלו. באוגוסט התברר, כי אתרים רבים אחרים, החבויים בדארקנט, נפרצו או נחסמו לחלוטין. כמה ימים לאחר מכן הובא למעצר אריק מואין מרקז, שנחשף כמנהל התשתית הגדולה ביותר בעולם לפורנוגרפיית ילדים. מאחורי פעולה זו ברשת TOR עומד ככול הנראה מבצע עוקץ שנוהל בידי ה-FBI

ושנועד למנוע הפצת פדופיליה ברשת. לטענת דויד, "מי שפרץ לתוך השרת יכול להתאים כל IP של משתמש TOR, ולפיכך לאתר כל משתמש TOR". מובן כי פריצה זו פגעה באופן משמעותי באפקטיביות של TOR כספקית אנונימיות.

סמיכות מעצרו של מרקז למעצרו של הבלדר מאל-קאעדה ומרכזיותה של הדארקנט בשני המקרים מעלה אפשרות סבירה של קשר בין השניים. לפי סברה זו, הרשויות האמריקאיות ניצלו את פרצת TOR לצורך ניטור גורמים מאל-קאעדה ומרשת הפדופילים; חשיפתן על ידי דויד הכריחה אותן לפעול כנגד מטרותיהן בטרם עת, מתוך חשש כי הללו ישנו את אמצעי התקשורת בעקבות חשיפת הפרצה. השערה זו מספקת הסבר אפשרי גם למערכת תקיפות המל"טים האגרסיבית שיזמה ארצות הברית בתימן בסמיכות למעצר הבלדר, אשר הובילה לחיסולם של 34 פעילי אל-קאעדה. יחד עם זאת, חוקרים שטענו לקיומו של קשר בין התרעת מחלקת המדינה לבין הפריצה הנרחבת לרשת TOR נסוגו במקרים רבים מטענתם, וזאת לאור חוסר ההתאמה בין המידע שהוביל לחשיפת רשת הפורנוגרפיה לבין מקור המידע שעשוי היה להוביל לניטור השיחה, למרות שנותרו עדיין כאלה הטוענים לסבירות גבוהה לקיומו של קשר זה.

הזכות לפרטיות לעומת האינטרס הביטחוני. בקרב המצדדים בפרטיות הגולשים, הדארקנט נהנה מצביון רומנטי, כזירה בטוחה לשיח פוליטי מחתרתי. בעולם שמבכה את מותה של הפרטיות על ידי ה-NSA ודומיו, רשת זו אפשרה לאופוזיציונרים, עיתונאים ובדלנים, לפרסם מידע תוך התחמקות מצנזורה ומעקב, ובכך אפשרו העלאת רעיונות ועובדות שאינם עולים בקנה אחד עם האינטרסים של משטרים אפלים. אולם, האירועים האחרונים הביאו לידיעת הציבור, כי דארקנט איננה רק כר לשיח פוליטי אלא תשתית להפצת נשק וטרור, לצד סמים ופדופיליה; יתרה מזאת, לאור שימוש הולך וגובר של פעילי הג'האד ודומיהם בדארקנט, ניתן לתארה כעת כסכנה ברורה ומיידית גם לביטחונם של אזרחים ברחבי העולם. לפיכך, ישנו צורך דוחק ביצירת כלים אשר ימנעו מארגוני טרור (וגם גורמים פליליים) לרתום את הדארקנט לצרכיהם.

בשנים האחרונות פותחו במערב אמצעים מרשימים לניטור תכנים ברשת הגלויה, אך לעומת זאת כמעט ולא קיים ארסנל דומה עבור הדארקנט. בכדי לוודא שיפותחו הכלים הנחוצים לניטור הרשת חיוני להעלות לסדר היום את העדויות המצביעות על הפיכתה של הדארקנט לתשתית מרכזית לטרור הגלובאלי. כפי שניתן להסיק מעבודתו של דויד, החוקרים הישראלים עומדים בחוד החנית של מחקר האינטרנט. לאור זאת, טוב תעשה ישראל אם תרתום חלק משמעותי מכישרונותיה להתמודדות עם האתגר הטמון בדארקנט. מעבר לתרומה העצומה לביטחון הלאומי והגלובאלי, יוזמה זאת עשויה לפתוח אופקים חדשים למיזמים ישראליים.

יותם רוזנר ואביעד מנדלבאום מתמחים בתכנית למחקר טרור ומלחמה בעצימות נמוכה
שון לונדון יועץ תקשורת בניו יורק, לשעבר בפרויקט לחקר הטרור במכון למחקרי בטחון לאומי