המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
INCORPORATING THE JAFFEE CENTER FOR STRATEGIC STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל-אביב

מבט על, גיליון 643, 16 בדצמבר 2014

כשצורכי הביטחון הלאומי ואכיפת החוק פוגשים אינטרסים עסקיים גלובליים

יורם הכהן

שלושה תהליכים מעניינים מתרחשים מזה מספר חודשים, כתוצאה ישירה מחשיפותיו של אדוארד סנואדן את היקף הגישה של שירותי הביטחון האמריקאים למידע פרטי, השמור ומעובד במערכות של חברות אמריקאיות גלובליות. תהליך אחד, הוא טכנולוגי במהותו, השני משפטי והשלישי עסקי. שלושתם מיועדים להצר את יכולותיהם של גופי הממשל האמריקאי השונים לגשת למידע פרטי למטרות של שמירת הביטחון הלאומי ואכיפת חוק.

סנואדן, מנהל מערכת מחשבים (system administrator), שעבד עבור קבלן משנה של ה-National Security Agency (NSA), העביר ביוני 2013 לידי העיתונאי גלן גרינוולד מה-גארדיין הבריטי עשרות אלפי מסמכים, המתעדים את היקפו הנרחב של איסוף המידע הפרטי על ידי שירותי הביטחון האמריקאים מחברות גלובליות אמריקאיות, דוגמת Google ,Facebook ,Microsoft ,Apple ,Yahoo ודומיהן. מהמסמכים עולה, כי באישורו של בית משפט מיוחד לענייני מודיעין, הפועל מכוחו של חוק ה-FISA (Foreign Intelligence Surveillance Act), נבנו ממשקים להעברת מידע אוטומטית מהחברות למחשבי ה-NSA. המידע שהועבר הינו מקיף, וכולל בקשות חיפוש מידע ממנועי חיפוש, דואר אלקטרוני, מסרים מידיים, וידיאו, שיחות VOIP, מסמכים שונים, וכן מידע על אודות מידע (metadata) לגבי כל אחד מפריטי המידע הנ"ל (ממי נשלח, למי, מתי, מאיזו כתובת IP וכד'). בנוסף, סנואדן כלל בגילויו פרטי מידע פיקנטיים אודות המעקב של ה-NSA אחר מנהיגי העולם, לרבות ממדינות שהן ידידות מובהקות של ארצות הברית.

לכאורה, גילויי סנואדן, היו אמורים להטריד בעיקר פעילי זכויות אזרח, החרדים לפגיעה בזכויות חוקתיות של אזרחים אמריקאים וזרים, ובכללן הזכות לפרטיות, להליך הוגן ולחופש ביטוי. בפועל עולה שסוכני השינוי העיקרי הפכו להיות חברות הטכנולוגיה הגלובלית.

עם שחרורה של הגרסה החדשה של מערכת ההפעלה לטלפונים הסלולאריים IOS8 על ידי חברת Apple, זו הודיעה, כי בגרסה זו יישום מנגנון הצפנה למערכת המסרים המידיים והשיחות שלה (iMassage ו-FaceTime), המונע מהחברה לפענח את תוכן התקשורת ואינו מאפשר לה לגלות מידע לרשויות אכיפת חוק. במקביל, חברת Google תכלול בגרסה החדשה של מערכת ההפעלה לטלפונים סלולאריים Andorid פתרון דומה. גם אפליקציית WhatsApp, שנרכשה על ידי Facebook, הודיעה על יישום של מנגנון הצפנה דומה במערכת העברת המסרים שלה. Google ו-Yahoo דיווחו, כי הן פועלות לאפשר ללקוחותיהן ליישם הצפנה במסגרת שירותי הדוא"ל שהן מספקות. עוד ועוד חברות מצהירות על יישום של פתרונות **טכנולוגיים** למניעת **יכולתן** לשתף פעולה עם השלטונות ולמלא אחר צווים המתקבלים מהם, גם אם צווים אלה מאושרים על ידי בית משפט.

במקביל מתעמתות החברות הגלובליות עם צווי הממשל **בשדה המשפטי**. חברת Microsoft החלה לפני מספר חודשים לנהל הליך משפטי בעקבות צו שהוציא שופט בית משפט שלום בניו-יורק לבקשת רשויות אכיפת חוק אמריקאיות לקבל מידע על אודות לקוחות שלה, המאוחסן בשרתי החברה באירלנד. שרתים אלה פועלים תחת משטר משפטי אירופי וצו בית המשפט האמריקאי סתר, בהיבטים מסוימים, זכויות של הלקוחות על פי דין זה. Microsoft החליטה להביא צו זה להכרעה משפטית בערכאה הגבוהה ביותר האפשרית מבחינתה, בטענה, כי אין לממשל האמריקאי סמכות חיפוש ותפיסה של תקשורת הנעשית במדינה זרה. עמדה זו נתמכה במשפט על ידי תאגידים גלובליים נוספים כ-Apple, cisco ועוד, שהתייצבו לצדה של Microsoft.

כשצורכי הביטחון הלאומי ואכיפת החוק פוגשים אינטרסים עסקיים גלובליים

מאת: **יורם הכהן** **מבט על**, גיליון 643, 16 בדצמבר 2014 **המכון למחקרי ביטחון לאומי**

השדה השלישי בו מתרחש, ככל הנראה, שינוי הוא **המרחב העסקי**. לאחר שנים של פיתוח מודלים עסקיים, שעיקרם היה מתן "שירותי חינם", דוגמת Facebook, Google ו-Twitter, המממנים את עצמם באמצעות מתן נגישות למידע האישי של המשתמשים ושירותי פרסום מקוונים על בסיסו, ייתכן שמתחיל להיווצר שוק של אספקת שירותי הגנת פרטיות לאזרחים. תהליך זה נמצא בראשיתו, אך קרנות הון סיכון מדווחות על אודות גידול בחברות הזנק הפועלות בתחום זה.

המוטיבציה של החברות הגלובליות לערוך שינויים טכנולוגיים במוצריהן וליישם הצפנת מידע של לקוחותיהם, כמו גם האתגר המשפטי הכרוך בבקשות לגילוי מידע בבית המשפט, נובעים מהבנתן של חברות אלה, כי עסקיהן בנויים על אמון המשתמשים. החשש שהן נתפשות כ"משתפות פעולה" עם גופי מודיעין ואכיפת חוק אמריקאיים רבי עוצמה מחייבת אותן לשדר ללקוחותיהן, כי הן שומרות על האינטרסים שלהם. עסקים אשר יספקו שירותי הגנת פרטיות רואים מולם שוק למוצרים, שיגנו מפני המדינות וכן מפני התאגידים הגלובליים, האוספים את המידע הרב על אודות האזרחים.

ההיסטוריה של ההצפנה המודרנית מלמדת, כי המצאות אקדמיות ויישום עסקי שלהן יכולים לגרום 'כאבי ראש' לגופי מדינה, כפי שקרה עקב פיתוח תפיסת ההצפנה במפתח ציבורי על ידי diffie ו-hellman בשנות ה-70 (וגם פיתוח אלגוריתם ייצור מפתחות ההצפנה RSA בעקבותיו). דוגמא נוספת, היא ההתנגדות שחווה ממשל קלינטון בשנות ה-90 בשל יוזמת ה- clipper chip להכניס מנגנון מובנה של דלת אחורית בחומרה המאפשרת תקשורת.

על רקע זה, ניתן לזהות מספר תהליכים, אשר התקדמותם עשויה לפגוע קשות בלחימה בטרור ואכיפת חוק במרחב הסייבר:

התהליך הראשון, הוא המשך הפיתוח והיישום של אמצעי הצפנה והגנת מידע, הנתונים לשליטתם הבלעדית של משתמשי הקצה, פועלים באופן מבוזר ואינם נדרשים לפונקציות ניהול מרכזיות לצורך פעולתן. ככל שאמצעים אלה יסתירו, בנוסף לתוכן התקשורת, גם נתוני metadata, הרי שיהיה קשה למפות ולזהות את הפעילות המתרחשת ובוודאי לבדל אותה מפעילות תמימה, שהיא עיקר השימוש ברשת האינטרנט. אמנם, לאחרונה נחלו רשויות אכיפת החוק האמריקאיות הצלחה בהתמודדות עם פעילות פלילית, שנעשתה תוך שימוש בשירותי הרשת האנונימיים של TOR, אך נדרשים לכך משאבים רבים ופרצות שימצאו עשויות להיסגר.

התהליך השני, אשר ניצניו החלו לפרוח מיד לאחר גילויי סנואדן, הוא פיתוחם של שירותי אינטרנט מדינתיים, כלומר, כאלה שסמכות השיפוט והאכיפה לגביהם, היא של מדינה ריבונית, שכן הם פועלים במדינה הריבונית בלבד ורוב המשתמשים בהם, הם אזרחיה. עדויות ליוזמות כאלה נרשמו, למשל, באירופה, רוסיה וסין. מעבר להשפעה העסקית של מגמה זו על חברות גלובליות, המשמעות האכיפתית היא, כי כדי לקבל מידע לצורך לחימה בטרור או אכיפת חוק משירותים מקומיים כאלה, ידרשו גופי אכיפת החוק למנגנון של סיוע אכיפה ומודיעין בין מדינות - על המשמעויות הפוליטיות והבינלאומיות של הסדרים מסוג זה. בחדירה סמויה לשירותים אלה טמונה, כמובן, סכנה למתיחות בין-מדינתית בשל הפרת הריבונות הכרוכה בכך.

התהליך השלישי הוא לחץ ציבורי במדינות שונות להסדיר באופן ברור יותר את הסמכויות ויכולת המעקב של גופי מודיעין ואכיפת חוק, הן ברמה מקומית והן ברמה הבינלאומית. עדות לכך הייתה יוזמה של סנאטורים דמוקרטים, בתמיכת ה-NSA, להגדיר ולגדר את סמכויות המעקב של ה-NSA. יוזמה זו נדחתה בסופו של דבר בשל התנגדותו של הרוב הרפובליקאי בסנאט. בנוסף, הנציבות האירופית מקדמת רגולציה בנושא פרטיות והגנת מידע אישי (data protection), והפרלמנט האירופי קיבל החלטה לפעול לפירוקם של "מונופולים דיגיטליים". אף שלכאורה מדובר בעניינים אזרחיים, ליוזמה זו תהא השפעה נרחבת, שכן היא שמה במרכז את היקף המידע הנאסף בשירותי המידע הגלובליים.

תהליכים אלה, ככל שיבשילו ויתרחבו, עשויים לאתגר את המאמצים לאכיפת חוק ולחימה בטרור ברחבי העולם, לרבות בישראל, ולהקשות עליהם. רכיב משמעותי של פעולות ההכנה לפשיעה ולטרור מתקיים היום במרחב הקיברנטי, ומתקיימת בו כמובן עיקרה של פעילות ה-cyber-terror ו-cyber-crime. היכולת לגשת למידע זה בשלבי ההכנות לצורכי מניעה, היא קריטית. על גופי האכיפה והמודיעין להבין את התהליכים והאינטרסים הנוגדים – אזרחיים, טכנולוגיים ועסקיים – ולוודא שמחד גיסא, הם אינם פוגעים באינטרסים אלה מעל הנדרש, ומאידך גיסא הם שומרים על יכולת לחימה בפשיעה ובטרור של המאה ה-21.