הקשר בין סמים, ביטקוין ופשע מאורגן

מאת עו"ד לילך צאירי-כהנוב ושרון ברק

הקדמה

במאמרינו זה נבקש לבחון את תופעת הפשע המאורגן בראי עידן האינטרנט והכלים הטכנולוגים המתקדמים שהוא מציע. בפרט נתמקד בביטקוין, המטבע הוירטואלי המסקרן והמצליח, והקשר שלו לרשת האפלה ולסחר האינטרנטי בסמים. כמו כן נדון במתודולוגיות ובפתרונות האפשריים, למה שמסתמן כאחד האיומים הגדולים הניצבים כיום מול רשויות האכיפה. האם הקידמה אכן עומדת עלינו לכלותינו?

סקירה של הפשע המאורגן באינטרנט

פשע מאורגן מוגדר כארגון מסודר והיררכי, מאוגד או בלתי מאוגן, הפועל בתבנית מאורגנת, שיטתית ומתמשכת, אשר נועד לעסוק בפעילות עבריינית, ובדרך כלל למטרות רווח כספי. ישנם ארגוני פשע הפועלים למען מטרות פוליטיות, אך לא נתמקד בהם במסגרת מאמר זה. השווקים בהם פועל הפשע המאורגן מאופיין על ידי כלכלה ענייה ומחסור באלטרנטיבה עבור הצרכנים (לרוב מטעמים חוקיים), כאשר המדינה מונעת מוצרים/שירותים מהצרכנים. הפעולות הבלתי חוקיות בהם עוסקים ארגוני פשע נעות החל מסחר בסמים, הלבנת כספים, דרך זנות, סחיטה, הימורים בלתי חוקיים, סחר בנשים, סחר במידע פנים, וכלה בחדירה לעסקים כשרים בצורה חוקית או בהשתלטות. "ארגוני פשע מאורגן מבינים שניתן לעשות כסף, ולא אכפת להם מהו המוצר" (Ernie Allen נשיאת המרכז לילדים מנוצלים ונעדרים) - **הרווח הכספי, ולא האלימות, הוא המנוע מאחורי ארגוני הפשע,** הקיימים עוד משחר הדורות. אימפריות קמו ונפלו, ואילו הפשע המאורגן הוכיח עמידות בפני כוחות הזמן וניסיונות הממשלות השונות להשמידו.

ארגוני הפשע מהווים תעשייה המגלגלת מיליארדי דולר, הם מצויים בתחרות גבוהה, ונתונים לסיכונים גדולים ולחץ רגולטורי מסיבי. כפועל יוצא מכך, נדרש כיום כל ארגון פשע לרמה גבוהה של תחכום בניהול העסקים, ידע, IT, לוגיסטיקה, מימון, הסתגלות והשכלה[2] (מ-IP Pau Fuk, 1999 - חברים בארגונים בהונג-קונג קיבלו מימון להשכלה מארגוני פשע, ובתום הלימודים הצטרפו לארגונים אלה).

<u>המגמות הגלובאליות השונות משפיעות גם על ארגוני הפשע</u>[4]:

- **שינויים כלכליים -** הכלכלה הופכת פחות ופחות מוחשית - הכסף הופך לא מוחשי, נכסים לא מוחשיים, מקומות עבודה ברשת.
- **גלובליזציה -** עסקים מתבצעים ברחבי העולם באופן חוצה מדינות וגבולות, ניתן לראות יותר שיתופי פעולה, עם שחקנים ממדינות שונות.

- **תקשורת -** מידע רב עובר בנתיבים וברשתות שלא ניתן לשלוט ולא ניתן לבטוח בהן, וכן ניתן להגיע באופן ישיר לקהל רחב בהרבה מהיום.

ראשי הפשע המאורגן היו מהראשונים להבין כיצד ניתן לנצל את הקדמה הטכנולוגית בתחום התקשורת בשנות ה-20 וה-30 של המאה ה-20 , במטרה להתרחב ולהעצים את השליטה שלהם על פעולותיהם ביומיום. **גם היום, כמו בשנות ה-30 העליזות, בהם פרח הפשע המאורגן בארה"ב, לומדים ארגוני הפשע כיצד לשלוט בטכנולוגיות החדשות, ומשלבים סייבר בפעילות המסחרית הענפה שלהם.** למעשה, הפשע המאורגן הוא שחקן מפתח במרחב הקיברנטי, כזה שבשורה התחתונה, ממש מעצב את האינטרנט, ואת הרגולציה המנסה לעצור אותו.

כמה רחב האיום? - פשע מאורגן מתבסס על נאמנות חזקה למשפחה ולחברים, ולעיתים גם על דת או אידיאולוגיה. דווקא מיקום גיאוגרפי ושליטה טריטוריאלית, הבסיס למדינות ולאומות, משחק תפקיד קטן בפשע המאורגן, ששחקניו הסתגלו באורח מדהים למרחב הקיברנטי[3]. הפשע המאורגן נמצא היום בכל מדינה, ויודע לנצל את הטכנולוגיה, לבסס קשרים, בריתות וקשרי עסקים על מנת להרחיב את מפעלם ברחבי תבל. ארגונים אלה מכונים **TCO - Transnational Criminal Organizations**[1]. החיתוך בין קבוצות אלה למפלגות פוליטיות, חברות פרטיות, ויחידים הינו מורכב והגבולות מטושטשים.

כדי להתנהל כארגון פשע באינטרנט, נדרש שילוב בין יכולות ניהול, יכולות ניהול פיננסי ויכולות לוגיסטיות, אך בניגוד לעולם ה"רגיל", נדרשות בנוסף גם יכולות טכניות, ובניגוד למדינות ולעסקים מסויימים, מתחוור כיום כי ארגוני הפשע סתגלניים בהרבה, והתקדמו עם הטכנולוגיה, תוך שהם מוצאים דרכים חדשות מגוונות לשפר את יכולות ניהול העסקים הבלתי חוקיים שלהם: הארגונים שומרים על ביזור, על מנת שלא להוות מטרה אחת עבור הרשויות והמתחרים שלהם; הם משגשגים בסביבה בה הרגולציה עמומה; ודווקא היחסים עם ארגוני פשיעה ממדינות אחרות הולכים ומתהדקים. גם הליכי הגיוס לארגון השתכללו - ארגוני הפשע אינם מסתפקים עוד במגויסים "גברתניים" שלא סיימו תיכון - הגיוסים מתבצעים בקרב בעלי תארים, חנונים והאקרים (Black Hats, מעין שכירי חרב של המרחב הקיברנטי), מגויסים טריים נשלחים ללמוד את הטכנולוגיות, ובל נשכח את בתי הסוהר עצמם, שכחלק מתוכניות השיקום מציעים לאסירים לימודי מחשב, כלומר אותם חברי ארגון פשע (מובן שהדבר נאמר בהכללה) שבים לרחובות משכילים יותר ומתוחכמים יותר. כך אימצו ארגוני הפשיעה את האינטרנט לניהול תעשיית הפורנוגרפיה באינטרנט, עסקי ההימורים, לביצוע הונאות פיננסיות, וכן את שוק הסמים - המאפיה פשוט השתלטה על הסחר בסמים בארה"ב, שוק הנאמד בשווי של כ-100 מיליארד דולר.

אין ספק שהאינטרנט מהווה כלי שרת ביד הארגונים, אשר הבינו את הפוטנציאל העצום הטמון בו כבר לפני כשני עשורים, חינכו את עצמם ואימצו את העולם האינטרנטי בזרועות פתוחות. האינטרנט מספק יותר חשאיות, פרטיות, עולם בו ניתן להכחיש ולהתכחש, והתחקות אחר אדם לעיתים בלתי אפשרית בהשוואה לסביבה הרגילה. בסביבה האינטרנטית ניתן לאתר מידע, לאמץ זהויות שונות, לקשור יחסים

ולנהל עסקים המתנהלים כולם ברשת, המטבע וירטואלי, ניתן להעביר מסרים מוצפנים, ניתן אף להצפין את עצם קיום התקשורת ועוד. בעקבות המעבר לעולם האינטרנטי, מצאו עצמם הארגונים בסביבה שופעת יכולות, ללא חוקים ברורים (החוק לעולם רודף מציאות), ואכיפה המנסה להחיל חוקים מהעולם ה"רגיל" על העולם האינטרנטי. גם ל-**TOCs** ברור, שעם התקדמות הטכנולוגיה יהיה להם קשה יותר לפעול, אך כיום הכלים העומדים לרשותם מהווים לא פחות מ"גן עדן", והם הצליחו למנף את טכנולוגיות המידע והתקשורת, כך שכיום קשה יותר להתחקות אחריהם, לאתר אותם ולהענישם, כפי שיפורט בהמשך. למעשה, החל מאמצע 2007 ונכון להיום, האיום הגדול ביותר לארגוני הפשע אינן רשויות האכיפה, כי אם הארגונים עצמם. התחרות על נתח שוק הינה גבוהה והגדרת הטריטוריה מאוד מטושטשת. על פי מחקרים, התחרות בין קבוצות הפשיעה מורידות את המחירים של היצע הסחורה הגנובה, כך למשל, עלות מספרי אשראי גנובים ירדה מ-7$ ב-2009 לכ-1$ (ירידה של כ-80%). לעיתים הפושעים אף יוצאים בהתקפות האחד כנגד השני, ואף היו מקרים בהם התפרסמו תמונות המתחרים באינטרנט. נתון מעניין נוסף העולה מהמחקרים, מצביע על כך שמספר המחשבים הנמצאים בשימוש מרחוק לביצוע פשעים (Bots) עולה, ובד בבד מספר השרתים יורד - נתון המצביע על מרכוז השליטה בביצוע פשע כגון - Spam, Phishing והתקפות DDoS, אשר נועדו לסחוט עסקים התלויים באינטרנט [1].

ביטקוינז (Bitcoins)

הכסף הומצא פעמים רבות באופן עצמאי, במקומות שונים ובזמנים שונים. המצאת הכסף לא הייתה מהפכה טכנולוגית או חומרית, אלא מהפכה מחשבתית. כסף הוא כל דבר שבני אדם מסכימים להשתמש בו כדי לייצג באופן שיטתי את ערכם של דברים אחרים לצורך ביצוע עסקאות ותשלומים. על אף שכיום כסף מזוהה עם מטבע, הרי הוא קיים הרבה לפני המצאת המטבע. בעבר, תרבויות שונות השתמשו בקונכיות, בקר, עורות, תבואה, מחרוזות ועוד ככסף. גם בימינו, בבתי כלא ובמחנות שבויים, סיגריות משמשות פעמים רבות כמטבע עובר לסוחר. בעצם, כיום מרבית הכסף בעולם קיים כמידע אלקטרוני במחשבים, ומרבית העסקאות מתבצעות באמצעות העברת מידע אלקטרוני מקובץ אחד לשני, ולא על ידי העברת מטבעות ושטרות. **כסף מתאפשר רק בזכות אמון הדדי** - מי שנותן משהו בעל ערך תמורת כסף, חייב להאמין שכאשר הוא ירצה בעתיד לקנות משהו אחר בעל ערך תמורת הכסף הזה, המוכר העתידי יסכים לכך. עצם העובדה שמישהו אחר מאמין במטילי זהב, בדולר או בכסף וירטואלי דוגמת ביטקוין, גורמת לחיזוק האמונה של האחרים במטילי זהב, בדולר או בביטקוין [6] [7].

כאשר נוצר הכסף בתחילה, הוא התבסס בעיקר על מתכת הזהב, שהיא נדירה, נדרש להשקיע מאמץ כדי להשיגה, וכמותה בעולם מוגבלת. בסופו של דבר השתחררה המערכת המוניטרית מהתלות בזהב, וכך למעשה נוצר מצב בו ניתן לייצר כמות אינסופית של ניירות ומידע אלקטרוני, ללא צורך ב"כיסוי" של זהב. למעשה ניתן למוטט כלכלות על ידי יצירת כספים חדשים ("Copy Paste"). בשנת 2006 סך כל המטבעות

והשטרות נאמר בפחות מעשירית מסך כל הכסף בעולם. וזוהי אחת הביקורות הקשות כנגד הכלכלה המודרנית, ואחד הפתרונות שמציע הביטקוין[8].

מעניין שעם זאת, במשבר הכלכלי האחרון ב-2008, כאשר התערער אמונם של בני האדם בדולר, זינק מחיר הזהב כמעט פי שניים, באופן אשר שיקף את אמונם המתחזק של הפרטים בזהב.

ביטקוין (Bitcoin) הוא מטבע דיגיטלי קריפטוגרפי פתוח ומבוזר[9]:

- מטבע - הוא מייצג ערך וניתן להעברה
- דיגיטלי - הוא נשמר בביטים, מנוהל ע"י מחשבים ונסחר על גבי הרשת
- קריפטוגרפי - מבוסס אלגוריתמים של הצפנה
- פתוח - קוד המקור פתוח והכל מתנהל בשקיפות מלאה
- מבוזר - כיוון שאין בו מרכז אחד, הוא לא כפוף לשום גוף, ממשלה או מוסד

הביטקוין פותח בשנת 2009 על ידי מי שכינה עצמו סאטושי נקאמוטו (איש מעולם לא פגש אותו), וכיום היא מתוחזקת על ידי קהילת מפתחים. התוכנה מאפשרת לכל אדם להוריד תוכנה פשוטה ו"לכרות" באמצעותה מטבעות, היא מאפשרת העברת תשלומי כסף אלקטרוני מצד אחד לשני בתוך רשת המשתמשים, מבלי להיעזר בתיווכו של צד שלישי (Peer-to-Peer). המערכת אינה כפופה לפיקוח של סמכות כלשהי, היא כוללת מערכת אמינה של תיעוד עסקאות, תוך שמירה על אנונימיות מלאה של הצדדים לעסקה.

ב-2011 התבצעו תקיפות של האקרים על מספר בורסות המרת הכספים של המטבע, וכן קרן ה-EFF (Electronic Frontier Foundation) הכריזה, כי בשל בעיות חוקיות לא תקבל עוד תרומות בביטקוינז[10]. בעקבות המאורעות שער המטבע צנח מכ-31$ בשיאו, לכ-17$, ומשם לכדי לכמה סנטים בודדים. המטבע התאושש ונסחר כיום בכ-20$. ב-09.12.12 קיבל הביטקוין מעמד של ספק אמצעי תשלום ובעל קידומת בנקאית בינלאומית[11]. המהלך מציב אותו במעמד שווה ל-PayPal. בעלי חשבון ביטקוין יוגדרו כבעלי חשבון בנק לכל דבר ועניין. זהו צעד נוסף בדרכו של הביטקוין להפוך לאמצעי תשלום מקובל ברחבי העולם. כעת יוכל ביטקוין להנפיק כרטיסי חיוב, לבצע העברות בנקאיות לבנקים אחרים ולהפקיד כסף בחשבונות של לקוחות. מערכת הבנקאות העולמית תוכל להתייחס לבעלי חשבון ביטקוין כמו אל כל חשבון בנקאי אחר.

איך זה עובד?

ארכיטקטורת PKI - מספר חשבון ביטקוין הוא צירוף של מספרים ואותיות, אליו מוצמדת סיסמה - **מספר החשבון** הוא **מפתח ציבורי** (כל אחד יכול להעביר אלי כסף), ואילו **הסיסמה** הינה **המפתח הפרטי** (רק מי שהמפתח ברשותו יכול להעביר כסף לחשבונות אחרים). יצירת חשבון לא כרוכה בהרשמה או הזדהות,

ומספר החשבונות אינו מוגבל. כל היסטוריית ההעברות בין החשבונות, מהיום בו נולד ביטקוין, נשמרת על אלפי המחשבים השותפים ברשת והיא מידע ציבורי פתוח. אבל הקשר בין החשבונות לבין זהות בעליהם תלוי רק בבעלי החשבונות, בדומה לכתובת דוא"ל. עובדה זו מעניקה לביטקוין מאפיין חשוב - **לראשונה בהיסטוריה ניתן לשלם ולקבל תשלום ברשת באנונימיות מוחלטת.** ניתן לקרוא לו המזומן של הרשת - כמו מזומן, אפשר להחזיק אותו בעצמנו, לשלם איתו ללא מתווכים וללא עמלות ואם רוצים, באנונימיות. כמזומן של הרשת הוא כמובן נהנה גם מיתרונות העולם הדיגיטלי - קל להעברה, לא תופס הרבה מקום, ניתן לחלק אותו לחלקים זעירים, אפשר לגבות אותו, להצפין אותו וכו'. רבים משווים את הביטקוין למקור הכסף המודרני, לזהב, שכן מספר המטבעות מוגבל, יש להשקיע משאבים כדי לכרות אותו, והוא אינו שואב את ערכו מכלכלת מדינה או מוסד כאלו או אחרים.

יתרונות מרכזיים:

אנונימיות ושמירה על הפרטיות - בכל הנוגע לביצוע תשלומים ברשת כיום, האופציה לפרטיות למעשה לא קיימת - לא ניתן לבצע תשלום מבלי להזדהות בשלב כלשהו בתהליך. הטענה המרכזית היא, שאתרים שאין להם שום צורך, דורשים קבלת פרטים מזהים כגון תעודת זהות ושם מלא כדי לבצע עסקה, כשעל פניו אין כל צורך בכך. בנוסף, לעיתים דווקא זה שמקבל את התשלום מבקש להישאר אנונימי - דוגמא מפורסמת הוא שוק הסמים ואתר דרך המשי (Silk Road) (כפי שיפורט בהמשך), שהלגיטימיות שלו מוטלת בספק, אך ישנם גם אתרים דוגמת ויקיליקס, המקבלים תרומות בביטקוינז, ונחשבים ללגיטימיים.
אינו סובל מאינפלציה - מספר מטבעות הביטקוינז בעולם מוגבל ל-21 מיליון, וכן בניגוד למטבעות וירטואלים אחרים או מטבעות בעולם "האמיתי", הביטקוין אינו סובל מאינפלציה. כאשר יכרו כל 21 מיליון המטבעות, לא ניתן יהיה "להדפיס" כסף נוסף, ולגרום להורדתו של ערך המטבע ממניעים שאינם כלכליים (ניתן יהיה להשתמש בחלקים קטנים יותר ויותר של המטבע).

ניתן לבצע תשלומים זעירים (Micro Payments) - בכל אמצעי תשלום אחר, למעט מזומן, ניתקל בחומת עמלות ובחסמי כניסה. ביטקוין פותר את העניין בשני מובנים - היכולת לשלוח סכומים כסף קטנים ביותר (ברמת הסנט הבודד) והיכולת לשלוח אותו לכל אחד, ללא צורך במערכת סליקה נפרדת, הגובה עמלות.

שקיפות - ביטקוין, המזוהה יותר מכל עם אנונימיות, הוא למעשה המטבע השקוף בעולם ולא רק מהבחינה של כמה כסף חדש יודפס ומי יקבל אותו - כל אחד יכול לבדוק כמה מטבעות נמצאים בכל רגע בכל חשבון ולראות איך הם עוברים בין החשבונות, אך כאמור אין דרך לקשר בין העסקאות לבין המשתמשים. הדבר תורם לביסוס האמון של המשתמשים במערכת.

ניהול כספים - כל מתכנת או יזם, יכול לפתח אפליקציה שמנהלת ועבירה כספים, זכות שהייתה שמורה עד כה רק לבנקים ולחברות ענק.

מטבע בטוח (קשה מאוד לזיוף) - קשה מאוד להאמין שזיוף הרשומות הציבוריות של ביטקוינז יצליח, שכן המזייף יזדקק למשאבי מחשב בכמות אדירה, העולה על משאבי כל המחשבים העומדים לרשות כלל רשת הביטקוינז.

חסרונות: זקוק לחשמל; חשש מתמיד מפריצת האקרים; וירוסים; ניצול לרעה על ידי כריה בקצב מוגבר;

ביקורת: כנגד המערכת נטען שהיא משמשת להלבנת הון, כי מדובר בסוג של הונאת פירמידה מתוחכמת או הונאת פונזי, לחילופין, כי מדובר בבועה מוניטרית.

יצירת רווח נקי (וכיצד הביטקוין מאפשר זאת) [9]

בתקופה שקדמה לאינטרנט, הדעה המסורתית של הקרימינולוגים הייתה שהתממשותה של חברה ללא כסף מנייר תסמן את דעיכתו של הפשע באמריקה, ואולי בעולם כולו. ההיגיון היה שללא כסף והעברות כספים מבוססות כסף מנייר, לא יהיה מה לגנוב, ובכך האינטרנט יוריד את הפשע המאורגן על הברכיים. עם זאת, בזכות סתגלנותה המופלאה, המאפיה מהר מאוד מצאה דרך לנצל את ההזדמנויות שזימנה לה הרשת. המרחב הקיברנטי, לא רק שלא הרע את מצבם של הארגונים, אלא הוא הפך כלי שרת בידם, והרע את מצב רשויות אכיפת החוק שניסו להילחם בארגונים.

באמצעות הטכניקות שיפורטו בהמשך, מצליחים ארגוני הפשע להגיע לקהל נרחב, תוך שמירה על האנונימיות שלהם ושל הצרכנים, הארגונים מצליחים לתקשר באופן חשאי בינם לבין עצמם, וכך גם החברים בארגון. העסקאות מושלמות באמצעות תשלום בביטקוינז, אשר עובר תהליך של הלבנת הון, וכך יוצרים הארגונים רווחים עצומים, חוקיים לכאורה, מבלי שתהיה לרשויות היכולת (על פניו) לעצור אותם או לתופסם.

מהי הלבנת הון? - הלבנת הון היא ההליך במסגרתנו כספים שהושגו בדרך לא חוקית מקבלים כסות של כספים חוקיים או לגיטימיים, לחילופין, מטשטשים העקבות הלא חוקיים של אותם כספים.

בעבר נטען לא אחת, כי טכנולוגיות חדשות, לרבות אלו של תעשיית הבנקאות עצמה, יובילו למהפכה של ממש בתחום הלבנת הכספים, ויקלו מאוד על תיעול הכספים הלא חוקיים לתוך המסחר הבינלאומי, להעבירו דרך עסקים לגיטימיים באופן המסתיר את מקורותיו, ומשם למשוך אותו. לביטקוין כמטבע וירטואלי קיימים מספר מאפיינים, ההופכים אותו מתוחכם ואטרקטיבי במיוחד, אם לא אידיאלי, בעיני מלביני כספים.

ראשית, בדומה למטבעות דיגיטאליים (כגון סוחרי מתכות יקרות) וכסף אלקטרוני (כרטיסים נטענים מראש), הביטקוין מאפשר העברת כספים חוצת גבולות גיאוגרפיים מבלי להזדקק למוסדות הפיננסיים המסורתיים, ולמעשה ללא כל מתווך כלל. בניסיונן למגר הלבנת כספים, הרשויות שמו דגש על חובת הדיווח של אותם מתווכים, אשר אינם רלוונטיים במקרה של ביטקוין. גם על מערכת סחר אלקטרוני כגון

PayPal חלה חובת דיווח במקרה של סחר מעל סכום מסויים. הוצאת המתווכים מחוץ לתמונה מחזירה את הרשויות 25 שנים אחורנית.

שנית, מאחר ואין כל צורך בקשר פנים מול פנים, או מגבלה של גבולות הגיאוגרפיים, ניתן לעקוף ביתר קלות את התשתית הפיננסית הקיימת, שכן המערכת ממש "מזמינה" גניבת זהויות. שלישית, העברת התשלום נעשית באופן אנונימי לחלוטין, כלומר מתאפשרת פתיחת חשבונות תחת שמות בדויים, זהויות מזוייפות, ופתיחת חשבונות מרובים. בנוסף, במקרה של ביטקוין, כל העברה אמנם מתועדת במערכת, אך הנתונים שנשמרים הם רק הסכום המועבר והכתובות הציבוריות (יש לזכור שהמערכת של ביטקוין מאפשרת גם לפתוח כתובת עבור עסקה מסויימת בלבד (למעשה, זוהי המלצת המפתחים). לבסוף, המהירות והקלות של ההעברות מהווה יתרון אדיר עבור המעורבים. בפרט לאורך העובדה שאין עלויות עסקה, כלומר ניתן כל סכום לפצל למספר סכומים קטנים, ולהעביר בקלות למספר מדינות אחרות ולמספר חשבונות נפרדים. על פניו, מדובר בכלי פיננסי אידיאלי להלבנת הון, אך הדבר אינו מובטח, כפי שיפורט בהמשך. אפשרות נוספת שעולה, היא כי ארגוני הפשע רואים במטבעות הוירטואלים מכשירים פיננסיים בעל פוטנציאל להשתלטות, מתוך מטרה בעתיד לשלוט דרכם על מהלכים מאקרו-כלכליים ואף להטות כוחות פוליטיים. בחרנו שלא להרחיב על האפשרות במסגרת עבודה זו.

תקשורת: מול הצרכנים, בתוך ובין ארגוני הפשע השונים

פרוטוקול TOR - (The Onion Route) - דפוס הפעולה של הפרוטוקול הוא כזה שהתקשורת בין שתי "נקודות" - מחשב המשתמש והאתר אליו הוא גולש, או שולח ההודעה ומקבל ההודעה - אינה מועברת בצורה ישירה אלא דרך שרתי ביניים. כל שרת מקבל הודעה מוצפנת מהשרת לפניו, מפענח את המידע המוסר לו מיהו השרת הבא בתור, בדרך זו כל נתב מוריד שכבת הצפנה אחת בעזרת המפתח הסימטרי שברשותו, מצפין את ההודעה באמצעות המפתח הציבורי של השרת הבא שהוגדר מראש, מעביר הלאה וחוזר חלילה. הנתב האחרון שמפשיט את ההודעה לחלוטין ומעביר את התוכן הלא מוצפן לידי הנמען. אמנם הטכנולוגיה פותחה למטרה חיובית של שמירה על חייהם של סוכנים ומשתפי פעולה, הרי רשת TOR הפכה ל**"הרשת האפלה"** הדומיננטית בדיוק בשל הקלות הבלתי נסבלת שניתן לעשות בה שימוש לפעולות לא חוקיות, תוך שמירה על אנונימיות כמעט מוחלטת. הדפדפן מאוד ידידותי למשתמש, ואין כמעט צורך בידע טכנולוגי כדי להפעילו.

הודעות מוצפנות בהצפנה א-סימטרית (במפתח ציבורי + מפתח פרטי) - **PKI** - מעבר לשמירה על זהות המעורבים, קיימת האפשרות **להצפין גם את תוכן ההודעה** ולהבטיח את **חשאיות המידע**. כלומר, גם אם מישהו יצליח ליירט את המידע בדרך, יהיה כמעט בלתי אפשרי לגלות את תוכנה.

שימוש בסטגנוגרפיה (הטמעה) - בניגוד לקריפטוגרפיה (הצפנה), בה עצם העברת המידע גלויה, אך תוכן המידע חסוי, הרי בדרך של הטמעה רק השולח והמקבל יודעים היכן מוטמע המידע, וכיצד ניתן "למשוך" אותו מתוך הקובץ המדובר, והתעבורה הופכת בלתי ניתנת לניטור. שילוב של טכנולוגיית הטמעה בדרך הפעולה, מוסיפה נדבך נוסף לדרגת הקושי של מי שמנסה מבחוץ להתחקות אחר תעבורת המידע.

כלים נוספים המאפשרים שמירה על האנונימיות - מעבר ל-Spoofing, ישנם שירותים ברשת כגון Anonimizer, המציעים באופן גלוי שירותים המאפשרים לשמור על אנונימיות. כל שנדרש הוא לגלוש לאתר ומשם לגלוש באופן חופשי בכל אתר אחר, מבלי שניתן יהיה להתחקות אחר המשתמש (על אף שאין לדעת האם אכן המפעילים של האתר לא שומרים רשומות של פרטי הגולשים).
שימוש ב-Disposable Emails - שרתי קש היושבים פיסית במדינות מרוחקות, בעלות רמת אכיפה נמוכה. כתובות הדוא"ל מוחקות את התוכן שלהן אחת ל-15 דקות. באופן זה מתאפשרת תעבורת מידע, הניתן לקריאה במשך פרק זמן מוגדר, ולא משאירה אחריה עקבות. דוגמאות: GuerillaMail.com, Mailinator וכו' - מציעים שירותי דוא"ל זמני וחד פעמי. דרך נוספת לשמור על זהות המעורבים.

העסקת Black Hats - בחלק מן המקרים לא נדרשים הארגונים כלל לידע טכנולוגי כלשהו. כל שעליהם לעשות הוא לפנות לשכירי החרב האינטרנטיים, אשר הופכים מקצועיים וזולים יותר, במקום האקרים "יודעי כל".

שימוש בפונקציית גיבוב (Hush) - מתוך מטרה לשמור על שלמות המידע (Integrity), ולוודא שגורם זר בכלל, או משטרתי בפרט, לא ערך בו שינוי. הפונקציה ממירה קלט חופשי באורך משתנה לשרשרת מידע באורך קבוע, בדרך כלל קצר בהרבה. פונקציית גיבוב טובה היא כזאת שבהסתברות גבוהה, תפיק פלט שונה עבור קלט שונה. הפונקציה מאפשרת יצירת חתימה לקובץ ומעקב אחר שינויים שחלו בו.

העברת כספים באמצעות Bitcoins - עצם הפעולה מתועדת במערכת, אך מאחוריה עומדים מספרים, ואין דרך לקשור אותם לבני אדם או ארגונים בעולם האמיתי. בנוגע לרוכשי הסמים, בעבר עמדו לרשותם טכנולוגיות כמו כרטיסי אשראי נטענים, אך גם בהליך זה היה עליהם להזדהות בעת רכישת הכרטיס. ביטקוין מאפשר דרך מתוחכמת יותר ואנונימית הרבה יותר. בנוסף, להבדיל מפדופיליה ברשת, שם הבעייתיות אף גדולה יותר שכן המוצר הוא לרוב קובץ דיגיטאלי והעברתו די פשוטה, במקרה של סמים יש להעביר לנמען את עדיין צריך להגיע המוצר הפיסי. הסוחרים מתגברים על קושי זה באמצעות מערכת הדואר וחברות שליחויות בינלאומיות, אשר אינן בודקות את תוכן החבילות המועברות, וכן חברות המתמחות בהשכרת תאי דואר לצרכים מסוג זה.

אתר www.קנאביס.com מפרסם שבימים אלו עובד צוות ישראלי על פיתוח מערך ההפצה ברחבי הארץ, באופן שיאפשר לצרכני הקנאביס בישראל ליהנות מרכישה נוחה בטוחה ואנונימית של קנאביס וחשיש עד

הבית דרך המחשב. האתר samim.onion טרם התחיל לפעול, אך הוא מתיימר לעשות בדיוק את זה. בינתיים, הסוחרים והצרכנים יכולים להתקשר באמצעות פרוטוקול TOR ב"דרך המשי", האתר שנחשב למקבילה השחורה של eBay, ומאפשר לסחור בכל מוצר אפשרי, החל מסמים, דרך פדופיליה וכלה בהזמנת רצח. כל שהמשתמש צריך הם שם משתמש וסיסמה. בנוסף, עומדת לרשותם האפשרות לפתוח אתרים ייעודיים לסחר בסמים, וכן להתנהל בפורומים למוזמנים בלבד (וכך מנסים להבטיח שמי שקיבל אישור כניסה הוא משתמש שניתן לבטוח בו).

גם שילוב של רק חלק מן האפשרויות מאפשר אנונימיות כמעט מוחלטת של המעורבים בהתקשרות ובעסקה.

יש לזכור שהטכנולוגיה המתוארת היא ניטראלית - באותה מידה שניתן לנצל אותה לרעה על ידי ארגוני הפשע, כך היא מאפשרת שימושים חיוניים וחשובים כגון קשר חשאי בין כתבים למקורות, חשיפת שחיתויות, משתפ"ים, חתירה תחת משטרים מדכאים וכו'. מאחר ובשלב זה לא ניתן לבחון את זהות הפועלים ברשת, אין דרך אמיתית לדעת מהו היקף הפעילות של ארגוני הפשע ברשת האפלה, אלא באמצעות ניתוח דפוסי גלישה והתנהגות. עם זאת, ניתן לטעון, כי גם אם הפעילות כיום היא בעיקר של פושעים הפועלים באופן אינדיבידואלי, הרי הטכנולוגיה היא ממש בבחינת "פרצה קוראת לגנב", ומאחר והיא תופסת תאוצה, אין ספק שלא רחוק היום בו מרבית הפעילות בה תתבצע על ידי ארגוני פשע.

פתרונות

בין אם קיים שימוש נרחב בפועל של ארגוני הפשע לסחר בסמים ברשת האפלה, ובין אם אנו עדיין בשלב מוקדם, בו הרשת מנוצלת בעיקר על ידי סוחרים אידבידואלים, אין ספק, שהרשת האפלה ואפשרות התשלום בביטקוינז מציגים מתווה איומים חדש, והרשויות צריכות לשנות את הגישה והכלים להתגוננות והתמודדות. ללא נקיטת פעולות משמעותיות ואפקטיביות, הרשת האפלה תהווה את התשתית העיקרית לפעילות הסחר בסמים של ארגוני הפשע, ממש כפי שהפכה להיות ערוץ השיווק וההפצה המרכזי בתעשיית הפורנוגרפיה לילדים, והרשויות יעמדו בפני שוקת שבורה. לרשות רשויות האכיפה עומדות למעשה שתי אפשרויות מרכזיות - הן יכולות לנסות לתקוף את הטכנולוגיה עצמה או לאמץ אותה ואת הכלים שהיא מציעה כדי לתקוף את ארגוני הפשע מתוך המערכת.

דרך ראשונה - מניעת הסיכון

ההיסטוריה מלמדת שכל ניסיון לעצור את הקדמה והטכנולוגיה, דינו לכישלון. דוגמת הניסיון לעצור את השימוש בטכנולוגית הטלפון והטלגרף, מאחר והם הקלו על פעילות ארגוני הפשע בשנות ה-30 היה צורך. מכל מקום, גם אם קבוצה כלשהי או רשויות אכיפת החוק יצליחו להביא למפלתה של טכנולוגיה, תקום תחתיה טכנולוגיה חדשה ומתקדמת יותר. כלומר, **ניסיון להפיל בדרך כלשהי את רשת TOR**, סביר מאוד שלא יצלח, וגם אם כן, רשת אחרת המאפשרת אנונימיות תקום תחתיה. כבר כיום קיימות רשתות אפלות

אחרות, מוצלחות יותר או פחות, וב-2009 הציגו 2 בכירים ב-HP רשת אפלה הפועלת על גבי תשתית רשת האינטרנט הרגילה, אשר אינה מצריכה דבר מלבד דפדפן[12]. בנוסף, אין לשכוח שגם כיום עומדים לרשות הפושעים כלים מתוחכמים פחות, אך יעילים לשמירה על הזהות, כגון אנונימייזר וכו'.

האם הפתרון טמון **בניסיון להתגבר על אפשרות הסתרת הזהות**, האנונימיות? - ייתכן:

ראשית, גם פרוטוקול TOR אינו חסין לחלוטין להתקפות. כך למשל, השתלטות על הנתב הראשי, מאפשרת מעקב אחרי ההודעה, איתור השולח והנמען. שנית, חוקרים גילו אפשרות למתקפות application-level מבוססות HTTP כנגד פרוטוקול TOR (forged webpage injection attack ו- target webpage modification attack)[13]. באפשרות מתקפות מסוג זה זו לזהות את המשתמש מבלי להיעזר בטכנולוגיות פולשניות, ומכאן שהן מהוות איום רציני עבור רשת זו, והזדמנות מצוינת עבור הרשויות. שלישית, אמנם טכנולוגיות זיהוי המתבססות רק על מאפיינים התנהגותיים עדיין מצויות בחיתוליהן[14], אך הן קיימות בהחלט. הן כוללות מעין טביעות אצבע קוגניטיבית אלקטרוניות - זיהוי לפי קצב הקלדת המשתמש, תבניות רעידות הידיים המשפיעות על רעידות העכבר ועוד... כלומר אין אפילו צורך בזיהוי ביומטרי, והמשתמש כלל לא מודע לעובדה שזיהו אותו, עוקבים אחריו, מאזינים לו או מקליטים אותו. מובן שפעולה מסוג זה עומדת בסתירה לזכות לשמירה על ה-Identity של המשתמש, וכן קיים חשש ממשי לפגיעה בפרטיות. סביר שהרשויות תטענה, כי זיהוי יתבצע רק במידה ותתגלה פעילות חשודה, אך הלכה למעשה, ככל הנראה לא תהיה למשתמשים דרך לוודא זאת.

מובן שמהלך מסוג זה, יתקל בהתנגדות חריפה של המשתמשים, ומכאן הדרך קצרה ליצירת טכנולוגיה חדשה, אשר תצליח לעקוף את הטכנולוגיות החדישות הללו.

ייתכן והפתרון טמון באימוץ מודל ביניים, דוגמת מודל ה-**Selectively Traceable Anonymity**[15], העונה על 4 קריטריונים: (1) המערכת שומרת על האנונימיות של משתמשים ישרים (honest), ופרטי הגלישה שלהם נותרים חסויים; (2) שרת יכול לדווח אודות משתמש מסויים אנונימי, וכן להכניס אותו לרשימה שחורה בגלישותיו העתידיות; (3) כל פרטי הגלישה של המשתמש עובר לדיווח נותרים חסויים; (4) משתמשים מיועדים לגבי מעמדם כחלק מרשימה שחורה לפני כניסתם לשרת. הלכה למעשה, האנונימיות נשמרת כל עוד לא בוצע פשע. מודל מסוג זה, תלוי ברמת שיתוף הפעולה של המשתמשים, וכמובן עולות שאלות לגבי הגדרת מהו פשע? אלו כללים יחולו? וכן, מה לגבי האפשרות לביצוע פעולות בלתי חוקיות באופן אנונימי, שאינה נמנעת אלא בדיעבד.

ניסיון להפיל את הביטקוין, גם הוא דינו להיכשל. מעניין לראות שעל אף הטלטלות העזות שחווה המטבע מאז בא לעולם, המשתמשים מביעים בו אמון רב, וכאמור זוהי אבן היסוד להצלחתו של מטבע כלשהו. גם אם ינסו להוציא מחוץ לחוק את החלפת הביטקוין במטבעות "אמיתיים", להפיל פעם נוספת את הבורסות למסחר בביטקוין או כל דרך אחרת, הביטקוין כבר קיבל חיים משל עצמו, מעמדו איתן וסביר שיעמוד בטלטלות נוספות[16]. ומכל מקום, גם אם יפול הביטקוין, יקום תחתיו מטבע וירטואלי חלופי.

בנוסף, לא בטוח שהטענה, כי הביטקוין מהווה את הדרך האולטימטיבית להלבנת כספים, אכן מחזיקה מים - **קיימות מספר מגבלות על האפשרות של הלבנת כספים באמצעות הביטקוינז**[9] - בעולם כיום נכרו קרוב ל-10 מיליון מטבעות ביטקוין, כלומר שווי של כ-100 מיליון דולר. אם יבצעו הלבנה בהיקף גדול, יהיה די קל לזהות אותה - מיעוט המטבעות יוצר תנודתיות גדולה, והמרה בסכומים גדולים תיצור לחצים על שער המטבע, ויכול למשוך תשומת לב לא רצויה. כמו כן, עולות שאלות משפטיות הנוגעות לאפשרות החלת חוקי איסור הלבנת הון על מטבעות וירטואלים, שקצרה היריעה מלדון בהן במסגרת עבודה זו. בנוסף, נקודה חשובה שיש להזכיר היא שעדיין מדובר במטבע וירטואלי, ובהנחה ומטרתם של ארגוני הפשע היא ליצור רווח בעולם הממשי, הרי חנויות ה-Change מהוות נקודת תורפה של המלבינים, ונקודת אור עבור הרשויות. עם זאת, סביר שככל שהטכנולוגיה תתקדם והמטבע יצבור תאוצה, גם לצוואר בקבוק זה ימצא פתרון.

דרך שניה - הפחתת האיום

הנחת יסוד היא, שפשע יתבצע לאחר שהעבריין שוקל את העונש וההסתברות האכיפה (גם יתפסו וגם יענישו), אל מול התועלת שתצמח לו ממעשה הפשע. אם התועלת גדולה, משתלם לו לבצע את המעשה. לכן, סביר שדרך הפעולה הנכונה היא לא ניסיון לתקוף את הטכנולוגיה מבחוץ, אלא להפעיל במתודולוגיות והליכים מהעולם "הרגיל" תוך שימוש בכלים טכנולוגיים, ובכך לנקוט בגישה מניעתית, לחילופין, להגדיל את ההרתעה ואת ההסתברות לתפיסת העבריין וענישתו. כלומר, דרך טובה יותר תהיה להסתגל למציאות החדשה, ממש כפי שעשו ארגוני הפשע, אשר פרצו את המבנה המסורתי מבוסס ההיררכיה בלבד, עליו עדיין מבוססות רשויות החוק, הצבא, סוכנויות ממשלתיות ועוד, והם מתנהלים במודל מפוזר יותר ומקימים קואליציות. הקונפליקט יוכרע על ידי מי שישלוט ויעשה את השימוש האפקטיבי ביותר בידע. האתגר הוא לא רק בטכנולוגיה, אלה בעיקר בהבנת אופן ההתארגנות והבניית תהליכי קבלת החלטות, העברת התקשורת והידע וכו'.

שימוש בכלים טכנולוגיים

הרשת האפילה היא כזו המבוססת על אמון (Trust), וזוהי גם נקודת התורפה שלה. כפי שרשת האינטרנט היא ברובה Untrusted, ונקודת המוצא היא שכ-80% מהמחשבים בעולם נגועים, כך ניתן להפוך גם את רשת ה-TOR לרשת Untrusted. ה-FBI שותל סוסים טרויאנים המרגלים אחר פעילות המשתמש, במסגרת מאבקו בפשע המאורגן, ומארגן פעולות בהיקף נרחב כדי להתמודד עם התופעה[17]. בפרט, ניתן לבצע תקיפה ממוקדת, במסגרתה מוטמע קוד באתר, המאפשר לדוגמא החדרת תועלת, מתוך מטרה שזו תנצל את משאבי המערכת, תמוטט את האתר ויתכן אף באופן שיהרוס את הגיבויים. מתקפה מסוג זה מצריכה ידע טכנולוגי נרחב, ובנוסף היא מצריכה מידע אודות האתר המותקף, מתקפה מעין זו לא מתאפשרת בפורומים סגורים למוזמנים בלבד. ניתן גם לייצר תקיפות דוגמת התקיפה המפורסמת של קבוצת אנונימוס על האתר לוליטה סיטי, המפיץ פורנוגרפיית ילדים. הקבוצה הפיצה תוכנה לא מאומתת לביצוע

הגלישה, ואשר תיעדה וניטרה את כתובות מחשב הקצה של המשתמשים [18]. מובן ששיטה זו מצריכה הכשרת כ"א מתאים לצורך מטרות אלו.

כמו כן, על אף ש-TOR חוסם פרוטוקולים שמשמשים לרוב להתקפות שלילת שירות, האתרים שלו פגיעים להתקפות בדיוק כמו אתרים באינטרנט הפתוח. חולשת המחשבים המאחסנים את שרתי ה- TOR מאפשרת למי שמעוניין, לפגוע בתוכן המאוחסן בהם או בפעילות הרווחת בהם. עם זאת, לאור הכלים העומדים לרשות בעלי האתרים, המאפשרים יצירת יתירות (Redundancy) במערכת, סביר מאוד להניח, שניסיונות לביצוע מתקפות, מתוך מטרה לפגוע בזמינות של המערכת, לא יעלו יפה, ובוודאי שלא יצליחו לייצר כל הרתעה או יקדם את הרשויות צעד בכיוון תפיסת העבריינים.

שיטור פרואקטיבי מבוסס מודיעין - שימוש בכלים סטנדרטיים מותאמים לעולם הסייבר

לטעמנו, יש לשנות את הגישה **לגישה פרואקטיבית**, כלומר לא זו המגיבה לאחר בפשע, אלא לכזו העוסקת באיסוף מודיעין, פעולות יזומות של רשויות האכיפה ומונעת פשעים עוד טרם התרחשו. נקודת המוצא היא שמשתמשים פועלים באותה צורה בכל מקום, ומעבר למעטה החשאיות ואנונימיות, יש להתייחס לרשת כאל מקום בו ניתן להשתמש באותן שיטות, כלים ומתודולוגיות הקיימות כבר היום, תוך התאמה לסביבה החדשה. כאמור, **הרשת האפילה היא כזו המבוססת על אמון (Trust), וזוהי גם נקודת התורפה שלה**. אם רשויות אכיפת החוק יפעלו נכון, הן תוכלנה להכשיר שוטרים, אשר ישמשו **כחפרפרות ויסתננו לרשת האפלה**, לפורומים ולקהילות הסגורות. היתרון העצום הוא, ששוטר אחד יכול בקלות להתחזות למספר רב של משתמשים, אין דרך להתחקות אחריו, וכך באמצעות כח אדם יחסית קטן, אך מיומן, ניתן לייצר עבודת מודיעין ופעולות בשטח. יתרון אדיר נוסף לעומת העולם "האמיתי" - סוכן חשאי אשר מצליח להפיל רשת סמים זהותו נחשפת, הוא מסכן את עצמו, הופך מטרה לארגוני הפשע הנותרים, ובוודאי שלא ניתן להשתמש בו פעם נוספת לאותה מטרה, על אף שהוכיח את כישוריו הלכה למעשה. להבדיל, סוכן חשאי ברשת האפלה, יכול להפיל ארגון פשע גדול, ולמחרת להמשיך בפעולתו תודות לחשאיות שמספקת הרשת.

יש לזכור שבניגוד לפורנוגרפיית ילדים, שם כלל העסקה מסתיימת ברשת באופן אנונימי על ידי העברת הקבצים, מבלי להותיר כל עקבות, הרי בעסקת סמים קיים המימד הפיסי של העברת הסחורה, המקל על רשויות החוק באיתור הצדדים והעמדתם לדין.

אמצעי נוסף העומד לרשות רשויות אכיפת החוק, אשר נדמה שהן אינן עושות בו שימוש מספיק הוא **פיתוח קשרים עם קהילת ההאקרים**, בדומה לביסוס קשרים עם משת"פים בעולם "האמיתי". אותם האקרים נמצאים ברשת, מכירים את הדרך בה היא עובדת, הם יכולים לשמש עיניים ואוזניים לרשויות מבלי שיצטרכו להגדיל את מצבת כח האדם. יש לזכור שבעלי היכולות הם ההאקרים, אך בעלת האינטרס היא רשות אכיפת החוק. עליה לרתום לשורותיה את אלו שיכולים לסייע בידה.

דרך נוספת להתמודדות עם התופעה היא **ניתוח מידע זמין**, ובאמצעותו לזהות חריגה מתבניות של משתנים, כגון התארגנות, זיהוי א-נומליה, יצירת פרופילים של המשתמשים וכו', ובאמצעותם היא יכולה למנוע את התרחשות הפשע, ולא רק להגיב לאחר מעשה. אלו כלים העומדים לרשות רשויות אכיפת החוק גם כיום, אך לא נעשה בהן שימוש מספיק.

שיתופיות - איחוד כוחות, משאבים ושיתוף פעולה בינלאומיים

בפרט חתימה על אמנת בודפשט ופרוטוקול שטרסבורג. כאמור, ארגוני הפשע אימצו מהר מאוד את היתרונות הגלומים ברשת האינטרנט, ובפרט האופן בו היא מסייעת להם לפרוץ גבולות גיאוגרפיים במסגרת העסקים שהם מנהלים. ברור אם כן, ששיתוף פעולה בינלאומי הוא אקוטי להצלחתן של הרשויות לעצור את הארגונים הללו.

בנובמבר 2001 נחתמה אמנת בודפשט לטיפול בפשעי מחשב (Cyber Crime). האמנה שנכתבה על ידי מועצת אירופה, בשיתוף מדינות משקיפות נוספות שאינן חברות במועצה (יפן, ארה"ב, קנדה ומדינות נוספות), והיא נכנסה לתוקף ביולי 2004. מטרותיה העיקריות של האמנה הן ליצור מדיניות משותפת ביחס לפשעי סייבר כדי להגן על החברה מפשעים אלה, בפרט על ידי אימוץ חקיקה הולמת ומיסוד שיתופי פעולה בנושא זה. האמנה מתמקדת בפשיעה באינטרנט וברשתות תקשורת נוספות, ובפרט בעבירות: הפרת זכויות יוצרים; הונאה מבוססת מחשב; פורנוגרפיית ילדים ופגיעה מכוונת באבטחת מידע ברשתות תקשורת. ב-2006 נוסף לאמנה פרוטוקול נוסף המגדיר פרסומים גזעניים וקסנופוביים (שונאי זרים), באמצעות תקשורת מתווכת מחשב, כעבירה פלילית.

המצב בישראל[5]: על האמנה חתומות 47 מדינות, לרבות ארצות הברית. ישראל נמצאת "בחברה טובה" לצד רוסיה וסין, אשר אינן חתומות על האמנה. בהזדמנויות שונות ישראל טוענת, כי העניין נשקל בחיוב, וכי הנושא בבדיקה (בינואר השנה, נאמר ש"זה עניין של כמה חודשים"). כיום שיתופי פעולה בינלאומיים הנדרשים לצורך טיפול בפשעי מחשב מתבססים בעיקר על הסכמה מרצון (לעיתים קרובות על בסיס היכרות אישית בין הרשויות), או באמצעות סיוע של משרד המשפטים. הכותבות ניסו להשיג את תגובתה של משטרת ישראל, אך לצערנו לא זכינו לשיתוף פעולה. מפרוטוקול ישיבת ועדת המדע והטכנולוגיה מינואר 2012[19], בה השתתפו גם נציגי המשטרה והמשרד לביטחון פנים, ניתן ללמוד כי למשטרת ישראל כוח של כ-15 שוטרים השייכים למפלג להב 433 האמונים על הנושא, והם מיומנים דיים. לטענת נציג המשטרה, העובדה שהכלים בהם משתמשת המשטרה אינם ידועים לכל, הינה חיובית, וייתכן והצדק עימו, אך ברור שלא ניתן לייצר בדרך זו הרתעה, וכן עם כל ההערכה למשטרת ישראל, קשה להאמין ש-15 שוטרים מסוגלים להתמודד עם המצב. נוכל לצטט מתוך דברי הסיכום של יו"ר ועדת המדע והטכנולוגיה, באותה ישיבה בה היא ממליצה למשטרת ישראל "להגביר את כוחה, את מיומנויותיה ואת כל מה שנדרש על מנת לפצח את אותן הצפנות, או כל צעד אחר שתמליץ עליו שם כצעד פרקטי ומועיל שיסייע בידינו לעמוד בשורה ראשונה עם מדינות כמו בריטניה ואחרות, שהן כנראה מצליחות יותר מאיתנו בפעילות הזו".

לסיכום

הפשע המאורגן היא תופעה הקיימת מזה עשורים. הארגונים אלימים ומתוחכמים, המתפתחים ומסתגלים לתנאי השוק, החוק והטכנולוגיה. העידן האינטרנטי מעצים את ארגוני הפשע, בשל היכולת להתנהל באנונימיות ובחשאיות כמעט מוחלטות. במאמר זה התמקדנו בעסקאות הסמים המתבצעות ברשת וכיצד ארגוני הפשע מנצלים את המטבע הוירטואלי, ביטקוין, לצורך עסקאות סמים והלבנת כספים שהינם מעמודי התווך של עולם זה. אך לא אבדה תקוותנו, שכן מקור הבעיה הוא גם המקור לפתרון.

על המחברות

עו"ד לילך צאירי-כהנוב סיימה בהצטיינות את תוארה הראשון במשפטים באוניברסיטת ת"א, והינה עורכת דין במקצועה. בימים אלו שוקדת על השלמת התואר השני שלה במנהל עסקים.

שרון ברק מהנדסת פיתוח בתעש, בעלת תואר ראשון בהנדסה כימית מאוניברסיטת בן-גוריון, סטודנטית לתואר שני במנהל עסקים באוניברסיטת תל אביב.

תודות

תודה ל**דרור דנסקי** ולעיתונאי **בר שם-אור**.

ביבליוגרפיה

[1] An Overview of Transnational Organized Cyber Crime, Etges, Rafael; Sutcliffe, Emma. Information Security Journal: A Global Perspective. Mar2008, Vol. 17 Issue 2, p87-94. 8p. 1 Chart

[2] Organized Crime and Cybercrime: Synergies, Trends, and Responses, Phil Williams, Global Issues Volume: 6 Issue: 2 Dated: August 2001 p22-26

[3] Organized Crime Goes Cyber, Bequai, Computers & Security, Volume 20, Issue 6, 1 September 2001, p475-478

[4] גדי אשד, הפשיעה המאורגנת בישראל ובעולם - מגמות ותהליכים, המשפט, מרץ 2005

[5] דו"ח שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה, ועדת המדע והטכנולוגיה, ינואר 2012

[6] קיצור תולדות האנושות, יובל נח הררי, עמ' 180, 2011

[7] A History of Money - From Ancient Times to the Present Day, Glyn Davies, University Of Wales Press, Cardiff, 2002

[8] Back to Gold - and Silver, Andrew M. Watson, The Economic History Review, Second Series, Volume Xx, No. I, 1967

[9] Virtual money laundering: the case of Bitcoin and the Linden dollar, Robert Stokes, Information & Communications Technology Law. Oct2012, Vol. 21 Issue 3, p221-236. 16p. Version of record first published: 11 Dec 2012.

[10] Bitcoin: A Bit Too Far? Jacobs, Edwin. Journal of Internet Banking and Commerce 16.2 (Aug 2011): 1-4

[11] http://www.themarker.com/wallstreet/1.1882317

[12] Researchers build browser-based darknet, Network Security, Jun2009, Vol. 2009 Issue 6, p20-20. 1p.

[13] A potential HTTP-based application-level attack against Tor, Xiaogang Wang, Junzhou Luo, Ming Yang and Zhen Ling,Future Generation Computer Systems, Volume 27, Issue 1, January 2011, p67-77

[14] http://www.haaretz.co.il/captain/net/1.1666822

[15] Anonymous IP-Address Blocking, Peter C. Johnson, Apu Kapadia, Patrick P. Tsang and Sean W. Smith, Department of Computer Science, Dartmouth College

[16] http://www.themarker.com/wallstreet/1.1690268

[17] http://www.fbi.gov/about-us/investigate/cyber/cyber

[18] חורים ברשת, ד"ר נמרוד קוזלובסקי, 01.01.12: http://www.holesinthenet.co.il/archives/35299

[19] פרוטוקול ישיבת ועדת המדע והטכנולוגיה, בתאריך ז' טבת תשע"ב, 02/01/2012