פשע קיברנטי כסיכון לביטחון הלאומי?

ליאור טבנסקי

המרחב הקיברנטי, שנוצר עם התפתחות טכנולוגיות המחשבים והתקשורת הדיגיטאלית, נכנס בעשורים האחרונים לחיינו. תקשוב מיושם לשיפור וייעול תהליכי העבודה, הלמידה והבידור ומשפיע על דפוסי הפעולה כמעט בכל תחומי הפעילות האנושית. רשת האינטרנט, שהפכה מסחרית ב־1988 וצמחה לנדבך משמעותי במרחב הקיברנטי, מאפשרת נגישות זולה ומיידית למידע על סוגיו, שיתוף ידע, עבודה משותפת מרחוק ועוד.

משמעויות הפשע הקיברנטי לביטחון הלאומי נגזרות מאופי השימוש בטכנולוגיה על ידי גורמים בעלי מניעים עוינים. המאמר מציע בחינה מכוונת מדיניות של משמעויות הפשע הקיברנטי לביטחון הלאומי. מבלי להתבסס על הערכות כספיות של היקף נזקי הפשע הקיברנטי. המאמר מתאר את שיתוף הפעולה בין פושעים לפשע המאורגן ולארגונים עוינים, ודובמסחור של יכולות התקיפה הקיברנטיות המתאפשר עם התפתחות הטכנולוגיה וצמיחת "השוק השחור" לשירותי מחשוב. נטען שהפשע הקיברנטי אינו מהווה איום על הביטחון הלאומי כיום. אולם, המאמר מזהה שני תנאים נפרדים שאם יתמלאו, הפשע קיברנטי עלול להפוך לאיום על הביטחון הלאומי.

הדרישה הציבורית לביטחון במרחב הקיברנטי עולה עם העלאת המודעות לאיומים. גם ללא עלייה אובייקטיבית בהיקף הפשיעה, אין להניח שהדרישה הזו תדעך. אחריות המדינה לאזרחיה אינה נעצרת במרחב הקיברנטי, וגם בתחום הזה ביטויה המעשי צריך להיקבע במסגרת תהליך פוליטי דמוקרטי על יסוד עובדתי מוצק.

תופעת הפשע הקיברנטי

טכנולוגיות ממוחשבות, שיושמו לשינוי וייעול תהליכי הייצור והעבודה בכל תחומי החיים, לא פסחו על תעשיית הפשע. המחשוב מאפשר פירוק משימות ליחידות

ליאור טבנסקי הוא דוקטורנט למדעי המדינה באוניברסיטת תל אביב. ליאור היה מלגאי בתכנית ניובאוור לתלמידי מחקר בשנים 2010–2012 במכון למחקרי ביטחון לאומי (INSS), אוניברסיטת תל־אביב.

קטנות וביזור העיבוד. הרישות מאפשר גישה גלובאלית למידע, והתמקדות בידע כמוצר בעל ערך. ההגדרה המוצעת לפשע הקיברנטי היא:

שימוש במרחב הקיברנטי למטרות אסורות, תוך ניצול התכונות המיוחדות המאפיינות את המרחב הקיברנטי הקיים, כגון: מהירות ומיידיות, הפעלה מרחוק, הצפנה והסוואה שתורמים לקושי בזיהוי הפעולה והמפעיל, ניצול הערך העולה של המידע דיגיטאלי לסוגיו, טיפול חוקי ומשפטי שונה במרחב הקיברנטי במדינות שונות.

הדיון בהגדרות של תופעת הפשע הקיברנטי ממשיך להתפתח. לפני למעלה מעשור, תהה גרבוסקי מה חדש בפשע הקיברנטי: האין אלה תופעות ותיקות המשתמשות בכלים חדשים?[1] אולם רוב החוקרים מנסים לנתח את הפשע הקיברנטי כתופעה ייחודית. מאג'יד יאר ממיין את הפשע לפי האובייקט הנפגע: נגד רכוש, אדם, מדינה.[2] שינדר וקרוס מיינים את הפשע לפי מידת האלימות: אלים ואלים פוטנציאלי, בלתי אלים (סחר בסמים, הלבנת הון) וצווארון לבן (פריצה, גניבה והונאה).[3] לפי ההגדרה של וול – "*the transformation of criminal or harmful behaviour by networked technology*"[4] – פשע קיברנטי התפתח בעקבות צמיחת התקשוב והמרחב הקיברנטי, והאפשרויות החדשות להשגה, שיבוש או מניפולציה של מידע למטרות רווח. בנוסף, ממיין וול את הפשע הקיברנטי לשלושה טיפוסים: עבירות הנוגעות לשלמות ותקינות מערכת המחשב (Hacking פריצה למערכות), עבירות שמסתייעות במרחב הקיברנטי (תקשורת מוצפנת בין עבריינים, מכירת תרופות מזויפות), ועבירות הנוגעות לתוכן המידע הממוחשב (גניבת סודות, הפצת תוכן פוגעני).

ניתן גם למיין את העבידות לפי תפקידו של המחשב.[5] גם "האמנה האירופית נגד הפשע הקיברנטי" מאמצת גישה דומה.[6]

המחשב כאמצעי לביצוע עבירה		
גישה אל והפצה של תוכן: סודות ידע תוכן פוגעני	שיבוש המידע או המערכת בכוונת זדון גניבת זהות הונאה	שימוש בתקשורת הטרדה סחר בחומר אסור דוא"ל זבל

המחשב כמטרה של העבירה			
גישה לא מורשית: Hacking	החדרת קוד זדוני: נוזקות, רוגלות, וירוסים	שיבוש של פעילות: DDoS	גניבה של שירות: שימוש לא מורשה

חלק ניכר מהפשיעה הקיברנטית אינו מהווה תופעה ייחודית או חדשנית: הטרדה, הונאה, תעמולה אסורה, פורנוגרפיה, גניבה, הלבנת הון, ריגול ועוד. הפעולות הללו משתמשות במרחב הקיברנטי. הנדבך נוסף הוא תופעות שכמעט

לא היו ברות־ביצוע לולא המרחב הקיברנטי: דוא"ל זבל, Click fraud, תוכנות זדוניות (Malware) לסוגיהן, רשתות מחשבים שבויים (Botnet),[7] גניבת זהות דיגיטאלית, הסוואה והצפנה[8] של מידע ותקשורת, חדירה ממחושבת למתקנים ממוגנים בעלי ערך רב וריגול אוטומטי מתמשך בארגונים מאובטחים המוציא "רכוש אינטלקטואלי" משליטתם.

פשיעה, על סוגיה, היא תופעה חברתית נפוצה. הסברים קרימינולוגיים לתופעה משלבים הנעה, הזדמנות, וקיומו של "שומר". ניתן לזהות שני סוגי מקורות להנעה האנושית לפעולה.[9] חלק ניכר מהמניעים להתנהגות עבריינית הנם אישיותיים־פנימיים (Intrinsic Motivation), ולא נקבעים בתהליך בחינה של שיקולי עלות־תועלת. אין סיבה להניח שבעקבות שימוש מוגבר בטכנולוגיה זו או אחרת, עצם ההתנהגות האנושית תשתנה. לפי כך אין זה מפתיע שבני האדם משתמשים גם במרחב הקיברנטי למילוי צרכיהם ורדיפה אחר מטרותיהם, הן באפיקים הנורמטיביים כגון לימודים, בידור, השכלה ועבודה, והן בפעולות האנושיות הוותיקות כגון לחימה ופשע. האסכולה הקלאסית בקרימינולוגיה מתבססת על רעיון הבחירה החופשית והערכה רציונאלית של תועלת צפויה בהתחשב בסיכוי להענש, ומפרשת את המוטיבציה לביצוע עבירה כהחלטה כלכלית־רציונאלית.[10] כלכלנים ופסיכולוגים עוסקים בניתוח ההתנהגות האנושית, כולל העבריינות, כנגזרת של שיקול עלות־תועלת רציונלי. מכלול הנסיבות החיצוניות המשתנה יכול לעודד פשיעה קיברנטית: זה קורה כשאדם מזהה פוטנציאל גדל לרווח ומעריך שהמחיר, הסיכוי לענישה, נמוך מהתועלת הצפויה. הרחבת החיבוריות הדיגיטאלית, יחד עם עליית ערך המידע הממוחשב, גורמים למצב שבו מוטיבציה חיצונית (Extrinsic Motivation) להתנהגות עבריינית עולה. בעוד שקיימים מנגנוני אכיפת חוק מסודרים במדינות המפותחות, במרחב הקיברנטי החדש תגובת המדינה לא הדביקה את השינוי הטכנולוגי. דוגמה טובה היא שוד בנק מסורתי לעומת גניבה ממוחשבת. האפשרות המסורתית לשוד כספים מסניף של בנק כרוכה בהתגברות על מערכי האבטחה, וסיכוי סביר להקלע לעימות עם שומרים חמושים. גם אם השוד עצמו יסתיים בהצלחה, לאורך השנים השודדים נרדפים על ידי רשויות החוק. עם התפתחות המרחב הקיברנטי התאפשר לנצל את פגיעותו גם לגניבה מבנקים. למשל, נפוץ השימוש ברשתות בנות אלפי מחשבים שבויים (Botnet)[11] לגניבה מתמשכת של פרטי הזדהות לאתרי בנקאות ושימוש בהם לגניבת סכומי כסף קטנים. לאור בעיית ווידוא הזהות (Attribution) במרחב הקיברנטי, והסיכוי לזיהוי הפושע קטן מאוד.[12] המוסדות הפיננסיים מודעים לסיכון העסקי הברור, ויחד עם מוסדות ההסדרה נוקטים באמצעי הגנה ומשקיעים בנושא אבטחת מידע, כדי לצמצם את מרחב ההזדמנויות לשודד הקיברנטי. עם זאת, הסיכון הפיזי המיידי שנוטל הגנב הקיברנטי עדיין נמוך מזה של שודד מסורתי.

היקף הפשע הקיברנטי והנזקים: הערכות בעייתיות

תופעת הפשע הקיברנטי נבחנת בדרך כלל בפרספקטיבות משפטיות (חקיקה ועניישה), קרימינולוגיות (מניעים וארגון), כלכליות (תמריצים וערך) או טכניות (אבטחת מידע). משפטנים עוסקים בהצבת גבולות להתנהגות מקובלת וסוגיות חוקיות של מניעה ואכיפה. קרימינולוגים מיישמים את הידע המקצועי להבנת התופעות החדשות. כלכלנים מתארים את מערכת התמריצים המשפיעים על תהליכי קבלת ההחלטות של שחקנים רציונאליים. אנשי אבטחת מידע עוסקים בסוגיות טכניות של התשתית הטכנולוגית: תוכנה, חומרה ותקשורת, תוך מיקוד בפגיעויות השונות ודרכי ההתגוננות. משפטנים, כלכלנים ואנשי אבטחת מידע שותפים בדעה שהיקף של הפשיעה הקיברנטית ועוצמת הנזק שלה נמצאים בעלייה מהירה ומתמשכת. ההערכה נסמכת על העובדה שהיקף המידע הדיגיטאלי גדל בקצב מעריכי, וגם החיבוריות של התקנים ממוחשבים צומחת. המרחב הקיברנטי מכיל הרבה יותר מידע, עם הרבה יותר נקודות גישה פוטנציאליות לחדירה בלתי מורשית. המסקנה היא שכל חדירה (Breach) חושפת היקף הולך וגדל של מידע.

הערכות כספיות של היקף הנזק של פשע קיברנטי מתפרסמות מאז שנות ה־90 ועד היום. חברות האבטחה מובילות את המחקר בנושא, ומפרסמות דו"חות למכביר. קיימות עשרות הערכות שונות, שמקורן במגזר העסקי והממשלתי בארה"ב, בריטניה, ומדינות מפותחות נוספות.[13] סקר של הבולשת הפדרלית העריך את הנזק לעסקים אמריקאיים ב־65 מיליארד דולר ב־2005.[14]

שר המסחר האמריקאי גארי לוק טען שהנזק השנתי לחברות אמריקניות כתוצאה מזיוף ופיראטיות (שימוש בלתי חוקיים בקוד מחשב) עומד על 200–250 מיליארד דולר.[15]

דו"ח בריטי מציג תג מחיר של 27 מיליארד ליש"ט לשנה: הנזק השנתי לאזרחי בריטניה הוערך ב־3.1 מיליארד ליש"ט, למגזר העסקי 21 מיליארד ליש"ט ולממשלת בריטניה 2.2 מיליארד ליש"ט נוספים.[16] בדו"ח שהוציאה חברת **סימנטק**, ממובילות שוק אבטחת המידע, נאמד הנזק הכספי הישיר שגורם הפשע הקיברנטי ב־114 מיליארד דולר בשנה ב־24 מדינות.[17] הערכות נוספות נוקבות בסדר גודל של מאות מיליארדי דולר בשנה.[18]

סכומי עתק הללו עוררו תהיות וספקנות, אולם השפעת הביקורת עד כה הייתה מוגבלת. לאחרונה פורסם נייר עמדה מאת שני חוקרים מחברת **מיקרוסופט**, שמנתח את התשתית הסטטיסטית הרעועה שביסוד הערכות הנזק של הפשע הקיברנטי הנעשות באמצעות סקרים.[19] כיצד ההערכות הללו נוצרו? בחינה של שיטות המחקר מגלה את הקלות בהערכת־יתר של היקף הנזק. ראשית, חסר מידע על השימוש שנעשה (או לא נעשה) במידע שנחשף. המקרים שקיים בהם מידע מוצק ספורים, בעוד שהיקף הנזק הפוטנציאלי הוא רחב. הבה נניח שנפרץ

מחשב המכיל קובץ, מאגר מידע בן אלף רשומות. נניח גם שמאגר המידע אינו מוצפן, והרשומות שבו כתובות בשפה טבעית. כל רשומה בקובץ מייצגות כרטיס אשראי תקף, על כל הפרטים הדרושים לשימוש בו: מספר, מספר CVV,[20] תוקף, שם, תעודת זהות וכתובת הבעלים, ופרטי חשבון הבנק המנפיק. במצב הזה הגנב רואה תמונה מלאה ואמיתית של המידע בקובץ. אולם גם במצב האופטימאלי, הגנב לא יכול להעריך את מלוא המשמעויות הכלכליות של המידע שהשיג. האם הפורץ יכול להעריך נכונה את הערך האמיתי של המידע שגנב? האם הקורבן, הנפרץ, יכול להעריך כראוי ? בגניבת רכוש אינטלקטואלי, תוצר של מחקר ופיתוח, הקורבן נוטה לזהות את הרווח המירבי שהיה רוצה לקבל בתום תהליך הפיתוח, הייצור והשיווק כנזק של גניבת המידע. השימוש בסקר, שיטה המתאימה לבירור תופעה שקשה לצפות עליה ולגילוי היסטוריה של הנסקרים, הוא השיטה העיקרית ללמוד על היקף הנזק. הסקר מאפשר להגיע למספר יותר גדול ומגוון של משיבים שמספקים הערכות משלהם לכמות האירועים והנזק. אך שיטת הסקר סובלת גם ממגרעות משמעותיות, המעסיקות אנשי מדעי החברה וסטטיסטיקאים.[21]

שנית, בהעדר מידע מספיק משתמשים בשיטות סטטיסטיות להגיע להערכה על בסיס פרטי מידע אחדים.

בעיות המדידה קיימות בכל תחומי הדיון באיומים הקיברנטיים, והן בולטות במיוחד כשמנסים לסייע לדיון כל ידי כימות הנזק בערכים כספיים. קיים קושי מהותי בהערכת הנזק, ועד כה נראה שההערכות הכספיות שנוצרות בהפעלה גסה של שיטות הסטטיסטיות כדי להציג השערה על סמך נתונים מעטים – מובילות להערכות יתר. בנוסף לסוגיות של מהימנות שיטות המחקר, מהימנות מקורות המידע, והתאמת השיטה הסטטיסטית למחקר, קיימת בעיה נוספת. ההערכות הכספיות כוללות לרוב גם מרכיבים עקיפים של נזק. הערכות כספיות כוללות פגיעה במוניטין הפירמה שסבלה מפריצה, השפעות שליליות על התנהגות הצרכנים שגורמות לתוצאות מאקרו־כלכליות, סוגיות של דיני נזיקין, ביטוח, הוצאות נלוות ועוד.

שאלות מרכזיות בהבנת התופעה נותרו ללא מענה ברור: האם כדאי להעריך את הנזק על פי השימוש שבוצע בפועל במידע, במקום על פי הפוטנציאל המירבי? אולי צריך להתייחס לערך הכספי של יצירת המידע, במקום להערכת מחירו בשוק כעת או בעתיד? ומה בדבר העלויות הנדרשות לאבטחה וחזרה לתפקוד תקין? תמונת המצב שעולה מתוך המקורות המקובלים אינה מהימנה, והנזק של הערכת היתר עלול להיות ביצירת תגובת־נגד: זלזול בחשיבותו של הפשע הקיברנטי. ביסוס הדיון בפשע הקיברנטי על הערכות הנזק הכפסיות פוגע בדיון מושכל בבעייה, וביכולת לעצב מדיניות ציבורית הולמת.

שיתוף פעולה בין עבריינים לארגוני טרור

הממשק בין עבריינים מקצועיים, הפשע המאורגן, וארגוני טרור – אינו חדש. גם אם נתבונן רק במציאות החיים הישראלית נזהה ששיתוף הפעולה מהסוג האמור גורם לנזקים ברמה הלאומית. מאז שנת 1996 התנהל המאבק התקשורתי ברכישת "דיסקים צרובים" תוך טענה שהרוח מופנה למימון טרור פלסטיני.[22] זאת, כחלק מקשר אמיץ בין שירותי הלבנת הון לצרכנים כמו ארגוני הטרור.[23] תופעת ענפה של גניבת מכוניות מישראל לשטחי יהודה ושומרון ליוותה את החוויה הישראלית לאורך שנים ארוכות. הבעיה כמעט ולא טופלה ברמה הלאומית, שכן האיום לא נתפס כבעיה ביטחונית: הנזק כוסה בידי חברות הביטוח וגולגל בהדרגה אל המבוטחים, המשטרה לא פעלה מחוץ לגבולות הריבונות הישראלית, והצבא שהפעיל מחסומים ביטחוניים קבועים על צירי תנועה ראשיים בחר להימנע מעיסוק בפושעים "הפליליים". בתקופת "אינתיפאדת המתאבדים", חל שינוי בדרכי הפעולה של אותם הפושעים הפליליים: ארגוני הטרור גייסו את מומחיותם של גנבי הרכב הפלסטיניים כדי להשתמש במכוניות עם לוחיות ישראליות לתחבורה, וגם כדי למצוא נתיבים כדי לחדור את מעגלי האבטחה ולהוביל אמצעי לחימה ומחבלים מתאבדים ללב הערים.

אפשרויות המעבר בין רצועת עזה לישראל מוגבלות יותר מאשר ביהודה ושומרון. חפירת מנהרות לכיוון רפיח המצרית נועדה לספק נתיבי הברחה לצרכים שונים. עסקי ההברחה יוצרים רווח כספי גדול לחופרי המנהרות ומפעיליהן, והתעשייה מתקיימת למרות מאמצי הסיכול הישראליים. המנהרות הפכו לבעיית ביטחון לאומי עקב הברחת אמצעי הלחימה וחומרים שונים מסיני לרצועת עזה, והברחת מחבלים מהרצועה לסיני.[24] המומחיות של ארגוני הפשע בחפירת מנהרות אפשרה את המתקפה ליד כרם שלום ב־25 ביוני 2006 שבה נהרגו 2 חיילים וחייל נוסף נחטף לשבי החמאס. במקרה הזה המומחיות הטכנית של חופרי המנהרות נוצלה בבירור לפגיעה בביטחון הלאומי של ישראל.

חלק מהבדואים ברצועת סיני מתפרנסים ממומחיות הניווט בשטח, ומספקים לאורך עשרות שנים "שירותי הברחה" לתוך מדינת ישראל. "הסחורה" המוברחת כללה בעבר הלא רחוק מאות נשים לשימוש בתעשיית המין וסמים. בשנים האחרונות, מוברחים באלפי אפריקאים לגבול ישראל. יש הטוענים שאלה מהווים אתגרים משמעותיים, אבל לא בעיה אמתית לביטחון הלאומי. אולם, הערכה זה משתנה ככל שהמומחיות של המבריחים משמשת לביצוע מתקפות טרור על ישראל.[25] הברחת מחבלים מעזה דרך סיני לישראל אפשרה את פיגועי הטרור בכביש 12 ב־18 לאוגוסט 2011, שם נרצחו 8 ונפצעו 40 ישראלים. הברחת המחבלים ואמצעי הלחימה הכניסה את העיר אילת לטווח ירי רקטות.[26] ההברחות הללו מסכנות בצורה ברורה ומיידית את הביטחון הלאומי.

בחינה מחודשת של משמעות הפשע הקיברנטי

אם נתבונן כעת בפשע הקיברנטי, נגלה שגם בו קיים שיתוף פעולה מסחרי דומה. בשנים האחרונות התפתח שוק שחור של מומחים טכניים ו"רועי" רשתות מחשבים שבויות, המפתח ומספק כלים ושירותים טכניים בתשלום.[27] שוק שירותי הסייבר השחור Crimeware as a Service (CaaS) גורם לנזקים כלכליים במדינות המפותחות, אף שהערכות הנזק הכספיות הנפוצות מוטות מאוד כלפי מעלה.

מי שמעדיף לפעול בכוחות עצמו, ואין בידיו משאבי מחקר ופיתוח – מגלה שכלי נשק קיברנטיים (חבילות תוכנה זדוניות – toolkits)[28] זמינים לכל בהורדה מהאינטרנט, לרוב בתשלום של עשרות עד אלפי דולר. הידע הוא מוצר בלתי נדלה; כך, שיתוף האחר ביכולות שהיו זמינות לך אינו פוגע בעוצמתך.[29] על רקע זה נוצר המצב שבו כלים עוצמתיים זמינים לכל דורש בעלות שולית. הרושם הנפוץ שהמרחב הקיברנטי מקל על גריפת רווח מפעילות פושעת לא נעלם מארגוני הפשע המאורגן.[30]

צמיחת כוח המחשוב ופריסת רשת האינטרנט אפשרו אמצעי חדש לביצוע פשיעה קיברנטית רחבת היקף: רשתות של מחשבים שבויים. Botnet הוא מקבץ של מחשבים אישיים, המחוברים לרשת, אשר הושתלה בהם תוכנה זדונית המאפשרת שליטה מרחוק ביכולות המחשבים הללו, וזאת מבלי לגרום לשיבוש פעולתם התקין. הדבקת המחשבים המחוברים לאינטרנט נעשית באמצעות ניצול פרצות ידועות שהמשתמשים ו מנהלי המערכות לא טיפלו בהם, להחדרת תוכנה זדונית. לאור ההיצע הגבוה, מחיר השימוש ב־Botnet נגיש כמעט לכל: חברת **מק'אפי** העריכה ב־2007 שכ־5% מהמחשבים האישיים המחוברים לרשת בעולם שבויים.[31]

אחת התופעות החדשות היא Advanced Persistent Threat (APT), או Adaptive Persistent Attack (APA)[32] – השימוש המורכב והרב שלבי בכלי נשק קיברנטיים לביצוע משימות מתמשכות ומוסתרות. התוקף אינו פועל בהיקף רחב כדי לנצל פגיעויות מוכרות, אלא שהיעד מוגדר היטב. התקוף משתמש במגוון של כלים, חלקם ייחודיים, תפורים למשימה. תקיפה שכזו מורכבת משלבים רבים, ויכולה ולהמשך לאורך חודשים ושנים. התוקף מתחיל באיסוף מודיעין על המבנה הארגוני של המטרה, וזיהוי בעלי תפקידים בכירים שלהם הרשאות גישה למירב המידע בארגון. איסוף המידע האישי נעשה תוך שימוש בפרטים גלויים, ושיתוף המידע הפרטי ברשתות החברתיות. לאחר זיהוי אנשי המפתח, נעשה מהלך ממוקד להדביק אותם. אחת השיטות היא SpearPhishing: החדרת סוס טרויאני באמצעות הודעת דוא"ל ממוקדת, משולח מהימן ועם תוכן רלוונטי, שחודרת את מנגנוני הסינון על ידי שימוש במידע האישי שנאסף. פתיחת ההודעה מאפשרת החדרת "סוס טרואיני": נוזקה לגישה מרחוק Remote Access Tool (RAT) למשאבי המחשוב בארגון, על ידי יצירת תקשורת ממחשב מורשה ברשת הפנימית. עם השגת

הגישה, הפושע הממוצע פועל במהירות כדי להשיג משהו בעל ערך ולממש אותו. לא כך בהתקפת APA, כשהמטרה היא גישה סמויה לאורך זמן, תוך התעלמות מפיתויים כספיים מיידים. ההתקפה נמשכת לאורך זמן ארוך, בין היתר כדי להתגבר על מערכות מניעת דלף המידע. במהלך ההתקפה, נעשות בדיקות לזיהוי סף תגובה של המערכת, ובמידת הצורך המידע הנגנב נחלק למנות קטנות, מוסווה בתוך תקשורת לגיטימית, ועובר מבלי לגרות את מערכות ההגנה. ההתקפה הממוקדת נדירה יותר ממתקפות סטטיסטיות, שכן היא יקרה בהרבה: APA דורשת איסוף מודיעין שיטתי, יכולת תכנון וניסוי, ואורך רוח לביצוע המשימה הממושכת.

בפרסקטיבה כלכלית נוצר מצב שמצד ההיצע, קבוצות ההאקרים שהצליחו לפתח וליישם כלי תוכנה לשליטה באלפי ומאות אלפי מחשבים, יצרו למעשה שירות, בעל ערך כלכלי. מצד הדרישה, לקוחות שונים – האקרים אחרים, חוקרים פרטיים, פושעים, ארגוני ריגול וארגוני פשע גדולים – מצאו שימושים שונים למוצר הזה. כך נוצר מודל עסקי Crimeware as a Service (CaaS), העתק "שחור" של מודל Software as a Service (SaaS), המנחה את תעשיית שירותי המחשוב מאז 2001.[33] ההצדקה הכלכלית של המודל ברורה: מעתה הלקוח לא נדרש לרכוש ציוד מחשב כדי להשתמש בשירותי מחשב. הלקוח יכול לרכוש רק את השירות המדויק שהוא זקוק לו ממפעילים גדולים, ולהשתמש בו על גבי הרשת, בתקשורת סטנדרטית. המודל עבר גלגולים אחדים במשך השנים, והיום הוא מוכר בזמלול Buzzword "מחשוב ענן" (Cloud Computing). היקף השוק העולמי לשירותי המחשוב כשירות מוערך ב 14.5 מיליארד דולר ב־2012.[34]

הבא נבחן את תופעת השוק השחור מנקודת המבט של ביטחון לאומי. קיומו של "שוק שחור" למכירת אמצעי לחימה קיברנטיים, שירותי פיתוח ומיקור־חוץ גורם לכך שרמת המיומנות הטכנית הנדרשת לכניסה לתחום הפשע הקיברנטי יורדת, שכן הפושע לא נדרש להחזיק ביכולת לפתח בעצמו את כלי הפריצה ושיטות הפעולה. אותה התשתית הטכנולוגית דרושה לחדירה ושימוש בלתי מורשים למשאבי מחשב, הן אם החדירה נועדה לרווח כספי והן לחבלה.[35] כך מתגלה סיכון נוסף: השימוש בכלים הקיימים למטרות חבלה ופגיעה בתשתיות חיוניות, במקום למטרות הצפויות של הונאה לגניבה ליצירת רווח כספי מהיר, עלול לגרום לנזק ביטחוני לאומי. המשך התפתחותו של מנגנוני הפשע הקיברנטי הופכת אפוא לבעיית ביטחון לאומי. ההגנה על תשתיות חיוניות (CIP) היא הסוגיה החשובות ביותר בתחום הביטחון הקיברנטי, והשוק השחור של אמל"ח קיברנטי מחריף אותה. המסחור של יכולות טכניות ומבצעיות מאפשר לגורמים רבים, ובהם ארגוני טרור קטנים ואף יחידים, גישה למשאבים עוצמתיים, שעלולים לשמש ככלי נשק קיברנטיים. קבוצת איומי הייחוס מתרחבת אפוא מעבר למדינות וארגוני טרור המוכרים, וצריכה לכלול כל גורם שיכול להשתמש בשירותים המסחריים

שמציעים ארגוני הפשע הקיברנטי. עם זאת, בהינתן השקעה מדינתית מתמשכת במחקר ופיתוח, היכולות הטכנולוגיות שנמצאות בשוק מפגרות בהכרח אחרי הטכנולוגיה שמפתחים בזרועות הביטחון ובאקדמיה. לפי כך, היכולות שזמינות בשוק יהיו פחותות מאלה הזמינות לארגונים מדינתיים המחזיקים יכולות מחקר ופיתוח עצמאיים, ונהנים מגיבוי מדינתי במשאבים ובארגון.

לקראת מימוש אחריות המדינה לביטחון קיברנטי

חוקרים ומעצבי המדיניות זקוקים לביאור המשמעויות של התופעה. ההערכות הכספיות של נזקי הפשע – אינן מספקות בסיס מוצק להבנת התופעה ולעיצוב מדיניות. לפי כך נדרשת בחינה של סדרי העדיפויות המיטביים לאור תמונת המציאות ומגוון האילוצים והמגבלות.

גם ללא הסכמה על הערכת הנזק הישיר והעקיף שגורם הפשע הקיברנטי, הוא עדיין משפיע על תפקודם של אזרחים, עסקים והחברה. אזרחים ועסקים קטנים נפגעים באופנים שונים מפשע קיברנטי. דוא"ל זבל, הונאות אינטרנטיות, גניבת זהות דיגיטאלית, פגיעה בפרטיות, סחיטה, ריגול כלכלי ופגיעה בקניין רוחני ורכוש אינטלקטואלי – כולן תופעות נפוצות, שפוגעות מדי פעם בחלק מהאזרחים והפירמות. אף שנראה שההערכות הנזק מוטות מעלה, התפתחות המרחב הקיברנטי מגדילה את היקף הנפגעים הפוטנציאליים ומרחיבה עוד יותר את מגוון הדרכים שבהם ניתן לבצע פשעים ועבירות נגד אזרחים ופירמות. לאור המודעות העולה יחד עם התרחבות מעשי הפשע, יש להניח שהאזרחים במדינות המפותחות ידרשו שהמדינה תנקוט בפעולות על מנת לספק ביטחון אישי וקבוצתי גם במרחב הקיברנטי. החשיפה התקשורתית הגוברת של אירועי אבטחת מידע ומתקפות קיברנטיות מצביעה על עניין גובר בסכנות של פשע הקיברנטי. סביר לצפות להופעת דרישה ראשונית של אזרחים שהמדינה, על זרועותיה, תפעל לספק ביטחון לאומי ואישי – גם במרחב הקיברנטי.

המדינה, שאחראית על חוק וסדר וביטחון אזרחיה, נדרשת לפעול כדי למזער את הנזק לאזרחיה. המדיניות תתפתח מתוך הבנת המשמעויות הרחבות של התופעה, מתוך דיון ציבורי מושכל. להלן סוגיות אחדות לפיתוח דיון שכזה.

רוב התופעות הנפוצות שנכללות בפשע קיברנטי – אינן נוגעות לענייני ביטחון לאומי. מה המשמעות של הפצת שנאה ועידוד הסתה נגד היהודים או מדינת ישראל, תוך השחתת אתרי אינטרנט ישראליים, הפצת תעמולה תוך שימוש בשיטות דוא"ל זבל וחדירה לחשבונות פרטיים ברשתות החברתיות, יצירת סרטונים וקמפיינים ברשת הפוגעים ברגשות הציבור ? האזרחים עלולים לחוש בלתי מוגנים במרחב הקיברנטי, וכבוד המדינה ורבים מאזרחיה עלול להיפגע כתוצאה מעלילות. ברמה הלאומית, מעבר לתחום המקצועי של יחסי־ציבור, זהו נזק זניח.

מה המשמעות של הונאה נפוצה – גניבת זהות דיגיטאלית, ושימוש בלתי מורשה בפרטים שלף אמצעי התשלום לגניבת כספי האזרח? כאשר אזרח נופל קורבן לפשע, רשויות המדינה צריכות, נדרשות וחייבות להתייחס ולטפל בנושא. לרשות המדינה עומד מגוון רחב של דרכי טיפול מערכתיות ופרטניות, וצריך לבאר את משמעות האירועים על מנת לבחור מדיניות הולמת. אולם מבחינת הביטחון הלאומי, קשה לראות נזק ברמה הלאומית – כל עוד מדובר בשיעורי פגיעה יחסית נמוכים, גם כשאלה גבוהים משיעור התפוצה של פשע מסורתי. אם פעילות הפשיעה הקיברנטית תתגבר למתמשכת ובהיקף רחב, עצם אמון האזרחים במוסדות המדינה צפוי להיפגע עקב חוסר יכולתם לספק סביבה בטוחה.

המצב הנוכחי במדינות המפותחות אינו משביע רצון. אם "ציות תמורת הגנה" זו תמצית החוזה החברתי בין האזרחים למדינה – בתחום הפשע הקיברנטי המדינה לא ממלאת את חלקה בחוזה. המענה לאתגרים החדשים דורש קודם כל הבנה ברורה של התופעות ומשמעותן. תהליכי התגובה, יצירת המדיניות ואכיפתה – מחייבים עדכוני תקינה וחקיקה. פעולות החקיקה, שמדרך הטבע מפגרות אחר ההתפתחות הטכנולוגית, נמצאות בסמכותה הבלעדית של המדינה. זרועות האכיפה הריבוניות, הפועלות בהתאם לתשתית הלגאלית הלאומית, יידרשו להקצות יותר משאבים לתחום מניעה, חקירה וענישה של פשע קיברנטי. על אף אופיו הבינלאומי של המרחב הקיברנטי, המדינה היא הגורם הבלעדי שנושא באחריות לביטחונם האישי של אזרחיה. הסכמים בינלאומיים, כגון "אמנת בודפשט – אמנה על פשעי מחשב" של מועצת אירופה[36] והיוזמות המתנהלות באו"ם,[37] בארגון הכלכלות המפותחות[38] ובאיגוד הטלקום העולמי (ITU),[39] מגבירים את שיתוף הפעולה בין רשויות ריבוניות. שיתוף פעולה בינלאומי עשוי לסייע לרשויות ריבוניות להילחם טוב יותר בתופעה, אך לא ניתן לראות בהסכמים בינלאומיים תחליף למדיניות ריבונית עצמאית. ראשית, שיתוף פעולה בין מדינות במערכת הבינלאומית האנרכית אפשרי במידה מוגבלת בלבד, ועל סמך אינטרס משותף. ייתכן שהמדינות הדמוקראטיות המפותחות יצליחו לגבש הסדרים בינן לבין עצמן, אולם הפער בהגדרת האיום בינן למדינות הסמכותניות נראה רב מדי. הדיון האמריקאי בנושא מתמקד בריגול התעשייתי המתמשך נגד הרכוש האינטלקטואלי פרי המחקר והפיתוח של המגזר העסקי והממשלתי של ארה"ב. לאורך שנים, מתגבר החשש של גורמים בכירים בקהילה העסקית והממשלתית מפני אובדן היתרון הכלכלי והאסטרטגי של ארה"ב בעולם כמעצמה מדעית־טכנולוגית חדשנית מובילה. בעצם, "אובדן" אינו המונח הנכון, שכן הידע לא הולך לאיבוד אלא נגנב במאמץ מדיני שיטתי, מאורגן ורחב היקף של סין להזניק את עוצמתה הכלכלית והצבאית באמצעות העתקת סודות המחקר האמריקאי.[40] הדיון בנושא הזה עובר בבירור מתחומי הכלכלה, אבטחת מידע או משפטים – לשיח ביטחוני,

כמעט לוחמני.[41] סין מצדה דוחה האשמות הללו על הסף, ומודאגת מהשימוש המערבי באינטרנט, בשם ערכי חופש הביטוי – לערעור יסודות המשטר הסיני.

שנית, הסמכות והריבונות של המדינה בשטחה מאפשרת לקדם מדיניות עצמאית: חקיקת חוקים ואכיפתם אינה תלויה בהסדר בינלאומי. בישראל, האירוע המכונה "פרשת ההאקר הסעודי" מדגים יציאת הדיון מגבולות אבטחת המידע לרמה הביטחונית. בתחילת 2012 מי שהזדהה כ־0xOmar פרסם ברבים רשימת פרטים אישיים ומספרי כרטיס אשראי של אלפי אזרחים ישראלים.[42] הפרטים שפורסמו היו ברובם המכריע ישנים, ומתוך כ־380 אלף הרשומות, היו כמה אלפים של מספרי אשראי תקפים. הנזק הישיר שנגרם לבעלי הכרטיסים עומד על אפס: חברות האשראי ביטלו את הכרטיסים והנפיקו חדשים, וממילא כל שימוש בלתי מורשה בכרטיס מכוסה בידי החברות. היקף הנתונים שנחשפו גם הוא אינו חריג: מדי יום נגנבים ברשת האינטרנט מיליוני רשומות מהסוג הזה. הפרטים נארזים לפי פרמטרים שונים, ונמכרים כ"Dumps" ללקוחות בשוק השחור שתיארתי לעיל.[43]

התברר שמדובר היה בהתקפה פשוטה: הושתלה רוֹגלה spyware בכמה אתרי סחר ישראליים שהעבירה נתונים, שמפעילי האתרים הללו שמרו תוך הזנחת יסודות אבטחת המידע. על אף חוסר המורכבות, והעדר נזק ממשי לאזרחים שהמתקפה גרמה, הפרשה זכתה לכיסו תקשורתי רחב ומתמשך במשך כשלושה שבועות, שבתחילתו התאפיין בפאניקה. האירוע הוצג כטרור אנטי־ישראלי, שכן במקום לממש את הרווח הכספי מהפריצה בחר הפורץ להשתמש בו כדי לזרוע פחד בישראלים.

ניתן לנתח את האירוע במגוון דרכים: אפשר לומר שהאזרחים חסרי מודעות לאבטחה, שהתקשורת חסרת אחריות ומנפחת ענין שולי וגורמת לפאניקה, שבעלי אתרי האינטרנט התרשלו ופשעו באי־אבטחת המידע שאספו, ושהמדינה התרשלה ביצירת סביבה בטוחה למסחר אינרטנטי ולשמירה על נתונים אישיים. אולם בכל ניתוח המסקנה המתבקשת היא שדרושה הגברת ביטחונם האישי והקיבוצי של האזרחים במרחב הקיברנטי. בסופו של דבר, הדרישה מופנית למדינה, שנושאת באחריות לביטחון אזרחיה. ניתן ורצוי לדון בהגדרת התופעות הבלתי רצויות והפליליות במרחב הקיברנטי, מידת הביטחון הראויה, חלוקת האחריות והגברת מודעות המשתמשים, גבולות המעורבות הממשלתית הרצויה ובדילמות נוספות הרלוונטיות לנושא. במדינה דמוקרטית, הסוגיות הללו ילובנו במסגרת דיון ציבורי ותהליך פוליטי. אין להניח שהדרישה לביטחון במרחב הקיברנטי תיעלם, שהבעיה תיפטר מעצמה, או שהמדינה תוכל להתנער מאחריותה לביטחון אזרחיה. במקרה הישראלי האמור, אין כל מניעה שרשויות המדינה יגיבו לדרישות השונות של האזרחים ויערכו שינויים בסביבה המשפטית והרגולטורית כדי להגביר את אבטחת המידע באתרי המסחר האלקטרוני. וויתור על ניסיונות הסדרה והאכיפה במרחב

הקיברנטי יאפשר למגוון הפשע הקיברנטי להמשיך להתפתח ולשגשג, עד לרמה שזה יציב איומים של ממש לסוגיות הביטחון הלאומי: אספקת שירות לגורמים עוינים לביצוע מתקפות קיברנטיות, והגברת היקף הפשע לרמה שתערער את הביטחון האישי והסביבה העסקית במדינה.

סיכום

ממשק מסוכן: הפשע הקיברנטי כסיכון הביטחון הלאומי

הפשע הקיברנטי מתפתח ומאתגר את המדינות המפותחות באופנים שונים. המידע הקיים על מקרי הפשע הקיברנטי מגיע מהדו"חות התקופתיים של גופים העוסקים בנושא: חברות ייעוץ, מחשוב, אבטחת מידע ורשויות אכיפת חוק. לאור הבעיות המובנות בזיהוי התופעה, השימוש הגס בשיטות סטטיסטיות להשגת אומדן כמותי, והכללת הנזק העקיף בהערכות הכפסיות – המידע הקיים אינו מהימן. נראה שההערכות הכספיות מציגות הטיה קבועה להערכת יתר. אולם, אף שהערכות על היקף הפשע מוטות מעלה, לפשע הקיברנטי פוטנציאל מסוכן.

המאמר בחן את משמעות התופעה לביטחון הלאומי. הניתוח מעלה שמגוון רחב של פשיעה קיברנטית אינו מהווה סכנה לביטחון הלאומי. תופעות כמו גניבה וריגול תעשייתי, הונאה, תוכן פוגעני, פשעי שנאה, השחתת אתרים, מניעת גישה לשירות וכיו"ב – עלולות להפוך לבעיית ביטחון לאומי אם שהיקפם יעלה מאוד ופעולתם תהיה ממושכת. לכן, כבר עתה ראוי להקדיש משאבים לצמצום הסכנה ולהקשות על פעילות הפושעים הקיברנטיים.

ניסיון העבר מלמד שגורמים עוינים משתמשים בשירותים ויכולות של ארגוני הפשע, ומגייסים את מומחיותם להשגת מטרות מבצעיות. בגלל קצב ההתפתחות הטכנולוגית, יכולות המחשוב המתקדמות של היום יהפכו כעבור שנים אחדות למוצרי־מדף זולים. השוק השחור של שירותי המחשוב מנגיש את היכולות המתקדמות למגוון רחב של גורמים, ומרחיב את העדויות המצטברות על השימוש בשירותי השוק השחור האמור מגבירות את החשש שגם במרחב הקיברנטי קיים ומתפתח שיתוף הפעולה בין גורמים עבריינים לארגונים עוינים.

על יסוד הניתוח שהוצג במאמר, מוצע להתמקד בשני ממשקים מרכזיים בין הפשע הקיברנטי לביטחון הלאומי:

1. אזרחים ועסקים נפגעים לעתים באופנים שונים מפשע קיברנטי. היקף הנזק אינו ברור: הערכות הנזק הרבות שמשמות בדיון אינן אמינות ומוטות כולן כלפי מעלה. גם ללא הסכמה על היקף ומידת הפגיעה באזרחים, עסקים ומדינות, המדינה נדרשת להגיב להזדמנויות ואתגרים של המציאות המתפתחת. מדינת הלאום היא הגורם האחראי לביטחונם האישי והקיבוצי של אזרחיה. עם ההתפשטות המתמשכת של המרחב הקיברנטי לכל תחומי

החיים, יש להניח שתגברנה הדרישות כלפי המדינה לנקוט בפעולות על מנת לספק ביטחון אישי ולאומי גם במרחב הקיברנטי. על אף אופיו הבינלאומי של המרחב הקיברנטי, המדינה תיאלץ להרחיב עד מאוד את עיסוקה בביטחון הקיברנטי. קווי המתאר של המעורבות המדינתית במרחב הקיברנטי מתבהרים בשנים האחרונות, כשאחת הסוגיות הטעונות בתחום היא המתח בין ערכי הפרטיות האינדיבידואלית ולערך הביטחון הקולקטיבי. במדינה דמוקרטית, תהליך עיצוב המדיניות הממשלתית בתחום הפשע הקיברנטי יהיה כרוך בדיון ציבורי, מאבק פוליטי וטיפול משפטני ממושך.

2. ארגוני הפשע מציעים משאבים, תשתית ואף שירות ללקוחות תמורת תשלום סביר. שאפשר לנצל את השוק הזה כדי לא רק לביצוע פשע שמניעיו כספיים, אלא גם לפגיעה ישירה בביטחון הלאומי. ההגנה על תשתיות חיוניות מפני איום קיברנטי היא סוגיה מרכזית בביטחון הקיברנטי, וחשיבותה עולה לאור התפוצה של גורמי הסיכון הפוטנציאליים שיכולים לרכוש אמצעי לחימה ולגייס "לוחמים" בשוק השחור של פושעי הסייבר. המסחור של יכולות טכניות ומבצעיות מוריד את סף הכניסה לזירת הלחימה הקיברנטית, מרחיב את איומי הייחוס מעבר למדינות וארגוני טרור גדולים, ומכביד את הנטל על רשויות הביטחון הלאומיות. לאור ניתוח משמעויות התופעה וזיהוי הממשקים המסוכנים בין הפשע הקיברנטי לביטחון הלאומי שהוצגו במאמר, מומלץ למקד כבר עתה תשומת לב מדינתית בטיפול בהם על מנת למנוע החרפת האיום. אולם, המדינה אינה יכולה לפתור את הבעיה לבדה. מימוש אחריות המדינה לביטחון הקיברנטי מחייב שיתוף פעולה בין בעלי העניין במגזר העסקי, האקדמי, הציבורי והביטחוני, כדי לספק ביטחון לאומית ואישית, למדינה ולאזרחיה, במרחב הקיברנטי.

הערות

1 P. N. Grabosky, Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies, 10*(2), 2001, pp.243-249.

2 Majid Yar, *Cybercrime and society: crime and punishment in the information age*, London: Sage Publications, 2006.

3 M. Cross, D. L. Shinder, *Scene of the cybercrime*. Burlington, MA: Syngress, 2008.

4 David S. Wall, *Cybercrimes: The transformation of crime in the information age* Cambridge, Polity, 2007, p. 10.

5 Alkaabi, A., G. M. Mohay, A. J. McCullagh and A. N. Chantler. "Dealing with the problem of cybercrime," Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, October 4–6, 2010, Abu Dhabi. http://eprints.qut.edu.au/38894/1/c38894.pdf

6 Offences against the confidentiality, integrity and availability of computer data and systems

Computer-related offences
Content-related offences
CoE, "Convention on Cybercrime" Budapest, 2001 http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

7 מדובר במספר מחשבים הנגועים בתוכנה זדונית, שמאפשרת שליטה מרחוק ושימוש סמוי ביכולות המחשבים הללו. השימוש הנפוץ ביכולת הוא למשלוח דוא"ל זבל, התקפת מניעת שירות מבוזרת, וגניבה מתמשכת של מידע. ראו:
https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html

8 הרעיון להצפנה באמצעות מפתח ציבורי Public key encryption – עומד ביסוד האלגוריתם RSA, שפותח בידי
Ron Rivest, Adi Shamir, Leonard Adleman והוצג ב־1978. הפטנט עליו פג ב־2000.
התוכנה Pretty Good Privacy (PGP), המאפשרת שימוש חופשי בהצפנה חזקה באמצעות מפתח ציבורי, פותחה ב־1991.

9 Ryan, Richard M., and Edward L. Deci. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions." *Contemporary Educational Psychology*, Vol. 25, No. 1 (2000): pp. 54-67.

10 Piquero, Alexis Russell, and Stephen G. Tibbetts. *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. New York: Routledge, 2002.

11 מספר המחשבים הנגועים לבדו אינו יכול לשמש מדידה הולמת לעוצמת הרשת והנזק הפוטנציאלי
Plohmann, Daniel, Elmar Gerhards-Padilla, and Felix Leder. *Botnets: 10 Tough Questions* ENISA, 2011.

12 David S. Wall, *Cybercrimes: The transformation of crime in the information age,* p. 221.

13 ראה למשל: דו"ח GAO-07-705-Cybercrime, עמ' 16–17 , יוני 2007.
http://www.gao.gov/assets/270/262608.pdf

14 *2005 FBI Computer Crime Survey*, p.10. http://www.fbi.gov/publications/ccs2005.pdf

15 Secretary of Commerce Gary Locke (Remarks at the Washington International Trade Association, Washington, D.C., July 22, 2009).

אצל
Hathaway, Melissa E. "Falling Prey to Cybercrime: Implications for Business and the Economy." Chap. 6 in: *Securing Cyberspace: A New Domain for National Security*. Queenstown: Aspen Institute, February 2012.

16 Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica: *The Cost of Cyber Crime*, 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf

17 "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually,"
http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02

18 Lesk, M. "Cybersecurity and Economics." *IEEE Security & Privacy,* 9, no. 6 (2011), p. 76.

Carl Bialik,"A Cybercrime Stat's Nine Lives," *The Wall Street Journal*, September 26, 2007
http://blogs.wsj.com/numbersguy/a-cybercrime-stats-nine-lives-194/tab/print/

19 Florencio, Dinei, and Cormac Herley. *Sex, Lies and Cybercrime Surveys*, Microsoft Research, 2012.
המחקר הופיע כמאמר המערכת בעיתון ה־*New York Times*
Florêncio, Dinei, and Cormac Herley. "The Cybercrime Wave That Wasn't" *The New York Times*, April 15, 2012, SR5.
https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=3&hpw

20 Card Verification Value – הקוד הסודי שמודפס על הצד האחורי של הכרטיס. השימוש בו מוודא את תקפות פרטי הכרטיס במקרים שזה לא נקרא באמצעות העברת הפס המגנטי.

21 הדיון חורג מגבולות המאמר. ראה פרק על סקרים אצל:
Dane, Francis C. *Evaluating Research: Methodology for People Who Need to Read Research*. Los Angeles: Sage, 2011.

22 "דיסקים מזויפים הם כסף לטרור האיסלמי"
http://www.ynet.co.il/articles/0,7340,L-2378873,00.html

23 Hunt, J. "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them." *Information and Communications Technology Law,* Vol. 20, no. 2 (2011): pp. 133-52.

24 שב"כ, "סקירה בנושא השימוש שעושה חמא"ס בתווך התת־קרקעי ברצועה", נובמבר 2008
http://www.shabak.gov.il/publications/study/Pages/hamas-tunnel-report.aspx

25 שב"כ, "הברחות אמל"ח לרצועת עזה מאיראן דרך סודאן וסיני", מאי 2011. http://www.shabak.gov.il/publications/study/Pages/Sudan120511.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93

26 http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/ipc_272.htm

27 Kshetri, Nir. "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures." In: *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, edited by Nir Kshetri. Heidelberg; London: Springer, 2010.
Glenny, Misha. *Darkmarket: Cyberthieves, Cybercops, and You*. New York, NY: Alfred A. Knopf, 2011.

28 אפשר למיין את כלי הנשק לסוגים, לפי השימוש המיועד:
- malware – **תוֹקעה**. תוכנה זדונית שמיועדת לשבש בסתר פעילות תקינה של מערכת ממוחשבת, וכך לפגוע בתהליך שמנוהל באמצעות אותה מערכת.
- spyware – **רוֹגלה**. תוכנה זדונית שמיועדת לאסוף נתונים בסתר ולעתים להעביר אותם ברשת;
- Scanners – מוכרות לאיתור פגיעויות
- Remote and local exploits – לניצול פגיעות מוכרת
- Network Sniffers – להאזנה של תקשורת
- Backdoor tools, Trojans – לגישה מרחוק והוצאת מידע

29 ראו:
Isaac Ben Israel, Lior Tabansky, "An Interdisciplinary Look at Security Challenges

in the Information Age." *Military and Strategic Affairs* 3, No. 3, December 2011, p. 24.

30 Williams. "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues* 6, No. 2, (2001) p. 5.

31 McAfee "Virtual criminology report: Organized Crime and the Internet" December 2007. http://www.mcafee.com/us/research/criminology_report

ראו גם:

"Kaspersky reveals price list for botnet attacks," July 23, 2009, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnet-attacks נראה שמחיר השימוש ממשיך לרדת.

32 http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html

33 *Software as a Service: Strategic Backgrounder*. Washington, D.C.: Software & Information Industry Association. February 28, 2001, http://www.siia.net/estore/pubs/SSB-01.pdf

34 https://www.gartner.com/it/page.jsp?id=1963815

35 ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד" **צבא ואסטרטגיה**, כרך 3, גיליון 1, מאי 2011.

36 CoE, "Convention on Cybercrime" מאז 2001, אשררו את האמנה 30 מתוך 46 המדינות החתומות עליה.

37 T. Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities regarding Cybersecurity*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

38 OECD, "Communique on Principles for Internet Policy-Making," June 29, 2011.

39 ITU, *National Cybersecurity Strategy Guide*, September 2011.

40 McConnell, Mike, Michael Chertoff, and William Lynn. "China's Cyber Thievery Is National Policy-and Must Be Challenged " *The Wall Street Journal*, January 27 2012.

Clarke, Richard. "How China Steals Our Secrets." *The New York Times,* April 2, 2012.

Gardels, Nathan. "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly." *New Perspectives Quarterly*, 27, No. 2 (2010), pp. 15-17.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, New York: Penguin Press, 2011.

U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission.*

41 Dunn, *Securing 'the Homeland',* Op. Cit.

42 רועי גולדנברג, "בנק ישראל: נגנבו פרטי 15 אלף כרטיסי אשראי". **גלובס**, 3 בינואר 2012. http://www.globes.co.il/serve/globes/printwindow.asp?did=1000712125

43 Dump: a stolen credit card or bank accounts and the associated customer data Holt, T. J., and E. Lampke. "Exploring Stolen Data Markets Online: Products and Market Forces." *Criminal Justice Studies*, 23, No. 1 (2010).