

תוכן

3	מבוא
4	פשיעת סייבר
4	הגדרת עבירות סייבר
5	טיפוסי עבירות סייבר
8	סוגי עבירות סייבר
10	היקפי עבירות סייבר בישראל ובעולם
14	מערך הטיפול המשטרתי בעבירות סייבר
14	מערך האכיפה בפשעי סייבר בעולם
16	סקירת מערך הטיפול המשטרתי בעבירות סייבר בישראל
20	פרקטיקות מיטביות להפעלה יעילה ומקצועית של יחידות סייבר משטרתיות
23	דיון
28	סיכום
29	ביבליוגרפיה

מבוא

המהפכה של המידע והתקשורת המהווה את אחד המאפיינים המרכזיים של ה"כפר הגלובאלי" ממשיכה וצוברת תאוצה ומאפשרת הפיכת רשת האינטרנט לתשתית לסחר אלקטרוני מכל הסוגים לפרסום לאגירה וגישה למאגרי מידע בלתי מוגבלים בגודלם כמעט לנושאי תרבות פנאי ותחביבים ועוד. במקביל להתפתחויות אלו התפתחה וצברה תאוצה פשיעת הרשת. סוג פשיעה זה המשלב פריצה למערכות מחשוב גניבת ידע ושימוש לא מורשה בו לסחיטה ואיומים או למכירה בשוק השחור, מסחר באלמנטים לא חוקיים כגון נשק וסמים, פורנוגרפיה ופדופיליה והונאות רשת, תקשורת בין ארגונים פליליים, הלבנת הון ועוד. הולך וצובר תאוצה ותחכום עקב רמת הסיכון הנמוכה יחסית למול פשיעה "פיזית" והורדת המגבלה של שהייה במקום הפשע. פשיעת הסייבר בימינו חוצה גבולות ואזורים גיאוגרפיים והופכת להיות מתוחכמת ומסוכנת יותר ויותר ככל שהשימוש ברשת האינטרנט ובמחשוב הופך להיות חלק רחב יותר ויותר בחיי היום יום. עם ההתפתחות המהירה של תוכנות ויכולות פריצה, קשה ויקר יותר ויותר לפרטים ולארגונים להגן על מערכות המחשוב מפני פריצה מרחוק, שימוש פלילי וגרימת נזק או גניבת מידע. בחלק מהמקרים הנפגעים כלל אינם מודעים כי המחשב שלהם נפרץ ומשמש כ"כח מחשוב" לצורך ביצוע פריצות או גרימת נזק לרשתות מוסדיות או ארגוניות שונות. בניגוד לטרור סייבר, פושעי הסייבר פועלים בעיקר לשם רווח כספי או טובות הנאה ולא בשל הצורך להפגין את כוחם כהאקרים.

הנזקים הנגרמים מידי שנה בשל פשיעת סייבר מוערכים במיליארדים רבים של דולרים. נזקים אלו מורכבים מפגיעה פיזית והשבתת יכולות ואובדן ימי עבודה וייצור עקב פגיעה ברשת, אובדן לקוחות ואמון, צורך בהשקעות גבוהות במערכות ובכח אדם להגנה מפני מתקפות סייבר ואובדן של מידע המהווה פטנט או קניין רוחני

בעבודה זאת נבחן את נושא ההתמודדות עם פשיעת סייבר בישראל, בהשוואה למבצע במדינות שונות בעולם והאם ישראל נמצאת היום במקום המאפשר התמודדות כזאת ברמה וביעילות מספקת.

בחלקה הראשון של העבודה יובאו הגדרות לפשיעת סייבר, כולל הגדרות משפטיות והגדרות הכלולות בחוק המחשב וכן תובא סקירה של סוגי פשיעת סייבר קיימים.

חלקה השני של העבודה יציג ממצאים מהיקפי פשיעת הסייבר בישראל ובמדינות שונות בעולם תוך הצגת מספרים ונתונים על היקף התופעה ויכולות ההתמודדות כפי שהוצגו בסקרים של ארגונים רשמיים העוסקים בנושא.

בחלקה השלישי של העבודה תוצג תצורת ההתמודדות של נערכות האכיפה בעולם ובישראל בפשיעת סייבר. בסקירה לגבי מערכות אכיפה במדינות נוספות יוצגו הפרמטרים המרכזיים שגובשו ללוחמה בפשיעת סייבר והפרקטיקות המומלצות. לגבי המצב בישראל, תוצג ההתפתחות של מערך הסייבר המשטרתי וכן מה הבעיות הקיימות במערך זה במיוחד לאור ממצאי דו"ח מבקר המדינה מ 2016 בנושא.

חלקה הרביעי של העבודה יכלול דיון בממצאים השונים בכדי לענות למעשה על שאלת המחקר ובכדי לתת המלצות ותובנות לגבי המשך הדרך בהתמודדות המשטרה בישראל עם פשיעת סייבר. כמו כן יוכן פרק סיכום ומסקנות לעבודה.

המחקר הינו מחקר איכותני ומסתמך על מאמרים שונים שפורסמו בתחום הלוחמה בפשיעת סייבר וכן על דוחות מקצועיים וסקרים שנערכו על ידי ארגונים באירופה, באו"ם ובארצות הברית, המטפלים ומרכזים את נושא הלחימה בפשיעת סייבר.

שאלת המחקר הינה: האם המשטרה בישראל מתמודדת עם פשיעת הסייבר ברמה מקצועית וטכנית דומה להתמודדות הבינלאומית עם הנושא?

פשיעת סייבר

הגדרת עבירות סייבר

ההגדרה המשפטית של עבירות סייבר (מחשב) מחלקת אותן לשני סוגים מרכזיים: עבירות פליליות המבוצעות כלפי המחשב, תוכנו ואופן פעולתו התקין בניגוד לחוק המחשבים עבירות פליליות המבוצעות באמצעות מחשבים, נקראות גם עבירות פליליות "קלאסיות" חוק המחשבים (התשנ"ה-1995) מפרט שורה של עבירות פליליות אשר המכנה המשותף להן הינו תקיפה פלילית של המחשב עצמו כולל פריצה למחשב, ייצור והפצה של תוכנות זדוניות (נוזקות) ווירוסים, שיבוש עבודת המחשב, הונאה בכרטיסי חיוב (גניבת זהות או כסף באמצעות כרטיסי אשראי), הימורים מקוונים מסוגים שונים דרך האינטרנט (פוקר, בלאק-ג'ק, רמי רולטה וכדומה), החזקה והפצה של חומר תועבה במיוחד תכנים פדופילים, גניבה של מידע או רכוש או קניין רוחני באמצעות המחשב ויצירה של מידע כוזב (זיוף תעודות ציבוריות, מסמכי זהות כוזבים וכדומה).

בנוסף לעבירות אלו מוגדרות ישירות על ידי חוק המחשבים, קיימת שורה שלמה של עבירות נוספות אשר אין הבדל אם התבצעו בצורה פיזית או על ידי המחשב, מבחינת ההתייחסות הפלילית אליהן. עבירות אלו כוללות "סחיטה ואיומים, הטרדה מינית, עבירות על חוק הלבנת הון ועבירות הקשורות לביטחון המדינה והעברת מידע חסוי או סודות רשמיים. חלק מעבירות אלו הוסדר במסגרת חוק פרסום תועבה והצגתה (התשל"ז 1977) המתייחס לפרסום אלקטרוני של דברי תועבה וחוק למניעת הטרדה מינית (התשנ"ח 1998) המסדיר את נושא ההטרדות המיניות באמצעות מחשב ומדיה אלקטרונית.

יש לציין כי תפישה והחרמה של מחשבים, טאבלטים, טלפונים חכמים וציוד אלקטרוני אחר ששימש לביצוע העבירות הנ"ל, אצל אדם פרטי, אינה דורשת צו בית משפט מיוחד וניתנת לביצוע, תוך כדי חיפוש במידה וצרכי החקירה מחייבים זאת. עם זאת, תפישת הציוד מותרת