דוח מבקר המדינה | אייר התשפ"ב | מאי 2022

נושאים מערכתיים

טיפול מערכת אכיפת החוק בעבריינות במרחב המקוון

טיפול מערכת אכיפת החוק בעבריינות במרחב המקוון

רקע

בעשור האחרון גדל היקף השימוש במרשתת (אינטרנט): המחשבים, הטלפונים החכמים והכלים הטכנולוגיים האחרים המבוססים על השימוש במרשתת הפכו בישראל ובעולם לכלי העבודה והתקשורת המרכזיים ולאמצעי הבידור העיקרי בשעות הפנאי, ומאוכסן בהם מידע רב הכולל בין היתר פרטים אישיים וזיכרונות, מידע כלכלי, תעשייתי, ציבורי וממשלתי. הנגישות של המרחב המקוון והמאפיינים הייחודיים שלו, ובהם אנונימיות, נדיפות הראיות, ביזוריות המידע, יכולות הצפנה על-טריטוריאליות, אוטומטיות וכן עלויות שימוש נמוכות ונגישות למספר בלתי מוגבל של קורבנות בתוך זמן קצר, הגדילו את היקף הפשיעה והטרור המתרחשים במרחב זה והפכו אותו לכר פורה ונגיש לביצוע עבירות פליליות. תחומי פשיעה רבים עברו למרחב זה, ואף נוצרו בו איומים חדשים המאתגרים את מערכות אכיפת החוק. כל אלו חושפים את המשתמשים בכלים הטכנולוגיים ובמרשתת למגוון פגיעות וסכנות אפשריות, ובהן עבירות נגד קטינים, עבירות הונאה וגניבת מידע וממון, סחר אסור באמצעי לחימה ובסמים, תקיפת מחשבים ורשתות תקשורת ומניעת גישה אליהם, והסתה לאלימות ולפשעי שנאה (להלן - עבריינות במרחב המקוון או פשיעת סייבר). בשנים האחרונות הכריזה משטרת ישראל על ההתמודדות עם פשיעת הסייבר בתור יעד ארגוני בעל חשיבות עליונה, נוכח השינויים המתהווים בעולם הפשיעה ומגמה ברורה למעבר הפשיעה למרחב המקוון.

ביקורת זו עוסקת בעיקרה בהיערכות של המשטרה להתמודד עם תחום פשיעה מסוים - פשיעת הסייבר - ולמול פושעים המנצלים את מרחב הסייבר לפגיעה בארגונים ובפרטים, ואינה עוסקת בשימוש המשטרה בכלים טכנולוגיים במסגרת פעילותה המודיעינית והחקירתית הכוללת הנעשית למול כלל תחומי האכיפה שהיא מקיימת[1].

יודגש כי העיקרון העומד ביסוד הביקורת הוא החובה המוטלת על המשטרה להפעיל את הכלים, האמצעים והציוד שברשותה אך ורק בהתאם להוראות החקיקה המסמיכה, לפקודות ולנהלים, ולפעול על פי ההנחיות המסוימות שהיא מקבלת מגורמי הייעוץ המשפטי בתיקים השונים. על המשטרה להקפיד בהקשר זה, כי המאבק בעברייני סייבר כמו גם הפעלת סמכויותיה בתחומי המודיעין והחקירה לא ייעשו בדרכים העלולות לפגוע בזכויות היסוד של הפרט ובפרטיותו שלא כדין.

1 ביקורת בנושא זה מתוכננת לשנת העבודה הבאה.

נתוני מפתח

כ-6 טריליון דולר
סכום הערכת הנזק המצטבר שגרמה העבריינות במרחב המקוון ברחבי העולם בשנת 2020 והוא צפוי לגדול בכל שנה ולהאמיר לסך 10.5 טריליון דולר בשנת 2025

כ-87%
מנפגעי עבירות במרחב המקוון בישראל בשנת 2019 (כמאתיים אלף איש), לא דיווחו למשטרה על העבירות שבוצעו נגדם לפי סקר הלשכה המרכזית לסטטיסטיקה (הלמ"ס)

כ-250%
הוא שיעור הגידול במספר תיקי החקירה במשטרה שעניינם עבריינות במרחב המקוון בשנים 2016 - 2020 (מ-2,506 ל-8,821 תיקים)

כ-75%
מהתיקים שחקרה המשטרה על עבריינות במרחב המקוון בשנים 2018 עד 2020 נסגרו (19,253 מתוך 25,707 תיקים), ובכ-63% מהם עילת הסגירה הייתה "עבריין לא נודע" (על"ן)

בכ-90%
מתיקי החקירה שנפתחו בשנים 2018-2020 על עבריינות במרחב המקוון, לא הוגשו כתבי אישום

53%
הוא שיעור התיקים שנפתחו בפרקליטות ועסקו בפשיעה כלכלית (הלבנת הון, הונאה ומכירת פרטי כרטיסי אשראי גנובים)

304 מיליון
מספר אירועי הכופרה שהתרחשו בעולם בשנת 2020

כ-350 מיליון ש"ח
הערכת משטרת ישראל לתקציב הכולל הנדרש להקמת מערכת היתוך מידע במשטרה, להצטיידות טכנולוגית מקיפה ולהעסקת יועצי סייבר מקצועיים. תקציב זה טרם הוקצה

פעולות הביקורת

בחודשים מרץ עד אוגוסט 2021 בדק משרד מבקר המדינה את טיפול מערכת אכיפת החוק בעבריינות במרחב המקוון, לרבות בנוגע להסדרה הנורמטיבית של המאבק בזירת פשע זו ולהכשרה המקצועית של בעלי התפקידים הייעודיים. הבדיקה נעשתה במטה המשטרה, ביחידת הסייבר הארצית בלהב 433 ובמחלקי הסייבר במחוזות המשטרה. בדיקות השלמה נעשו ביחידת הסייבר הארצית בפרקליטות המדינה ובמחלקת ייעוץ וחקיקה במשרד המשפטים, במשרד לביטחון הפנים (להלן - המשרד לבט"פ) וכן במערך הסייבר הלאומי.

במסגרת הבדיקה עקב משרד מבקר המדינה אחר יישום המלצות הדוח שפורסם בשנת 2017 בנושא "התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת"[2].

הדוח שבנדון הומצא לראש הממשלה ולוועדה לענייני ביקורת המדינה של הכנסת ביום 15.2.22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו שולחן הכנסת ולא יפורסמו.

ממצאי דוח הביקורת והמלצותיו נכונים למועד המצאתו האמור לעיל.

תמונת המצב העולה מן הביקורת

- **התמודדות עם פשיעה בתחום הכופרה** - על אף הגידול בשיעור של 150% בהיקף הפשיעה בתחום הכופרה בעולם שהוערך בשנת 2020 בכ-20 מיליארד דולר, והנזק הכלכלי הכבד שנגרם למשק הישראלי, המוערך כאמור במאות מיליוני ש"ח, לא נמצא כי המשטרה גיבשה תוכנית להתמודדות עם תופעת פשיעה ייחודית זו.
- **שביעות רצון האזרחים מטיפול המשטרה מעבריינות מקוונת** - כמחצית מבין הנפגעים מעבירות במרחב המקוון שדיווחו על כך למשטרה, טענו בסקר הלמ"ס לשנת 2019 כי לא היו מרוצים מטיפול המשטרה ו-84% מהם הביעו חוסר שביעות רצונם מגישתה. בשנת 2020 השיבו 51% מהמשתתפים בסקר הלמ"ס, כי אם ייפגעו מפשיעה ברשת ידווחו על כך לגורמים חוץ-משטרתיים או לא ידווחו על כך כלל.
- **פעילות מרכז הסייבר הארצי** - מרכז הסייבר הארצי (מס"א) בלהב 433 פועל ללא מתודולוגיה מפורטת וללא ציוד טכנולוגי מתאים. מצבת כוח האדם במס"א מתבססת בעיקרה על כוח אדם המצוי בתחלופה גבוהה: שני קציני משטרה, שני סטודנטים וחמש בנות שירות לאומי.
- **המרשתת כמרחב ללא שליטה והגנה** - תמונת המצב המודיעינית לשנת 2020 העלתה כי המרשתת היא מרחב שבו אין למדינה שליטה, ובתחומו היא אינה מצליחה להגן על האינטרסים הביטחוניים והכלכליים שלה ושל תושביה, לרבות בהיבט הביטחון האישי והפרטיות.

2 מבקר המדינה, **דוח שנתי 67ב** (2017), עמ' 1851.

- **פערי שיתוף פעולה עם גופי ביטחון ומערך הסייבר הלאומי** - הגם שיש צורך מודיעיני ומבצעי במיסוד שיתוף הפעולה בין המשטרה ובין גופי מערכת הביטחון, בדגש על קהיליית המודיעין, אין ממשקי עבודה קבועים בין הגופים.

- **סגירת תיקי חקירה שעניינם עבריינות במרחב המקוון** - יותר מ-25% מ-36,009 התיקים שפתחה המשטרה בשנים 2018 עד 2020 וסווגו כ"קשורים לאינטרנט" נסגרו על הסף; 75% מיתר תיקי החקירה נסגרו, רובם (כ-63%) בעילת על"ן (משלא נמצא מי שביצע את העבירה או כשאין חשד לזהותו); הטיפול בתיקי החקירה הללו נמשך זמן קצר של עד עשרה ימים, ורוב התיקים נסגרו בתוך פחות מחודש.

- **התמודדות עם תקיפות דיגיטליות מורכבות** - הידע המקצועי הקיים כיום במשטרה משמש בעיקר לחקירת תיקי עבריינות פשוטים יחסית, ובפרט תיקים שעניינם תקיפות דיוג וסחיטה מינית ברשת, אך עלו פערים בדבר יכולת החוקרים להתמודד עם תקיפות דיגיטליות מסוימות.

- **מחסור באמצעים לתקיפה וסיכול פשיעת סייבר** - קיים מחסור ניכר בציוד בסיסי ומתקדם ביחידות הסייבר והזירה הטכנולוגית (זי"ט), שאינו עומד בהלימה עם תוכניות הרכש של המשטרה לשנים 2019 עד 2020. המחסור באמצעים האמורים פוגם ביכולת האיסוף המודיעינית ובאמצעי התקיפה לסיכול פשיעת סייבר ומקשה על החוקרים לאתר פעילות עבריינית במרחב המקוון ולהתחקות אחריה. בהיעדר אמצעים טכנולוגיים כאמור מתקשה מערך הסייבר והזי"ט למצות ראיות דיגיטליות בכלל האירועים.

- **פעילות יחידת הסייבר בפרקליטות המדינה במישור האכיפה הוולונטרי** - פעילות הפרקליטות במישור האכיפה הוולונטרי (לפיו היא פונה למפעילי אתרים הכוללים תוכן שאינו חוקי כדי להסירו) נעשית ללא הסמכה מפורשת בחוק, אלא מכוח הסמכות השיורית של הממשלה ומכוח סמכויות העזר של היועץ המשפטי לממשלה. הפרקליטות פועלת במישור זה לבקשת עובד ציבור שנפגע או גורם ממונה בהסכמת העובד, אך אינה פועלת במישור זה עבור נפגעים מקרב הציבור הרחב. בבג"ץ שפורסם באפריל 2021 הומלץ לפרקליטות לשקול יוזמת חקיקה מסדירה ומפורטת לגבי מכלול האכיפה הוולונטרית כמו שנעשה בחלק ממדינות המערב.

- **פעילות הנהלת בתי המשפט להסרת פרסומים נגד שופטים** - החל בשנת 2015 הפעילה הב"ה אכיפה וולונטרית עצמאית לשם הסרת פרסומים נגד שופטים. בשנת 2016 ביצעה הנהלת בתי המשפט (הב"ה) 97 פניות למפעילי אתרים ומספר זה ירד בהדרגה עד שבשנת 2019 בוצעו 3 פניות, ובשנת 2020 לא בוצעו פניות כלל. פעילות זו, אשר לא נכללה במפורש במסגרת הסמכות המנהלית שהוקנתה בחוק בתי המשפט למנהל בתי המשפט, עוגנה בנוהל פנימי שעודכן בדצמבר 2019 באישור היועץ המשפטי לממשלה.

- **ההסדרה החוקית של המאבק בפשיעה המקוונת** - ישנם פערים שהצטברו לאורך שנים בשל הצורך בהסדרה ובתיקוני חקיקה בתחום האכיפה כנגד פשיעת סייבר, אשר טרם עודכנו. החקיקה הקיימת אינה מספקת מענה שלם ומעשי לאיום במרחב המקוון ואינה מותאמת להתפתחות הטכנולוגית המהירה. הממצאים האמורים ממחישים את הצורך לתת כלים אפקטיביים לגורמי אכיפת החוק בפעולתם מול הפשיעה ובהסדרה חוקית עדכנית של סמכויות גופי האכיפה.

מס"א פועל כל ימות השנה בכל שעות היממה, מתפקד בתור גוף לאומי ומשרת את כלל מערכות האכיפה והביטחון. משרד מבקר המדינה מציין לחיוב את פעילותו של מס"א, על אף המחסור בכוח אדם מיומן ובאמצעים טכנולוגיים מתאימים.

עיקרי הממצאים הביקורת

- מומלץ כי חטיבת הסיגינט-סייבר באגף חקירות ומודיעין, המופקדת על בניין הכוח ועל תפיסת ההפעלה שלו, תקדם מתווה למיצוב מעמדו של מס"א במערך הסייבר המשטרתי, שיכלול הסדרה מפורטת של תפקידיו, של מתודולוגיית העבודה שלו, ושל משאבי האנוש והמשאבים החומריים הדרושים לו. זאת, במסגרת הוראות החקיקה המסמיכה, הפקודות והנהלים.

- מומלץ כי המשטרה תגבש תפיסת הפעלה עדכנית, הכוללת: עדכון המבנה הארגוני הקיים; הסדרת תשתית פעילותם של כל גופי המודיעין, החקירות והמבצעים במערך הסייבר המשטרתי, בדגש על ההיבט הטכנולוגי; אפיון ממשקי העבודה בין הגופים המשטרתיים וקביעת שיתופי הפעולה הנדרשים בינם ובין הגופים הנוגעים בדבר במרחב הממשלתי ובזירה הבין-לאומית.

- על המשטרה להטמיע את הלקחים העולים מתמונת המודיעין בתוכניות העבודה שלה כדי לצמצם את פערי האיסוף הניכרים בנוגע לעבריינות במרחב המקוון.

- מומלץ כי הוועדה המתמדת[3] תיישם את המלצות הצוות המשותף שהקימה, בדבר חיזוק שיתופי הפעולה הבין-רשותיים, ובהם גופי אכיפה וביטחון. אלו יסייעו למשטרה לשפר את יכולותיה באיסוף מידע מודיעיני, ברכישת ידע מקצועי ומיומנויות טכנולוגיות, לשם טיוב אמצעי החקירה בפענוח פשיעה ואיתור חשודים באירועי עבריינות במרחב המקוון.

- מומלץ כי משרד המשפטים יקדם הסדרה של פעילותה הוולונטרית של יחידת הסייבר בפרקליטות המדינה, יבחן דרכים לקיום ההגנה הניתנת לעובדי ציבור בצורה שווה וישקול מתן מענה גם לנפגעים מקרב הציבור הרחב למול היכולות והמשאבים הנדרשים. כן מומלץ כי פרקליטות המדינה תשקול להנגיש לכלל הציבור את שירותי האכיפה במישור הוולונטרי בשים לב לכך שתיעוד ההליכים יהיה שקוף לציבור, ויתבצע התיעדוף הנדרש בהתאם לכלים ולמשאבים העומדים לרשותה.

- מומלץ כי משרד המשפטים בשיתוף כלל הגורמים הרלוונטיים, יפעל לקדם את התיקונים הנדרשים בחקיקה הקיימת בנושא חקירת עבירות ואיסוף ראיות בזירה הטכנולוגית ובמרחב המקוון, תוך בחינת השפעתם על כלל זכויות הציבור באמצעות איזון בין צורכי מערכת אכיפת החוק ובין הזכויות המוקנות לפרט בדין.

3 ועדה מתמדת בין-ארגונית להכוונה ולתיאום של הפעילות במאבק בפשיעה החמורה והמאורגנת ובתוצריהן.

מומלץ כי המשטרה תבחן את הדרכים להשלמת הפערים הנוגעים למומחיות הנדרשת בתחומי הסייבר לביצוע משימות מודיעין, חקירות ומבצעים במסגרת הטיפול בעבריינות במרחב המקוון.

סיכום הממצאים בקשר לטיפול המשטרה בתיקי פשיעת סייבר

סיכום

בשנים האחרונות מסתמנת עלייה תלולה של מאות אחוזים בהיקף העבריינות במרחב המקוון בישראל ובעולם, הכוללת עבירות באמצעות תוכנות מחשב המסתייעות בטכנולוגיה מתקדמת לצורך ביצוע פשיעה גם במרחב הפיזי. העבריינות במרחב המקוון מסכנת את הפרט, את הציבור הרחב, את המסחר המדינתי והגלובלי ואף את ביטחון המדינה; היא עלולה לאיים על חיי אדם, על שלומם של נשים, של גברים ושל ילדים והיא פוגעת בקניינם ובפרטיותם. בשנת 2020 נאמדו נזקיה הכוללים של פשיעת הסייבר ברחבי העולם בכ-6 טריליון דולר, והם צפויים לעלות מדי שנה בשנה. האתגרים הכרוכים בטיפול בנושא מורכבים והם מחייבים, בין השאר, שיתוף פעולה רציף בין מדינות ובין ארגונים בין-לאומיים העוסקים בכך.

בישראל, המשטרה היא הגורם המרכזי המופקד על הטיפול בעבריינות במרחב המקוון. הממצאים העולים בדוח זה מלמדים, כי המערך הקיים במשטרה אינו מגובה בתפיסת הפעלה עדכנית; אינו כולל כוח אדם מיומן במקצועות הסייבר בהיקף הנדרש לצרכים; ואינו מצטייד באמצעים הטכנולוגיים הנדרשים לביצוע עבודתו בשלמותה. על פי נתונים משנת 2019, קיימת תופעה של תת-דיווח למשטרה על פגיעות מעבריינות מקוונת.

ההערכות בדבר התגברות משמעותית של הפשיעה במרחב המקוון בשנים הקרובות מחייבות את גורמי האכיפה להגביר את ההיערכות שלהן באופן שיובטח המענה האכיפתי הדרוש. מוצע כי המשטרה תרכז מאמץ הן בבניין הכוח והן בהפעלתו למאבק בעבריינות במרחב המקוון, בתמיכת המשרד לבט"פ ובהתאם להמלצות המפורטות בדוח זה. לצד האמור, על המשטרה להקפיד כי כל פעולה הנעשית באמצעים הטכנולוגיים שברשותה, לרבות פריצה למערכות מחשב פרטיות ולמכשירים סלולריים, תיעשה תוך שמירה על זכויות הפרט ובהתאם לאישורים המשפטיים הדרושים.

על הפרקליטות והב"ה לפעול להסדרה ולהסמכה של חלק מפעולות האכיפה שהן נוקטות בהן. הסדרה זו נדרשת הן משום הצורך לאזן בין צרכי מערכת אכיפת החוק ובין הזכויות המוקנות לפרט בדין והן משום שהעתיד צופן עלייה באירועי עבריינות במרחב המקוון, אשר ידרשו פעולה מתואמת ומתוכננת.

טיפול מערכת אכיפת החוק בעבריינות במרחב המקוון

מבוא

במאה העשרים ואחת הפעילות האנושית בחברות שונות ברחבי העולם מתרחשת בשני מרחבים מקבילים: במרחב הפיזי המוחשי ובמרחב הדיגיטלי המקוון[4] (להלן - המרחב המקוון). המרחב המקוון הוא מרחב וירטואלי על-טריטוריאלי המתקיים ברשתות תקשורת גלובליות ובמערכות עיבוד מחשב שבהן וביניהן מתקיימת תקשורת מקוונת. נפח הפעילות במרחב המקוון הולך וגדל עם הזמן, ובפרט בעקבות השימוש הגובר בטלפונים חכמים, והיא מקיפה כמעט את כל תחומי החיים הפרטיים והציבוריים - במקומות העבודה, בבתי המגורים, בכלי הרכב, ברחובות הערים, בעת שגרה ובעת חירום.

בעשור האחרון גדל היקף השימוש במרשתת (אינטרנט): המחשבים, הטלפונים החכמים והכלים הטכנולוגיים האחרים המבוססים על השימוש במרשתת הפכו בישראל ובעולם לכלי העבודה והתקשורת המרכזיים ולאמצעי הבידור העיקרי בשעות הפנאי, ומאוכסן בהם מידע רב הכולל בין היתר פרטים אישיים וזיכרונות, מידע כלכלי, תעשייתי, ציבורי וממשלתי.

ביולי 2021 פרסמה הלשכה המרכזית לסטטיסטיקה (להלן - הלמ"ס) את תוצאותיו של הסקר החברתי שנעשה בישראל בשנת 2020 בקרב בני 20 ומעלה[5], ולפיו 90% מהישראלים המשתייכים לקבוצת גיל זו השתמשו במרשתת, ו-86% מהם השתמשו בה באמצעות מכשיר הטלפון החכם. לשם השוואה, בשנת 2010 רק 68% מתושבי ישראל השתמשו במרשתת.

המשתמש במרשתת גולש במנועי חיפוש לאיתור מידע. המידע המאוחסן במרשתת מאונדקס[6] בשלושה רבדים מרכזיים שלכל אחד מהם רמת נגישות שונה:

1. הרשת הפתוחה (Clear Web) - מכילה מידע מאונדקס שהגישה אליו חופשית והיא נעשית באמצעות הרשתות החברתיות ומנועי חיפוש סטנדרטיים כמו גוגל. רובד זה מכיל רק כ-4% מכלל המידע המצוי במרשתת.

2. הרשת העמוקה (Deep Web) - מכילה מידע שאינו מאונדקס[7], והגישה אליו נעשית רק באמצעות הרשאות ייחודיות.

3. הרשת האפלה (Dark Web) - מכילה מידע שאינו מאונדקס, והגישה אליו מתאפשרת באמצעות תוכנות ייעודיות ומערכת מוצפנת.

4 **The Cyber Space** - המרחב הקיברנטי.

5 הלשכה המרכזית לסטטיסטיקה, הודעה לתקשורת - **לקט נתונים מתוך הסקר החברתי בנושא שימוש באינטרנט** (6.7.21).

6 מאונדקס - מסודר וממוין על פי מפתח.

7 מוסר המידע יכול למנוע את הגישה אליו ממנועי החיפוש הגלויים.

ניתן לדמות את המידע המאונדקס במרשתת לקרחון שרק חלק קטן ממנו נראה מעל פני המים וחלקו הגדול מוסתר בהם, כמתואר בתרשים שלהלן:

תרשים 1: **סוגי המידע המאונדקס במרשתת**[8]

בעשור האחרון חלה התפתחות ניכרת בכלים הטכנולוגיים, בזמינות הממשקים בין מערכות המידע השונות ובפריסת רשתות תקשורת. הקיבולת של רשתות אלה הולכת וגדלה וכך גם החיבוריות שלהן. כמו כן השתפרה נגישותו של המרחב הווירטואלי באמצעות הרשתות האלחוטיות, הטלפונים החכמים, המחשבים הנייחים והניידים והיישומונים השונים. תמורות אלו הביאו לגידול בהיקף השימוש במרשתת בתחומים רבים, ובהם המסחר, הרשתות החברתיות, תקשורת ההמונים והמידע העסקי, המדינתי והאישי ולהגברת התלות במחשבים ובמידע הממוחשב.

הנגישות של המרחב המקוון והמאפיינים הייחודיים שלו, ובהם אנונימיות, נדיפות הראיות, ביזוריות המידע, יכולות הצפנה על-טריטוריאליות, אוטומטיות וכן עלויות שימוש נמוכות ונגישות למספר בלתי מוגבל של קורבנות בתוך זמן קצר, הגדילו את היקף הפשיעה והטרור המתרחשים במרחב זה והפכו אותו לכר פורה ונגיש לביצוע עבירות פליליות (להלן - עבריינות במרחב המקוון

8 הנתונים לקוחים ממגוון פרסומים בנושא ולפיהם הרשת האפילה גדולה פי 500 (מוערך) מרשת האינטרנט הגלויה (World Wide Web). White paper: the deep web: surfacing hidden value 2001 http://quod.lib.umich.edu/cgi/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104

או פשיעת סייבר). תחומי פשיעה רבים עברו למרחב זה, ואף נוצרו בו איומים חדשים המאתגרים את מערכות אכיפת החוק. להלן בתרשים 2 מדרג העבירות במרחב המקוון[9].

תרשים 2: **מדרג העבירות במרחב המקוון בהתאם לרמת המקצועיות הנדרשת לפיענוחן**

על פי נתוני דוח הצוות המשותף (ראו להלן), בעיבוד משרד מבקר המדינה.

המסחר המקוון, הרשתות החברתיות, תקשורת ההמונים והמידע העסקי, המדינתי והאישי הפכו אטרקטיביים עבור גורמי הפשיעה כאשר המוטיבציה של חלק נכבד מהם היא רווח כספי וטובות הנאה. כל אלה חושפים את המשתמשים בכלים הטכנולוגיים ובמרשתת למגוון פגיעות וסכנות אפשריות, ובהן עבירות נגד קטינים, עבירות הונאה וגניבת מידע וממון, סחר אסור באמצעי לחימה ובסמים, תקיפת מחשבים ורשתות תקשורת ומניעת גישה אליהם, והסתה לאלימות ולפשעי שנאה.

בדוח הסיכונים הגלובליים לשנת 2021 שפרסם הפורום הכלכלי העולמי[10] נכללה פשיעת הסייבר בסיכון שהוגדר "כשל באבטחת סייבר" ודורג רביעי בחומרתו ברשימת עשרת הסיכונים

9 פירוט והרחבה של סוגי העבירות והנזקים ראו בפרקים להלן.

10 הפורום הכלכלי העולמי (World Economic Forum) הוא ארגון ללא מטרות רווח שמקיים כנסים בין-לאומיים שבהם משתתפים בכירי הפוליטיקאים, הכלכלנים, אנשי העסקים והעיתונאים כדי לדון בנושאים הבוערים בענייני רפואה, סביבה וכלכלה, והוא מנפק מפעם לפעם דוחות מקיפים הנחשבים אמת מידה בין-לאומית מהימנה.

הממשיים והמיידיים[11]. על פי הדוח האמור, התקפות סייבר עלולות להביא להתפוררות כלכלית, להפסדים פיננסיים, למתחים גיאופוליטיים ולאי-יציבות חברתית[12].

בשנת 2020 העריך המשרד לביטחון הפנים (להלן - המשרד לבט"פ) כי המעבר מפשיעה במרחב הפיזי לפשיעה במרחב המקוון הוא אחד מהאתגרים שמדינת ישראל תתמודד איתם בשנים הקרובות. בדוח שפרסמה באותה שנה הרשות לאיסור הלבנת הון ומימון טרור נכתב כי הגידול בהיקף השימוש במרשתת הביא את גורמי הפשיעה להאיץ את השימוש במרחב המקוון לביצוע פעילות עבריינית, וכי בתחומי פשיעה רבים אין עוד צורך במרחב הפיזי. עוד נכתב בדוח כי בתקופת מגפת הקורונה נוצרו פרצות במרחב המקוון שאותן ניצלו גורמי הפשיעה[13].

הגורמים המטפלים בעבריינות במרחב המקוון במשטרת ישראל: פקודת המשטרה קובעת כי תפקידי המשטרה כוללים, בין היתר, מניעת עבירות וגילוין, תפיסת עבריינים ותביעתם לדין וקיום הסדר הציבורי, ביטחון הנפש והרכוש[14]. בשנים האחרונות הכריזה המשטרה על ההתמודדות עם פשיעת הסייבר בתור יעד ארגוני בעל חשיבות עליונה, נוכח השינויים המתהווים בעולם הפשיעה ומגמה ברורה למעבר הפשיעה למרחב המקוון. בשנת 2014 הקימה המשטרה באגף חקירות ומודיעין (להלן - אח"ם) מערך לטיפול בפשיעת סייבר בהתאם לפקודת ארגון (להלן - פק"א) משנת 2013. המערך כולל יחידות מבצעיות ומטה מקצועי: ברמה הארצית - חוליית סייבר במטה הארצי, חטיבת הסיגינט סייבר במטה אח"ם, ויחידת סייבר ייעודית בלהב 433 (להלן - היחידה הארצית או יחידת הסייבר בלהב); ברמה המחוזית - מחלקי פשיעה מקוונת וזירות טכנולוגיות פורנזיות (זי"ט) שהוקמו הן במחוזות והן בתחנות.

התמודדות המשטרה עם הפעילות העבריינית במרחב המקוון נעשית על בסיס חקיקה שהתפתחה בשנות התשעים של המאה העשרים. בשנת 1995 חוקק החוק המרכזי שעוסק בטיפול בעבירות בהם מעורב מחשב, הוא חוק המחשבים, התשנ"ה-1995 (להלן - חוק המחשבים). חוק המחשבים מבקש להגן על האינטרסים הרבים שמגלם המרחב המקוון עבור החברה מפני ניצול לרעה של מרחב זה על ידי העבריין. כפי שיפורט להלן בפרק בנושא "ההסדרה החוקית של המאבק בפשיעה המקוונת", כעבור 26 שנה, אין בחוק הקיים מענה למספר ההולך וגובר של פעולות עבריניות במרשתת לצד קשת חידושים טכנולוגיים ואיומים שהתפתחו לאורך השנים במרחב המקוון, נתון שמשפיע על התמודדותה של המשטרה עם העבריינות במרחב זה.

זאת ועוד, המשטרה פועלת ליישום אמנת מועצת אירופה בדבר פשעי סייבר (להלן - אמנת בודפשט)[15]. ישראל הצטרפה לאמנה ביולי 2014 במעמד של משקיפה ובאופן מלא לאחר חתימה ואשרור בספטמבר 2016. אמנת בודפשט היא אחת מאמנות הליבה של מועצת אירופה, והיא מכוונת באופן מוצהר לטיוב הטיפול בעבירות כגון אלה: הפרת זכויות יוצרים, מרמה

11 ראו: World Economic Forum, **The Global Risks Report 2021**, 16th Edition, p. 11.

12 שם, עמ' 89.

13 הרשות לאיסור הלבנת הון ומימון טרור, **דוח שנתי 2020** (2021), עמ' 3, 39, 64.

14 סעיף 3 בפקודת המשטרה [נוסח חדש], התשל"א - 1971.

15 אמנת בודפשט היא האמנה הבין-לאומית הראשונה המתייחסת לטיפול בפשעי מחשב במרשתת על ידי תיאום בין מערכות החקיקה של המדינות החותמות, שיפור מערכי החקירה והגברת שיתוף הפעולה בין המדינות. נציגי 46 מדינות חתמו על האמנה ו-30 מדינות אשררו אותה. האמנה פתחה בשנת 2001 להצטרפות מדינות ונכנסה לתוקף בשנת 2004.

באמצעי תקשוב, חומר פורנוגרפי על ילדים, פשעי שנאה ופעולות נגד אבטחת רשת. האמנה כוללת פירוט של סמכויות והליכים, לרבות חיפוש ברשתות מחשב והאזנת סתר חוקית לרשתות מחשב. הגשמת המטרה האמורה תיעשה, על פי האמנה, בשלושה אמצעים עיקריים: תיאום בין רכיבי העבירות המהותיות במערכות החקיקה הפלילית של כל מדינה ומדינה[16]; יצירת בסיס לסמכויות בתחום סדר הדין הפלילי הדרושות לחקירה ולהעמדה לדין על כלל העבירות במרחב המקוון[17]; יצירת משטר מהיר ויעיל של שיתוף פעולה בין-לאומי, והסדרת המסגרת להפעלתו בכל שעות היממה לצורך סיוע הדדי בין המדינות החברות.

פעולות הביקורת

בחודשים מרץ עד אוגוסט 2021 בדק משרד מבקר המדינה[18] את טיפול מערכת אכיפת החוק בעבריינות במרחב המקוון, לרבות בנוגע להסדרה הנורמטיבית של המאבק בזירת פשע זו ולהכשרה המקצועית של בעלי התפקידים הייעודיים. הבדיקה נעשתה במטה המשטרה, ביחידת הסייבר בלהב ובמחלקי הסייבר במחוזות המשטרה. בדיקות השלמה נעשו ביחידת הסייבר הארצית בפרקליטות המדינה ובמחלקת ייעוץ וחקיקה במשרד המשפטים, במשרד לבט"פ וכן במערך הסייבר הלאומי (להלן - מס"ל). במסגרת הבדיקה עקב משרד מבקר המדינה אחר יישום המלצות הדוח שפורסם בשנת 2017 בנושא "התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת"[19].

ביקורת זו עוסקת בעיקרה בהיערכות של המשטרה להתמודד עם תחום פשיעה מסוים - פשיעת הסייבר - ולמול פושעים המנצלים את מרחב הסייבר לפגיעה בארגונים ובפרטים, ואינה עוסקת בשימוש המשטרה בכלים טכנולוגיים במסגרת פעילותה המודיעינית והחקירתית הכוללת הנעשית למול כלל תחומי האכיפה שהיא מקיימת.

יודגש כי העיקרון העומד ביסוד הביקורת הוא החובה המוטלת על המשטרה להפעיל את הכלים, האמצעים והציוד שברשותה אך ורק בהתאם להוראות החקיקה המסמיכה, לפקודות ולנהלים, ולפעול על פי ההנחיות המסוימות שהיא מקבלת מגורמי הייעוץ המשפטי בתיקים השונים. על המשטרה להקפיד בהקשר זה כי המאבק בעבריינים סייבר כמו גם הפעלת סמכויותיה בתחומי המודיעין והחקירה לא ייעשו בדרכים העלולות לפגוע בזכויות היסוד של הפרט ובפרטיותו שלא כדין.

16 בדגש על הגדרת העבירות הפליליות האלה: פריצות והאזנה לא-חוקית למערכות מחשב, שיבוש מידע ומערכות מחשב, שימוש לרעה במערכות מחשב, מרמה וזיוף באמצעותן, הפקה, הפצה והחזקה של חומרי תועבה שבהם מופיעים ילדים, הפרת זכויות יוצרים וזכויות נלוות להן במרחב המקוון.

17 כגון: שימור מהיר של מידע במערכות מחשב, חיפש ותפיסת מערכות מחשב, האזנת סתר חוקית לתעבורת נתונים במרשתת ועוד.

18 מבקר המדינה פרסם בשנים האחרונות כמה דוחות העוסקים בנושא הסייבר: **דוח שנתי 69ב** (2019), "היערכות גופים חיוניים להגנת סייבר"; **דוח שנתי 67ב** (2017), "התמודדות משטרת ישראל עם פשיעת סייבר מתוחכמת - נושאים חוצי ארגונים"; **דוח שנתי 67א** (2016), "היבטים בהיערכות המדינה להגנת המרחב הקיברנטי"; דוח ביקורת מיוחד, "הגנה על קטינים במרחב המקוון", פברואר 2022.

19 מבקר המדינה, **דוח שנתי 67ב** (2017)**,** עמ' 1851.

הדוח שבנדון הומצא לראש הממשלה ולוועדה לענייני ביקורת המדינה של הכנסת ביום 15.2.22 והוטל עליו חיסיון עד לדיון בוועדת המשנה של הוועדה לענייני ביקורת המדינה.

מתוקף הסמכות הנתונה למבקר המדינה בסעיף 17(ג) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] ובשים לב לנימוקי הממשלה, לאחר היוועצות עם הגופים האמונים על אבטחת המידע הביטחוני ובתאום עם יו"ר הכנסת, משלא התכנסה ועדת המשנה האמורה, הוחלט לפרסם דוח זה תוך הטלת חיסיון על חלקים ממנו. חלקים אלה לא יונחו שולחן הכנסת ולא יפורסמו.

העבריינות במרחב המקוון - מאפיינים, מגמות ונזקים

האיומים הטמונים בעבריינות במרחב המקוון נחלקים לשלושה מרחבים מרכזיים: (א) מרחב האיום על ביטחון המדינה; (ב) מרחב האיום הפלילי - איום על הביטחון הפיזי והכלכלי של האזרחים והתאגידים שפועלים במדינה שלא לתכלית פגיעה בביטחון הלאומי; (ג) האיום הפוטנציאלי - תופעות במרחב המקוון שאינן פליליות ואינן מסכנות את הביטחון הלאומי, אך יש בהן פוטנציאל עתידי לפגיעה בביטחון הפיזי וברכוש. דוח זה להלן יתמקד במרחב האיום הפלילי.

מאפייני העבריינות המקוונת במרחב האיום הפלילי

מאפייני העבריינות במרחב המקוון דומים ברובם למאפייני העבריינות במרחב הפיזי, אולם יש לה גם מאפיינים ייחודיים משלה. על פי רוב, העבריינות במרחב המקוון משלבת שימוש בכלים טכנולוגיים מתקדמים של הצפנה ואיסוף מידע ושיתופי פעולה בין עבריינים הרוכשים ומוכרים שירותי פשיעה במרשתת (ראו להלן). למעשה, כיום אפשר לבצע פעילות עבריינית במרחב המקוון ולהקשות באופן ניכר את האיתור והזיהוי של העבריינים בלא כל צורך בידע נרחב[20]. המעבר של הפשיעה ה"קלאסית" לממד החדש מאתגר את מערכת אכיפת החוק שמתמודדת עם פשיעה זו.

ההתפתחות הטכנולוגית כוללת את תחום הנכסים הווירטואליים (ראו להלן), שבבסיסו עומדת אלגוריתמיקה מתמטית מתקדמת, והמסחר בו מתבצע באמצעות נותני שירותים ייעודיים (VASP)[21] ובאמצעות מחזיקים בנכסים ברשת הפתוחה וברשת האפלה (ראו להלן). האיומים החדשים של העבריינות במרחב המקוון עלולים להתממש באמצעות ארבעה סוגים של עבירות:

עבירות נתמכות סייבר

עבירות אלה עברו מהמרחב הפיזי למרחב המקוון והן מתבצעות לרוב באמצעות המחשב, אך ניתן לבצע אותן גם בכלים טכנולוגיים אחרים. להלן דוגמאות לעבירות מסוג זה:

20 כך, למשל, כלי חינמי כמו VPN (Virtual Private Network) יוצר חיבור מאובטח בין המשתמש לבין המרשתת באופן שמעניק לו שכבת פרטיות ואנונימיות נוספת ומאפשר להסתיר את פעילותו ואת המקום שלו; דין וחשבון הצוות המשותף של הוועדה המתמדת לבחינת היבטי פשיעה במרחב המקוון (מרץ 2021) (להלן - דוח הצוות המשותף), עמ' 28.

21 Virtual Asset Service Provider - בתי עסק העוסקים בשם לקוחותיהם בסחר בנכסים וירטואליים, לרבות מטבעות וארנקים דיגיטליים.

א. הונאות המבוססות על "הנדסה חברתית"[22] ובהן הונאות דיוג (phishing)[23] לשם קבלה במרמה של נתוני אשראי ופרטים אישיים.

ב. סחר בסמים, באמצעי לחימה ובסחורה מזויפת.

ג. ביצוע עבירות הקשורות בזנות ועבירות מין נגד קטינים.

ד. סחיטה מקוונת על רקע מיני (Sextortion)[24].

עבירות מבוססות סייבר

לרוב עבירות אלה מכוונות כנגד מחשבים, רשתות או מערכות מידע ממוחשבות, ולא ניתן לבצע אותן ללא חיבור למרשתת ובלי להשתמש במחשב או בכלי טכנולוגי אחר המחובר למרשתת. כפי שיפורט להלן, זירות מסחר רבות זמינות במרחב המקוון, והן מציעות סחורות ושירותים לא חוקיים למכירה וקנייה:

22 Business CEO Fraud Schemes / Email Compromise: הונאות הכוללות מזימות שבהן עבריינים משתלטים על כתובת דואר אלקטרוני של קורבנות כדי לשלוח הוראות תשלום מזויפות למוסדות פיננסיים או לאנשי קשר עסקיים, כדי לגנוב כספים או לגרום בהונאה לכך שיועבר מידע אשר ישמש לביצוע הונאה פיננסית (מתוך אתר הרשות לאיסור הלבנת הון ומימון טרור, משרד המשפטים).

23 דיוג (Phishing): אחד האמצעים הנפוצים של הונאה המבוססת על הנדסה חברתית. מטרתו גניבת מידע באמצעות התחזות לאתר או לישות אחרת המוכרים במרשתת ושליחת הודעות במסר מיידי או בדואר אלקטרוני. המידע עשוי לכלול שמות משתמש, סיסמאות ופרטים פיננסיים. בהודעה המשתמש מתבקש ללחוץ על קישור שמעביר אותו לאתר מזויף ובו הוא מתבקש למסור פרטים אישיים שאותם מבקש המתחזה לגנוב. אמצעי הדיוג משמשים גם להחדרת תוכנות זדוניות למחשב האישי, לטלפון החכם או לכלים הטכנולוגיים האחרים וכן לפריצה לחשבונות בנק ולביצוע שוד כספי. (מתוך אתר מערך הסייבר הלאומי - כיצד תוכלו לזהות במהירות הודעת דיוג www.gov.il/he/departments/general/fishingemails, ואתר חברת check point www.checkpoint/cyber-hub/threat-prevention/what-us-phishing/).

24 איום על אדם או על קבוצה להפיץ תוכן מיני הקשור אליהם מתוך כוונה לסחיטה כספית או טובת הנאה אחרת. בתמורה לכסף או לטובת ההנאה מובטח שלא לחשוף את התוכן המיני (מתוך אתר איגוד האינטרנט הישראלי: www.isoc.org/netica/question-and-answers/online-scams/sextortion).

תרשים 3: **הסחר בשירותים בלתי חוקיים במרשתת**

* The internet organized crime threat assessment (iocta) - Europol Ec3 - מכירה והשכרה של שירותים עבריניים ברשת הגלויה, העמוקה והאפלה. בין השירותים: שירותי דיוג, כופרה ופריצה.

** Sophos - cybersecurity evolved, The state of Ransomware 2021 - www.secure2.sophos.com/en-us/content/state-of-ransomware.aspx, מערך הסייבר הלאומי - מהי מתקפת כופרה www.gov.il/he/departments/guides/prepare_for_ransomeware.

*** ארנק דיגיטלי הוא תוכנה שמותקנת על גבי מחשב, שרת מרוחק או טלפון סלולרי ונעשות בו פעולות אחסון או משיכה והעברה של מטבעות קריפטוגרפיים[25]. לכל ארנק כזה כתובת גלויה ומפתח פרטי. ביצוע פעולות בארנק מתאפשר באמצעות שימוש במפתח פרטי של המשתמש ובו רצף של 51 ספרות ואותיות.

**** המקור: משרד המשפטים.

עבירות המתבצעות באמצעות נכסים וירטואליים

החל בשנת 2009 נעשה שימוש בנכסים וירטואליים, כגון מטבעות קריפטוגרפיים לביצוע תשלומים והעברות כספיות, המנותקים משליטת מתווכי המערכת הפיננסית המסורתית של הבנקים המרכזיים וממערכת התשלומים הממשלתית. זהות המשתמשים בנכסים הווירטואליים אינה ניתנת לחשיפה, למעט באתרי ההמרה של הנכסים הווירטואליים. אף שהשימוש בנכסים וירטואליים לצורכי תשלום, השקעה והעברת ערך אינו נעשה בהכרח בניגוד לחוק, הרי

25 מטבע קריפטוגרפי הוא נכס וירטואלי שגלום בו ערך כלכלי. הוא משמש אמצעי חליפין לצורכי השקעה ומסחר ומושתת על קריפטוגרפיה (הצפנה) מורכבת. המטבע פועל על תשתית של טכנולוגיית ספרי חשבונות מבוזרים במערכת המכונה "בלוקצ'יין" הרושמת את כל העברות המטבע הקריפטוגרפי באופן אנונימי, ולעיתים גורמים עבריניים משתמשים בו לביצוע פעולות פליליות מגוונות.

שהעמימות הכרוכה בו והיותו מנותק ממתווכים מקשים על הוכחת מעורבותם של המשתמשים בסוג זה של תשלום בביצוע עבירה והופכות אותו לכלי נוח להלבנת הון אנונימית. הלבנת הון זו נעשית באמצעות המרת כספים למטבעות קריפטוגרפיים ורכישת נכסים במרחב הפיזי באמצעותם. היקף הסחר במטבעות קריפטוגרפיים נאמד ביולי 2021 בכ-2.5 עד 3 טריליון דולר[26].

עבירות המתבצעות במרחב הפיזי ומטביעות חותם ראייתי דיגיטלי

על פי מסמך שהפיץ אח"ם בנושא "הרצף החקירתי" משנת 2018, מהפכת המידע ותפוצת השימוש בטלפונים החכמים ובמרשתת הביאו לכך שעבירות רבות במרחב הפיזי כוללות שימוש באמצעי ממוחשב ואחסון נתונים בענן, דבר המותיר ראיה דיגיטלית. כך לדוגמה, עבירות אלימות, רכישה ומכירה של חומרים ממכרים וגניבה עשויות להסתייע ברכיב ממוחשב ולהטביע חותם דיגיטלי העשוי לשמש בבוא העת כראייה בהליך הפלילי. אומנם עבירות אלה נעשות במרחב הפיזי, אך בעת ביצוע חקירה הן מחייבות מיומנות טכנולוגית למיצוי הראיות הדיגיטליות ואף שיתוף פעולה בין-לאומי בשל המורכבות בביצוע החקירה בזירות שונות.

הרשת האפלה - המקור לרכישת שירותים וכלים עבריינים

המונח "הרשת האפלה" הוא שם כולל לרשתות תקשורת אנונימיות ומוצפנות המבוססות על תשתית מרשתת. רשתות אלה אומנם משתמשות ב"נתיבי התעבורה" של המרשתת, אך הן פועלות על פי פרוטוקולי תקשורת שונים. בפועל, תשתיות הרשת האפלה ואתרים ברשת האפלה משמשים כר פורה לפעילות לא חוקית ברמות חומרה שונות.

מקורות הרווח של העבריינים במרחב המקוון מבוססים על ביצוע העבירה וכן על מכירה של מידע ושל כלי פריצה לצד שלישי. אחד מהתחומים שהתפתחו ואפשרו לעבריינים נגישות לכלי פשיעה ולמידע פלילי הוא אספקת שירותי עבריינות מקוונת (Crime as a Service).

באתרים שברשת האפלה פועלות זירות סחר המיועדות לרכישה ומכירה של מידע וכלים לביצוע פשיעה כמו סחר בסחורה גנובה ומזויפת, רכישת ציוד צבאי, סחר בסמים מסוגים שונים, סחר במטבעות מזויפים, שימוש בנתוני כרטיסי אשראי גנובים, התקנת תוכנות זדוניות ואספקת שירותים פליליים, כגון חדירה למערכות מאובטחות, למחשבים אישיים ולארנקים דיגיטליים[27]. כדי לשמור על אנונימיות המסחר, התשלום מתבצע במרבית המקרים באמצעות מטבעות קריפטוגרפיים. להלן בתרשים פירוט סוגי הפעילות העבריינית המתבצעת ברשת האפלה:

26 **דוח מבקר המדינה 73ג** והאסמכתאות שם (טרם פורסם).

27 Europol - darknet: world's largest illegal dark web marketplace taken down 12 jan 2021. www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down -.

תרשים 4: **הפעילות העבריינית ברשת האפלה**

על פי נתוני 2021 Global Threat Report, 31 ;CROUDSTRIKE.COM, בעיבוד משרד מבקר המדינה.

* מונטיזציה - ניצול נכסים דיגיטליים כדי להפיק הכנסה כספית.

בעשור האחרון גדל היקף הפעילות בזירות הסחר שברשת האפלה: בשנת 2011 נרכשו בהן מוצרים ושירותים באמצעות מטבעות קריפטוגרפיים בסך כולל של 1.7 מיליון דולר; בשנת 2015 גדל סכום זה לכ-300 מיליון דולר ובשנת 2019 הוא הגיע לכ-730 מיליון דולר. בשנת 2021 היה מספר המשתמשים ברשת האפלה יותר מחצי מיליון, ובהם יותר מ-2,400 מוכרים בכ-320,000 עסקאות שבהן שולמו יותר מ-17,500 מטבעות קריפטוגרפיים מסוגים שונים[28]. על פי ממצאי דוח היורופול לשנת 2020, בשנה זו חל גידול בפשיעת סייבר המבוצעת כ"שירות" לעבריינות מקוונת[29]. להלן בלוח מקבץ מוצרים ושירותים פליליים הניתנים לרכישה ברשת האפלה:

28 Europol - darknet Darknet interactions and bitcoin - a crypto activity report (2019). מרבית המטבעות היו מסוג ביטקוין.

29 Europol, "Internet Organized Crime Threat Assessment", pp. 16 - 17; הובא במסמך של יחידת הסייבר שבפרקליטות המדינה.

לוח 1: **מוצרים ושירותים פליליים הניתנים לרכישה ברשת האפלה**[30]

המוצר או השירות	המחיר בדולר
פרטי כרטיס האשראי*	65 - 25
פרטי חשבון הבנק	120 - 40
פרטי חשבון PAYPAL	180 - 120
פרטי חשבונות הכוללים מטבעות קריפטוגרפיים	810 - 300
פרטי חשבונות ברשתות החברתיות	80 - 35
פרטי חשבונות של אתרים לצפייה ישירה בטלוויזיה	44 - 4
פרטי חשבונות דואר אלקטרוני	40
אישורים מזויפים מסוגים שונים (דרכון, תעודות זהות)	6,500 - 50
תוכנות זדוניות לחדירה למחשב	5,000 - 50
תוכנות זדוניות למטרות כופרה	750
תקיפה ומניעת פעילות של מערכות ממוחשבות ואתרי מרשתת (DDos)	1,000 - 15
תקיפת מערכות מחשב באמצעות "סוס טרויאני"[31]	300
פריצה לאתרי מרשתת והשתלטות עליהם	1,000 - 150

* יצוין כי מחיר פרטי כרטיס האשראי הישראלי הוא היקר ביותר.

נזקי העבריינות במרחב המקוון

כאמור, העבריינות במרחב המקוון כוללת עבריינות טיפוסית, ובפרט בתחומי המרמה, ההונאה וההטרדה המינית, לצד עבריינות ייחודית בתחום פשיעת הסייבר.

החל במרץ 2020, בתקופת מגפת הקורונה (בשל השהות הממושכת בבתי המגורים), גברה החשיפה הכללית של המשתמשים לאתרים לא חוקיים שבהם נעשו ניסיונות הונאה, סחר בסמים, הימורים ושימוש בנכסים וירטואליים לשם הלבנת הון. על פי דוחות של האינטרפול

30 מתוך Positive Technologies - 2018 The criminal cyber services market ptsecurity.com; privacyaffairs.com - dark web price 2021.

31 "סוס טרויאני" הוא תוכנה זדונית המתחזה לקובץ המצורף לדואר אלקטרוני, לקישור או לתוכנה, ועם התקנתה על המחשב היא מבצעת תקיפת סייבר או גורמת נזק אחר.

והיורופול לשנת 2020, בשנה זו חלה עלייה ניכרת בפשיעת סייבר. גם ה-FBI דיווח על עלייה דומה בתקופת המגפה וציין כי מספר התלונות שהוגשו לו בעניין זה גדל פי שלושה. כמו כן, לפי ניטור נתונים של חברת גוגל, בינואר 2020 סווגו 1.6 מיליון אתרי מרשתת כאתרי דיוג, ובינואר 2021 גדל מספרם ל-2.1 מיליון (עלייה של כ-31%)[32].

על אף הסכנות והאיומים הטמונים בעבריינות במרחב המקוון, קשה לאמוד במדויק את היקף נזקיה בשל הפיזור הרחב של אירועי התקיפה בתחומי המרמה, ההונאה, הסחיטה והכופרה המסתיימים בהעברת סכומי כסף לעבריינים מבלי דעת או בהסכמה כפויה, בחשיפת מידע רגיש או במניעת גישה למידע השייך הקורבן.

תופעת תת-הדיווח בנוגע למקרי הפשיעה שמתבצעים במרחב המקוון בישראל

בדצמבר 2020 פרסמה הלמ"ס את סקר הביטחון האישי לשנת 2019 שבחן את מידת ההיפגעות של תושבי ישראל מעבריינות - המדווחת והלא מדווחת למשטרה, ואת תחושת הביטחון האישי שלהם[33]. הסקר מבוצע פעם בשנה בהזמנת המשרד לבט"פ בקרב בני 20 ומעלה בלבד, והוא מסייע בתכנון מדיניות מבוססת נתונים. מנתוני הסקר עולה כי ב-2019 כ-4% מהאוכלוסייה בישראל נפגעו מעבירות במרחב המקוון.

בנובמבר 2021 פרסמה הלמ"ס את הסקר החברתי לשנת 2020, שנערך בקרב 7,249 איש בני 20 ומעלה המייצגים כ-5.7 מיליון איש בגילים אלו. מנתוני הסקר עולה כי ב-2020 - 20% מקרב האוכלוסייה בישראל (1.1 מיליון איש) נפגעו מפשיעה ברשת: 23% מבני 20-44 ו-10% מבני 65 ומעלה[34]. 49% מהמרואיינים בסקר השיבו כי אם יפלו קורבן לפשיעת רשת, ידווחו על כך למשטרה.

> מנתוני הלמ"ס עולה כי בשנת 2019 כ-87% מנפגעי עבירות במרחב המקוון (כ-195,750 איש) לא דיווחו למשטרה על העבירות שבוצעו נגדם; מרביתם ציינו את חוסר היכולת של המשטרה לטפל במקרים כאלה ואת העדפת לדווח על הפגיעה לגורם אחר. מבין אלה שדיווחו למשטרה על הפגיעה, כמחציתם ציינו שלא היו מרוצים מטיפול המשטרה ו-84% מהם הביעו חוסר שביעות רצון מגישתה[35]. בשנת 2020 השיבו 51% מהמשתתפים בסקר הלמ"ס, כי אם ייפגעו מפשיעה ברשת ידווחו על כך לגורמים חוץ-משטרתיים או לא ידווחו על כך כלל.

בתגובתה מינואר 2022 על ממצאי הביקורת כתבה המשטרה, כי זה יותר מעשור היא בוחנת את שביעות רצונו של ציבור הפונים למשטרה מגיל 18 ומעלה באמצעות "סקר השירות", שמטרתו לאתר נקודות לשיפור ולשימור בשירות המשטרתי. לאורך השנים נמצא בעקביות כי יחס השוטרים לפונה הוא הגורם המרכזי לשביעות רצון הציבור מהשירות; וכי גם כאשר הטיפול

32 Google safe browsing As published in TESSIAN Must Know Phishing Statistics 2021.

33 **סקר ביטחון אישי 2019**, פורסם ב-30.12.20.

34 לקט נתונים בנושא "פרטיות, בטיחות סייבר ופשיעה ברשת", מתוך: **הסקר החברתי 2020 - ישראל בעידן הדיגיטלי**, 23.11.21. שאלון הסקר נערך בשיתוף פעולה עם מטה ישראל דיגיטלית במשרד ראש הממשלה.

35 **סקר ביטחון אישי 2019**, תרשים מס' 1, עמ' 13, 21.

המשטרתי לא הניב את התוצאות הרצויות, הרי שהפגנת יחס מכבד ואכפתי כלפי האזרח, נכונות לעזור לו במציאת פתרון לבעייתו ועדכונו במצב הטיפול מגבירים את שביעות רצונו מהשירות. לפיכך, העלאת שביעות הרצון בקרב אזרחים שקיבלו שירות מהמשטרה תוביל בסופו של דבר להעלאת שיעורי הדיווח. כמו כן המשטרה מקדמת בשנתיים האחרונות ציר לטיפול מניעתי הבא לידי ביטוי בהגברת המודעות של אזרחים להגנה מפני עבריינות במרחב המקוון, ובכלל זה פרסומים בתקשורת, באתר המשטרה וברשתות החברתיות, הכוללים התרעות לציבור לגבי תופעות פשיעה ברשת ודרכי התמודדות עימן.

בד בבד עם מאמציה להעלות את מידת שביעות הרצון של האזרחים מיחס השוטרים כלפיהם, מומלץ כי המשטרה תפיק את הלקחים הנדרשים מהסיבות לתופעת תת-הדיווח העולות מנתוני הלמ"ס, ובפרט מהנתון ולפיו רוב נפגעי העבירות אינם מדווחים על כך למשטרה עקב חוסר היכולת שלה, לדבריהם, לטפל בעבריינות במרחב המקוון.

1. בדוח הצוות המשותף שפרסמה הוועדה המתמדת במרץ 2021[36] (להלן - דוח הצוות המשותף) צוין כי תופעת תת-הדיווח קיימת גם בקרב המגזר העסקי מחשש לפגיעה תדמיתית ופרסום שלילי, ובשל שיקולים כלכליים ובהם חשיפה לתביעות כספיות מצד לקוחות וגורמים נוספים העלולים להיפגע מתקיפת סייבר של מאגרי מידע הנוגעים אליהם.

2. בשנת 2019 דווח בעולם על גידול של כ-30% במספר ההונאות במרחב המקוון; בין היתר התרחשו בו כ-6,000 פריצות לחברות אשראי ובהן נגנבו יותר מתשעה מיליארד רשומות הכוללות פרטים אישיים. בשנת 2020 תפסו רשויות האכיפה בעולם מטבעות קריפטוגרפיים בשווי של יותר ממיליארד דולר באתרי סחר בלתי חוקיים[37].

לפי הערכות בין-לאומיות, הנזק הכלכלי המצטבר שגרמה העבריינות במרחב המקוון ברחבי העולם בשנת 2020 הסתכם בכשישה טריליון דולר - פי שניים מהנזק המוערך בשנת 2015[38], והוא צפוי לגדול בכל שנה בכ-15% ולהאמיר לסך 10.5 טריליון דולר בשנת 2025.

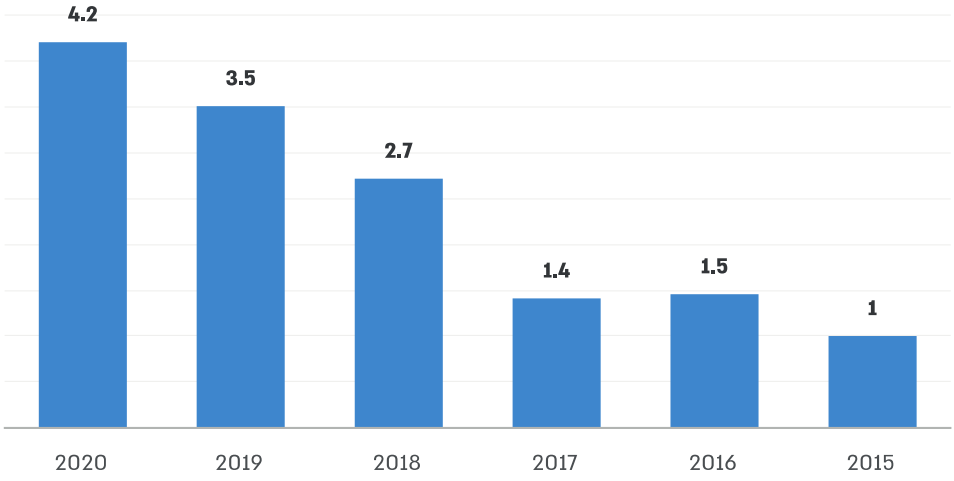
הנזק הכלכלי שדווח ל-FBI האמריקני עקב פשיעת הסייבר מתואר בתרשים שלהלן:

36 במסגרת המאבק בפשיעה החמורה והמאורגנת בישראל הוקמה בשנת 2006 ועדה מתמדת בין-ארגונית להכוונה ולתיאום של הפעילות במאבק בפשיעה החמורה והמאורגנת ובתוצריהן. הוועדה המתמדת הוכפפה לצוות בראשות ראש אגף חקירות ומודיעין במשטרה (אח"ם) וחברים בה נציגים בכירים מגופי אכיפה מרכזיים נוספים. הוועדה המתמדת הקימה צוות "שולחן עגול" בראשות ראש אגף מחקר ברשות לאיסור הלבנת הון ומימון טרור - הצוות המשותף של הוועדה המתמדת - ובו חברים נציגי המשטרה, יחידות סמך של משרדי האוצר והמשפטים ופרקליטות המדינה. במרץ 2021 פרסם הצוות המשותף של הוועדה המתמדת דוח לבחינת היבטי פשיעה במרחב המקוון; משרד המשפטים - מחלקת ייעוץ וחקיקה: "צוות העל - המלצות לחשיבה מחודשת" (29.5.18).

37 https://www.justice.gov/criminal-ccips/ccips-documents-and-reports.

38 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Headline_cybercrime_statistics_for_2019-2021.

תרשים 5: **הנזק הכלכלי שגרמה פשיעת סייבר בארה"ב, 2015 - 2020 (במיליארדי דולר)**[39]



המקור: Statista - Amount of money damage caused by reported cyber crime to the IC3 from 2001 – 2020
https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us

נתוני העבריינות במרחב המקוון בישראל

על פי מסמכי אח"ם, ארגוני הפשיעה בישראל מממנים את פעילותם במרחב הפיזי, בין היתר, באמצעות הונאת זרים במרחב המקוון, ובכלל זה משלוח הודעות דיוג וביצוע הונאות "פורקס"[40] ושימוש בנכסים וירטואליים. הלבנת ההון הבלתי חוקי נעשית אף היא באמצעות נכסים וירטואליים. תופעות של שירותי פשיעה בתשלום כמו פריצה לחשבונות ולמערכות מחשוב או נטילת מידע רגיש בעל ערך כלכלי מתוך מערכות ממוחשבות (כפי שפורטו לעיל) עלו בכמה חקירות פליליות שליוותה יחידת הסייבר בפרקליטות המדינה המטפלת בתיקים מסוג זה (ראו להלן).

כאמור, מנתוני סקר הלמ"ס עולה, כי ב-2019 כ-4% מהאוכלוסייה בישראל נפגעה מעבירות במרחב המקוון. העבירה המקוונת השכיחה ביותר הייתה התחזות או גניבת זהות ברשת (36.4%), גניבה ו/או הפצת מידע (34.2%) וכ-10% מהנשאלים דווחו כי עברו הטרדה מינית ברשת.

מנתוני המשטרה, הפרקליטות וממס"ל עולה, כי תחומי הפעילות הפלילית במרחב המקוון כאמור מגוונים וכוללים נוסף על עבירות מחשב גם עבירות בתחום ההונאה והמרמה, כדלקמן[41]:

39 המידע מבוסס על דיווחים ל-IC3, Internet Crime Complaint Center, מדור של ה-FBI.

40 Forex (Foreign Exchange) - זירת מסחר במטבע חוץ במרחב המקוון המשמשת יעד להונאת משקיעים הפעלת זירות פורקס בלתי חוקיות משמשת להלבנת כספים תוך ביצוע עבירות מס בידי ארגוני פשיעה בארץ ובעולם (להלן - פורקס).

41 הדברים הובאו בדוח הצוות המשותף.

על פי נתוני המשטרה בעשרת החודשים הראשונים בשנת 2020 חל גידול של כ-58% במספר עבירות ההונאה הקשורות למרשתת ביחס לשנת 2019. בשנת 2020 גדל מספר ההתראות על אירועי סייבר שהתקבלו במרכז המבצעי של מס"ל מאזרחים ובתי עסק ב-50% בהשוואה לשנת 2019. כמו כן, בשנים 2018 עד 2019 53% מהתיקים שנפתחו בפרקליטות עסקו בפשיעה כלכלית (הלבנת הון, הונאה ומכירת פרטי כרטיסי אשראי גנובים).

על אף האמור לעיל, אין ברשות הגופים הממלכתיים נתונים עדכניים על אודות היקף התופעה בישראל, וקיים קושי לקבל תמונת איומים אמינה וברורה.

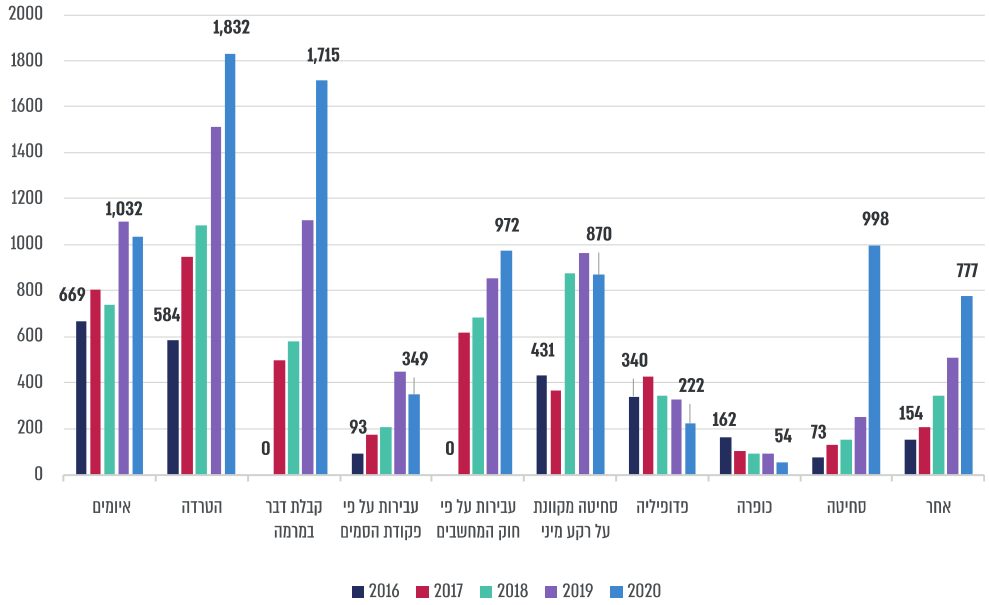
בתשובת המשטרה נכתב כי בכוונתה לוודא כי תוצא הודעת ריענון ליחידות השטח לגבי סימון תיקי עבריינות במרחב המקוון כ"קשורים לאינטרנט". כמו כן היא תבחן את האפשרות לפתח כלי ממוחשב במערכת הנתונים של תיקי החקירות במשטרה (הפל"א) שייתן התראה לחוקרים בתיקים הקשורים לתחום האמור. זאת ועוד, היא תבחן פלטפורמה מתאימה להיתוך כלל המידע המודיעיני והחקירתי בתחום העבריינות במרחב המקוון אשר יסייע למרכז הסייבר הארצי (מס"א - ראו להלן) לגבש את תמונת האיום הפלילי בנושא זה.

כאמור, בשנת 2020, עם פרוץ מגפת הקורונה, חל גידול ניכר בהיקף העבירות שהתבצעו במרחב המקוון, וגורמים עבריינים ניצלו את המשבר שנוצר לפעילות עבריינית בתחום הנכסים הווירטואליים. עוד על פי נתוני המשטרה, בשנת 2020 חלה התגברות בתחום הפשיעה המקוונת, וחל גידול של כ-20% במספר תיקי החקירה שעניינם הונאה שנפתחו במשטרה בין היתר בגין מכירת מוצרים פיקטיביים הקשורים בקורונה, שימוש בתוכנות זדוניות למטרות גניבת מידע פיננסי מהציבור, מתקפות דיוג וביצוע תרמיות מתוחכמות. כמו כן חל גידול של כ-45% במספר תיקי החקירה שעניינם עבירות מחשב ובייחוד בגין פריצות ליישומון WhatsApp ובגין סחיטה מקוונת על רקע מיני. הערכת המשטרה הייתה שמגמת פשיעה זו תתחזק גם בשנת 2021.

בתרשים שלהלן מוצגת עקומת הגידול במספר התיקים שעניינם עבריינות במרחב המקוון שנפתחו בשנים 2016 עד 2020, בחלוקה לסוגי הפשיעה הרווחת: התחזות/גניבת זהות[42]; קבלת דבר במרמה; דיוג; סחיטה מינית; תקיפת מחשב ומאגרי מידע, איומים, עבירות סמים והסתה.

42 לרבות גניבת זהות של תאגידים וזיוף חשבוניות על שם חברות קיימות.

תרשים 6: **תיקי חקירה שעניינם עבריינות במרחב המקוון, 2016-2020 (בחלוקה לסוגי הפשיעה הרווחת)**



המקור: דוחות שנתיים של מערך הסייבר הארצי שבלהב 433, משטרת ישראל.

מהתרשים עולה כי בשנים 2016 עד 2020 חל גידול של כ-250% במספר תיקי החקירה שעניינם עבריינות במרחב המקוון (מ-2,506 ל-8,821); וכי מספר התיקים שעניינם עבירות מרמה, סחיטה והטרדה גדל - פי שלושה ויותר.

את המגמות בתחום הפשיעה המקוונת בישראל בשנים 2016 - 2020, ניתן לראות בלוח שלהלן:

לוח 2: **שיעור השינוי במספר התיקים בקשר לעבירות במרחב המקוון, 2016 - 2020**

סיווג התיק	2016	2017	2018	2019	2020	מגמה	מגמת עלייה או ירידה
איומים	669	805	738	1,098	1,032		עלייה
הטרדה	584	946	1,086	1,513	1,832		עלייה
קבלת דבר במרמה	0	495	579	1,105	1,715		עלייה
עבירות על פי פקודת הסמים	93	176	209	449	349		עלייה
עבירות על פי חוק המחשבים	0	619	686	855	972		עלייה
סחיטה מקוונת על רקע מיני	431	366	875	961	870		עלייה
פדופיליה	340	426	344	329	222		ירידה
כופרה	162	104	91	89	54		ירידה
סחיטה	73	131	149	250	998		עלייה
חוק המאבק בטרור	0	236	236	159	110		עלייה
הסתה	0	0	61	88	185		עלייה
התחזות כאדם אחר	383	320	238	300	287		ירידה
אחר	154	209	343	506	777		עלייה
סך הכול	**2,889**	**4,833**	**5,635**	**7,702**	**9,403**		**עלייה**

על פי נתוני דוחות מערך הסייבר הארצי בלהב, בעיבוד משרד מבקר המדינה.

נתונים על תלונות ותיקי חקירה שעניינם עבריינות במרחב המקוון

אזרח שמבקש להגיש תלונה במשטרה עושה זאת באמצעות קישור במרשתת או באמצעות הגעה לאחת מתחנות המשטרה שבמחוזות. כדי לפתוח תיק יהיה עליו לתאר את פרטי המקרה על גבי טופס ולסמן את נושא התלונה. תיקים שעניינם עבירות במרחב המקוון מסומנים כ"קשורים לאינטרנט".

חוק סדר הדין הפלילי [נוסח חדש], התשמ"ב-1982, מקנה למשטרה את הסמכות לסגור תיקים פליליים בכפוף לעילות שונות. במקרים שבהם קצין החקירות מוצא כי יש תשתית ראייתית לביצוע עבירה פלילית, אך אין חשוד בביצוע העבירה, ולא ניתן בחקירה סבירה, בהתחשב בכלל הנסיבות, להגיע לזהות של חשוד, הוא מסווג את התיק בעילה של עבריין לא נודע (להלן - על"ן) בהתאם לסמכותו ומנמק את החלטתו[43].

43 לעיתים העבריינים הפועלים במרחב המקוון אינם מצויים בשטח ישראל, ולא מתאפשר איתור שלהם או שאין סמכות חוקית לחקור אותם, לפיכך במקרים רבים התיקים נסגרים בעילת על"ן.

1. מרכז הסייבר הארצי הפועל תחת אח"ם ביחידת הסייבר בלהב (להלן - מס"א) מבצע בחינה של נתוני התיקים שנפתחים באופן הכולל, בין היתר, תמונה יומית של הפשיעה הארצית, ניתוח תיקים, פילוח סוגי העבירות והמלצות לפעולה, והוא מעביר ליחידות השטח את הדיווחים באופן שוטף.

בשנת 2019 כתבו חטיבת הסיגינט-סייבר וחטיבת החקירות מתודולוגיה לטיפול בתופעות של עבריינות במרחב המקוון המיועדת לדרגי הפיקוד של מטה חטיבות אח"ם, מחלקי הסייבר ויחידות ההונאה ביחידות המרכזיות ובמחוזות. מתודולוגיה זו מתמקדת בסחיטה מקוונת על רקע מיני ובהונאות המבוססות על הנדסה חברתית (ראו לעיל). בהנחיות נקבע כי במקרה שהמוביל הראייתי (החשוד בעבירה) נמצא מחוץ לגבולות ישראל, יש לסגור את התיק בעילת על"ן. עלה כי מכלל התיקים שנפתחו בשנים 2018 עד 2021 נסגרו 75%, וב-63% מהם עילת הסגירה הייתה על"ן.

עוד נקבע במתודולוגיה כי על החוקר לתעד ככל הניתן את פרטי החשוד ואת פרטי ההתקשרות בינו ובין הקורבן בתיק החקירה, כדי לצמצם את תופעת סגירת התיקים ולמנוע מקרים נוספים.

בדיווח שניתן למפכ"ל בספטמבר 2020 נכתב כי מרבית תיקי החקירה בתחום ההונאה במרחב המקוון נסגרו על אף שנמצא מוביל ראייתי. כמו כן נכתב, כי נמצאו מקרים שבהם התיקים הסגורים לא נבחנו, לא בוצעה בהם בקרה על עבודת החוקר והנתונים שבידי המשטרה אינם משקפים את תמונת המצב בתחום ההונאה.

> מניתוח נתונים שנמסרו לביקורת ויפורטו להלן בפרק בנושא "חקירת העבירות במרחב המקוון" נמצא כי בשנים 2018 - 2020 נפתחו במשטרה 36,009 תיקים[44] שעניינם עבריינות במרחב המקוון ומהם נגנזו על הסף 10,302 תיקים (כ-29%). מתוך יתרת התיקים (25,707), נסגרו 19,253 תיקים (כ-75%). מתברר עוד כי מתוך התיקים שנסגרו, בכ-63% מהם עילת הסגירה היא עבריין לא נודע (על"ן).
>
> סגירת תיקים בהיקף כה רחב ראויה כשלעצמה לבחינה ומעידה שדרושות פעולות נוספות שיסייעו להביא לאיתור העבריינים ולצמצום תופעות הפשיעה במרחב המקוון, בדגש על הגברת שיתוף הפעולה הבין-לאומי עם גורמי אכיפה רלוונטיים בחו"ל. מומלץ כי המשטרה תיישם את ההנחיות לתיעוד של פרטי התיקים שנסגרו ככלל, ועל אירועים שבהם המוביל הראייתי בתיק החקירה אינו בשטח ישראל בפרט, כדי לאפשר ניתוח והפקת תובנות בזיקה למגמות הנוגעות לפשיעה במרחב המקוון וזאת בראי מגמת העלייה במספר תיקי החקירה הנפתחים למול מגמת הירידה בהגשת כתבי אישום בתיקים אלו.

2. בשנים 2018 - 2020 מספר כתבי האישום שהוגשו מכלל התיקים שנפתחו בפשיעה מקוונת עומד על ממוצע של כ-10% מהתיקים בלבד כמתואר בלוח להלן.

44 **תיקים** - תיקי חקירה מסוג פ.א., ט"מ וכללי.

לוח 3: **מספר תיקי החקירה וכתבי האישום שהוגשו בתיקים "קשורים לאינטרנט" לעומת כלל תיקי החקירה וכתבי האישום, 2018 - 2020**

שנת פתיחה	מספר תיקים "קשורים לאינטרנט"	כתבי אישום בתיקים "קשורים לאינטרנט"	שיעור כתבי אישום ביחס לכלל התיקים	מספר תיקים כולל	כתבי אישום (ללא הסדר מותנה)	שיעור כתבי אישום ביחס לכלל התיקים
2018	6,724	809	12%	320,712	46,964	14.6%
2019	9,496	905	9.5%	301,149	45,478	15.1%
2020	10,173	989	9.7%	287,127	44,015	15.3%

המקור: תמצית תמונת המודיעין לשנת 2020, מחלקת מחקר מודיעין, משטרת ישראל והשנתון הסטטיסטי של משטרת ישראל, 2018,2019 ו- 2020.

כלל הנתונים האמורים מצביעים, מחד גיסא על גידול במספר תיקי החקירה שעניינם עבריינות במרחב המקוון (כ-51%) וירידה בכמות התיקים הכלליים (כ-10%), ומאידך גיסא על מגמת עלייה בשיעור כתבי האישום בתיקים הכלליים (כ-5%) אל מול ירידה בשיעור התיקים הקשורים לאינטרנט שבהם מוגשים כתבי אישום (כ-19%).

בתגובתה על ממצאי הביקורת כתבה המשטרה כי היא פועלת במישור הפנים-ארגוני לאיתור כלים טכנולוגיים שיסייעו בהתמודדות עם עבריינות במרחב המקוון. כמו כן היא פועלת באמצעות מס"א ליצירת קשר עם משטרות בעולם לשם קידום הטיפול בתיקי חקירת עבריינות במרחב המקוון.

סגירת תיקים בהיקפים של כ-75% ומיעוט הגשת כתבי אישום לעומת מספר התיקים שנפתחו עשויים להצביע על האתגרים העומדים לפני המשטרה בטיפול בתיקים אלו ועל יכולתה המוגבלת לתת מענה מיטבי לציבור הישראלי בתחומי פשיעה זו. מומלץ כי המשטרה תבחן ותנתח את מכלול הנתונים האמורים לצורך הערכת הצמיחה העתידית הצפויה, מיפוי הפערים ביכולת לספק מענה, גיבוש תפיסת הפעלה להתמודדות עם נתונים אלה, והכנת תוכנית עבודה לצמצום פערים שתכלול את הגברת שיתוף הפעולה הבין-לאומי. פעילות בדרך זו תתרום להעלאת אמון הציבור במשטרה שעשוי להשתקף בהגברת הנכונות לדווח לה על היחשפות לעבריינות במרחב המקוון.

אירועי כופרה

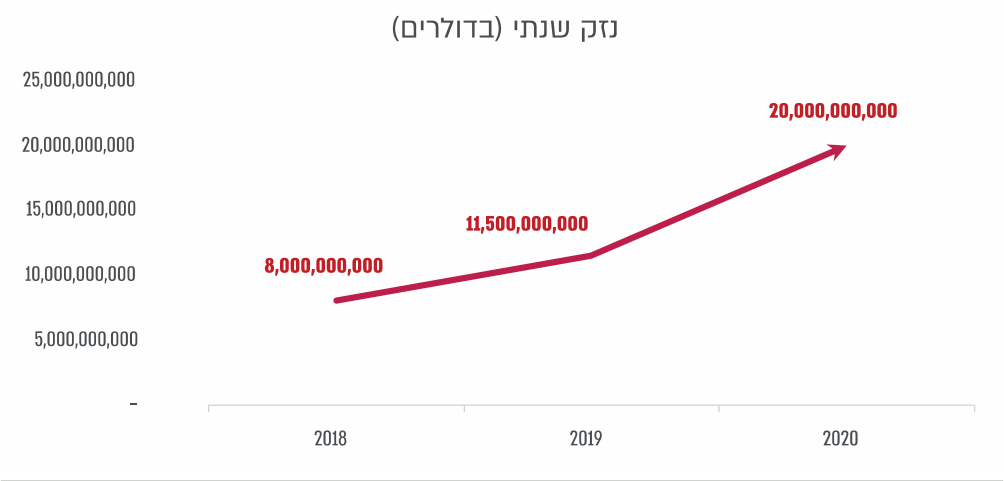
דוגמה לתיקי חקירה שעניינם עבירה הגורמת לנזקים כלכליים כבדים בישראל הם תיקי הכופרה, הנסגרים ברובם בעילת על"ן. במקרים אלה כאמור, העבריין חודר למערכת מחשב, מצפין את המידע ומבקש תשלום כספי - כופר - בתמורה לשחרורו.

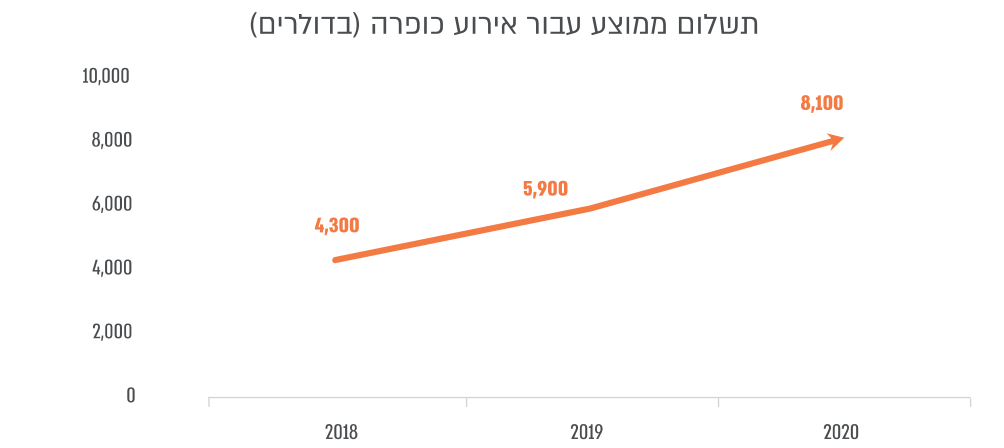
על פי ניתוח נתונים עולמי, בשנת 2017 אירעו בעולם כ-184 מיליון אירועי כופרה; בשנת 2018 גדל מספרם לכ-204 מיליון; ובשנת 2020 הוא הגיע לכ-304 מיליון[45].

מהנתונים בעולם עולה כי מספר אירועי הכופרה והנזק המצטבר שגורמים אירועים אלה גדלים משנה לשנה, ובשנים 2018 עד 2020 גדל מספר האירועים כמעט פי 1.5, והיקפם הכספי הכולל עלה מ-8 מיליארד דולר ל-20 מיליארד, כמתואר בתרשימים שלהלן.

45 ראו: Statista - Annual number of ransomware attacks worldwide 2016-2020

תרשים 7: **נתונים על נזקי אירועי כופרה בעולם, 2018 - 2020**





המקור: The growing threat of ransomware
.http://purplesec.us/resources/cyber-security-statistics/ransomware/

בסקר בין-לאומי נוסף שנעשה בינואר 2021 ובו השתתפו יותר מ-5,400 מומחי טכנולוגיות מידע מהעולם, ובהם 100 ישראלים, נבדק היקף התופעה של תקיפות כופרה בחברות פרטיות בשנים 2017 עד 2021. הממצאים העלו כי 54% מבתי העסק שהשתתפו בסקר נפגעו מתקיפות כופרה, וכי 96% מהם שילמו כופר בסך מיליוני דולר. עוד עולה מהממצאים כי בקרב המשתתפים בסקר שיעור בתי העסק שנפגעו מאירועי כופרה הוא 37% בממוצע, ובישראל 49%[46].

46 הנתונים נלקחו ממאמר שפורסם באפריל 2021, Sophos - cybersecurity evolved, The state of Ransomware 2021.

לפי סקר שנעשה בישראל ב-2017, והובא במסמך ניתוח מצב שפרסם מס"ל ביוני 2020, מבין 570,000 בתי עסק בישראל 13% (74,100) נפגעו מאירוע סייבר, ומהם כ-0.9% (667) היו אירועי כופרה. בסקר נוסף שנעשה בישראל ב-2020 מספר אירועי הכופרה נותר דומה.

מנתוני הסקר עולה כי כמעט אחד מכל מאה בתי עסק בישראל שנפגעו נחשף לאירוע כופרה ועם הזמן נפגעים מאירועי כופרה עוד ועוד בתי עסק גדולים ובהם מאות עובדים. על פי התחשיב הכלכלי שפורסם בסקר, הנזק למשק הישראלי כתוצאה מאירועי כופרה נאמד בסך כ-333 מיליון ש"ח בשנה[47].

במצגת שהציגה חטיבת הסיגינט סייבר לראש להב 433 בנושא האתגרים המרכזיים בנוגע לאירועי כופרה צוין כי בשנים 2018 - 2020 נפתחו במשטרה 115 תיקי חקירה בלבד בגין אירועי כופרה ועל פי האמור במצגת "רוב התיקים נגנזו בעילת על"ן או חוסר עניין לציבור".

השוואה של נתונים אלה לנתונים העולים מהסקרים שנעשו בארץ ובעולם בקשר לאירועי כופרה מעידה שמספר הדיווחים של אזרחים או בתי עסק בישראל למשטרה על אירועי כופרה הוא קטן ושולי לעומת מספרם ההולך וגדל בפועל. לאור הגידול הנרחב בעבירות אלה בשנים האחרונות ובהינתן תופעת תת-הדיווח למשטרה כאמור, ניתן להעריך כי שיעור הנפגעים בשנת 2021 אף גבוה מהמתואר לעיל.

במסגרת ההצגה לראש להב 433 מינואר 2021 נעשתה הערכה בנוגע לאירועי הכופרה והסחיטה, וניתנו המלצות ראשוניות לטיפול בתופעה ובהן הקמת קבוצות עבודה, תיעדוף משאבי והקמת מאגר טכנו-מודיעיני במס"א.

על אף הגידול בשיעור של 150% בהיקף הפשיעה בתחום הכופרה בעולם שהוערך בשנת 2020 בכ-20 מיליארד דולר, והנזק הכלכלי הכבד שנגרם למשק הישראלי, המוערך כאמור במאות מיליוני ש"ח, לא נמצא כי המשטרה גיבשה תוכנית להתמודדות עם תופעת פשיעה ייחודית זו.

בתגובת המשטרה על ממצאי הביקורת נכתב כי באירוע כופרה מאוקטובר 2021, שבו הותקף בית חולים בישראל, התקיים שיתוף פעולה בין המשטרה לבין מס"ל וצה"ל, בתיאום עם גורמי אכיפה בין-לאומיים. על בסיס אירוע זה עתיד להתגבש מתווה לאומי לטיפול באירועי כופרה על ידי המערכים הנוגעים בדבר.

מוצע כי המשטרה תרכז מאמץ לשיפור יכולותיה בתחום זה כדי לתת מענה הולם לאירועי הכופרה שהציבור נפגע מהם. מתן מענה הולם לנושא זה ישפיע גם על אמון הציבור בעבודת המשטרה בתחום הפשיעה במרחב המקוון.

47 נתונים אלה אינם כוללים את נזקי הכופרה שנגרמו לאזרחים פרטיים ולבתי עסק כתוצאה מפשיעת סייבר אך הם לא דיווחו עליהם.

בתגובתה האמורה מינואר 2022 הודיעה המשטרה כי בימים אלה מקיים ראש חטיבת הסייבר עבודת מטה בשיתוף יחידת הסייבר הארצית, שמטרתה לגבש תפיסת הפעלה משטרתית להתמודדות עם אירועי כופרה.

גופי ממשל בישראל המעורבים בהגנה על מרחב הסייבר

1. **מערך הסייבר הלאומי (מס"ל):** אירועי התקיפה במרחב הסייבר על ארגונים, על מוסדות שלטון ועל גופים המספקים שירותים חיוניים לציבור, מהווים איום אסטרטגי על ביטחון המדינה. את ההגנה מפני איומים אלה מספקים מס"ל וגופים שונים בקהיליית המודיעין. מס"ל הוא גוף ממלכתי שהוקם מכוח החלטות ממשלה משנת 2015, אשר משימתו העיקרית היא להגן על מרחב הסייבר הלאומי ולפעול להעלאת חוסנו על ידי ניהול אירועי סייבר והתמודדות עימם ברמה הלאומית[48]. פעילות מס"ל מבוססת על תחום טכנולוגיות המידע, תוך ביצוע פעולות ביטחוניות, אופרטיביות ורגולטוריות שתכליתן למנוע מהאיום להתממש[49]. במסגרת זו מס"ל מפעיל את המרכז הארצי לניהול אירועי סייבר (CERT) עבור כלל הגופים במשק, ובו מוקד טלפוני ייעודי לקבלת תלונות על אירועים כאמור. מס"ל משתף פעולה עם המשטרה במשק שבין תחומי האחריות של הגופים.

   בהתייחסות מס"ל מינואר 2022 נכתב כי הוא אינו גוף הנמנה עם גורמי אכיפת החוק ואינו אמון על הגנה מפני פשיעה במרחב המקוון. מרבית עיסוקו הוא ברובד המידע הטכנולוגי ולא ברובד התוכן הגלוי במרחב המקוון.

2. **משרד המשפטים:** (א) פרקליטות המדינה - בשנת 2015 הוקמה בפרקליטות המדינה יחידה ארצית שנועדה לגבש את מדיניות התביעה בנוגע להגשת כתבי אישום בגין עבירות שהתבצעו במרחב המקוון, ולרכז את המאבק בעבריינות במרחב המקוון בכלל היבטיו; (ב) הרשות להגנת הפרטיות - הגוף המאסדר את זכות היסוד לפרטיות ולהגנת מידע אישי, לרבות נתונים צבורים במאגרי מידע דיגיטליים, ואוכף את חוק הגנת הפרטיות, התשמ"א-1981, ואת חוק חתימה אלקטרונית, התשס"א-2001; (ג) הרשות לאיסור הלבנת הון ולמימון טרור - מופקדת, בין היתר, על איסוף מודיעין פיננסי ועל סיוע לגופי האכיפה והביטחון בישראל במניעה, באיתור ובחקירה של עבירות הלבנת הון, עבירות מקור[50] ומימון טרור; וכן באסדרה של גופים פיננסיים במשק מכוח חוק איסור הלבנת הון, התש"ס-2000, ובמאבק כלכלי בארגוני טרור בשיתוף גופים עמיתים בחו"ל.

גופי ממשל נוספים עוסקים בעקיפין בהגנה מפני תקיפות סייבר, ובהם רשות המיסים הפועלת במישור האזרחי והפלילי לשם גביית מיסים, ישירים ועקיפים, לרבות מיסים המוטלים על עסקאות שמתבצעות באמצעות נכסים וירטואליים ומיסים על הכנסות לא חוקיות; רשות שוק ההון, ביטוח וחיסכון, המפקחת על נותני השירותים הפיננסיים בין השאר בקשר לחובות על פי חוק ועל מתן רישיונות והיתרים לנותני שירותים פיננסיים ובהם נותני שירותים בנכסים

48 החלטות ממשלה מס' 2443 ו-2444, 15.2.15.

49 תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018.

50 עבירות שנקבעו באופן ייחודי ופורטו בתוספת הראשונה לחוק איסור הלבנת הון, התש"ס-2000.

וירטואליים; וגופי ביטחון שונים הפועלים בתחומי אחריותם לסיכול פעולות טרור ולשמירה על ביטחון המדינה.

תרשים 8: **פריסת גופי האכיפה המעורבים במאבק במרחב המקוון**

טיפול המשטרה בעבריינות במרחב המקוון

היערכות המשטרה למאבק בפשיעה במרחב המקוון

על פי הערכת המצב לשנת 2021 שקיים סגל הפיקוד הכללי, אחד מחמשת האיומים העיקריים שעימם צריכה המשטרה להתמודד הוא פשיעת הסייבר. תוכנית עוצמ"ה[51] שפיתחה מחלקת אסטרטגיה באגף התכנון של המשטרה (להלן - אג"ת) בעקבות הערכת המצב האמורה קבעה שהמיקוד האסטרטגי של המשטרה יכלול האצה טכנולוגית בשאיפה להשגת עליונות טכנולוגית על גורמי הפשיעה במרחב המקוון, שמשמעה בהקשר זה: תשתיות טכנולוגיות - הגנת תשתיות, אבטחת מידע והיערכות לקליטת מסת מידע; לחימה בפשיעה - זיהוי טכנולוגיות חדשניות והטמעתן במשטרה בטווחי זמן קצרים, שימוש באנליטיקה לקבלת החלטות מושכלות, פיתוח כלי בינה מלאכותית והרחבתם, שימוש באמצעים מתקדמים והצמחת יוזמות מקומיות, הרחבת הכישורים הטכנולוגיים של שוטרי השטח וחיזוקם; ושירות דיגיטלי - גיבוש תפיסת שירות ארגונית, הרחבה ומיצוי של אמצעי השירות המקוון לאזרח, שירות מותאם אוכלוסיות ומתן הסברה לאזרח.

בדוח משנת 2017 העיר מבקר המדינה כי הגידול הניכר בעבירות המתבצעות במרחב המקוון ובנזקיהן והתעצמות היכולות הטכנולוגיות שמשמשות את העבריינים, מדגישים את חובתה של המשטרה להקים מערך מקצועי שיבטיח טיפול יעיל בפשיעת הסייבר המתוחכמת טכנולוגית וייתן מענה למאפייני פשיעה זו. משרד מבקר המדינה בחן את החלטות המשטרה לאורך השנים בקשר למיקומו במדרג הארגוני ולסמכויותיו של המערך לחקירת עבירות מחשב ומיצוי ראיות ממחשב במשטרה (להלן - מערך הסייבר והזי"ט) ולהלן הממצאים.

תפיסת ההפעלה של מערך הסייבר והזי"ט

המאבק בעבריינות במרחב המקוון הצריך את היערכותה האסטרטגית של המשטרה בהיבטי גיבוש מתודולוגיה סדורה, טכנולוגיה עדכנית וכוח אדם ייעודי - לפי תפיסת הפעלה ארגונית כוללת. בשנת 2017 החליט פיקוד אח"ם על מבנה ארגוני חדש, ולפיו הוקם מטה מקצועי שאחראי לבניין הכוח המשטרתי העוסק במאבק בעבריינות במרחב המקוון ולהתעצמות מערך הסייבר והטכנולוגיה על פי כמה עקרונות מנחים שנקבעו. זאת, לצד מערך השטח הביצועי שכולל את יחידות המשטרה, את התחנות במחוזות ברחבי הארץ ואת יחידת הסייבר בלהב.

ביולי 2019 פרסם אח"ם נוהל מעודכן העוסק בנושא "הפעלת המערך לחקירת עבירות מחשב ומיצוי ראויות ממחשב". הנוהל הגדיר את אלה: מיהות עובדי מערך הסייבר המשטרתי, ייעוד מערך עבירות המחשב ותחומי האחריות של כל אחת מהיחידות במבנה הארגוני של המערך. לפי הנוהל מערך הסייבר והזי"ט פרוס בשטח לפי המדרג הזה: (א) יחידות ארציות בלהב 433;

51 ערכים וממלכתיות, ציבור, מקצועיות, האצה טכנולוגית.

(ב) יחידות מחוזיות - מחלקי סייבר; (ג) תחנות המשטרה - משרדי זי"ט. בתרשים שלהלן פירוט המבנה הארגוני העדכני של מערך הסייבר והזי"ט, ותחומי האחריות במערך.

תרשים 9: **מבנה ותחומי האחריות במערך הסייבר והזי"ט**

על פי נתוני אח"ם, בעיבוד משרד מבקר המדינה.

1. התפיסה שעמדה ביסוד המבנה הארגוני משנת 2017 נועדה, בין היתר, לאפשר למחלקי הסייבר במחוזות להתפנות לטיפול בעבירות המחשב באמצעות העברתם לפיקוד היחידה המרכזית (ימ"ר) בכל מחוז, חלף כפיפותם ליחידת חקירות ההונאה במחוז. בלוח שלהלן התפלגות תיקי חקירת העבריינות במרחב המקוון שנפתחו בשנת 2020 בכל אחד ממחוזות המשטרה.

לוח 4: **תיקי חקירה שעניינם עבריינות במרחב המקוון שנפתחו בשנת 2020 בכל אחד מהמחוזות**

המחוז	מספר תיקי החקירה שנפתחו
דרום	1,564
חוף	1,057
ירושלים וש"י	1,628
מרכז	2,065
צפון	1,340
תל אביב	2,101

על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

על פי הנתונים בלוח קיים פער של כ-50% במספר התיקים שנפתחו בעבירות במרחב המקוון בין מחוז חוף, המחוז שבו נפתח מספר התיקים הקטן ביותר, ובין מחוז תל אביב, שבו נפתח מספר התיקים הגדול ביותר.

הנתונים מצביעים על שונות ניכרת במספר התיקים שנפתחו בשנת 2020 בכל אחד מהמחוזות.

על פי תפיסת ההפעלה של המשטרה, העבריינות במרחב המקוון מתרחשת בזירה על-טריטוריאלית. נוכח העומס ההולך וגובר על קציני החקירות בתחנות וביחידות ברחבי הארץ, ישנה חשיבות בבחינה וניתוח של הנתונים האמורים ושל הסיבות לשונות הקיימת בין המחוזות. משום כך, מומלץ שאח"ם יבחן את עומסי העבודה במחלקי הסייבר במחוזות השונים, כדי לטייב את דרך הטיפול בתיקים ולהביא למיצוי חקירתי.

2. מחלקי הסייבר במחוזות כפופים פיקודית למפקדי המחוזות, ומהבחינה המקצועית הם כפופים לשתי חטיבות באח"ם - לחטיבת חקירות ולחטיבת הסיגינט-סייבר, והם מבוקרים על ידן בהתאמה. ממסמכי מחוזות המשטרה עולה כי תיקי חקירה מנותבים למחלקי הסייבר באופן מבוזר, והם מגיעים אליהם מחמישה מקורות שונים: יחידות המחוז השונות; האח"ם המחוזי; מוקד הסייבר הארצי; היחידה הארצית; ניטור תיקים עיתי של ראש המחלק.

על אף האמור בנוהל אח"ם לעיל בנוגע לתפקידי מחלקי הסייבר במחוזות, ראשי המחלקים דיווחו בפגישות פנימיות כי עיקר העבודה נעשית בתחום מיצוי הראיות הדיגיטליות לצורך חקירת תיקי עבירה כלליים במרחב הפיזי ולא בחקירת תיקי פשיעת סייבר. על השוטרים במחלקי הסייבר מוטלות משימות מחוזיות, ובפרט משימות כלליות המוטלות על הימ"ר, שאינן נוגעות כלל לעבריינות במרחב המקוון. ככלל, יכולותיהם הטכנולוגיות של המחלקים

דלה, ומידת המומחיות של השוטרים המועסקים בהם אינה עולה על רמת ההכשרה הבסיסית, הגם שהטיפול בתיקי פשיעת הסייבר מצריך זאת. בנסיבות אלה המחלקים אינם כשירים על פי רוב לטפל בתיקי עבירות מחשב וחומר מחשב, אלא בעיקר בתיקי עבירות שבוצעו באמצעי תקשוב דיגיטליים, לרבות מרמה והונאה.

יצוין כי בסיכום דיון שהיה בפברואר 2020 בפורום ראשי מחלקי הסייבר במחוזות נכתב כי יש "שעטנז של המחלקים בכפיפות הפיקודית והמקצועית. לא ברור מי עושה מה, גם ברמת המטה".

בשנת 2020 הניע אח"ם עבודת מטה בתחום החקירות והמודיעין בעבירות מרמה והונאה עקב כשלים שנמצאו בטיפול בתלונות בנושא זה (להלן - עמ"ט הונאה). אחת המסקנות שסוכמו במסגרת עמ"ט הונאה נוגעת לארגון מחדש של מערך הסייבר והזי"ט מטעמים אלה: חוסר אחידות בין מחוזות; תת-דיווח בעבירות הונאה במרשתת; טיפול לא יעיל ומיושן; היעדר מענה מקוון לתלונות; היעדר בסיס נתונים אחיד ויכולת ניתוח מידע; פער מקצועי של חוקרי אח"ם; חולשה של כלל היחידות באיתור תופעות פשיעת סייבר בזמן אמת; היעדר טכנולוגיה לאיתור תופעות פשיעת סייבר; יחידות ההונאה המחוזיות מתמקדות בתיקים העוסקים בפרשיות בעלות היקף חקירה גדול על חשבון תיקים בעלי היקף מצומצם יותר.

בדיון בראשות המפכ"ל שהתקיים במאי 2021 התקבלה החלטה פיקודית לרכז את הטיפול בפשיעת הונאה ובפשיעה המקוונת במחוזות ולהקים שלוחות הונאה במרחבים. נוסף על כך הוחלט על הכפפת כלל מחלקי הסייבר לאח"ם המחוזי ולראשי ענפי החקירות (רענ"ח) במחוזות, כמפורט בתרשים שלהלן:

תרשים 10: **הכפיפות הפיקודית של יחידות הסייבר במחוזות החל ב-1.9.21**

על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

עבודת המטה שנעשתה באח"ם בשנת 2020 חשפה חולשות יסודיות בעבודת מערך הסייבר והזי"ט המשפיעות על מידת המועילות של הטיפול הקיים בעבריינות במרחב המקוון, בדגש על היקפה של פשיעת הסייבר הגדלה מדי שנה בשנה. בהחלטת המפכ"ל ממאי 2021 לא ניתן מענה שלם לחולשות שהוצגו בעבודת המטה.

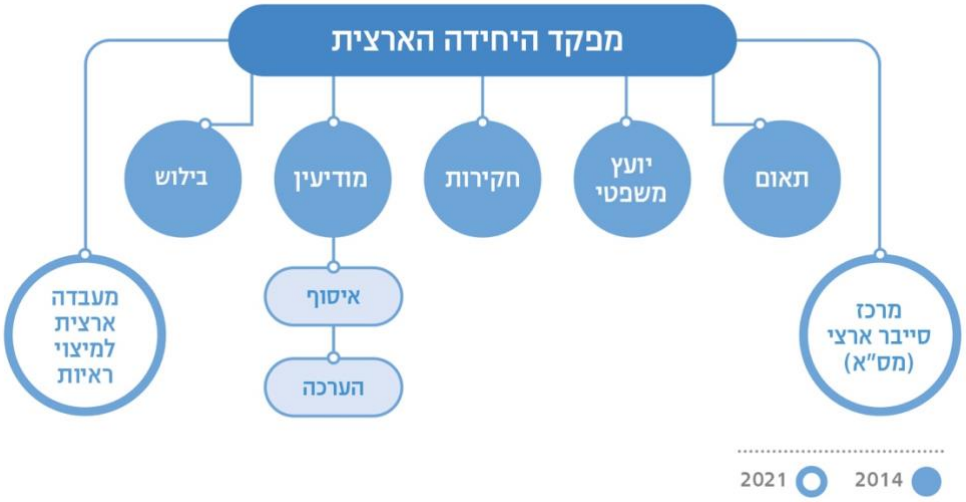
במציאות שבה קיימות חולשות בעבודת מערך הסייבר, כפי שעלה בעבודת המטה, נדרשת קבלת החלטות שיהיה בהן כדי לחולל שינוי פיקודי מהותי, אשר יוביל להשגת יעדיו המבצעיים של המערך האמור, אולם עד מועד תום הביקורת גובשה אך טרם אושרה תפיסת הפעלה שונה ולא ננקטו פעולות מעשיות לצמצום הליקויים התפקודיים שהועלו בעבודת המטה.

בתגובת המשטרה נכתב כי ההחלטה ממאי 2021 היא תחילתו של תהליך חשוב שתכליתו מתן מענה לטיפול בפשיעה המקוונת ובעבירות ההונאה בהיבטים החקירתיים והמניעתיים. כחלק מהתהליך נכתבה תפיסת הפעלה הקובעת את אחריות הטיפול בין היחידות. עוד נכתב בתגובה כי "בהמשך ובהתאם לתכניות העבודה העתידיות, יידרשו משאבים נוספים למתן מענה שלם לטובת התמודדות עם החולשות בתחום חשוב ומאתגר זה".

יחידת הסייבר בלהב

בהתאם לפקודת ארגון ייעודית הוקמה בשנת 2014 בלהב 433 יחידת סייבר ארצית בתור יחידה אופרטיבית המצויה בראש מדרג החקירות והמודיעין של העבריינות במרחב המקוון. בתרשים שלהלן מתואר מבנה היחידה הארצית לפי הפק"א האמורה בהשוואה למבנה הקיים בפועל במועד הביקורת.

תרשים 11: **המבנה הארגוני של היחידה הארצית, 2014 ו-2021**



כפי שעולה מהתרשים ויפורט להלן, לאחר הקמת היחידה הארצית בלהב הוקם מס"א אשר החל לפעול במסגרתה, אולם פעילותו טרם הוסדרה.

הקמת מרכז הסייבר הארצי (מס"א)

בדוח הצוות המשותף של הוועדה המתמדת משנת 2021 נכתב כי תפיסת ההפעלה הרצויה בנוגע להתמודדות עם פשיעה במרחב המקוון תעסוק בתשתית הטכנולוגית, במודיעין, במבצעים, באסטרטגיה ובשותפויות; וכן במרכיבים של שיתוף פעולה בין-לאומי, ניהול ויישום פרויקטים בתחומי האיסוף, העיבוד והחקירה, הממשק המקוון עם האזרח ועם הסקטור הפרטי-פיננסי, המעטפת המשפטית ואיתור וניהול של שותפויות עם האקדמיה. לשם גיוון אמצעי האיסוף, ייעול המענה המבצעי וביסוס שיתוף הפעולה הבין-ארגוני והבין-לאומי במאבק בעבריינות במרחב המקוון הקימה המשטרה ביולי 2015 את מס"א ביחידת הסייבר בלהב.

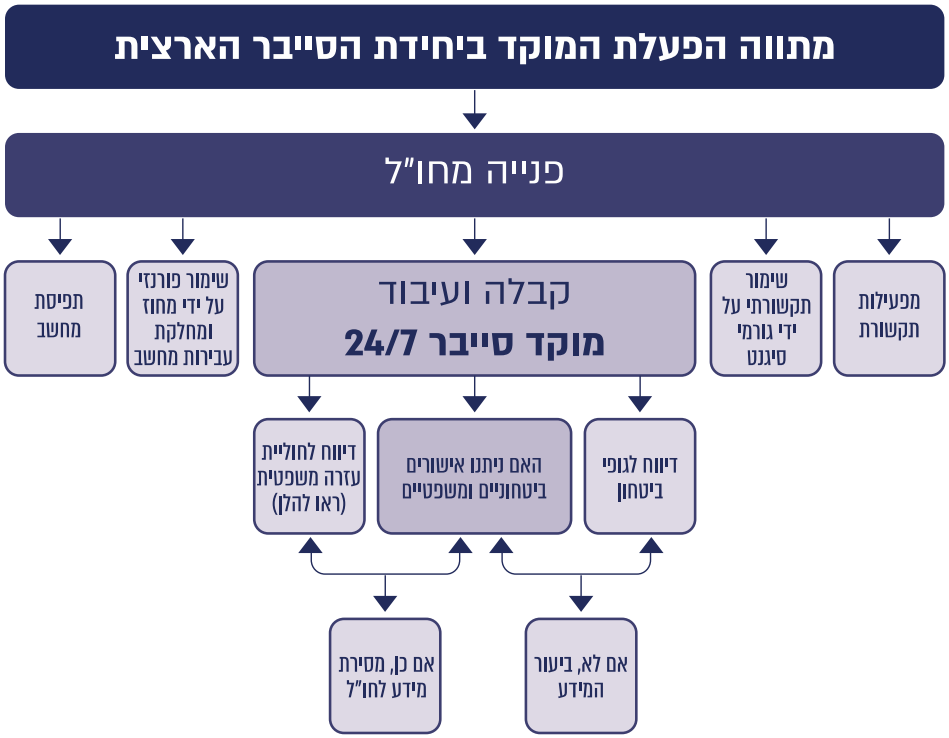
הקמת מס"א נועדה ליישם את אמנת בודפשט באמצעות הפעלת מוקד 24/7 למטרת הענקת סיוע מיידי לכלל יחידות המשטרה[52] ולמדינות החברות באמנה - הן בניטור המרחב המקוון, הן בחקירת עבירות בזירה זו והן בהליכים מקדמיים הנוגעים אליהן; ובפרט שימור מידע[53], הקפאת

52 ראו להלן בתת-הפרק בנושא "חקירת העבירות במרחב המקוון" את פירוט פעילותו של מס"א באפיק זה.

53 כהגדרתו בסעיפים 29 ו-30 באמנת בודפשט.

מצב ראייתי, זיהוי מגמות ותופעות של פשיעת סייבר והצעת מענה לטיפול[54]. נוסף על כך מס"א מספק לפונים אליו סיוע טכנולוגי, מידע משפטי ואיכון חשודים לביצוע עבירות בזירה האמורה. מס"א משתף פעולה עם יותר ממאה רשויות אכיפה בעולם ועם מספר רב של חברות היי-טק במגוון צירים - מודיעיניים ופעילות בשעת חירום. בתרשים שלהלן מתואר מתווה הפעלת מס"א בהתאם להוראות אמנת בודפשט.

תרשים 12: **מתווה הפעילות של מס"א לצורך סיוע למדינות החברות באמנת בודפשט**



1. **איוש מס"א:** בסיכום כנס הוועדה המתמדת שהיה במאי 2018 נכתב כי "לשם המשך עבודה בעלת רציפות מקצועית, שתיצור זיכרון ארגוני, יש לגייס שוטרי קבע שיאיישו את מס"א". בעניין איוש מס"א פנה מפקד היחידה הארצית לראש להב כמה פעמים החל בשנת 2016, ובשנת 2020 אף הדגיש בעניין זה כי פעילות מס"א הולכת וגדלה משנה לשנה, ותחלופת בנות השירות הלאומי מדי שנתיים עלולה ליצור חלל מבצעי ניכר בהתמודדות המשטרה עם פשיעת הסייבר; למנוע רציפות תפקודית מקצועית ויעילה, ולפגוע בהכשרה ובזיכרון הארגוני. אולם פניותיו האמורות נענו באופן חלקי בלבד.

54 מס"א מפרסם דוחות יומיים, שבועיים ושנתיים, ומעביר אותם לידיעת יחידות המשטרה העוסקות בעבריינות במרחב המקוון. דוחות אלה מציגים את תמונת הפשיעה הארצית, תובנות מפילוח נתונים מתיקים במערכת הממוחשבת של תיקי החקירה במשטרה ("הפלא") שנפתחו וסווגו כקשורים לאינטרנט, תופעות פשיעה מרכזיות והמלצות לפעולה.

עלה כי טיוטת פק"א שהכין אג"ת בשנת 2019 בנוגע לארגון להב 433, אשר אמורה לכלול את פעילות מס"א, טרם אושרה. בין היתר, אמורה הפק"א להגדיר את תפקידיו וסמכויות של מס"א ולקבוע את היקף המשימות בהתאם לתקנים שייקבעו בה. להלן בתרשים פירוט המבנה הנוכחי של מס"א.

תרשים 13: **מבנה מרכז הסייבר הארצי ותחומי עיסוקו, 2021**

המקור: מס"א, משטרת ישראל.

ממסמכי יחידת הסייבר בלהב עולה כי מס"א פועל כל ימות השנה בכל שעות היממה, בלא תקן ובמצבה של שני קציני משטרה בדרגת רפ"ק, שני סטודנטים וחמש בנות שירות לאומי. על אף הפניות של מפקד היחידה הארצית בנוגע לפערי התקינה והאיוש במס"א, טרם חל שינוי בנושא.

בתגובת המשטרה נכתב בעניין זה כי בהתאם להחלטת ראש אח"ם, החל במרץ 2022 תועתק פעילות מס"א מיחידת הסייבר הארצית לחטיבת הסיגינט-סייבר במטה אח"ם. במסגרת המעבר מגבשת החטיבה תפיסת הפעלה מותאמת הכוללת דרישה לתקינה רלוונטית ואיוש. עם זאת, במסגרת תוכנית העבודה של המשטרה לשנים 2022 - 2023,

תועדפו בעיקר תוכניות בתחומים אחרים (בדגש על טיפול בפשיעה בחברה הערבית), ואילו עבודת המטה בנושא חיזוק מס"א לא תועדפה ברמה הארגונית.

> משרד מבקר המדינה מעיר למשטרה כי ההתבססות על כוח אדם המצוי בתחלופה גבוהה אינה מספקת את המענה התפקודי הדרוש למס"א כדי למלא את כל התפקידים שיועדו לו במערך הסייבר והזי"ט, בדגש על יישום החובות המוטלות על המשטרה מכוח אמנת בודפשט.

2. ממסמכי אח"ם עולה כי מס"א מפעיל שני מנגנונים מבצעיים מקבילים בכפיפות דואלית - מנגנון אחד בכפוף ליחידת הסייבר בלהב[55], ומנגנון שני בכפוף לחטיבת הסיגינט-סייבר במטה אח"ם לביצוע פעילות מודיעינית: איסוף, ריכוז והפצה של התראות על תוכנות זדוניות ואיומים בתחום הסייבר למשטרה ולשותפי חדר המצב בארץ ובעולם; טיפול בבקשות עזרה בין-משטרתיות באמצעות מחלקת תיאום מבצעי (מת"ם) בחטיבת המודיעין; וביצוע פעילות מבצעית: מתן סיוע מקצועי ובלעדי לחדרי המצב ולמוקדי הפעילות במס"ל, בגופי ממשל נוספים, ולגורמים הרלוונטיים לשם יישום אמנת בודפשט. בלוח להלן פירוט הפניות שבהן טיפל מס"א בשנים 2018 - 2020 במסגרת יישום ועדת בודפשט.

לוח 5: **סיכום פעילות מוקד 24/7 של מס"א, 2018 - 2020**

	2018	2019	2020	סה"כ
בקשות סיוע מגורמי חו"ל למס"א	40	74	80	194
בקשות סיוע ממס"א לגורמי חו"ל	103	53	54	210

המקור: מס"א.

נוכח ריבוי המשימות והכפיפויות של מס"א, הממוקם פיזית ביחידה הארצית בבניין להב 433, נקבע בהחלטת חטיבת הסיגינט-סייבר מיוני 2018 כי המנגנון השני במס"א יוצב במטה אח"ם, אולם החלטה זו טרם יושמה.

3. על פי נוהל אח"ם, היחידה הארצית תסייע לחטיבת הסיגינט-סייבר בהנחיה מקצועית, בהכשרה ובהדרכה של כלל החוקרים ואנשי המודיעין. כמו כן עליה לסייע לגורמי המטה בחטיבות המטה בגיבוש תפיסת ההפעלה בכל הנוגע לטיפול המשטרתי בעבירות מחשב. נכון למועד סיום הביקורת גיבשו חטיבת החקירות וחטיבת הסיגינט-סייבר שלושה מסמכי הנחיות קצרים לחוקרים (Playbooks) הכוללים תיאור תופעות פשיעה בולטות במרחב המקוון ומתודולוגיות לטיפול בתיקי חקירה בנושאים אלו: סחיטה מקוונת על רקע מיני; מרמה והונאה; הונאת דמי מקדמה ("עוקץ הלוואות").

55 מוקד ידע חקירתי לתחומי פשיעת הסייבר: ניטור כלל האירועים שבטיפול המשטרה ובניית תמונת מצב אחודה; מתן סיוע מקצועי (במתווה Help Desk) לכלל יחידות המשטרה בראי סדר המשימות הארגוני (הצי"ח - ציון ידיעות חיוניות); וסנכרון אירועי פשיעת הסייבר ברמה הארצית הבין-ארגונית.

הביקורת העלתה כי אין למחלקי הסייבר במחוזות מתודולוגיית עבודה כתובה, וכי שלושת מסמכי ההנחיות שגיבשו חטיבת החקירות וחטיבת הסיגינט-סייבר אינם עונים על הצורך במתודולוגיית טיפול סדורה ומפורטת לשלל תופעות הפשיעה במרחב המקוון.

בתגובת המשטרה נכתב כי ההנחיות הקיימות הן התחלה של יישום בפועל של מתודולוגיה בתחום זה על בסיס ניתוח רוחבי של תופעות פשיעה במרחב המקוון, וכי בכוונת החטיבות המקצועיות - חטיבת הסיגינט-סייבר, חטיבת החקירות וגורמי מס"א - להמשיך בניתוח תופעות נוספות ובמתן הנחיות לשטח.

התמודדות עם סוגי פשיעה במרחב המקוון דורשת, בין היתר, מוכנות טכנולוגית והקצאת משאבים טכניים ואנושיים המבוססים על נתוני הפשיעה המקומית והעולמית. נמצא כי מס"א ממלא תפקידים מהותיים ומרכזיים במאבק הכלל-משטרתי בעבריינות במרחב המקוון במישור הפנים-ארגוני, במישור הבין-ארגוני, ברמה הלאומית וברמה הבין-לאומית, אך זאת ללא מעמד מוסדר במבנה הארגוני וללא מתודולוגיה מפורטת.

נוכח זאת, מומלץ כי חטיבת הסיגינט-סייבר, המופקדת על בניין הכוח המשטרתי ועל תפיסת ההפעלה שלו, תקדם מתווה למיצוב מעמדו של מס"א במערך הסייבר והזי"ט, שיכלול הסדרה מפורטת של תפקידיו, של מתודולוגיית העבודה שלו, ושל משאבי האנוש והמשאבים החומריים הדרושים לו.

בניין הכוח המשטרתי

חטיבת הסיגינט-סייבר, שהוקמה בשנת 2014 באח"ם, החלה בשנת 2020 להרחיב את ייעודה ואת פעילותה למטרות אלה: לשמש יחידת מטה ארצית המופקדת על בניין הכוח האסטרטגי של המאבק בפשיעה מתוחכמת ובפשיעה חמורה במרחב המקוון, לרבות באמצעות גיבוש תפיסת הפעלה; לפתח נגישות טכנולוגית-מבצעית; ולאסוף מידע דיגיטלי על סוגיו השונים ולמצות אותו. לבקשת המשרד לבט"פ, בפברואר 2020 גיבש אג"ת טיוטת פק"א בעניין ארגונה מחדש של החטיבה כאמור, ובה נקבע כי החטיבה תופקד על הפיתוח, הגיבוש וההטמעה של תורת הפעלה ושל נהלים בתחומי האיסוף, ההפקה והעיבוד של תוצרי הסייבר והסיגינט במשטרה. נכון לאוגוסט 2021 טרם אושרה טיוטת הפק"א האמורה.

על פי טיוטת הפק"א שגובשה בפברואר 2020, חטיבת הסיגינט-סייבר נועדה לעסוק בבניין הכוח המודיעיני והמבצעי של המשטרה, בדגש על תחום איסוף המידע ועיבוד תוצריו.

1. בשנת 2021 החלה החטיבה לשקוד על הפיתוח והרכישה של אמצעים טכנולוגיים בעיקר למטרות איסוף מידע מודיעיני במרשתת ועל מחקר תשתיתי של מאפייני הפשיעה בזירת התקשורת הדיגיטלית ובמרחב המקוון.

עלה כי טיוטת פקודת ההקמה של חטיבת הסיגינט-סייבר מפברואר 2020 - לא אושרה.

יצוין כי טיוטת הפק"א אינה מסדירה את חלוקת התפקידים בין חטיבת הסיגינט-סייבר ובין חטיבת המודיעין.

בתגובתה ציינה המשטרה כי היא רואה חשיבות באישור פק"א חדשה; הנושא קיבל את אישורו של מנכ"ל המשרד לבט"פ בפברואר 2020, ובמועד סיום הביקורת הנושא עדיין מצוי בשיח בין המשרד לבט"פ ובין המשטרה. תגובת המשרד לבט"פ מינואר 2022 אישרה את האמור בתגובת המשטרה.

עוד נמצא כי אח"ם לא הגדיר את חלוקת התפקידים בין חטיבת הסיגינט-סייבר ובין יחידות אחרות, לרבות חטיבת המודיעין, יחידת הסייבר בלהב 433 ואגף טכנולוגיה ותקשוב (אטו"ב), בעיקר בתחומי האיסוף, המיצוי וההיתוך של המידע המודיעיני. גם ממשק העבודה של מס"ל עם החטיבה, במובחן מהממשק שקיים בינו ובין מס"א, לא הוסדר בנוהל עבודה.

בתגובת המשטרה נכתב כי בעקבות השינויים בהקמת חטיבת הסיגינט-סייבר, המעבר הצפוי של מס"א לחטיבה ושינוי הכפיפות הפיקודית של מחלקי הפשיעה המקוונת, המשטרה תקדם עדכון של נוהל הקיים באח"ם בנושא הפעלת המערך לאיסוף וחקירות סייבר בראי חוצה חטיבות.

2. **מרכז קשר רשתי:** אחד מהתחומים המרכזיים של פשיעת הסייבר הוא תחום ההונאה הרשתית. כדי להתמודד עם התופעה הקימו מדינות במערב אמצעי קשר מקוונים שמאפשרים למסור ולקלוט מידע ותלונות, ולהעביר את המידע ואת התלונות לטיפול היחידות הרלוונטיות במערכת אכיפת החוק המקומית. להלן דוגמאות למדינות שמפעילות מרכז קשר רשתי:

א. בריטניה - הקמה של Action Fraud - מרכז איסוף וניתוח של מודיעין ואירועים הקשורים להונאות ועבירות סייבר.

ב. ארה"ב - הקמה של Internet Crime Complaint Center- IC3[56].

ג. אוסטרליה - הקמה של גוף המכונה ACORN (Australian Cyber Crime Online Report Network). גוף זה הוטמע לתוך Australia Cyber Security Centers Report Cyber - פלטפורמה מקוונת לדיווח על פשיעת סייבר.

56 גוף המסונף ל-FBI. אתר המרשתת של הגוף מאפשר בין היתר להגיש תלונות של נפגעי עבירות במרחב המקוון, לפרסם מידע והנחיות לציבור כיצד להתמודד עם פשיעת סייבר על סוגיה השונים, להעביר התראות לציבור ולפרסם דוחות שנתיים ונתונים סטטיסטיים על סוגי פשיעת הסייבר ונזקיה.

הביקורת העלתה כי לא הוקם בישראל מרכז קשר רשתי. מומלץ כי המשרד לבט"פ ישקול לאמץ את הדגם שהופעל בארה"ב, בבריטניה ובאוסטרליה במאבק בפשיעת הסייבר, ולהקים מרכז קשר רשתי שיסיע לגופי האכיפה לאגם את המידע הקיים בנושא עבור גורמי החקירה והמבצעים במשטרה, בייחוד בתחומי המרמה וההונאה.

בתגובתו למשרד מבקר המדינה מינואר 2022 ציין המשרד לבט"פ כי נושא זה ייבחן ותיערך למידה של הנושא בהתאם להמלצת הביקורת.

נוכח האמור לעיל ולשם ייעול המאבק בעבריינות במרחב המקוון חסר הגבולות, מומלץ כי המשטרה תגבש תפיסת הפעלה עדכנית, הכוללת: עדכון המבנה הארגוני הקיים; הסדרת תשתית פעילותם של כל גופי המודיעין, החקירות והמבצעים במערך הסייבר והזי"ט; אפיון ממשקי העבודה בין הגופים המשטרתיים וקביעת שיתופי הפעולה הנדרשים בינם ובין הגופים הנוגעים בדבר במרחב הממשלתי ובזירה הבין-לאומית. כמו כן מומלץ שהמשטרה תגבש תובנות בנוגע להיקף הפשיעה על סוגיה השונים ותפעל לכתיבת מתודולוגיה ותוכניות פעולה מפורטות שייתנו מענה ראוי לאיומים במרחב זה.

בתגובת המשטרה נכתב כי שיפורי הטכנולוגיה ותופעות הפשיעה במרחב הסייבר משתנים בטווח זמנים מהיר ומחייבים דינמיות ויצירתיות בהתמודדות עימן. תפיסות ההפעלה, ממשקי העבודה והכלים הנדרשים נבחנים במסגרת דיונים של החטיבות המקצועיות באח"ם ונציגי יחידת הסייבר הארצית.

התמודדות עם סוגי פשיעה במרחב המקוון דורשת, בין היתר, מוכנות טכנולוגית והקצאת משאבים טכניים ואנושיים המבוססים על נתוני הפשיעה המקומית והעולמית. מומלץ כי המשטרה תשקול העמדת משאבים אלו כנדרש.

בהקשר זה כתבה המשטרה כי בשנת 2021 אישר המפכ"ל הקצאת משאבי התעצמות טכנולוגית לתחום הסייבר בסך 22 מיליון ש"ח לשנת העבודה 2022 כמענה ראשוני, וכי היא מכירה בעובדה שיש להמשיך ולהקצות משאבים לצרכים הטכנולוגיים הרבים הנובעים מהאתגרים הייחודיים בהתמודדות עם הפשיעה בזירה זו. אשר ליחידת הסייבר הארצית, חלק משגרת העשייה של היחידה הוא העשרת ידע רלוונטי המבוצעת באופן עצמאי. תופעות פשיעה, פרסומי מחקר ומגמות עתידיות מגולמים במסגרת השיקולים בקביעת תוכנית המודיעין ויעדי היחידה.

הפעילות המשטרתית בתחום המודיעין - איסוף ומחקר

איסוף מודיעין משטרתי על אודות פעילות עבריינית נעשה באמצעות מיצוי מידע משני מקורות עיקריים: אנושיים (יומינט - סוכנים ומודיעים) וחומריים (על פי רוב, סיגינט - באמצעי התקשורת השונים), הן במרחב הפיזי והן במרחב המקוון.

גופי המודיעין העוסקים בפשיעת סייבר

על פי פקודות המשטרה, חטיבת המודיעין באח"ם, שבראשה עומד קצין בדרגת תת-ניצב הכפוף לראש אח"ם, היא הגוף המופקד על איסוף המודיעין, על ניתוחו ועל הערכתו עבור גופי החקירה מחד גיסא ועבור יחידות המטה מאידך גיסא. בחטיבה שלוש מחלקות, והן עוסקות במחקר מודיעין, בהיתוך מידע ובשיתוף מידע בין-לאומי.

1. המידע המודיעיני המצוי בידי המשטרה בתחום העבריינות במרחב המקוון מסתמך, בין היתר, על מקורות יומינט ועל ציתות לתעבורת תקשורת (סיגינט). איסוף המודיעין בתחום העבריינות במרחב המקוון מותנה בחיבור טכנולוגי לאמצעי תקשוב דיגיטליים ולמקורות וירטואליים - הן במרשתת הגלויה והן ברשת האפלה. במצב הנוכחי יש ביזור של גופי המודיעין במשטרה העוסקים באיסוף, בניתוח ובמחקר של מידע מודיעיני בתווך האינטרנטי. להלן בתרשים תיאור גופי המודיעין במשטרה העוסקים באיסוף, ניתוח והערכה של מודיעין ברשת.

תרשים 14: **גופי המודיעין במשטרה העוסקים באיסוף, בניתוח ובהערכה של מידע מודיעיני ברשת**

ניו מדיה – דוברות משטרת ישראל

מחלקת ניו מדיה בדוברות המשטרה מפעילה פרופילים של משטרת ישראל ברשתות חברתיות שונות במרשתת במסגרתן יכול האזרח לפנות בהודעה ולדווח על אודות חשד לאירוע פלילי מסוג סדר ציבורי והסתה. האזרחים מתייגים את משטרת ישראל לפוסטים המציגים חשד לפעילות פלילית או חשש לחיי אדם.

היחידות המשטרתיות האמורות עוסקות באיסוף מודיעין בקשר לפשיעת סייבר אך אינן מאורגנות במבנה אחיד והיררכי, וחלקן אף אינן כפופות מקצועית ומנהלית לחטיבת המודיעין המרכזית באח"ם.

בפברואר 2020, בדיון שהתקיים בנושא רה-ארגון חטיבת הסיגינט והקמת מטה הסייבר בחטיבה, התריע סמנכ"ל בכיר לתכנון תקצוב ובקרה במשרד לבט"פ, כי על המשטרה להמשיך ולחדד את תחומי האחריות של החטיבה ולעגן אותם בנוהלי עבודה, בדגש על פעולות העלולות להיות חופפות בין חטיבות האח"ם השונות, כגון מיצוי מידע המבוצע הן בחטיבת הסיגינט-סייבר והן בחטיבת המודיעין, וכן ממשקי עבודה שלהן עם יחידות כגון מס"ל, היחידה הארצית ומחלקי הסייבר במחוזות. אולם פעולות אלה טרם הושלמו.

בתגובת המשטרה נכתב כי כל יחידה אחראית לטיפול בפשיעה שבתחומה על בסיס תמונת המודיעין שהיא מייצרת. בתחום פשיעת הסייבר הגוף המרכזי לאיסוף מודיעין הוא מחלק המודיעין שביחידת הסייבר הארצית. לצד זאת פועל מס"א לאיסוף מידע ממקורות שונים ומנתח תמונת מודיעין רחבה יותר. מחלק המודיעין ביחידת הסייבר הארצית ומס"א פועלים בהתאם לנוהלי חטיבת המודיעין ולהנחיותיה, בדומה לכל גוף איסוף מודיעין אחר במשטרה.

הביזור הקיים של יחידות המודיעין באח"ם, במטה הארצי ובמחוזות: חטיבת המודיעין, חטיבת הסיגינט-סייבר, מודיעין יחידת הסייבר בלהב, המודיעין במחוזות וחטיבת הדוברות, עלול להקשות על המשטרה לאגם משאבים ולרכז ידע, מיומנות מקצועית, מומחיות ויכולות איסוף וניתוח מודיעין במרחב המקוון הן בבניין הכוח והן בהפעלתו. יוצא אפוא כי הביזור הקיים מקשה על ביצוע של פיקוח ובקרה ברמה הארצית על טיב הטיפול של אח"ם בתיקי העבריינות במרחב המקוון. מומלץ למשטרה לשקול לאגם משאבים בתחומי איסוף ומחקר מודיעין במרחב המקוון, באופן שיסייע בהגברת המיומנות והיכולות בתחום זה.

2. בעקבות עמ"ט הונאה (ראו לעיל) הושקה בנובמבר 2020 תוכנית חלוץ (פיילוט) שעניינה הפעלת מוקד ארצי של היתוך מידע בתחומי ההונאה, אשר ינטר, יעשיר ויפיץ את המידע ליחידות הרלוונטיות לשם יצירת שינוי תודעתי באמון הציבור; זיהוי מגמות עומק וקביעת מדיניות טיפול; ראייה כוללת וארוכת טווח של טיפול בעבירות הונאה; יצירת תפיסת הפעלה של כלל אח"ם בנושא; שילוב יכולות בתוך המשטרה ומחוצה לה; ומציאת פתרונות אסטרטגיים בתחומי האכיפה והמניעה. יצוין כי מדובר במוקד לענייני הונאה בלבד, שאינו זהה למרכז הקשר הרשתי המופעל במדינות המערב שנזכרו לעיל.

צוות העבודה שהוקם לבחינת הקמתו של המוקד הארצי כלל בממצאיו ניתוח תמונת מודיעין בתוך המשטרה והוא קבע, בין היתר, כי יש חוסר אחידות בין המחוזות וכן כפילות בטיפול בתחומים דומים; חסר אפיון מקוון לעבירות בתחום ההונאה; וכי מחלקי הסייבר עוסקים בפשיעה שאינה בהכרח פשיעת סייבר ואין להם משאבים לטיפול בעבירות סייבר מורכבות.

במחצית 2021 הסתיימה הכנת תוכנית החלוץ. על פי מסקנותיה יש להקים באופן קבוע מוקד היתוך הונאה ארצי, ולהקצות לו 20 תקני כוח אדם הכשירים לעסוק בתחומי המודיעין, המחקר והטכנולוגיה, לשם ביצוע, בין היתר, של משימות אלה: סינון מידע, איתור הזדמנויות לתקיפת תשתיות וגורמי עבריינות חוזרת, ואיתור תיקים בעלי עניין ציבורי או כאלה המייצגים נפגעים רבים.

יצוין כי דוח הצוות המשותף התייחס לתוכנית החלוץ וציין כי פעילות המוקד עשויה לתרום לאיתור יעדים לטיפול אכיפתי ולגיבוש צי"ח[57] אסטרטגי ליחידות האיסוף.

במאי 2021 החליט מפכ"ל המשטרה שלא להפעיל מוקד הונאה בהיקף שנבחן בתוכנית החלוץ, אלא להפעיל חוליה מצומצמת ברמה הארצית שתתכלל את הטיפול באירועי סייבר חוצי מחוזות ותווסת עומסי פרשיות בין המחוזות.

מהאמור עולה כי תוכנית החלוץ להפעלת מוקד הונאה השיגה את מטרותיה ועל כן הומלץ להקים מוקד הונאה כאמור, אולם יישומה הקבוע בעתיד לא צפוי לצאת אל הפועל.

במצב דברים זה על המשטרה להמשיך ולעקוב אחר ההשפעות של אי-היישום המלא של התוכנית בשים לב לצרכי האכיפה בתחום זה.

בינואר 2022 הודיעה המשטרה למשרד מבקר המדינה כי הקמת מרכז הונאה סייבר הוא פרויקט בעל חשיבות רבה, וכי היא שואפת להביאו לכדי מימוש בהקדם. לשם כך, ועד לגיוס המשאבים הדרושים, תפעיל חטיבת הסייבר את מס"א גם במישורים אלו.

איסוף מידע מודיעיני

על פי נוהלי אח"ם, המודיעין המשטרתי עוסק באיסוף מידע מהמרשתת וממקורות בעולם הפיזי, ותפקידיו הם כדלקמן: (א) לשקף את המציאות בתחום העבריינות במרחב המקוון באמצעות בניית תשתית ידע בנושא בשיתוף גורמים אזרחיים רלוונטיים וגורמי מודיעין עמיתים; (ב) להפעיל תשתיות אסטרטגיות בתחום אחזור מידע בנושא; (ג) ניתוח מידע ומתן תמונת מודיעין בפרשיות חקירה במרחב המקוון; (ד) הפקת מידע מכלים טכנולוגיים סמויים ופיקוח על תהליך ההפקה, בכפוף להנחיות אח"ם.

1. **פערי המידע המודיעיני:** על פי תמונת המודיעין לשנת 2020, התגברות העבריינות במרחב המקוון נובעת מהנגישות של אמצעים טכנולוגיים למיסוך וטשטוש זהות המשתמש במרשתת, הזמינים לכל דורש, ואשר מאפשרים לעבריינים לבצע פעילות פלילית בזירה זו תוך שמירה על אנונימיות. לפיכך קיים פער מודיעיני איסופי ניכר בתחום עבירות המין והפדופיליה, על אף ריבוי האיומים הקיימים בתחום זה במרחב המקוון נוכח חשיפתם המוגברת של ילדים ובני נוער ליישומונים. זאת ועוד, קיימת סכנה לזליגה של טכנולוגיות ופיתוחים מהשוק הפרטי, וייתכן שאף מהמגזר הביטחוני, לשוק הפלילי באמצעות מומחי אבטחת מידע הסוחרים בפיתוחים אשר נוצרו במהלך עבודתם במגזרים אלה. אולם קיים פער מודיעיני בנושא ומספר הידיעות בנושא הוא מצומצם.

57 ציון ידיעות חיוניות - תוכנית העבודה של המודיעין הכוללת מיקוד בנושאים מסוימים.

המלצות צוות "עליונות טכנולוגית בשיטור", שהוקם במשטרה כדי לבחון באופן מערכתי את אתגרי השיטור בתחומים הטכנולוגיים, מיוני 2021, מלמדות כי המשטרה נדרשת לאוסף של יכולות טכנולוגיות המאפשרות את תכליותיה הארגוניות באמצעות מידע מודיעיני איכותי, מספק ורלוונטי, תוך הקדמת העבריין, סיכול כוונותיו וחשיפתו. תפיסת ההפקה של התוצר המודיעיני הנדרש צריכה להתבסס על מעורבות של יחידות המשטרה בתחנות, במחוזות וביחידות הארציות, בכל שלבי התהליך: גיבוש ההתראות והיעדים, שימוש באמצעים טכנולוגיים לאיסוף, היתוך המידע ומיצויו בידי קציני מודיעין ועל ידי הבינה המלאכותית, והעברת מידע אופרטיבי לגורמים המבצעיים לשם סיכול הפעילות העבריינית.

תמונת המצב שהפיקה חטיבת המודיעין בשנת 2020 והצפי לשנת 2021 הצביעו על התרחבות הליקויים בתחום האיסוף במרחב המקוון כדלקמן:

א. בשנים 2018 - 2020 נפתחו כ-26,400 תיקי חקירה שעניינם עבירות שונות שבוצעו באמצעות מחשב, אולם רק ב-10% מהתיקים הוגשו כתבי אישום. לשם ההשוואה, בתקופה האמורה הגישה המשטרה כ-15% כתבי אישום מכלל תיקי החקירה. על פי מחלקת המחקר בחטיבת המודיעין "האחוז הנמוך יחסית של כתבי האישום מצביע על הקושי באיסוף ראיות מספיקות להגשת כתבי אישום ברוב התיקים".

על פי תמונת המודיעין, ב-90% מתיקי החקירה בעבירות במרחב המקוון לא הוגשו כתבי אישום עקב מידע חסר. נתונים אלו עשויים להצביע על הקושי באיסוף מידע לשם השגת ראיות מספיקות בתיקי החקירה.

בשנת 2020 התרחב השימוש ביישומונים מוצפנים כפלטפורמה לפעילות פלילית מגוונת (סחר ויבוא סמים, סחר באמל"ח וברכוש גנוב, מכירת אלכוהול בלתי חוקית, עבריינות מין, זנות, הונאה, זיוף, הלבנת הון, הימורים ואלימות), וזאת נוסף על השימוש ביישומונים אחרים להחלפת מסרים.

> על פי תמונת המודיעין, עלו פערים ביכולת המשטרה לאיסוף מודיעין המתבסס על תעבורת מסרים ועל ראיות הנוגעות לביצוע עבירות פליליות ביישומונים מסוימים.

ב. חטיבת המודיעין הצביעה על אינדיקציות להמשך השימוש באמצעים פיננסיים אלקטרוניים לצורכי תשלום עבור טובין ושירותים פליליים, ביצוע הונאות וכן העברת כספים בין גורמים פליליים ללא דיווח לרשות המיסים ולרשות לאיסור הלבנת הון ומימון טרור על פי פקודת מס הכנסה [נוסח חדש] וחוק איסור הלבנת הון, התש"ס-2000. במסגרת פעילות זו, העוקפת את המגבלות הרגולטוריות, נעשה שימוש באמצעים אלה: מטבעות וירטואליים, אתרי סליקה, יישומוני תשלום, קודים לשימוש במכשירים למשיכת מזומנים, אמצעים ל"הלוואות חברתיות" ואחרים.

כן תועד שימוש במלביני הון מקצועיים והצבת מכשירים למשיכת מזומנים לביטקוין הפרוסים במקומות שונים, ללא פיקוח, המשמשים לפעילות עבריינית.

מן הנתונים עולה כי עלו פערים ביכולת המשטרה לאסוף מידע מודיעיני של עבירות המתבצעות באמצעי תשלום מסוימים.

ג. פעילות פלילית ברשת האפלה - על פי מסמכי חטיבת המודיעין קיימים פערי מידע ניכרים בתחום הפעילות הפלילית ברשת האפלה, ולכן אין אינדיקציות ברורות לגבי היקף הפעילות שלה (ראו לעיל בפרק העוסק ב"עבריינות במרחב המקוון - מאפיינים, מגמות ונזקים").

ד. פלטפורמות מוצפנות נעשו כלי חשוב בפעילותם של מבריחי נשק וסמים הפועלים בגבולות לבנון, ירדן ומצרים. כמו כן קיימות אינדיקציות לתשתיות פלסטיניות העוסקות בהונאת אתרי ממשל ישראלי במרשתת, אשר נועדו לספק מקור הכנסה לתשתיות טרור.

תמונת המצב המודיעינית לשנת 2020 העלתה כי היעדר כלים טכנולוגיים מותאמים מגבילים את יכולת איסוף המודיעין על תשתיות מבריחי נשק וסמים באמצעות המרחב המקוון ועל תשתיות העוסקות בהונאת אתרי ממשל ישראלי במרשתת, הפועלות בשיתוף פעולה עם ארגוני טרור.

בתגובתה צינה המשטרה כי על אף היעדר כלים טכנולוגיים מתאימים ביצעה יחידת הסייבר הארצית פעילות יזומה בשיתוף פעולה עם גופים מקבילים בחו"ל ובהתבסס על מידע יומינטי ועל ניטור רשתי.

ה. הפעילות הפלילית במרחב המקוון הפכה למנוע צמיחה כלכלי והתפתחותי עבור עבריינים מהדרגים הנמוכים והבינוניים. רובם היו בעבר עברייני רכוש ופשיעת רחוב אשר השכילו להבין את הפוטנציאל הכלכלי הטמון בביצוע העבירות באמצעות המרשתת ואת היעדר האכיפה המשטרתית בזירה זו. ההתעצמות הכלכלית ורצונם של העבריינים להרחיב את פעילותם גורמים לצמיחתן של כנופיות בהיבטים של קריירה עבריינית, הון שחור ומאבקי שליטה בין קבוצות מתחרות.

תמונת המצב המודיעינית לשנת 2020 העלתה כי המרשתת היא מרחב שבו אין למדינה שליטה, ובתחומו היא אינה מצליחה להגן על האינטרסים הביטחוניים והכלכליים שלה ושל תושביה, לרבות בהיבט הביטחון האישי והפרטיות.

על המשטרה להטמיע את הלקחים העולים מתמונת המודיעין בתוכניות העבודה שלה כדי לצמצם את פערי האיסוף הניכרים בנוגע לעבריינות במרחב המקוון.

בתגובת המשרד לבט"פ נכתב, כי האתגרים בתחום פשיעת הסייבר עולים בהערכת המצב בתחום ביטחון הפנים ואף סומנו כנושאים למיקוד אסטרטגי. כמו כן, בהתאם למדיניות השר לבט"פ, בתוכנית העבודה לשנת 2022 תבוצע עבודת מטה לבחינת מענה לעבירות נגד מבוגרים במרחב המקוון, בין שבאמצעות הרחבת מוקד 105 ובין שבאמצעות הקמת מוקד חדש.

2. **אתגרי האיסוף במרחב המקוון:** ממסמכי המשטרה והוועדה המתמדת עולה כי הואיל והמרחב המקוון פרץ את גבולות השיפוט הטריטוריאליים, נדרשת בין היתר חשיבה מחודשת בנוגע להפעלת האיסוף המודיעיני בחו"ל בלי לפגוע בריבונות של מדינות זרות.

א. חדירה לשרתים מרוחקים - איסוף מודיעין בזירה על-טריטוריאלית מותנה במקרים רבים בחדירה לשרתי מחשב הממוקמים במדינות זרות. זירה זו טומנת בחובה קשיים משפטיים עקב החשש לפגיעה בריבונות המדינה שבה מצויים שרתי המחשב.

ב. סחיטה מינית - בהנחיה מקצועית שגיבשה חטיבת הסיגינט-סייבר בנושא "טיפול בתופעות פשיעה במרחב המקוון"[58] תוארה תופעת פשיעה שעיקרה סחיטה מינית תמורת כופר. מדובר בתופעה עולמית שארגוני אכיפה רבים נאבקים בה, והיא מהנפוצות ביותר בתיקי חקירה הקשורים לפשיעה במרחב המקוון. היקפה - עשרות אירועים בשבוע בישראל ומיליוני קורבנות ברחבי העולם בסכומים שנאמדים במיליוני דולרים. יש במשטרה כמה מתודולוגיות לטיפול בתופעה, אולם צוין בהנחיה האמורה במפורש כי "ככלל קיים פער ניכר בטיפול המודיעיני של משטרת ישראל בתופעה זו. יש לפעול לטובת יישום אסטרטגיה של מניעה באמצעות תיעוד, שימור וניתוח קשרים עם פרופילים חשודים גם כאשר מרבית התיקים נסגרים בעילת על"ן. בנייה של מאגר נתונים יוכל לשמש לשיתוף פעולה עם סוכנויות אכיפה במדינות שמהן מגיעות מרבית הכנופיות המייצרות את תופעת הפשיעה הזו. חוליית הונאה ארצית תהיה אמונה על תיעוד ושימוש הנתונים".

נמצא כי נכון למועד סיום הביקורת, מס"א אוסף את הנתונים הנוגעים לתופעת הפשיעה מסוג סחיטה מקוונת על רקע מיני, והנתונים מפורסמים בדוחות שהוא מנפיק. עד מועד סיום הביקורת לא נמצא כי מאגר הנתונים של מס"א משמש לניתוח המידע המופיע בו ולגיבוש אסטרטגיה של מניעה או טיפול מודיעיני כלשהו בתופעת פשיעה זו.

בתגובת המשטרה נכתב כי מעבר מס"א לחטיבת הסיגינט-סייבר נועד בין היתר להמשיך ולפתח את יכולות המשטרה בניתוח מיטבי של המידע שאוגרת מס"א עבור גיבוש אסטרטגיות עתידיות לטיפול בפשיעת סייבר.

3. **מודיעין מסכל במרחב המקוון:** דיונים שהיו באח"ם העלו כי איסוף מודיעין התקפי (פרו-אקטיבי) - באופן יזום ובאמצעות פצחנים - הוא אמצעי הכרחי לסיכול פשיעה במרחב המקוון, וכי היחידה הארצית נועדה לתקוף ולא להגיב למתקפות. על פי נוהל אח"ם משנת 2019, איסוף התקפי כולל פעילות "וובינט"[59] המבוססת על דיאלוג מלא שמתקיים בין הגורם אוסף המודיעין המשתמש בפרופיל פיקטיבי, ובין היעד שהוא מושא האיסוף; וזאת במתווים של טקסט, מדיה קולית או מצולמת.

ממסמכי אח"ם עולה כי למחלקי הסייבר במחוזות יש יכולת מוגבלת בתחומים מסוימים לשם סיכול פעילות עבריינית במרחב המקוון. בהחלטת סגל הפיקוד הכללי בנוגע לתפיסת ההפעלה החדשה של מחלקי הסייבר במחוזות מאפריל 2021, נקבע שהכפפתם של

58 המסמך נכתב בשנת 2019, אושר על ידי חטיבת החקירות כהנחיית עבודה והופץ במחוזות בשנת 2020.

59 Web-Intelligence - מודיעין ממקורות גלויים.

המחלקים לראש ענף חקירות במחוזות תכלול מיסוד של מערכים מבצעיים תומכים, לרבות מודיעין יומינטי, סיגינטי ומחקר (בילוש, איסוף והערכה).

ממסמכי אג"ת ואח"ם עולה כי תפקיד התקיפה המודיעיני הוטל על חטיבת הסיגינט-סייבר בדומה לחוליות העוסקות בתחום זה ב-FBI, והיא מנסה לקדם את העניין באמצעות התקשרות עם ספקיות מהמגזר העסקי. בדיון שהיה במטה הארצי ביוני 2021 הובהר כי טרם התגבש במשטרה נוהל לאיסוף מודיעין אקטיבי (התקפי), וכי יש לתת לתחום זה מענה הן בטווח הקצר והן בטווח הארוך.

הביקורת העלתה כי תחום המודיעין המבצעי ההתקפי שנועד לחשיפה, לאיתור ולמניעה של פשיעת סייבר נמצא בשלבי הרצה ופיתוח.

עקב חשיבות הנושא מומלץ שאח"ם ישלים את גיבושו ואישורו של הנוהל, ויפעל להשלמת ההתקשרויות הנדרשות להפעלת הנוהל.

בינואר 2022 הודיעה המשטרה למשרד מבקר המדינה כי הנוהל מצוי בשלבי אישור אחרונים, ועם קבלת הערות כלל הגורמים הנוגעים בדבר ואישורו, יופץ הנוהל ותוסדר פעילות המשטרה בתחום.

שיתופי פעולה בין המשטרה ובין גופי חוץ מקומיים וזרים

המאבק העולמי בעבריינות במרחב המקוון מחייב נקיטת פעולות מגוונות לאיתור מוקדי הפשיעה ומניעתה לצד ביצוע חקירות פליליות, באמצעות הרחבת השימוש במידע מסכל הנוגע לתקיפה, להצפנה ולהעברה של נכסים וירטואליים, המתקבל בין היתר ממקורות אלה: ממשקי עבודה רציפים בין רשויות השלטון, החלפת מידע תדיר בין רשויות האכיפה לעמיתיהן בחו"ל ושיתוף פעולה עיתי עם גופים עסקיים במגזר הפרטי.

להלן פרטים בקשר לאפיקי שיתוף הפעולה של המשטרה עם קהיליית המודיעין הישראלית ועם רשויות האכיפה הזרות, בדגש על החלפת מידע מודיעיני ואיתור חשודים בפשיעת סייבר.

1. בדוח הצוות המשותף עלה כי למשטרה ולגופי קהיליית המודיעין (מוסד, שב"כ, צה"ל) אין נוהלי עבודה משותפים הנוגעים לשיתוף במידע מודיעיני, לרכש ציוד טכנולוגי, למתודולוגיית איתור חשודים וחיפוש בחומרי מחשב ולהטמעת ידע והכשרה. בהתאם לזאת, אין בין הגופים שיתוף פעולה מבצעי שיטתי אלא במקרים אקראיים בלבד. ביולי 2021 דנה הוועדה המתמדת בין היתר ביישום המלצות דוח הצוות המשותף. בדיון זה לא נדונו ההמלצות הנוגעות לשיתוף הפעולה בין המשטרה ובין גופי קהיליית המודיעין.

עלה כי הגם שיש צורך מודיעיני ומבצעי במיסוד שיתוף הפעולה בין המשטרה ובין גופי מערכת הביטחון, בדגש על קהיליית המודיעין, אין ממשקי עבודה קבועים בין הגופים.

מומלץ כי הוועדה המתמדת תיישם את המלצות הצוות המשותף בדבר חיזוק שיתופי הפעולה הבין-רשותיים, ובהם גופי אכיפה וביטחון. אלו יסייעו למשטרה לשפר את יכולותיה באיסוף מידע מודיעיני, ברכישת ידע מקצועי ומיומנויות טכנולוגיות, לשם טיוב אמצעי החקירה בפענוח פשיעה ואיתור חשודים באירועי עבריינות במרחב המקוון.

יצוין כי בדוח הצוות המשותף של הוועדה המתמדת נכתב כי גורמי הפשיעה במרחב המקוון נהנים מהאפשרות לבצע פשיעה בסכומי כסף קטנים אשר משיאים להם רווח בהיקפים גדולים, שכן המרשתת מאפשרת לתוקפים לפגוע באנשים רבים במקומות שונים בעולם בלחיצת כפתור אחת. אולם כאשר לא מונחת בפני גופי החקירה במדינות השונות תמונת המצב הכוללת של היקף הפשיעה הגלובלי, הרי שאין להם תמריץ לנהל חקירות מקומיות או בין-לאומיות בעלויות גבוהות בגין פגיעה קונקרטית במתלונן יחיד או בקבוצה קטנה של נפגעים בסכומים קטנים, ולכן יש להקים צוות עבודה מודיעיני קבוע בראשות המשטרה וגופי אכיפה נוספים.

על פי דוח הצוות המשותף, אי-גיבושה של תמונת מודיעין אחודה בין גופי המודיעין בישראל מונעת שיתוף פעולה אפקטיבי עם גורמי חקירה במדינות אחרות. מומלץ כי צוות המודיעין של הוועדה המתמדת, שבו שותפים כלל גורמי האכיפה, ידון על אפיקי היישום של המלצת הצוות המשותף להקים צוות עבודה מודיעיני בין-ארגוני, שיגבש תמונת מצב רחבה על אודות תופעות הפשיעה במרחב המקוון.

2. 12 נציגי משטרה מוצבים דרך קבע ב-12 מדינות ברחבי העולם[60] ועוסקים במסגרת תפקידם, בין היתר, בסיוע למאבק בעבריינות במרחב המקוון. נוסף על כך, המשטרה החליטה כי שוטר נוסף יחל את עבודתו כנציג נודד[61] שמושבו בישראל. מת"ם בחטיבת המודיעין מפעילה ממשק עבודה רציף עם נציגים אלה. אולם ממסמכי אח"ם עולה כי קיימת שונות במאפייני הפעילות המודיעינית של נציגי המשטרה בחו"ל, וכי בחלק מהמקומות מרחב הפעולה מצומצם ויכולת המעקב אחר השיח המבצעי והתשתיתי בחו"ל נמוכה.

3. המשטרה חברה בכמה ארגונים בין-לאומיים, ונציגיה משתתפים בפורומים לשיתוף פעולה בין-משטרתי. עיקר שיתוף הפעולה בינה ובין רשויות אכיפה עמיתות מתמקד בחקירות נקודתיות ולא באופן מערכתי ורחב.

א. בפברואר 2020 הציג נציג המשטרה במרכז היתוך הסייבר באינטרפול[62] שני מקרים לדוגמה שבהם המשטרה קיבלה סיוע בהעשרת מידע, כגון מידע על שרתים בתיק הונאה, מציאת חשוד במסגרת חקירה בארץ שהיה קשור לחקירה שהתנהלה בחו"ל

60 נציגי המשטרה מוצבים במדינות אלה (בסוגריים מפורטות מדינות הכיסוי): ארה"ב (ארה"ב וקנדה), איחוד האמירויות הערביות (אפריקה והמזרח התיכון), הולנד (הולנד, בלגייה ואנגלייה), ברזיל (ברזיל, ארגנטינה, בוליביה), רומניה (רומניה, בולגריה, הונגריה ופולין), רוסיה (רוסיה, אוקראינה ומולדובה), קולומביה (קולומביה, פרו, פנמה ומקסיקו), סין (סין ויפן), צרפת (צרפת, ספרד, שווייץ ואיטליה), תאילנד (תאילנד והודו), ארגונים בין-לאומיים: צרפת - אינטרפול והולנד - יורופול (גרמניה, אוסטרייה וצ'כיה).

61 ואלה מדינות הכיסוי של נציג זה: דרום אפריקה, מרוקו, ירדן, מצרים ואתיופיה.

62 Cyber Force Center (cfc) - מטה הסייבר של האינטרפול שבו חברות 194 מדינות. המטה ממוקם בסינגפור.

וחיבור המידע. עם זאת, במסגרת דיון בפורום ראשי מחלקי הסייבר ביולי 2020 דיווח מפקד מס"א דאז כי מאחר שישראל אינה חברה באיחוד האירופי ואינה חלק מארה"ב, היא מוגבלת בקבלת מידע מרשתות השיתוף שלהן: ה-e-evidence (של האיחוד האירופי) וה-act cloud (של ארה"ב). משום כך ניתן לקבל ממדינות האיחוד האירופי וארה"ב באופן שוטף רק נתונים כלליים. ניתן לקבל תכנים פרטניים רק במסגרת בקשות לעזרה משפטית המתבצעות באמצעות חטיבת המודיעין באח"ם, אשר אורכות זמן רב.

מפקד מס"א אף מסר למשתתפים בדיון האמור כי ארגון היורופול[63] הקים מערך לטיפול בעבירות מקוונות בעולם הפיננסי, וכי נדרש שיתוף פעולה אסטרטגי בין המשטרה ליורופול לשם קבלת מידע מודיעיני איכותי מהמערך האמור.

בחוות דעת מפורטת שהפיצה חטיבת הסיגינט-סייבר לגורמי אח"ם באוקטובר 2020 הועלה הצורך בהערכה מחודשת של תפיסת ההפעלה של נציגות ייעודית בתחום הסייבר בזירה הבין-לאומית[64]. אולם בדצמבר 2020 הונחתה החטיבה לבחון את התאמתו של נציג נודד לצרכים שפורטו לעיל. בתגובתה ציינה המשטרה כי תפקידו של נציג הסייבר הנודד יהיה, בין היתר, חיזוק ממשקי הפעילות הבין-לאומית בתחום הפשיעה המקוונת. בתגובת משרד החוץ לממצאי הביקורת מדצמבר 2020 צוין כי החל בקיץ 2018 מוצב במטה היורופול בהאג נציג מטעם המשטרה בעקבות חתימה על הסדר מינהלי בין הגופים.

נמצא כי למשטרה אין אפיקי שיתוף פעולה קבועים עם רשויות אכיפה זרות, בעיקר עם גורמי האכיפה בארה"ב, ובכך נפגעת יכולתה להחליף מידע מודיעיני עם גופי שיטור רלוונטיים במדינות שוחרות סייבר, העשויה לסייע לה בסיכול פשיעה חמורה במרחב המקוון.

בתגובת המשטרה נכתב כי היא רואה חשיבות רבה בקידום חתימה על הסכם עם היורופול לשם שילובה בפעילות המבצעית הבין-לאומית בתחום המאבק בפשיעת הסייבר. המשטרה הביעה את עמדתה הרשמית בנושא, ומתנהלים דיונים בינה ובין גופים חוץ-משטרתיים הנוגעים בדבר. המשרד לבט"פ ציין בתגובתו כי הוא רואה חשיבות רבה בקידום חתימה על הסכם של מדינת ישראל עם ארגון היורופול לצורך שיפור יכולת הטיפול בעבירות סייבר בתחום הפיננסי והוא שותף לדיונים המתנהלים בנושא עם גורמים שונים.

בהינתן כי העבריינות במרחב המקוון היא חוצת גבולות, יש חשיבות בקיום קשרי חוץ עם ארגונים מדינתיים ובין-לאומיים לשם מניעת הוצאתן לפועל של תקיפות סייבר, לזיהוי עבריינים ולאיכון מוקדי פשיעה.

63 EUROPOL - סוכנות אכיפת החוק האירופית.

64 המסמך האמור כלל המלצה לסגור את הנציגות בסינגפור בשנת העבודה 2021 ולהציב במקומה נציג מומחה במטה הסייבר של היורופול בהולנד, אשר יופעל בתחומי מודיעין שונים לפעילות מול מערכים ייעודיים במדינות שוחרות סייבר.

מומלץ כי המשטרה תרכז מאמץ בקידום שיתוף פעולה עם גופים עמיתים נוספים ברחבי העולם ועם ארגונים בין-לאומיים הנוגעים בדבר. כמו כן מומלץ כי פיקוד אח"ם יבחן עם המשרד לבט"פ ועם משרד החוץ את האפשרות להשתלב במערך החדש שהוקם ביורופול בשנת 2020 לטיפול בעבירות סייבר בתחום הפיננסי.

משרד החוץ ציין בתגובתו כי הוא והמשטרה נושאים ונותנים עם הנציבות האירופית על חתימת הסכם לחילופי מידע פרטי (International Agreement on the Exchange of Personal Data).

4. **שיתופי פעולה עם המגזר העסקי:** בדיון בוועדת הכנסת לענייני ביקורת המדינה שהתקיים בדצמבר 2020, אמר ראש מדור אסטרטגיה וסייבר בחטיבת הסיגינט-סייבר בעניין טיפול המשטרה בפשיעת סייבר, כי יש משבר אמון בין המגזר הפרטי-עסקי ובין המשטרה בכל הקשור ללחימה בפשיעת סייבר, ולכן קורבנות הפשיעה יטו לפנות ברוב המקרים לעמותה רלוונטית או לאיגוד האינטרנט הישראלי במקום להגיש תלונה במשטרה. חברות רבות התנגדו לחשיפה של אירועי סייבר מחשש שגילוי כזה עלול להביא להתקפות נוספות או לפגיעה במוניטין שלהם[65].

נמצא כי יש גורמים במגזר העסקי-פיננסי שאינם נוטים לדווח למשטרה על עבירות במרחב המקוון הידועות להם, והדבר עלול להשפיע על היקף המידע המצוי ברשות המשטרה על אודות היקף הפשיעה בזירה זו ועל מאפייניה.

הפיקוח על הבנקים בבנק ישראל עוקב אחר התרחשויות של אירועי סייבר מהותיים בקרב המערכת הבנקאית המפוקחת על ידו, וזו נדרשת לדווח לבנק ישראל על אירועים מהותיים. נתונים אלה אינם כוללים מספר גדול של אירועי סייבר שאינם עומדים בקריטריון הדיווח של הוראות בנק ישראל, כמו אירועי עוקץ במכשירי כספומט. בשנים 2017 עד 2021 (אוקטובר) דיווחה המערכת הבנקאית על 141 אירועי סייבר במגוון תחומי פשיעה מקוונת, לרבות אירועי דיוג (30 אירועים) ו-Sim Swap[66] (27 אירועים). נוסף על אירועים אלה המדווחים לבנק ישראל מתרחשים ברמה השוטפת אירועי סייבר שאינם מחויבים בדיווח, לרבות אירועי דיוג נוספים.

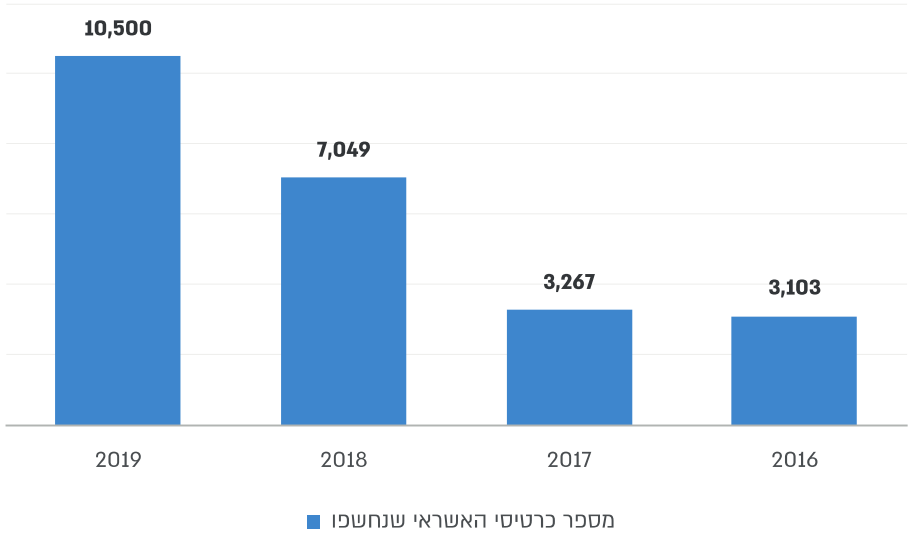
על פי מסמכי המשטרה מ-2019 מסתמנת עלייה חדה במספר אירועי העוקץ במכשירי כספומט, אולם המערכת המשטרתית אינה יכולה לעקוב אחר התופעה בשל תת-דיווח.

מהנתונים בסקר החברתי שפרסמה הלמ"ס בנובמבר 2020, נכתב כי מבין אלה שנפגעו מפשיעה ברשת (1.1 מיליון איש), כ-20% (220,000 איש) נפגעו מהונאה בנקאית או מגניבת פרטי כרטיסי אשראי.

65 חברת דירוג האשראי "מידרוג" **נזקי המוניטין בעקבות מתקפות סייבר עלולות לגבות מחיר עסקי מחברות - דוח מיוחד**, אוקטובר 2020.

66 Sim Swap הוא שירות המאפשר ניוד של מספר טלפון המזוהה עם כטיס טלפון (SIM) אחד לאחר. שיטה זו מנוצלת לעתים למתקפת סייבר במסגרתה תוקפים מתחזים לקורבנות באמצעות מידע מזהה בסיסי שהצליחו לאסוף בכרטיס הטלפון ומבקשים מנציג חברת הסלולר לנייד את מספר הטלפון לכרטיס חלופי שברשותם.

תרשים 15: **מספר כרטיסי האשראי שפרטיהם נחשפו לפי נתוני המערכת הבנקאית, 2016 - 2019**



מהתרשים עולה כי בשנת 2019 מספר כרטיסי האשראי שפרטיהם נחשפו זינק ביותר מ-330% לעומת מספרם בשנת 2016, והגיע ל-10,500.

בדוח הצוות המשותף הומלץ למסד שיתוף פעולה בין גופי האכיפה ובין המגזר הפיננסי כדי ללמוד את הכלים ואת פרקטיקות העבודה ולהפיק תובנות חקירתיות ומניעתיות; זאת בשים לב ליכולות המודיעין שמפיק המגזר האמור. יצוין כי באפריל 2021 הנחה ראש אח"ם את האגף לקדם את שיתוף הפעולה עם המערכות הפיננסיות.

נמצא כי אין קשר רציף וקבוע ואין ממשקי עבודה בין מערך הסייבר והזי"ט במשטרה ובין גורמי אבטחת המידע במגזר הפיננסי והעסקי. בעקבות הנחיית ראש אח"ם מאפריל 2021, מומלץ שאח"ם יגבש מתווה לשיתוף פעולה ברובד המודיעיני עם גופים רלוונטיים בתאגידים בנקאיים ומסחריים המקיימים ניטור אפקטיבי אחר ניסיונות הונאה ומרמה במרחב המקוון.

5. **ממשק עבודה עם מס"ל:** כאמור מס"ל הוא גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר מפני תקיפות חמורות ועל הקידום והביסוס של עוצמתה של ישראל בתחום זה. מס"ל פועל בעת שגרה לחיזוק תמידי של רמת ההגנה של המערכות הממוחשבות של הארגונים במשק המשרתות את אזרחי המדינה.

א. בדוח מבקר המדינה מ-2017 הועלה הצורך לחבר בין הידע והיכולות של מס"ל ובין אחריות המשטרה להתמודד עם פשיעת סייבר. ואומנם ממסמכי המשטרה עולה כי החל בשנת 2018 גדל היקף שיתוף המידע והידע בין הגופים האמורים, ובמיוחד בין

מס"ל ובין חטיבת הסיגינט-סייבר באח"ם, במקרים שבהם היה לשני הצדדים עניין בטיפול המשטרה באירועי סייבר פליליים.

נכון לסוף שנת 2021, במסגרת ממשק העבודה בין מס"ל ובין המשטרה שמוסד בשנת 2018, התבצעה חקירה משותפת במספר פרשיות של פשיעת סייבר.

ב. בשנת 2020 גובשה טיוטת מזכר הבנות למיסוד מנגנון שיתוף הפעולה בין הגופים בתחומים המודיעיני-מבצעי, התשתיתי והאסטרטגי (להלן - המזכר).

יצוין כי יחידת הסייבר בפרקליטות מסרה את השגותיה על המזכר ועל נספחיו למשתתפי דיון שעסק בנושא ביולי 2020.

בספטמבר 2020 התקיים דיון בראשות המשנה לפרקליט המדינה (עניינים פליליים) ובהשתתפות נציגים ממס"ל, מהמשטרה, ממחלקת ייעוץ וחקיקה ומיחידת הסייבר בנושא "יחסי מערך הסייבר הלאומי ומשטרת ישראל". בדיון סוכם כי מס"ל והמשטרה יבחנו את הערות הפרקליטות, ואם אלו יתקבלו יתוקנו המזכר והצעת חוק הסייבר בהתאם. במקרה שתיוותר מחלוקת, היועץ המשפטי לממשלה יכריע בדברים. על פי תגובת המשטרה, המפכ"ל דאז וראש מס"ל דאז אישרו את טיוטת המזכר והיא ממתינה לאישור סופי של הפרקליטות.

בשנת 2021 החלו מס"ל והמשטרה לשתף פעולה בהיבטים מסוימים.

נמצא כי עד תחילת שנת 2022 לא נחתם המזכר בין מס"ל ובין המשטרה.

בשים לב להסתייגויות שפירטה יחידת הסייבר בפרקליטות בנוגע לתוכן המזכר, מומלץ שגורמי אח"ם יפעלו בנוגע לתיקון הוראות טיוטת המזכר באופן שיטיב לשקף את האיזון הראוי בין ההגנה על מאגרי המידע ועל המערכות הממוחשבות של גופים במשק ובין צורכי המאבק בעבריינות במרחב המקוון.

בתגובת מס"ל נכתב בהקשר זה כי נוכח התובנות והמסקנות העולות משיתוף הפעולה הנוכחי, מס"ל מבקש לגבש עדכון למזכר.

מומלץ כי מס"ל והמשטרה יקדמו את החתימה על מזכר ההבנות לאחר עדכונו ויפעלו ליישומו.

חטיבת המודיעין זיהתה פערים בנוכחות המשטרתית במרחב המקוון, שבאים לידי ביטוי בין היתר, באי-מיצוי חקירת העבריינות במרחב זה. בהיעדר אכיפה הפכו פירות הפשיעה, ובייחוד אלה המתקבלים באתרי ההימורים והסחר הבלתי חוקיים, ל"מנוע צמיחה" כלכלי המממן את הפעילות העבריינית בישראל בתחומים שונים, גם במרחב הפיזי. הערכת המודיעין לשנת 2021 אף העלתה כשלים מהותיים בטיפול המשטרה בעבריינות במרחב המקוון בהיבטים שונים, ובפרט בנוגע לאיסוף המידע הדרוש למניעת פשיעה ולאיסוף ראיות לשם העמדה לדין, לאכיפת החוק ולהרתעה.

בתגובתה ציינה המשטרה כי פעילות האיסוף של יחידת הסייבר הארצית נמצאת בעלייה מתמדת, וכי השינוי בתפיסת ההפעלה של מחלקי הפשיעה המקוונת במחוזות יתרום לשינוי הפערים ולצמצומם.

חקירת העבירות במרחב המקוון

ככלל, הפעילות החקירתית של המשטרה נעשית בשני אפיקים: (א) חשיפה - פעילות יזומה של המשטרה לאיתור מוקדי פשיעה, כגון הימורים וסחר בסמים; (ב) גילוי - פעילות מגיבה לאיתור מובילי פשיעה שנעשית בעקבות קבלת תלונות, כגון הונאות. את החקירות מבצעות על פי רוב יחידות החקירה השונות ברחבי הארץ ויחידות החקירה הארציות, ובפרט להב 433.

ביצוע החקירות ביחידה הארצית

1. על פי נוהל אח"ם, סמכויות החקירה של פשיעת הסייבר מסורות ללהב, והיא מטפלת בעניינים כדלקמן: (א) עבירות מחשב ייחודיות שחקירתן צורכת זמן, מומחיות ואמצעים מיוחדים; (ב) עבירות מחשב הנוגעות לנושאים בעלי עניין ציבורי ייחודי; (ג) עבירות מחשב בעלות היבט ביטחוני הדורשות שיתופי פעולה עם גורמים ביטחוניים וסיווג ביטחוני גבוה; (ד) עבירות מחשב הנוגעות לתשתיות חיוניות ברמה הלאומית; (ה) עבירות מחשב הדורשות שיתוף פעולה עם גורמי חקירה בחו"ל. כמו כן ראש אח"ם, ראש להב וראש חטיבת החקירות רשאים להחליט על טיפול יחידת להב בכל עבירת מחשב אחרת, לרבות עבירה המסתייעת במחשב.

   כאמור לעיל, עם פרוץ מגפת הקורונה, הוגברה הפעילות הפלילית במרחב המקוון בייחוד בתחומי ההונאה, הסחיטה, ובפרט באמצעות דרישות הכופרה, הסחר המקוון בסמים ופעילות ההימורים במרשתת[67]. בעמ"ט הונאה שהוצג למפכ"ל ב-9.9.20 צוין כי על פי דיווחים שהועברו למשטרה מבנק מסחרי וחברת אשראי עם פרוץ מגפת הקורונה, חלה עלייה של 1,400% באירועי גניבת כרטיסי אשראי, עליה של 230% באירועי גניבת זהות ברשת ועליה של 422% באירועי הונאות באתרי ממשלה. נוסף על כך, על פי נתונים שפרסם האינטרפול, ברבעון הראשון של שנת 2020 נרשמה עלייה של 59% בניסיונות הדיוג וההונאה המקוונת ועלייה של 36% בנוזקות ובדרישות כופרה[68].

2. בשנים 2018 - 2020 נפתחו במערך הסייבר והזי"ט כולו 36,009 תיקי חקירה שסווגו כ"קשורים לאינטרנט"[69]. ביחידת הסייבר הארצית נפתחו באותן שנים 255 תיקי חקירה בלבד. מבין התיקים שנפתחו בלהב הועברו לפרקליטות 43% מהתיקים ונסגרו 26% מהתיקים כמתואר להלן.

67 https://www.statista.com/statistics/1258261/covid-19-increase-in-cyber-attacs/ (18.8.21); Technology, "Cybercrime study reveals rise in incidents during COVID-19 pandemic", 27.7.21.

68 INTERPOL, "INTERPOL report shows alarming rate cyberattacks during COVID-19", 4.8.20.

69 תיקי חקירה מסוג פ.א., ט"מ (טיפול מותנה) וכללי.

לוח 6: **סטטוס הטיפול בתיקים ביחידת הסייבר הארצית בלהב 433, 2018 - 2020**[70]

סטטוס התיקים	מספר התיקים
פרקליטות - תביעות	111 (43%)
גנוז	67 (26%)
בחקירה	37 (15%)
החלטה שיפוטית[71]	36 (14%)
בתהליך סגירה/ממתין להצמדה	4 (2%)
סה"כ	**255**

על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

3. **תשומות מס"א לתחום החקירות:** כאמור לעיל, מס"א הוא יחידה אופרטיבית בלהב הממלא תפקידים בתחומים שונים המסייעים לתחום החקירות.

א. החל בשנת 2020 ניסחה חטיבת הסיגינט-סייבר מסמכי ייעוד עבור מס"א המטילים עליו תפקידים נוספים ומשימות שאינו רשאי לבצען על פי הפק"א ונוהל אח"ם.

נמצא כי מס"א פועל בתחום החקירות ללא הרשאה, תוך התמודדות עם הקשיים שיפורטו להלן, הנובעים בעיקר מהפער בין סמכויותיו לבין המשימות והתפקידים שעליו לבצע:

(1) מדי יום ביומו מס"א פועל לסנכרון אירועי פשיעת סייבר הידועים למשטרה באמצעות סריקה יומית של כל תיקי החקירה בתחום העבריינות במרחב המקוון שנפתחו בכל תחנות המשטרה, במחוזות ובלהב[72]. מטרת הפעילות האמורה היא לאפשר למס"א, בין היתר, לתאם בין היחידות החוקרות במשטרה - לשם מניעת כפילויות בתיקי החקירה ומניעת אובדן מידע, לייעל את ביצוע החקירה באמצעות זיהוי תיקים בעלי שיטת פעולה דומה וריכוז הטיפול בהם ביחידה אחת, ולהעביר משאבים לגורם המטפל המתאים.

על פי מסמכי חטיבת הסיגינט-סייבר, פעילות מס"א באפיק זה משקפת את אחת ממשימותיו המרכזיות - להיות מרכז היתוך מידע ובינה בתחום אכיפת הפשע

70 תיקי חקירה בסיווג פ.א. וט"מ (טיפול מותנה) בלבד.

71 מדובר בתיקים שנמצאים בהליך משפטי בבית המשפט.

72 במערכת הפל"א נוסף בשנת 2014 שדה "האירוע קשור לאינטרנט", אשר באמצעותו ניתן לאחזר מידע לגבי תיקי חקירה שעניינם עבירות במרחב המקוון.

במרחב המקוון, על בסיס סריקת תיקי חקירה בארץ הקשורים למרשתת והעשרה ידנית של מידע.

הועלה כי הפקת הדוח היומי של מס"א נעשית באמצעות טיוב נתונים ידני שאינו ממוחשב.

טיוב נתונים רבים בתחום הפשיעה המקוונת באופן ידני אינו יעיל, ובהיקפי מידע ניכרים אינו מדויק ואף יכול להכביד על רציפות פעילותו הכוללת של מס"א בתחום הסיוע ליחידות החוקרות. מומלץ כי היחידה הארצית תפעל לצייד את מס"א במערכת הטכנולוגית הנדרשת שתאפשר לייעל את הפקת הדוח היומי ותדייק את ממצאיו.

(2) הסיוע שמציע מס"א למערך הסייבר והזי"ט נעשה באמצעות מסירת המלצות אופרטיביות של מס"א לקציני החקירות במחוזות המשטרה ולחוקרים בתחנות לגבי הפעולות הנדרשות בתיקי החקירה. במצגת למפכ"ל של עמ"ט הונאה מספטמבר 2020 נכתב כי בכל הקשור לתיקי חקירה שעניינם עבריינות במרחב המקוון, לא אותרו המלצות מס"א לקציני החקירות במחוזות ולחוקרים בתחנות וכן לא אותרו פעולות שנעשו ליישומן.

נמצא כי מס"א אינו מתעד את ההמלצות שהוא מפיץ ליחידות המשטרה במערך הסייבר ואת פירוט תוכנן ואינו מקבל מהן משוב בנוגע ליישום המלצותיו. מומלץ אפוא, כי לשם שימור הידע הארגוני ואפיון מועילות פעילותו יתעד מס"א את ההמלצות שמסר ליחידות המשטרה במערך הסייבר והזי"ט, כדי לעקוב אחר היקף הפעולה בתחום זה ואחר תרומתה להגברת המניעה והאכיפה במרחב המקוון.

(3) על פי מסמכי חטיבת הסיגינט-סייבר, מס"א אחראי לתיאום הממשק הארגוני עם חברות טכנולוגיות בארץ ובעולם בהיבטים טכנו-מודיעיניים, בזיקה לחקירות בארץ ובעולם. במסגרת זו משמש מס"א הגורם המתווך המרכזי[73] בין יחידות המשטרה וגופים ממשלתיים נוספים ובין חברות תוכן ושירות מהמרחב המקוון בישראל ובחו"ל (להלן - פלטפורמות) לשם העברת מידע באופן בלתי מחייב (להלן - הציר הוולונטרי).

בפועל, נמצא מס"א בקשר עם כ-50 פלטפורמות המספקות לו מידע על מספרי IP וכן נתוני לקוח של משתמשים ביישומונים במרחב המקוון (שהם על פי רוב מעורבים בחשד לעבירה או שנשקפת סכנה לשלומם) המבוקשים על ידי גורמים משטרתיים וחוץ-משטרתיים בתיווך מס"א. בשנת 2019 המציא מס"א לחברות האמורות כ-722 צווים שיפוטיים מכוח חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת), התשס"ח-2008, לקבלת נתונים כאמור בתוספת מאות בקשות

73 CPOC - Central Point of Contact

ללא צו לקבלת מידע שאותן מגיש מס"א לגורמי הבירור המשפטי Legal (Investigation Support) של חברות אלה.

> פעילות מס"א בציר הוולונטרי נעשית ללא הסמכה בפק"א, בנוהל או בחקיקה. בהיעדר הסדרה פורמלית ושקופה של פעילות מס"א הנתונה לפיקוח ולבקרה, היא מתבצעת ללא מימון ייעודי, ולכן מס"א אינו מקבל את מלוא המשאבים הנדרשים לו לשם ביצועה.
>
> הועלה גם, כי מס"א אינו מתעד את מידת ההיענות של הפלטפורמות בארץ ובחו"ל לצווים השיפוטיים שהמציא להן ולבקשות שהגיש. בנסיבות אלה אין ברשות מס"א נתונים בדבר אופן יישום הצווים והערכת מידת מועילותם.

יצוין כי הצווים השיפוטיים אינם מחייבים את הפלטפורמות הממוקמות בחו"ל, ולכן ההיענות הוולונטרית לביצועם ולשיתוף הפעולה עם מס"א נעשית מצידן באופן דיסקרטי וללא שיתוף לקוחותיהם. זאת בהינתן כי המידע המבוקש נועד להגנה על האינטרס הציבורי הכללי - למנוע ביצוע עבירה פלילית או פיגוע טרור, לסייע לחקירת משטרה ולהציל חיי אדם.

> כאמור, פעילות מס"א בציר הוולונטרי טרם הוסדרה. במצב הקיים מס"א אינו נתון לפיקוח רגולטורי בנוגע לאמצעים שהוא נוקט בפעילותו לשמירה על זכויות של לקוחות הפלטפורמות מושא בקשותיו לקבלת נתונים ומידע, לרבות הגנת הפרטיות וחופש הביטוי.

ב. יצוין כי ביולי 2020 ובפברואר 2021 פנתה חטיבת הסיגינט-סייבר לפיקוד אח"ם בבקשה להעביר את מס"א מהיחידה הארצית לפיקודה. בפנייתה פירטה טעמים הנוגעים לפעילותו של מס"א המצדיקים לדעתה העברה כזו.

> מן המקובץ עולה כי מס"א מתפקד בתור גוף לאומי והוא משרת את כלל מערכות האכיפה והביטחון. פעילותו הרב-תחומית של מס"א נעשית, כאמור, בידי שני קצינים, שני סטודנטים וחמש בנות שירות לאומי ובמערכות מחשוב מיושנות באופן שמקשה את טיוב הנתונים, את תיעוד ההמלצות של מס"א ואת המעקב אחר יישומן.
>
> משרד מבקר המדינה מציין לחיוב את פעילותו של מס"א על אף המחסור בכוח אדם מיומן ובאמצעים טכנולוגיים מתאימים. מומלץ להסדיר את כלל התפקידים והמשימות המוטלות על מס"א, לבחון מחדש את מיקומו במבנה הארגוני של המשטרה, להקצות לו את התקנים ואת המשאבים החומריים הנחוצים לו ולוודא כי במסגרת פעילותו האמורה נשמר האיזון בין הצרכים המודיעיניים והחקירתיים של המשטרה ובין זכויות הפרט.

ג. עובר להקמתו, מס"א יועד לקבל דיווחים יומיים מאת כלל יחידות המשטרה במערך הסייבר והזי"ט, ממס"ל, מגופים ממשלתיים, מקהיליית המודיעין, מגופים בין-לאומיים

ומשותפים מקצועיים במגזרים העסקי והשלישי ומגורמים באקדמיה. נוהל אח"ם קובע כי מס"א יבנה תמונת מצב מקיפה וכוללת לאירוע פשיעת הסייבר, שתכלול זיהוי מגמות ותופעת פשיעה ברמה הארצית והצעת מענה לטיפול.

לפי נוהל אח"ם, מס"א מפיק שלושה דוחות עיתיים: (א) דוח יומי - נועד לשם זיהוי וסנכרון אירועי פשיעת סייבר ברמה הארצית, זיהוי מגמות ותופעות פשיעה והצעת מענה מבצעי לטיפול; (ב) דוח שבועי - נועד לשם דיווח לפיקוד המשטרה וליחידות השטח על אודות הנעשה במס"א והצגת תמונת מצב על אודות פשיעת הסייבר בשבוע הנתון, המצביע על תופעות פשיעה מתהוות ומידת התעצמותן; (ג) דוח שנתי - סיכום מתכלל של תמונת פשיעת הסייבר הארצית.

יצוין כי סיכומי מס"א מצביעים על מגמת עלייה בתחום הפשיעה המקוונת בישראל בכלל סוגי העבירות, אולם בלי שהנתונים בישראל הושוו לנתונים שנאספו על ידי גופי קהיליית המודיעין, הגופים במגזר הפיננסי והעסקי, הגורמים במגזר השלישי ובאקדמיה; הגם שמס"א מקבל מפעם לפעם דיווחים מגופים חוץ-משטרתיים.

הועלה כי מס"א אינו מקבל דיווחים שוטפים ומלאים מכלל הגופים החוץ-משטרתיים העוסקים בפשיעת סייבר. לפיכך, סיכומי מס"א השנתיים מציגים תמונה חלקית לגבי מצב העבריינות במרחב המקוון בישראל, ואין בהם השוואה לנתונים בנושא זה שפורטו בדוחות מקבילים של גופים פיננסיים ושל גופים מהמגזרים העסקי והשלישי ולפרסומים אקדמיים.

על פי נוהל אח"ם המסדיר את פעילות המערך, חוליית הסייבר במטה הארצי, הכפופה לחטיבת החקירות באח"ם, נועדה לפקח ולערוך בקרה על ניהול תיקי הסייבר במחוזות.

נמצא כי בקרות שעושה חוליית הסייבר על ניהול תיקי החקירה בנושא במחוזות, אינה כוללת בדיקת יישום המלצות מס"א. לשם ייעול ניהול תיקי החקירה במחוזות מומלץ שחטיבת החקירות תשקול כיצד לנהל מעקב ובקרה בנוגע ליישום המלצות מס"א על ידי כלל יחידות מערך הסייבר והזי"ט.

המשטרה ציינה בתגובתה את החלטתו של ראש אח"ם להעתיק את פעילות מס"א מיחידת הסייבר הארצית לחטיבת הסיגינט-סייבר החל במרץ 2022. במסגרת המעבר תגבש החטיבה תפיסת הפעלה חדשה המותאמת לגוף מטה ובכלל זה דרישה לתקינה ואיוש.

ד. בעקבות תלונות המתקבלות מהציבור במוקד 119 של מס"ל, הוא מעביר דיווחים שגרתיים למשטרה (באמצעות מס"א) על אודות פעילות עבריינית במרשתת, בדגש על ניסיונות הונאה ובעיקר לגבי הודעות דיוג שהופצו משרתים בחו"ל. זאת בהתאם לנוהל העבודה שנקבע בין הצדדים ולאחר שמס"ל בודק אם יש בפעילות זו אינדיקציות לאירוע הכולל עבירת סייבר כנגד מחשב. אם מדובר במקרי פשיעה המזוהים כמרמה מקוונת יועבר הטיפול לידי המשטרה. הגם שהמשטרה היא בעלת הסמכות לטפל בדיווחים אלה באמצעי סיכול וחקירה, מס"א מתקשה למנוע את המשך הפצת הודעות

הדיוג בהעדר הסמכה מפורשת בחוק, והוא נאלץ להפנות בחזרה את הדיווחים למס"ל בבקשה לא פורמלית לפעול למניעת ההפצה באמצעות קשריו עם הגופים הנוגעים בדבר בחו"ל.

משנת 2019 עד אוגוסט 2021 הועברו 456 דיווחים בין מס"ל לבין מס"א על אודות פעילות עבריינית במרשתת. בשנים אלה הועבר בין שני הגופים מידע על 270 אירועי דיוג (phishing), 3 אירועים הנוגעים לקשרי חוץ ו-183 אירועי כופרה, סחיטה, ניסיונות הונאה וסוגים נוספים של פשעי סייבר. מס"ל פעל במרבית האירועים הללו להפסקת האירועים בין היתר באמצעות קשריו עם עמיתיו בחו"ל.

מהנתונים ניכר כי החלפת הדיווחים והמידע בין מס"ל למס"א מסייעת לטפל בפעילות העבריינית במרשתת. אולם נמצא כי למס"א אין את האמצעים והיכולת האופרטיבית לטפל במידע שמעביר לו מס"ל.

בתגובתו ציין מס"ל כי מניעת הישנות אירועי הדיוג מצויה בסמכות המשטרה מאחר שהיא צריכה להיעשות באמצעות מעצר האחראים לאירועים אלה, ולא בניסיונות בלתי יעילים להתחקות אחר עמודי הדיג במרשתת "הקמים חדשות לבקרים".

בתגובתה הודיעה המשטרה כי אם המשרד לבט"פ יבוא בדברים עם מס"ל כדי לגשר על הפער שהעלתה הביקורת, המשטרה תשתף פעולה.

נוכח זאת, על המשרד לבט"פ לבוא בדברים עם מס"ל ועם הגופים הממשלתיים הנוגעים בדבר, כדי לגשר על הפער שבין האחריות והסמכות המוקנית למשטרה לטפל בסיכול פשיעת סייבר ללא כלים מקצועיים מחד גיסא, ובין היכולות האופרטיביות של מס"ל אך ללא סמכות חוקית להפעילן במקרי פשיעה, מאידך גיסא.

בתשובתו ציין מס"ל כי נוהל העבודה נמצא בדיונים עם הפרקליטות ועם המשטרה.

המשרד לבט"פ ציין בתשובתו את מענה המשטרה המתייחס למעבר פעילות מס"א לחטיבת הסיגינט-סייבר במטה אח"ם. על פי התשובה, במסגרת עבודת מטה שנעשתה בנושא, עלו פערי תקנים ביחידה הארצית, אולם אלו לא תועדפו ארגונית בתוכנית העבודה לשנים 2022 - 2023. המשרד לבט"פ יבחן את הפערים לכשיועברו תוצרי עבודת המטה. עוד צוין כי במסגרת המעבר מגבשת חטיבת הסיגינט-סייבר תפיסת הפעלה שתהיה תואמת את פעולתו של מס"א כגוף מטה.

ה. חוק עזרה משפטית בין מדינות, התשנ"ח-1998, קובע כי שר המשפטים רשאי לאשר בקשה לעזרה משפטית שהתקבלה ממדינה אחרת[74]. כמו כן החוק מסמיך את שר

74 סעיפים 2 ו-3 לחוק: הבקשה נוגעת, בין היתר, לאחד או יותר מאלה: המצאת מסמכים, גביית ראיות, פעולות חיפוש ותפיסה, העברת ראיות ומסמכים אחרים, העברת אדם להעיד בהליך פלילי או להשתתף בפעולת חקירה, העברת מידע וחילוט רכוש, מתן סעד משפטי, אימות מסמך ואישורו או ביצוע פעולה משפטית אחרת בקשר לעניין אזרחי או פלילי. סמכות שר המשפטים הואצלה למפכ"ל, לראש חטיבת המודיעין באגף החקירות ולראש המחלקה לתפקידים מיוחדים בחטיבת המודיעין שבאגף החקירות של המשטרה, למעט הסמכות לסרב לבקשה מטעם מדינה אחרת.

המשפטים להגיש למדינה אחרת בקשה לפעולת חקירה, לגלות ראיה או חפץ, לתפסם או להעבירם לישראל ולקבל מידע בקשר לעניין פלילי שמתנהל בישראל[75].

המחלקה הבין-לאומית בפרקליטות המדינה מרכזת את הטיפול בבקשות לעזרה משפטית מטעם שר המשפטים. תהליך העברת הבקשות לעזרה משפטית מישראל לחו"ל ומחו"ל לישראל כולל קבלת דרישה לביצוע פעולות חקירה, בין היתר, באמצעות מס"א, דרך ניהול הקשר עם גופי אכיפה בחו"ל באמצעות חוליית עזרה משפטית במת"ם שבחטיבת המודיעין וטיפול בבקשות על ידי פרקליטות המדינה. במקרים שבהם אותר חשוד בחו"ל והוא נדרש לצורכי חקירה, המשטרה מעבירה למדינה שבה אותר החשוד בקשה לעזרה משפטית באמצעות המחלקה הבין-לאומית בפרקליטות כאמור.

ממסמכי חטיבת המודיעין וכן מדוח הצוות המשותף עולה כי ישראל הפכה ל"יצואנית פשיעה" מקוונת, ובפרט בתחום ה"פורקס". תופעה זו מהווה קרקע פורייה לגורמים עבריינים העוסקים בהונאות ובעבירות פיננסיות נוספות, ופירותיה משמשים, בין היתר, למימון ארגוני פשיעה ישראליים.

חוליית עזרה משפטית בין מדינות בחטיבת המודיעין הודיעה למשרד מבקר המדינה, כי ניהול בקשות לעזרה משפטית נעשה באמצעות קובץ אקסל ולא באמצעות "תוכנת מחשב חכמה", ולכן כדי לבחון תיקי פשיעה במרחב המקוון לפי פרמטרים, החוליה נדרשת לסנן את התיקים הרלוונטיים מבין יותר מ-1,000 תיקים, ואין אפשרות לספק באופן מיידי נתונים מספריים על בקשות אלה.

הועלה כי אין לחוליית עזרה משפטית במת"ם נתונים ותיעוד על אודות כמות הבקשות בנושא שבהן היא מטפלת. היעדר מאגר נתונים מפורט בחוליית עזרה משפטית מקשה על מת"ם לבצע פיקוח ובקרה בנוגע לטיפול בבקשות לעזרה משפטית ולוודא כי הבקשה הועברה לגורם הרלוונטי וכן לקבל את תוצאות הטיפול בבקשה. היעדר מאגר נתונים מפורט כאמור מקשה לבצע פיקוח ובקרה בנוגע לטיפול בבקשות לעזרה משפטית ולוודא כי הבקשה הועברה לגורם הרלוונטי וכן לקבל את תוצאות הטיפול בבקשה. מומלץ כי מת"ם תפעל לתיעוד כל הבקשות המוגשות לעזרה משפטית ותעקוב אחר השתלשלות הטיפול בבקשות ובתיקי החקירה נשוא בקשות אלה. מעקב כאמור עשוי לשקף חסמים טכניים, פרוצדורליים ומהותיים ולאפשר בחינה של דרכים שיאפשרו לקצר את משך הליכי החקירה בחו"ל. כמו כן מומלץ, שניהול הבקשות האמורות ייעשה באופן מקוון, באמצעים טכנולוגיים מתקדמים ולא באופן ידני.

ביצוע החקירות במחוזות המשטרה

נוהלי אח"ם קובעים כי מחלקי הסייבר במחוזות המשטרה ירכזו את הטיפול בעבריינות במרחב המקוון בתחומי הפעילות של המחוז: בתיקי חקירה של המחלק; בסיוע ליחידות אחרות במחוז

75 ובלבד שרשות שלטונית בישראל מוסמכת לעשות בישראל פעולה מהסוג המבוקש. ראו: סעיפים 52 - 54 לחוק האמור.

בתיקי חקירה של עבירות באמצעי תקשוב; בסיוע מקצועי לכלל יחידות המחוז באיסוף ראיות ממחשב, במיצוי ראיות דיגיטליות ובסיוע טכני.

מגמת העלייה בעבריינות הנעשית באמצעות המרחב המקוון לצד תמונת המצב של תת-דיווח למשטרה שבות ועולות בהקשרים רבים, והערכת המשטרה היא כי מגמה זו תלך ותתגבר. עם זאת, ממסמכי המשטרה עולה כי תיקי חקירה רבים שנפתחים בקשר לעבריינות זו נסגרים ברובם בעילות שונות, המצביעות על חוסר היכולת הראייתית לאתר את העבריין, גם במקרים שבהם קיים "מוביל חקירתי". במקרים רבים קיים קושי לשייך את העבירה בתיק חקירה בודד לתופעה נרחבת יותר, חוצת מחוזות, הניתנת לאפיון, לגילוי ולפיענוח. מספרם הגדול של תיקי החקירה שעניינם תופעות פשיעה שהמשטרה מתקשה לטפל בהן "[יוצר] לחץ מיותר על מערך החוקרים בתחנות". לפיכך, לעיתים ההנחיה המקצועית לחוקרים היא שאם אין יסוד סביר להניח כי מדובר בחשוד ישראלי, יש לסגור את התיק[76].

כאמור, על פי נתוני המשטרה, בין השנים 2018 - 2020 נפתחו 36,009 תיקים. מתוך 25,707 תיקי חקירה פליליים[77] נסגרו 19,253 תיקים (כ-75%)[78]. בלוח להלן פירוט נתוני פתיחה וסגירה של התיקים על ידי המחוזות השונים. הנתונים מתייחסים לתיקי חקירה בסיווג פ.א. וט"מ (טיפול מותנה). הם אינם כוללים תיקים שטופלו על ידי היחידות הארציות או על ידי משמר הגבול.

76 הדברים עלו בכמה מסמכי הנחיה שהפיק אח"ם לטיפול בתופעות הפשיעה במרחב המקוון: הנדסה חברתית, תופעת "עוקצי הלוואות" - הונאת דמי מקדמה; הונאת סחיטה מקוונת על רקע מיני.

77 תיקים - תיקי חקירה מסוג פ.א. וט"מ.

78 סגירת תיקים נעשית על פי הוראות חוק סדר הדין הפלילי [נוסח משולב], התשמ"ב - 1982; פקודת המשטרה מס' 14.01.01 בנושא "אירוע תלונה ומידע אחר על עבירה - דיווח, סיווג וטיפול" (23.8.20); פקודת המשטרה מס' 300.01.152 בנושא "נימוקים ושיקולים לסגירה של תיקים פליליים" (1.2.14); הנחיית פרקליט המדינה מס' 1.3 "סגירת תיקים בעילת "חוסר ראיות" ובעילת "העדר אשמה" (2.9.19).

לוח 7: **תיקי החקירה הנוגעים לעבריינות במרחב המקוון בחלוקה למחוזות, 2018 - 2020**

המחוז החוקר	מספר תיקי החקירה שנפתחו	מספר התיקים שנסגרו	שיעור התיקים הסגורים
מחוז דרום	3,687	2,978	81%
מחוז חוף	2,907	2,183	75%
מחוז ירושלים	3,461	2,532	73%
מחוז מרכז	5,070	4,100	81%
מחוז צפון	3,665	3,016	82%
מחוז ש"י	1,301	724	56%
מחוז תל אביב	4,816	3,561	74%
סה"כ	**24,907**	**19,094**	**76%**

על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

מהנתונים עולה כי שיעור גניזת התיקים במחוזות המשטרה עומד בממוצע על 76%, ולמעשה מרבית התיקים "הקשורים לאינטרנט" נסגרים.

בביקורת עלה כי מתוך כלל התיקים שנפתחו והנוגעים לעבריינות במרחב המקוון, ב-29% מתיקי החקירה סוגרת המשטרה על הסף תיקים בעילת "אין עבירה פלילית"[79]. עוד עולה כי במאי 2021 הציגה חטיבת הסיגינט-סייבר למפכ"ל נתונים על הפערים בטיפול בתיקים אלו ועל פי הנתונים שהוצגו, בשנת 2020 נפתחו 14,077 תיקי חקירה שסומנו כ"קשורים לאינטרנט"[80], אולם כ-75% מהם (10,639 תיקים) נסגרו בעילות שונות: כ-45% בעילת "עבריין לא נודע" וכ-36% מהם בעילת "אין עבירה פלילית".

כאמור, על פי נתוני המשטרה מתוך 19,253 תיקי חקירה פליליים שנסגרו[81], בכ-62.5% מהם עילת הסגירה היא על"ן. להלן ניתוח עילות גניזת התיקים בין השנים 2018 - 2020:

79 סגירת תיק בעילה של "אין עבירה פלילית" היא למעשה, סגירה על הסף הנעשית כאשר נתברר, בכל שלב שהוא לאחר קבלת התלונה, כי המעשה נשוא התלונה אינו מהווה עבירה פלילית ואז יבוטל התיק הפלילי וחומר החקירה ייגנז כ"חומר כללי". תיקים אלו אף לא נכללים במסגרת הנתונים שמציגה המשטרה לציבור כתיקי חקירה.

80 המקור לנתונים אלו הוא מאגר תיקים רחב יותר הכולל גם תיקים בסיווג פ.א., כללי, ט ו-ט"מ.

81 לא כולל התיקים שנסגרו על הסף בעילת "אין עבירה פלילית".

לוח 8: **עילות גניזת תיקים בכל מחוז, 2018 - 2020**[82]

המחוז	עבריין לא נודע	חוסר ראיות	נסיבות העניין לא מתאימות לפתיחה בחקירה/העמדה לדין	אחר	סה"כ תיקים סגורים
דרום	1,733 (58%)	495	703	47	2,978
חוף	1,344 (62%)	348	453	38	2,183
ירושלים וש"י	1,873 (58%)	508	790	85	3,256
מרכז	2,895 (71%)	505	627	73	4,100
צפון	1,885 (63%)	512	582	37	3,016
תל אביב	2,303 (65%)	298	909	51	3,561

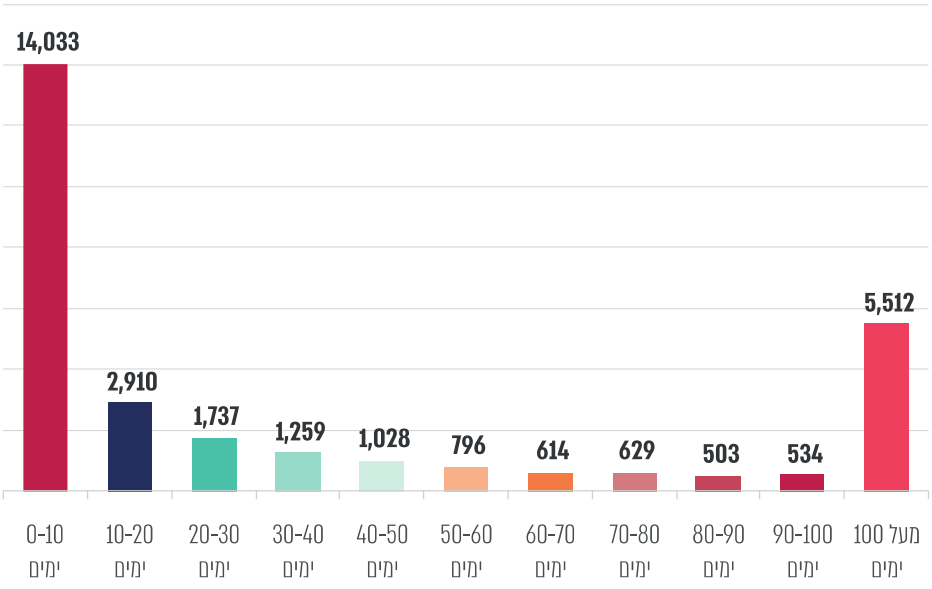
על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

עוד מתברר מנתוני המשטרה, כי למעלה ממחצית התיקים הסגורים[83] (63%) נסגרים בתוך 30 ימים ממועד פתיחת התיקים. הנתונים מפורטים בתרשים שלהלן:

82 הנתונים כוללים תיקי חקירה מסוג פ.א. וט"מ ואינם כוללים תיקים שטופלו על ידי יחידות ארציות או על ידי משמר הגבול

83 הכוונה לכל סיווגי התיקים שנסגרו (פ.א., ט"מ וכללי).

לוח 9: **משך זמן הטיפול בתיקים שנסגרו, 2018 - 2020**



על פי נתוני תיקים במשטרת ישראל, בעיבוד משרד מבקר המדינה.

מהנתונים האמורים עולה כי בשנים 2018 - 2020 למעלה מ-45% מהתיקים נסגרים בעשרת הימים הראשונים לאחר פתיחתם; למעלה מ-60% מהתיקים נסגרים בתוך 30 ימים ממועד פתיחתם וכ-19% מהם נסגרים לאחר תקופה של למעלה מ-100 ימים. עוד נמצא, כי 3,843 תיקים (13%) נסגרו ביום פתיחתם.

נתונים אלה מצביעים על קושי ניכר ביכולות החקירה המשטרתיות בתחום העבריינות במרחב המקוון.

בתגובתה ציינה המשטרה כי ההתמודדות עם כלל האתגרים הנוגעים לעבריינות במרחב המקוון מחייבת מענה מערכתי הכולל בין היתר שינוי ארגוני של מערך הסייבר המשטרתי וביצוע הכשרות מקצועיות מתאימות, אשר יביאו בעתיד לשינוי בנתוני סגירת התיקים.

המיומנות המקצועית בחקירת פעילות עבריינית ברשת

בדיון בפורום ראשי המחלקים במחוזות נטען כי יש מחסור בידע על נכסים וירטואליים חדשים. כמו כן הועלה כי החוקרים מתקשים לגבש בקשות לצווי חילוט של מטבעות קריפטוגרפיים וכספים שהתקבלו כתוצאה מסחר בהם.

לנוכח נתונים אלה יצוין כי בסקירת מדור אכיפה כלכלית בכנס הוועדה המתמדת מאוקטובר 2018 הועלתה הצעה שבמקרים שבהם קורבן העבירה הוא גוף פיננסי איתן (כדוגמת בנקים

וחברות אשראי), "יתכן שיש מקום להסתפק בהליך האזרחי שאותו גוף מנהל מול מבצע העבירה".

הפרקטיקה המשטרתית הקיימת מתרכזת באיסוף מידע ממקורות גלויים, הגם שמידע יקר ערך אינו נגיש לחוקרים בחיפוש פשוט אלא באמצעות כריית מידע ברשת האפלה; דבר הדורש ידע ומיומנות ייחודיים.

ניתוח אקראי שעשתה הביקורת של שמונה תיקי חקירה שעניינם עבריינות במרחב המקוון העלה כי אין ברשות החוקרים מתודולוגיה כתובה בנוגע לתחקור פעילות עבריינית בתשתית ענן שנעשית על גבי תשתית מרכזית של פלטפורמות מובילות; או בנוגע ליכולת להתחקות אחר נתיב תקיפה מרובה זרועות שמעורבים בו יותר גורמים פליליים מאשר עבריין סייבר מקומי. כך לדוגמה, חקירת פעילות עבריינית המעלה חשד לגניבת מטבעות מארנק דיגיטלי מחייבת חקירה מהירה בהתאם למתודולוגיה סדורה, כדי לפענח את נתיב התקיפה ולהשיב את הגניבה לבעליה.

> הביקורת העלתה כי הידע המקצועי המצוי ברשות חוקרי המשטרה בתחום הנכסים הווירטואליים אינו מספק להם כלים מקצועיים לשם פענוח עבירות מורכבות במרחב המקוון.

בתגובת המשטרה נכתב כי בשנת 2021 התקיימו שני מחזורים של הכשרות ייעודיות, להיכרות החוקרים עם עולם המטבעות הקריפטוגרפיים. כמו כן מפעם לפעם מועברים בחטיבת החקירות תכנים לימודיים בתחום זה, באמצעות וובינרים, כנסים מקצועיים לראשי מחלקי הסייבר במחוזות ולחוקרי מערך הסייבר והזי"ט.

> לאור הפערים בידע המקצועי המצוי ברשות חוקרי המשטרה, מומלץ למשטרה להקנות לחוקרים במערך הסייבר והזי"ט ידע מקצועי על בסיס מתודולוגיה מתאימה שתכלול סדר פעולות שתפקידן להתחקות אחר הפעילות העבריינית במרשתת.

עוד עלה כי חקירת עבירות במרחב המקוון מחייבת גם הצטיידות בארגז כלים מקצועי, ובכלל זה טכניקות תקיפה רשתית, שימוש באמצעים טכנולוגיים, הבנה של תעבורת המידע במערכות ענן, מעקב שוטף אחר הפעילויות בזירה וניתוחן. ניתוח תיקי החקירה כאמור ומענה למספר שאלות מקצועיות שהתקבל מחטיבת הסיגינט-סייבר וממחלקי הסייבר במחוזות העלו את הממצאים הללו:

> הידע המקצועי הקיים כיום במשטרה משמש בעיקר לחקירת תיקי עבריינות פשוטים יחסית, ובפרט תיקים שעניינם תקיפות דיוג וסחיטה מינית ברשת, אך עלו פערים בדבר יכולת החוקרים להתמודד עם תקיפות דיגיטליות מסוימות.

בתגובתה על ממצאי הביקורת הודיעה המשטרה בינואר 2022 כי היא תקדם הכשרות חיצוניות לצורך חיזוק המקצועיות של סגל המערך.

הנתונים דלעיל מצביעים על כך שיותר משליש מהתלונות שהוגשו למשטרה בגין עבירות במרחב המקוון נסגרו על הסף. ההיקף הגדול של סגירת תיקים ללא טיפול כלל מעלה את החשש כי המשטרה מתקשה בזיהוי עבריינות בתחום זה ובהבנת מאפייניה. נוכח זאת, על המשטרה לבחון את נסיבות סגירת התלונות ולהפיק את הלקחים הנדרשים לגבי הנהלים הנדרשים וההכשרות הנדרשות לשם איתור רכיבי העבירות בנושא.

בתרשים להלן סיכום כלל הממצאים הנוגעים לטיפול בתיקי חקירה שעניינם עבריינות במרחב המקוון.

תרשים 16: **סיכום הממצאים בקשר לטיפול המשטרה בתיקי עבריינות במרחב המקוון**

בשנים האחרונות הולכים וגוברים אירועי הפשיעה במרחב המקוון. הדברים באים לידי ביטוי, בין היתר, בגידול הניכר במספר תיקי החקירה שעניינם עבריינות במרחב המקוון - מ-6,724 בשנת 2018 ל-10,173 תיקים בשנת 2020. אף על פי כן הממצאים מצביעים על תופעה נרחבת של תת-דיווח למשטרה על עבירות אלו לצד סגירת תיקי חקירה בהיקף ניכר - יותר מ-25% מהתיקים שנפתחים נסגרים על הסף, ו-75% מיתר תיקי החקירה נסגרים, רובם (כ-63%) בעילת על"ן (משלא נמצא מי שביצע את העבירה או כשאין חשד לזהותו). עוד נמצא כי הטיפול בתיקי החקירה שעניינם עבריינות במרחב המקוון נמשך זמן קצר של עד עשרה ימים, ורוב התיקים נסגרים בתוך פחות מחודש. נתונים אלו, לצד הפערים בידע, בהכשרות ובהצטיידות הטכנולוגית שיוצגו בפרקים שלהלן, מחייבים בחינה, ניתוח והפקת תובנות. המשטרה תידרש להתמודד עם העבריינות במרחב המקוון גם בשנים הבאות, ועל כן מומלץ שכל אלו יובילו לפעולות שיסייעו בהגדלת הטיפול המשטרתי לשם איתור יעיל יותר של העבריינים, במטרה להתמודד בצורה מיטבית וכמותית עם הפשיעה במרחב זה.

מניעת עבריינות על ידי הסברה לציבור

פקודת המשטרה הטילה על המשטרה לפעול למניעת עבירות נוסף על גילוין. מניעת עבריינות במרחב המקוון כוללת בהקשר זה ועל פי התוכנית האסטרטגית של המשטרה הסברה לציבור באמצעות מסירת מידע חיוני בנושא.

פשיעת סייבר מתפשטת במרחב המקוון, בין היתר, כתוצאה ממידע חסר בקרב הציבור בנוגע למאפייני הפשיעה, סכנותיה ונזקיה. בקרב גורמי המקצוע אין חולק כי יצירת ערנות ומודעות לפשיעת סייבר בקרב הציבור הרחב היא אמצעי ראשון במעלה להתגוננות מפני פשיעת סייבר. ההסברה המשטרתית בתחום זה עשויה לכלול: זיהוי ניסיונות דיוג באמצעות דואר אלקטרוני ויישומוני מסרים; הגנה על מכשירים ביתיים באמצעות עדכוני תוכנה ועדכוני מערכת הפעלה, גיבויים, התחברות לרשתות פומביות ועוד. יצוין כי מס"ל מייצר תוכני הדרכה בנושאי סייבר ואבטחת מידע, הן לארגונים ולעסקים והן לציבור הרחב ברשתות החברתיות ובערוצי התקשרות השונים.

בינואר 2022 כתבה המשטרה למשרד מבקר המדינה, כי יחידת הסיגינט-סייבר וחטיבת הדוברות מובילות פעולות של הסברה והגברת תודעה בקרב הציבור, בעיקר באתר המשטרה במרשתת וברשתות החברתיות, לרבות אלה: פורטל הפשיעה המקוונת, הודעות מתפרצות במדיה הדיגיטלית לגבי תופעות פשיעה בעת התרחשותן, מדריכים ולומדות, ופעילות הסברה מותאמת לאוכלוסייה הערבית. כמו כן, המשטרה משתתפת בשבוע המודעות לנושא שמקיים מס"ל.

1. התמודדות יעילה עם תקיפות סייבר הכוללות שיבוש מידע, הפרעות תקשורת והונאה, מצריכה את הטמעתם של אמצעים טכנולוגיים המיועדים להקשות על העבריינים לבצע חדירה לחומר מחשב. כאמור, האמצעים הידועים הם תוכנות אנטי וירוס ופלטפורמת אבטחה, זיהוי ותגובה של נקודות קצה (EDR), המיועדות לאתר ולמנוע את הפעלתן של תוכנות זדוניות ונוזקות מוכרות, ומערכות חומת-אש אשר מנטרות וחוסמות פריצות לרשת התקשורת או למחשב יחיד. נוסף על כך, קיימים אמצעים טכנולוגיים מתקדמים הניתנים

להטמעה בידי ארגונים ומוסדות כדי למנוע פגיעות סייבר עוד ברובד ה-DNS[84]. ברובד זה, המשמש "ספר טלפונים" של המרשתת, ניתן לחסום מתקפות סייבר ולמנוע את הפניית הנפגע לאתרים זדוניים ולאתרים הנשלטים בידי גורמים זדוניים[85].

כנגד תקיפות אלה ניתן להשתמש באמצעים טכנולוגיים חדשים אשר אינם ידועים לציבור, כפי שמנחה מס"ל את הגופים שכפופים לפיקוחו. אמצעים אלה ניתנים לרכישה, בין היתר, מחברות מסחריות גלובליות המציעות שירותי DNS Resolving המכילים מנגנוני דחייה של הפניית המשתמשים ליעדים זדוניים, כתחליף לשירות שאותו מציעות ספקיות המרשתת המקומיות (ISP).

סיכול התפשטות נזקי העבריינות במרחב המקוון מצריך יצירת מודעות גבוהה בקרב כל שכבות הציבור לאחריות המוטלת עליהן לנקוט אמצעים כדי למנוע פגיעה כמעט ודאית בהן כתוצאה מפשיעת סייבר. טיפול המשטרה כאמור אינו כולל הסברה לציבור בקשר לאמצעי הגנה מומלצים במערכות ממוחשבות, כמפורט לעיל. הואיל ואבטחת רובד ה-DNS במרשתת מקטינה את הסיכון לפגיעה במערכות המחשוב והתקשורת, מומלץ כי המשטרה תבחן את האפשרות להדריך את הציבור להטמיע את אמצעי ההגנה האלה במערכות הממוחשבות שברשותם; או לרכוש שירותי DNS Resolving כאמור.

2. דוח הצוות המשותף פירט כמה המלצות לגבי ייעול השירות לציבור בתחום הסברת הסייבר, לרבות אלה: חיזוק שיתוף הפעולה הבין-ארגוני ופיתוח תוכניות חינוכיות להיכרות עם הסיכונים ברשת לכלל הגילים במערכת החינוך; פתיחת אתרים ודפים ברשתות החברתיות השונות כדי להעביר מידע ומסרים בדרכים שונות ולקהלים שונים ולתת אפשרות לציבור להעלות תכנים רלוונטיים; פרסום נרחב באמצעי התקשורת הכתובה והדיגיטלית להעברת מידע לכלל הציבור; סנכרון הפרסומים המקצועיים של כלל הגופים, ובכלל זה התכנים, אופן הפרסום שלהם ומועד הפרסום.

ייעול השירות כאמור מותנה גם בהגברת המודעות על אודות גורמי האכיפה השונים בממשל שאליהם ניתן לפנות ולדווח על אירועי פשיעת סייבר או על ניסיונות תקיפה, לרבות הצטרפות למיזם Block של עמותת איגוד האינטרנט (ISOC-IL) המצייד את הציבור הרחב בידע ובכלים להתגוננות מפני עבריינות במרחב המקוון[86].

84 מערכת שמות המתחם (Domain Name System).

85 מכתב מאיגוד האינטרנט הישראלי (ע"ר) למשרד מבקר המדינה בנושא "מישורי היערכות נדרשים של רשויות המדינה בנושא פשיעת סייבר" (29.6.21). יצוין כי עמותה זו פרסמה בשנת 2021 מסמך מדיניות מקיף על אודות איומי אבטחה וסכנות פגיעה בפרטיות במרחב המקוון הקיימות במערכות ה-DNS, ואת האמצעים הטכנולוגיים שניתן לאמץ כדי לספק מענה לאיומים אלו - ברמות גופי הממשל, הארגונים והמשתמשים הפרטיים.

86 https://block.org.il.

הממצאים מצביעים על הצורך בהשלמת פעולות ההסברה הנדרשות לציבור הרחב וחיזוק שיתוף הפעולה הבין-ארגוני בנושא זה. מומלץ כי המשרד לבט"פ יבחן דרכים להעלאת מודעות הציבור לאמצעי ההגנה הנדרשים והנגישים לו מפני פגיעה במרחב המקוון באמצעות פרסום בערוצי תקשורת מגוונים ובאמצעות שיתוף פעולה בתחום ההסברה בין המשטרה ובין גופים ממשלתיים וגורמים חוץ-ממשלתיים הנוגעים בדבר.

בתגובתו כתב המשרד לבט"פ כי ככלל, לטעמו נושא זה מצוי באחריות מס"ל. עם זאת, לאור העובדה כי למשטרה ולמשרד לבט"פ יש קשר ישיר למאבק בפשעי סייבר וכמובן למניעתם, וכן לאור העובדה כי מענה המשטרה כולל רשימה של תוכניות להעלאת המודעות הציבורית לפשיעה מקוונת, ישמח המשרד לבט"פ להיענות לשיתוף פעולה שיוביל מס"ל. בתגובת מס"ל מפברואר 2022 נכתב בהקשר זה, כי מס"ל מגבש תוכניות משותפות עם המשרד לבט"פ לשם העלאת המודעות הציבורית להגנת סייבר, בדגש על פשיעה מקוונת. זאת, בהתאם למגמה הקיימת של שיתוף פעולה בין הגופים האמורים, אשר ראוי שתמשיך ואף תגדל.

התכנון והניהול של משאבי האנוש במערך הסייבר והזי"ט

פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 קובעת כי חיפוש במחשב ייעשה רק על ידי איש משטרה, שהוכשר לכך על ידי המשטרה, המוסמך לבצע את החיפוש אחר ראיות דיגיטליות (להלן - חוקר מיומן). בישיבת יחידת הסייבר הארצי מיוני 2014 סיכם ראש אח"ם, כי ראש חטיבת החקירות יקיים ועדות איתור למועמדים לאיוש תפקיד זה במחוזות המשטרה. על פי נתוני המשטרה, בשנים 2015 עד 2021 התקיימו 12 מחזורים של הקורס "חוקר מיומן" ובהם הוכשרו 245 משתתפים.

במסגרת דיוני הצוות המשותף של הוועדה המתמדת בשנת 2020 הציג ראש חטיבת הסיגינט-סייבר פערים מהותיים בנוגע לתהליכי האיתור, המיון, ההשמה ושימור כוח האדם לאורך זמן של הגורמים המקצועיים הרלוונטיים במשטרה המופקדים על המאבק בעבריינות במרחב המקוון. בדוח הצוות המשותף הומלץ על בנייה ויישום של תוכנית עבודה מפורטת לצמצום הפערים בתחומי ההון האנושי, התשתית, הכלים הטכנולוגיים ומתודולוגיית האכיפה בתחומי העבריינות במרחב המקוון.

הועלה כי במשטרה גובשה, אך טרם אושרה, הגדרת תפקיד ייחודית עבור "חוקר סייבר" לעבירות תקיפת מחשב וחומר מחשב, המובחנת מההגדרה הכללית של "חוקר מחשב מיומן", הנוגעת לכלל העבירות שבוצעו במרחב המקוון ובאמצעי תקשוב דיגיטליים.

מערך הסייבר - הוצאת חוקרים מיחידות הסייבר המחוזיות

בסיכום פגישת עבודה של ראשי מחלקי הסייבר שהייתה בנובמבר 2019 נכתב, כי החוסר במשאבי האנוש הוא הבעיה המרכזית שעמה מתמודדים המחלקים במחוזות המשטרה. כאמור לעיל, מנתוני המשטרה עולה כי בממוצע מאוישים תקני החוקרים במחלקי הסייבר בשלושה עד שישה חוקרים בלבד, ישנה פרישה מוגברת של מומחים ותיקים, היעדר כוח אדם איכותי במערך הסייבר, העדר תגמול הולם, הסבת החוקרים למשך זמן ממושך למשימות שאינן נוגעות לתחום הסייבר במיוחד במחוזות חוף וצפון. בפגישה שהייתה ביולי 2020 דיווח נציג מחוז חוף כי המצב במחוז לא מאפשר להתעמק בתיקי סייבר כנדרש, מאחר שמעט החוקרים במחלק נאלצים לעסוק בתיקים אחרים בהתאם לסדרי הקדימויות של הפיקוד. ראש מחלק מרכז שיקף בדיון את הפער שבין כמות תיקי הפשיעה במרחב המקוון שאותרו על ידי מס"א לבין היכולת לחקור אותם באמצעות מצבה של שני חוקרים בלבד המועסקים במחלק הסייבר.

בנובמבר 2020 מיפה ראש חוליית עבירות מחשב את התקן והמצבה של יחידות הפשיעה המקוונת בכל המחוזות. מתברר כי בכל המחוזות הוצאו חוקרים שייעודם לעבוד ביחידות הפשיעה המקוונת לסייע בפעילות שונה מזו שיועדה להם במחוז. במיפוי עלה כי במסגרת היותם של החוקרים כפופים ליחידות הימ"ר במחוזות הם נדרשים לבצע משימות שאינן קשורות לתחום עיסוקם, כך לדוגמה, מתוך מצבה של תשעה עובדים ביחידת הפשיעה המקוונת שבמחוז צפון, סופחו שניים למשימות אחרות במחוז.

בעקבות האמור, נבדק מצב התקן שקבעה המשטרה לחוקרי עבירות מחשב במחלקי הסייבר במחוזות אל מול המצבה שלהם, ולהלן הממצאים[87]:

87 מתוך טבלת כוח אדם תקן מול מצבה של המשטרה מיולי 2021. הנתונים הם של התקן והמצבה של חוקרי עבירות מחשב ומפקדי צוות ומחלק חקירות הסייבר בכל מחוז.

לוח 10: **נתוני תקן ומצבה של מחלקי הסייבר במחוזות**

	ימ"ר צפון	ימ"ר חוף	מחלק הסייבר[88] אח"מ תל אביב	יח' חקירות הונאה דרום וצפ"ם נגב	צפ"ם שרון ומרכז	ימ"ר ירושלים וש"י	סה"כ
תקן	7	7	11	6	6	9	46
מצבה	9	8	9	4	5	7	42
מוקצים בפועל לזי"ט[89]	4 (44%)	3 (37%)	3 (33%)	3 (75%)[90]	2 (40%)	2 (29%)	17

על פי נתוני משטרת ישראל, בעיבוד משרד מבקר המדינה.

מניתוח הנתונים בלוח מתברר כי בארבעה מתוך ששת המחוזות לא הושלם איוש תקן המשרות הקיים. נוסף על כך, בכל המחוזות חלק ממצבת החוקרים הוקצה למשימות שאינן חקירת פשעי סייבר, אלא למשימת מיצוי ראיות של משרדי הזי"ט. למעשה, מתוך מצבת כוח האדם בכל מחוז כ-38% (בממוצע) מחוקרי המחשב אינם עוסקים בתפקידים שיועדו להם במחלקי הסייבר. למעשה, מדובר בפער של 54% בין כוח האדם שהוקצה ודרוש לפעילות מחלקי הסייבר במחוזות לבין כוח האדם שמבצע את הפעילות.

בתשובתה של המשטרה היא עדכנה כי לאחר החלטת המפכ"ל ממאי 2021 להעברת מחלקי הסייבר מהימ"ר לכפיפות האח"מ המחוזי הושארו חלק מהשוטרים בימ"ר לצורך מתן מענה למיצוי ראיות. בהתאם לנתונים שיוצגו להלן, קטן מספר החוקרים בתקן ובמצבה אף ממספרם לפני החלטת המפכ"ל:

לוח 11: **נתוני התקן והמצבה המעודכנים של מחלקי הסייבר במחוזות**

	סייבר מחוז צפון	סייבר מחוז חוף	סייבר מחוז תל אביב	סייבר מחוז דרום	סייבר מחוז מרכז	סייבר מחוז ירושלים	סה"כ
התקן	7	5	9	6	6	6	39
המצבה	7	5	7	5	4	6	34

המקור: תשובת המשטרה מינואר 2022.

88 צוות סיגנטי משולב.

89 מתוך מצבת החוקרים.

90 במחוז דרום כל חוקרי פשיעה מקוונת פועלים במקביל גם בתחום הזי"ט.

פער זה בכוח האדם שפועל ביחידות הסייבר המחוזיות והקצאתם של חוקרי סייבר למשימות מיצוי ראיות בתחום הזי"ט צמצמו את כוח האדם שעוסק בפועל במשימות המחוזיות בתחום הסייבר ועלולים להביא לעומס במספר התיקים הממוצע לשנה שכל חוקר נדרש לטפל בהם. הדברים מקבלים משנה תוקף לנוכח נתוני התקן והמצבה המעודכנים בלוח שלעיל.

מומלץ כי המשטרה תבחן את הצרכים המקצועיים שהצביעו עליהם הצוות המשותף וחטיבת הסיגינט-סייבר בנוגע להגדרת התפקיד הנדרשת עבור חוקרי פשיעת סייבר ואת הנתונים הנוגעים לפערי התקינה מול המצבה בפועל ותגבש הסדרה כוללת של ניהול כוח האדם המקצועי במחלקי הסייבר. נוכח הצמצום בתקן (15%) ובמצבה (19%) של כוח האדם שפועל ביחידות הסייבר המחוזיות, על המשטרה לבחון האם גריעת החוקרים מעבודתם הסדירה במחלקי הסייבר פוגעת ביכולת הטיפול בעבירות במרחב המקוון ובמענה שניתן לציבור.

עוד יצוין כי ממסמכי חטיבת הסיגינט-סייבר עולה כי נדרשים יועצי סייבר, בין היתר, לשם מתן הכשרות מקצועיות ייעודיות בעלות של כשמונה מיליון ש"ח, ולשם כך נדרש תקציב ייעודי.

משרדי הזי"ט

משרדי הזי"ט הוקמו בשנת 2016 ובמהלך השנים השקיעה המשטרה משאבים לתגבור וחיזוק המשרדים באמצעות גיוס כוח אדם וברכישת המערכות הטכנולוגיות המתאימות. בבדיקת התקן והמצבה שבמשרדי הזי"ט בשנת 2021 התברר שיש פערים משמעותיים בין התקינה של משרדי הזי"ט (153) לבין המצבה (202). למעשה, מדובר בעודף של תפקידי חוקר מיומן הפועלים במעבדות פורנזיות ביחידות שאינן מתוקננות בתוכנית הזי"ט.

לוח 12: **התקן והמצבה במשרדי הזי"ט והכפיפות ליחידות השונות במשטרה**

מחוז	צפון	חוף	מרכז	תל אביב	דרום	ירושלים וש"י	להב - 433	מג"ב + את"ן	סה"כ
תקן	13	22	31	24	26	27	9	1	153
מצבה	24	27	39	32	32	33	10	5	202
עודף באיוש התקן	11	5	8	8	6	6	1	4	49

מנתוני הלוח עולה כי בכל המחוזות הוקצו חוקרים ושוטרים למשרדי הזי"ט בכ-33% ויותר מכוח האדם הנדרש על פי התקינה שנקבעה למשרדים אלה. העובדים הללו נגרעו מעבודתם ביחידות השונות במחוזות ובכך הקצאתם משנה את התפקיד שהם מבצעים באופן סדיר במחוזות ומאידך, יצרה מחסור של כוח אדם המיועד על פי התקינה הקיימת לעבוד בתפקיד אחר במחוז.

בתגובת המשטרה נכתב כי תקינת הזי"ט נקבעה בשנת 2015 בהתאם לגודל התחנה, וכי מאז נפח הראיות הדיגיטליות גדל באופן ניכר, הן בהיבט האגירה והן בתדירות השימוש. לפיכך יש להמשיך ולתכנן את המשמעויות המשאביות בתחום הפורנזיקה הדיגיטלית, לרבות הצורך במענה טכנולוגי מתאים לפוטנציאל הגלום בחומר מחשב, לשימוש חקירתי, מודיעיני וראייתי.

מומלץ כי המשטרה תפעל להסדרה של תקינת כוח האדם הנדרשת לפעילותם של משרדי הזי"ט על פי הצרכים המקצועיים בתחום התקשוב והטכנולוגיה.

כוח אדם זמני במשטרת ישראל

משרד מבקר המדינה התריע בביקורת הקודמת מ-2017, כי פרופיל כוח האדם שביכולתו להתמודד עם אתגרי הפשיעה המקוונת שונה מפרופיל כוח האדם הנדרש משוטרים העוסקים במשימות משטרתיות מסורתיות, והצביע על פערי שכר משמעותיים בין השכר של מועמדים לגיוס לתפקידים בתחום הסייבר במשטרה ובין השכר המקביל בעבודה אזרחית בתחום הסייבר באופן המקשה על גיוס כוח אדם מתאים טכנולוגית למשטרה[91].

במהלך 2020 החליטה המשטרה כי על מנת לעמוד בקצב המהיר של השינויים הטכנולוגיים, נדרש גיוס כוח אדם טכנולוגי צעיר ובעל פוטנציאל גבוה והצבתו במערכים המקצועיים הקיימים במחוזות כדי להוות מכפיל כוח משמעותי בלוחמה ובמניעת פשיעת סייבר. במסגרת ההסדרה נכתב כי בחינת הנושא מעלה כי המערכים המקצועיים במחוזות יצאו נשכרים מהמהלך כיוון שישנם פערים בהיקף כוח האדם ובמיומנויות המקצועיות הנדרשות ביחידות אלה, ובאפריל 2021 החלו בתהליכים למיסוד תהליך אסטרטגי לטובת איתור כוח אדם מקצועי ורלוונטי לעולמות הסייבר.

הנחת היסוד בהחלטת המשטרה היא הקושי לאתר שוטרי קבע לתחום הסייבר לאור התחרות הקשה עם חברות בשוק הפרטי ופערי השכר שהמשטרה אינה יכולה להתחרות בהם. נוסף על כך, יש צורך חיוני בכוח אדם צעיר בעל יכולת להתמודד עם אתגרים ולהסתגל במהירות לפלטפורמות טכנולוגיות ומידע דיגיטלי משתנה, ועל כן הוחלט על ארבעה מסלולי גיוס כוח אדם זמני כמתואר בלוח שלהלן.

91 דוח מבקר המדינה 67ב, עמ' 1896 - 1898.

לוח 13: **התקן והמצבה של כוח האדם הזמני בתחום הסייבר נכון לאוגוסט 2021**

	שח"ם[92] ייחודי לעולמות הסייבר	בני/בנות שירות לאומי	מתנדבים	חמה שמ"ז[93]
התקן	40	40	--	30
המצבה	18	25	12	5

מן הנתונים בלוח עולה כי במסלולי גיוס כוח האדם הזמני, ובמיוחד ביחס לשמ"זים, קיים פער בין התקן לבין המצבה ולמעשה, גם הפתרון הזמני שגיבשה המשטרה אינו נותן מענה מלא לבעיית גיוס כוח האדם לטיפול בפשיעה מקוונת.

באוגוסט 2021 מסרה המשטרה למשרד מבקר המדינה, כי בכוונתה לעדכן את תנאי העסקתם של השמ"זים בשל הפער שעדיין קיים בין תנאי המשק לבין התנאים המוצעים להם, לרבות טבלאות השכר, תקצוב הכשרות עבורם, אפשרויות קידום ואפשרות הארכת ההסכם עימם.

הסתמכות על עובדים זמניים בתחום הסייבר במשטרה אינה יכולה למלא את המחסור בכוח אדם מיומן וקבוע. הממצאים האמורים מצביעים על הצורך בבחינה של דרכים נוספות לצמצום הפער בין הצרכים במערכי הסייבר והזי"ט לבין כוח האדם שהמשטרה מסוגלת לגייס, ולצורך זה בין היתר, לבחון את העלות הכלכלית הנוספת הדרושה לכך.

בינואר 2022 הודיעה המשטרה למשרד מבקר המדינה כי היא מקיימת משא ומתן עם משרד האוצר בנושא עדכון שכר השמ"ז הטכנולוגיים. כמו כן במסגרת הסכם גג השכר שנחתם בין הגופים האמורים נבחנת האפשרות לשדרג את שכר כוח האדם המקצועי בתחום זה, הזמין לגיוס.

התכנון והניהול של המשאבים החומריים במערך הסייבר והזי"ט

בדיון מפברואר 2021 בלשכת המפכ"ל בנושא התוכנית האסטרטגית של המשטרה לשנת 2021 נרשם מפי המפכ"ל כי מהבחינה הטכנולוגית על המשטרה "להיות תמיד צעד לפני הפשיעה. אנליטיקה, בינה מלאכותית, סייבר, היערכות לקליטת מסת מידע, הגנת תשתיות ואבטחת מידע, חזון טכנולוגי... חיזוי אירועים על בסיס ניתוח המידע".

92 שירות חובה במשטרה.

93 שירות משטרה זמני - אנשי מקצוע המועסקים בתנאי שכר מיוחדים על פי סיכום בין משרדי האוצר והבט"פ.

משרד מבקר המדינה בדק את מידת ההתאמה של הציוד שיש במשטרה ואת היקף הרכש הנדרש של העזרים והכלים הטכנולוגיים לשם מניעת עבירות ואיתור עבריינים במרחב המקוון. להלן הממצאים:

התשתית הטכנולוגית והציוד

בשנים 2018 עד 2020 אפיינה משטרת ישראל את יעדי ההצטיידות של יחידות הסייבר, הארצית והמחוזית, וכן את יחידות הזי"ט בתוכניות רכש. תוכניות הרכש כללו אמצעים טכנולוגיים שונים ובהם: מחשבים פורנזיים, אמצעי אחסון מידע נייחים וניידים, מחשבים ומסכים ורישיונות לתוכנות מחשב מגוונות ובהן תוכנות פורנזיות. עלות רכישת הציוד הסתכמה בשנת 2019 בסך 7.838 מיליון ש"ח ובשנת 2020 בסך 11.475 מיליון ש"ח, כמתואר להלן:

לוח 14: **עלות הרכש המתוכנן ליחידות הסייבר והזי"ט, 2019 - 2020 (באלפי ש"ח)**

היחידה	2019	2020
יחידת הסייבר במחוזות	3,765	1,570
היחידה הארצית (להב - סייבר)	655	1,005
יחידת הזי"ט	3,418	8,900

על פי נתוני המשטרה, בעיבוד משרד מבקר המדינה.

לפי הנתונים בלוח, עלות הרכש המתוכנן ליחידות הסייבר והזי"ט גדלה בשנים 2019 עד 2020 בכ-46%, אולם מרביתה יועדה למחלקי הזי"ט: 44% מעלות הרכש לשנת 2019 ו-77% מעלות הרכש לשנת 2020.

על אף יעדי הרכש שקבעה המשטרה ליחידות הסייבר והזי"ט, בדיונים שונים ובבדיקות עיתיות שנעשו ביחידות השונות התברר כי קיים מחסור ניכר בציוד בסיסי ומתקדם ביחידות הסייבר והזי"ט, שאינו עומד בהלימה עם תוכניות הרכש לשנים 2019 עד 2020.

על פי תוכנית הרכש לשנת 2019, העלויות הכרוכות במילוי החוסרים בציוד הן כדלקמן: חידוש רישיונות, תפעול שוטף והכשרות לשימוש במערכות הטכנולוגיות במשרדי הזי"ט - כ-3.4 מיליון ש"ח; חידוש רישיונות, תפעול שוטף והתעצמות בציוד הטכנולוגי במחלקי הסייבר במחוזות - כ-3.8 מיליון ש"ח; כל האמור ביחידת הסייבר בלהב - כ-655,000 ש"ח; בסך הכול כ-8 מיליון ש"ח. על פי תוכנית הרכש לשנת 2020, העלות המתכללת להשלמת הציוד בהתאם לרכיבים האמורים עבור 80 משרדי הזי"ט הסתכמה בכ-8.9 מיליון ש"ח; עבור המחוזות - כ-1.57 מיליון ש"ח; ועבור יחידת הסייבר הארצית - כ-1.05 מיליון ש"ח ובסך הכול כללא מיליון ש"ח לצורך הצטיידות מערך הסייבר והזי"ט.

המחסור באמצעים האמורים פוגם ביכולת האיסוף המודיעינית ובאמצעי התקיפה לסיכול פשיעת סייבר ומקשה על החוקרים לאתר פעילות עבריינית במרחב המקוון ולהתחקות אחריה. בהיעדר אמצעים טכנולוגיים כאמור מתקשים מערכי הסייבר והזי"ט למצות ראיות דיגיטליות בכלל האירועים.

יצוין כי המחסור כאמור אוזכר גם בדוחות הבקרה שביצע קצין פשיעה מקוונת ארצי בפברואר ובאפריל 2021 במחלקי פשיעה מקוונת במחוזות תל אביב והצפון[94].

על פיקוד אח"ם לקדם את צמצום פערי הרכש וההצטיידות באמצעים טכנולוגיים ובמשאבים חומריים נוספים למאבק בעבריינות במרחב המקוון כאמור.

התקשרויות לביצוע רכש טכנולוגי: רכש של אמצעים וכלים מבצעיים של המשטרה הכרחי לצורך עמידתה של המשטרה באתגרים שעומדים בפניה במרחב המקוון. כדי לעמוד באתגר זה החליטה המשטרה שיש להתעצם בכלים שעומדים לרשותה בשים לב להתקדמות הטכנולוגית שמאתגרת אותה אך גם מספקת פתרונות חדשים.

בינואר 2021 פנתה המשטרה אל משרד האוצר וביקשה לשרטט לפניו את הקשיים שבהם נתקלה ברכישת אמצעים טכנולוגיים, ובהם הצורך לבחון את התאמת המוצר לצורכי המשטרה טרם רכישה והקושי בכתיבת מפרט טכני של האמצעי הטכנולוגי ללא היכרות מספקת עם הפתרונות הקיימים בשוק.

המשטרה כתבה כי ביצוע בדיקת התאמה של מוצר אשר כוללת התקנה שלו על מערכות המשטרה תוך התנסות מעשית בכלים ובחינת ההתאמה במסגרת ניסוי והתנסות היא הכרחית בסוג זה של אמצעים, ויש לבחון את התאמת המוצר בפעילות שטח ולא בתנאי מעבדה. המשטרה הוסיפה כי המצב המשפטי הנוכחי מקשה עליה לרכוש אמצעים טכנולוגיים בהתאם לחוק ולתקנות חובת המכרזים והליכי RFI ו-RFD (בקשה לקבלת הצעות וביצוע הדגמה). משרד האוצר טרם השיב לפנייה זו.

מן המקובץ עולה כי בפני המשטרה ניצבים חסמים משפטיים לביצוע רכש המוצרים הטכנולוגיים הנדרשים.

בתגובתו על ממצאי הביקורת מינואר 2022 כתב משרד האוצר, כי במסגרת דיוני התקציב הוסכם כי החל בשנת 2022 יינתן תקציב תוספתי של 55 מיליון ש"ח עבור פרויקטים טכנולוגיים במשטרה. סכום זה נוסף על סכום של 40 מיליון ש"ח שכבר הועבר לקרן הטכנולוגיות של המשטרה, ובסך הכול עומדים לרשותה 95 מיליון ש"ח בכל שנה עבור פיתוח טכנולוגיות. במסגרת הסיכומים נאמר כי התקציב יוקצה, בין היתר, למיזמי תשתיות ופיתוח הנוגעים למאבק בעבריינות המקוונת, כגון חוות שרתים ומערכות איסוף מודיעין וניתוחו.

94 קצין פשיעה מקוונת ארצי פועל במדור סיוע חקירתי בחטיבת החקירות במשטרה.

כדי לממש את התוכנית האסטרטגית ואת יעדי המפכ"ל, מומלץ שאח"ם ימפה את צורכי מערך הסייבר והזי"ט בתחום המשאבים החומריים, בדגש על החסרים בציוד הטכני ובאמצעים הטכנולוגיים, יחשב את עלותם ויעביר לבחינה ולאישור פיקוד המשטרה הבכיר את המיפוי הכולל לשם קבלת החלטה בנוגע לרכש הנדרש.

תקצוב

1. במרץ 2021 מינה המפכ"ל צוותי עבודה אסטרטגיים בנוגע לתפקיד השוטר העתידי בהיבטי חקירה, סיכול ומניעה, תוך גיבוש חזון טכנולוגי רב-ממדי. ביוני 2021 הגיש למפכ"ל את מסקנותיו צוות "עליונות טכנולוגית בשיטור" בראשות קצין בדרגת תת-ניצב, ובעקבות זאת המליץ הצוות על הקמת מערכת היתוך מידע מבוססת בינה עסקית ומלאכותית (A.I) הכוללת, בין היתר, התרעות מורכבות מבוססות זיהוי פנים ואמצעים נוספים וכן יכולת עיבוד תמונה וסרט עם מידע גלוי לשם יצירת התרעות מודיעיניות על בסיס זיהוי אובייקטים וזיהוי קשרים ביניהם. ואלה המשימות הנדרשות לכך: הקמת בריכת נתונים[95], ניתוח נתונים ממערכות, אלגוריתמיקה למימוש בינה עסקית ומלאכותיות ופיתוח לקבלת התרעות במערכות טכנולוגיות משיקות. עלות ההיערכות המשוערת מסתכמת ביותר מ-251.5 מיליון ש"ח.

2. באפריל 2021 הציגה חטיבת הסיגינט-סייבר בפני המפכ"ל וראש אח"ם כמה כיווני פעולה מרכזיים להתנעת תהליך ההתעצמות של המשטרה בתחום הסייבר. בתחום הטכנולוגי מופו הצרכים המשטרתיים, ונמצאו פערים ניכרים במספר הכלים הטכנולוגיים הדרושים במערך הסייבר והזי"ט. הכלים הטכנולוגיים הדרושים כללו כלי איסוף מודיעין, מחקר, יועצים והכשרות ייעודיות, וניתנה הערכה תקציבית של כ-90 מיליון ש"ח להצטיידות באמצעים אלה.

   יצוין כי דוח הצוות המשותף המליץ כי צוות מחשוב וטכנולוגיה של הוועדה המתמדת יבצע מיפוי צרכים לרכישה של כלים מרכזיים להתמודדות עם אתגרי פשיעת הסייבר - הן ברמה המודיעינית והן ברובד החקירתי, כנהוג בשוק הפיננסי שבו מוצעים כלים רבים, ולכן יש לבחון רכישת מוצרי מדף קיימים עבור גופי האכיפה, במקום לשקוד על פיתוח עצמי של כלים חדשים.

ההצטיידות בכלים טכנולוגיים מתקדמים הכרחית כדי לאפשר למשטרה להתמודד עם האתגרים של הפשיעה המקוונת באופן מיטבי, אולם העלויות של ההצטיידות בכלים טכנולוגיים אלה הן משמעותיות וצפויות להיות מאות מיליוני ש"ח. מומלץ כי המשטרה ומשרד האוצר יבחנו את האופן שבו ניתן יהיה להסיר חסמים תקציביים שעומדים בפני המשטרה כדי לממש באופן המיטבי את הצורך בהתעצמות הטכנולוגית המתבקשת ולנוכח הפשיעה הגואה במרחב המקוון.

95 Data lake - צורת אחסון נתונים שמטרתה לאסוף את כל המידע הקיים בארגון בנושא מסוים במאגר מרכזי אחד, ללא הבחנה בין צורתם או תבניתם של הנתונים.

בתגובתה הודיעה המשטרה כי היא מקבלת את ההמלצה ותפעל עם משרד האוצר בנושא. בתגובת המשרד לבט"פ למשרד מבקר המדינה נכתב כי לאחרונה העבירה המשטרה למשרד לבט"פ בקשה להקמת מדור פשיעה דיגיטלית שייעודו יחידת מטה מקצועית הנושאת באחריות להליכי פיקוח, בקרה, הכוונה, אפיון והטמעה בקרב מערכי ההונאה, הפשיעה המקוונת והפורנזיקה הדיגיטלית ביחידות החקירה ומיצוי הראיות הפרוסות במשטרה. על פי האמור בתשובה, פקודת ארגון בנושא זה אושרה על ידי מנכ"ל המשרד לבט"פ ב-12.1.22 והועברה לאישור השר.

לאור המלצות הצוות המשותף והצרכים שהועלו במשך השנים מאז הביקורת הקודמת, מומלץ כי הוועדה המתמדת תבצע מיפוי צרכים של תשתית טכנולוגית להתמודדות כוללת עם העבריינות במרחב המקוון, אשר ישמש בסיס להליכי בחינה והחלטה לצורך שיפור היכולות המבצעיות הקיימות של המשטרה. במסגרת זו יש לתת את הדעת על התאמת מערכות המידע לצורכי המודיעין והחקירות, הנגשת הכלים הטכנולוגיים, פיתוח מאגרי המידע, מקורות המידע ותהליכי עיבוד המידע וניתוחו.

הכשרת בעלי תפקידים למאבק בעבריינות במרחב המקוון

בניית תוכנית עבודה בתחום הלמידה, ההדרכה וההשכלה נועדה להבטיח את פיתוחו של ההון האנושי ולהקנות, הלכה למעשה, לעובדים ומנהלים כאחד, ידע וכלים מקצועיים לפיתוח מיומנויות. תכנון ההדרכה אמור להתמקד בשתי אבני דרך: התאמת המענה ההדרכתי לסוגי האוכלוסיות הפועלות בכל תחום (כך, למשל, הבחנה בין הדרג המבצעי לדרג הפיקודי ובין דרג המטה לדרג השטח) והתאמת המענה ההדרכתי למחזור חיי העובד.

המאבק בעבריינות במרחב המקוון מחייב שימוש בכלים טכנולוגיים ומיומנויות מקצועיות חדשניות לשם מניעת העבירות, חקירתן, זיהוי החשודים והעמדתם לדין. תוכנית עבודה להכשרת בעלי תפקידים העוסקים במאבק בעבריינות במרחב המקוון אמורה גם להתאים את תוכני ההכשרות למגמות ולשינויים המתרחשים בתחומי הטכנולוגיה ולהשפעותיהם על הפשיעה. ידע רחב ומיומנויות מקצועיות חדשניות הם חלק מהותי מכשירותם של בעלי התפקידים הנוגעים בדבר - בכל רשויות החקירה, התביעה והשפיטה, בנוגע לכלל היבטי הפעילות הארגונית והבין-ארגונית, במישורים המודיעיניים, החקירתיים, המבצעיים, המחקריים והמשפטיים.

בפורום ראשי מחלקי הסייבר במחוזות, המתקיים מפעם לפעם, עלו כמה פעמים צרכים ופערים הנוגעים לתחום הידע וההכשרות של בעלי התפקידים: בפברואר 2020 דיווחו ראשי מחלקי הסייבר כי בקרב דרג הפיקוד במשטרה אין הבנה של תחום פשיעת הסייבר, ולכן יש צורך בהכשרת מפקדים בתחום זה. ביולי 2020 הם העלו קשיים הנוגעים למטבעות קריפטוגרפיים וציינו כי חסר ידע בנושא בכל גופי האכיפה. במרץ 2021 הועלה כי יש לקיים הכשרות נוספות מלבד אלו המקובלות כדי להעלות את הרמה המקצועית בכל רבדי הפעילות המשטרתית בטיפול בעבריינות במרחב המקוון.

הממצאים מצביעים על פערי ידע בנוגע לשימוש בכלים טכנולוגיים ומיומנויות מקצועיות חדשניות לשם מניעת העבירות, חקירתן, זיהוי החשודים והעמדתם לדין. קיום הכשרות בתחום הסייבר חיוני כדי לאפשר למשטרה ולמערכת המשפט להשתלב בעשייה הדיגיטלית של יתר הרשויות העוסקות בטיפול בעבריינות במרחב המקוון ולשתף פעולה עם ארגונים עמיתים בחו"ל, שבהם כבר הוטמעו השינויים הטכנולוגיים הנדרשים להתמודדות עם העבריינות בזירה זו. ההכשרות המקצועיות לחוקרי הסייבר, לדרג הפיקודי, לפרקליטים ולשופטים דרושות גם כדי לחזק את אמון הציבור ביכולתם של גופי האכיפה ובתי המשפט לתת מענה לעבריינות בזירה זו.

הכשרת שוטרים בעידן הדיגיטלי

באפריל 2021 פרסמו אגף ההדרכה והמכללה הלאומית לשוטרים (להלן - המכללה) תוכנית מקיפה להקמת מרכז הכשרות ייעודי לשיטור דיגיטלי (להלן - תוכנית ההכשרות לשיטור דיגיטלי). בעבודת המטה שקדמה לתוכנית זוהו פערים ניכרים בין הדרישות המקצועיות העדכניות הנדרשות משוטרים בכל הדרגים לנוכח הסתגלותם של העבריינים להתקדמות

הטכנולוגית - הן במרחב הפיזי והן במרחב המקוון - ובין כשירותם החלקית להפעיל את סמכויותיהם במציאות משתנה זו.

1. לפי התוכנית האמורה, רוב בעלי התפקידים במשטרה ילמדו את מקצועות השיטור בעידן הדיגיטלי, בהתאם לתו תקן ארגוני שייקבע לכל אחד מהם. זאת בשונה מהמצב הנוכחי ולפיו רק לשוטרים העוסקים בחקירת פשעי סייבר מוקנה הידע בתחומים אלה. במסגרת המוצעת יוכשרו שוטרי שטח, שוטרי פנים ושוטרים ממערך הסייבר וכן מפקדי תחנות, מרחבים ומחוזות.

התוכנית קובעת כי המציאות מחייבת את המשטרה להפוך למשטרה "חכמה" שבה לשוטר מיומנויות מתאימות להתמודד עם העולם הדיגיטלי והשינויים הטכנולוגיים ולהיות שחקן רלוונטי מול ארגונים מקבילים בחו"ל. בדרך כלל הכשרות השוטרים כוללות את הקורסים הנדרשים האלה: קורסים בסיסיים, קורסים מתקדמים וקורסי פיקוד. כמו כן מתקיימות הכשרות ייעודיות על פי מקצוע השיטור: סייר, בוחן תנועה, חוקר וכדומה; בתוספת הכשרות רוחביות לכל השוטרים, ימי עיון ייעודיים והשתלמויות. לפי תוכנית ההכשרות לשיטור דיגיטלי, בעידן החדש יש להכשיר את השוטר גם להתמודדות עם העבריינות במרחב המקוון ולהקנות לו מיומנות נוספות ובהן, בין היתר: אוריינטציה טכנולוגית בסיסית; הכרת עולם הרכב הדיגיטלי, ובכלל זה מערכות מולטימדיה, רכבים אוטונומיים ומצלמות מהירות; זיהוי ארנקים דיגיטליים; חיפוש ב"בית חכם"; אפיון זירה שבה נמצאו מצלמות, אנטנות ורכיבים טכנולוגיים נוספים[96].

> תוכנית ההכשרות לשיטור דיגיטלי מיועדת כאמור לרוב בעלי התפקידים במשטרה, אולם היא אינה מיועדת למוקדנים וליומנאים המשרתים בתחנות המשטרה.

בתגובתה אישרה המשטרה כי אכן נדרשת הכשרה ייעודית למוקדנים וליומנאים אולם אין לה עדיין את כוח האדם ואת הכלים הנדרשים לשם הכשרתם.

> נוכח המחסור בידע, במידע, בכלים ובתשומות פיקודיות הנוגעים לעבריינות במרחב המקוון, על המשטרה להיערך לקיום הכשרה מקצועית ייעודית ומשמעותית לשוטרים בכל הדרגים, שבאמצעותה ירכשו את המיומנויות הנדרשות בעידן הדיגיטלי לשם ביצוע מיטבי של התפקידים המוטלים עליהם.

2. ממסמכי אגף ההדרכה עולה כי המצב הנוכחי מחייב שינוי תפיסה בפיקוד המשטרה ומתן משאבים ותשומות להקמת מרכז ההכשרות לשיטור דיגיטלי שבמרכזו קורסים להקניית ידע, הנגשת כלים טכנולוגיים ויצירת מנגנון לכשירות מבצעית של השוטרים בכל הדרגים. תוכנית ההכשרות לשיטור דיגיטלי כוללת שלושה שלבים: שלב א' - הפעלת תוכנית הרצה בשנת 2021 שעיקרה מתן מענה לבעלי תפקידים מוגדרים במשטרה; שלב ב' - הפעלת תוכנית עוגן בשנת 2022 ובכלל זה קיום כלל הקורסים למעט הכשרות רוחביות; שלב ג' -

96 ביוני 2021 כתב איגוד האינטרנט הישראלי למשרד מבקר המדינה כי נדרשת הכשרת סייבר ייחודית גם לשוטרים המשרתים במרכזי השירות לאזרח, המקבלים את תלונות הציבור, מאחר שהם אינם מודעים להשפעות הפגיעה המקוונת על הפרט.

הפעלת תוכנית מלאה בשנים 2023 עד 2025 לשם הכשרת כל השוטרים בהתאם לתו התקן הארגוני שנקבע להם.

על פי נתוני המכללה, לשם ביצוע שלב א' נדרשת השלמה של שמונה תקני משרות חסרים בדרגות רב-פקד, פקד ונגד; לביצוע שלב ב' נדרשים 27 תקנים נוספים; ואילו לביצוע שלב ג' נדרשת תוספת של 45 תקנים בסך הכול.

נכון למועד סיום הביקורת סגל הפיקוד הבכיר של המשטרה טרם אישר את תוכנית ההכשרות לשיטור דיגיטלי; לא אושר תקציב ייעודי ולא אושרה תוספת התקנים. לפיכך עד מועד תום הביקורת, התוכנית לא החלה לצאת לפועל, ובענף שיטור דיגיטלי במכללה מתקיימים רק קורסים בסיסיים הנוגעים לעבירות מחשב, שאינם עוסקים בשמירת כשירות השוטרים בעידן הדיגיטלי וברכישת המיומנויות הדרושות לכך.

בתגובתה פירטה המשטרה את הפעולות שנעשו במכללה לשוטרים והודיעה כי יופנו משאבים עבור הכשרות לכלל הגורמים לרבות הדרג הפיקודי, וכן לגופים שעימם נמצאת המשטרה בשיתוף פעולה. המשטרה תקדם את הלמידה של שיטות ההדרכה בתחומי הסייבר מארגונים עמיתים בחו"ל, שיכללו ביקורים והשתתפות בכנסים מקצועיים ייעודיים. עוד נכתב בתגובת המשטרה כי הוחלט על הקמת מדור פשיעה דיגיטלית בחטיבת החקירות אשר תעבוד בשיתוף חטיבת הסיגינט-סייבר לשם התכנון והפיתוח של ההכשרות הייעודיות לחוקרי הפשיעה המקוונת. בד בבד - עדיין נדרש להמשיך לפתח ולתקצב הכשרות נוספות לאוכלוסיות השוטרים השונות.

בתגובת המשרד לבט"פ נכתב כי פקודת ארגון בנושא זה אושרה על ידי מנכ"ל המשרד ב-12.1.22 והועברה לאישור השר.

3. בדצמבר 2020 ביצעה חטיבת המודיעין במשטרה, לבקשת חטיבת הסיגינט-סייבר, סקירה של הכשרות בארגונים ובמוסדות בחו"ל עבור בעלי תפקידים בתחום הסייבר (להלן - מסמך ההכשרות), על פי מסמך ההכשרות, ישנם קורסים וסמינרים בחלק מהמדינות הניתנים בחינם ואף מאפשרים הסמכה מרחוק של בעלי תפקידים באמצעות קורסים מקוונים או סמינרי רשת (וובינר).

לוח 15: **הכשרות סייבר במוסדות וארגוני אכיפת חוק ברחבי העולם**

המדינה	סוג ההכשרה	הארגונים המכשירים
ארה"ב	מיצוי מודיעין גלוי; הכשרה טכנית; מחקר ופיתוח; בדיקה והערכה; פיתוח יכולות ניתוח סייבר תומך מודיעין; חקירות פליליות במרחב המקוון; אכיפת החוק הפדרלי והמדינתי - לתובעים ולשופטים; חקירת פשע אלקטרוני ברשת חברתית מקוונת	מרכז הסייבר לאכיפת חוק (LECC); מרכז ההגנה לפשיעת סייבר (DC3); משרד המשפטים - פשעי מחשב וקניין רוחני (CCIPS); FBI - Cyber Shield Alliance; מרכז הכשרה לאכיפת החוק הפדרלי (FLETC); המכון הלאומי לזיהוי פלילי במחשב (NCFI); המרכז הלאומי להכשרת צדק פלילי (NCJTC); ועוד
האיחוד האירופי	אוסינט[97] וטכנולוגיית מערכות מחשוב; אבטחת מידע והגנת סייבר; הרשת האפלה ומטבעות מבוזרים; תחקור אתרים	האקדמיה לפשיעת סייבר של הסוכנות לאכיפת החוק של האיחוד האירופי בבודפשט (CEPOL[98]).
בריטניה	חקירות מרשתת; פשיעת סייבר	משטרת לונדון
אוסטרליה	הכשרה בין-ארגונית של סוכנויות ביטחון בתחום אבטחת הסייבר הלאומי	המרכז הממשלתי לאבטחת סייבר (ACSC)
קפריסין	פשיעת סייבר ואופן השימוש בראיות דיגיטליות	המכון לביטחון ציבורי, סייבר וביטחון לאומי (UNIC)
הודו	הכשרות שונות במבנה ללוחמה בפשיעת סייבר	האקדמיה הלאומית לשוטרים - המחלקה לפשעים דיגיטליים (NDCRTC)

המקור: אח"ם - חטיבת המודיעין, "מענה אודות הכשרות סייבר בחו"ל" (13.12.20).

הנתונים המפורטים בלוח מצביעים על מגוון מערכי הכשרה ייעודיים לשוטרים בתחום הפשיעה הדיגיטלית במערכות אכיפת החוק במדינות שונות בעולם. במועד סיום הביקורת נמצא, כי גורמי ההכשרה במשטרה החלו בחינה ראשונית בלבד של האפשרות לשלב את תכניות ההכשרה המפורטות במסמך כחלק ממערך ההכשרות או להיעזר בהן לצרכי שיתוף פעולה בין-לאומי.

97 Open Source Intelligence – OSINT, מודיעין ממקורות גלויים.

98 European Union Agency for Law Enforcement Training - האקדמיה לפשיעת סייבר של הסוכנות לאכיפת החוק של האיחוד האירופי.

מומלץ לאגף ההדרכה ולמכללה להשלים את בחינת מידת התאמתן של מגוון תוכניות ההכשרה המפורטות במסמך ושילובן במערך ההכשרות המיועדות עבור שוטרים ולתפריט המוצע בתוכנית ההכשרות לשיטור דיגיטלי. מומלץ כי המשטרה תקדם שיתוף פעולה בין-לאומי בתחומי ההכשרות המקצועיות, לרבות ברישום לקורסים מקוונים שניתנים בחו"ל.

בתגובתה ציינה המשטרה כי בכפוף להקצאת תקציבים ייעודיים, ענף שיטור דיגיטלי במכללה פועל להקמת מערך קשרי חוץ אל מול גורמים מקצועיים בארץ ובחו"ל.

הכשרת חוקרים ותומכי חקירה במדעי הסייבר

1. דוח הצוות המשותף של הוועדה המתמדת העלה כי יש במשטרה מחסור בחוקרים מיומנים הבקיאים באופן הפעולה של השווקים ונותני השירותים הפליליים ובטיפולוגיות הפעילות העבריינית במרחב המקוון. לרבים מן החוקרים חסר ידע בנוגע לאופן שבו מבוצעת הונאת משקיעים רחבת היקף וחוצת גבולות באמצעות נכסים וירטואליים, והם אינם מיומנים בזיהוי היבטי סייבר במסגרת הפעילות הפלילית והפעילות הפיננסית של החשודים, המצריכים הסתייעות במומחה לפשיעת סייבר ואת מעורבותו בתיק החקירה.

ניתוח תוכניות ההכשרה המפורטות בתיקי היסוד העלה, כי התוכניות נוגעות רק במקצת התכנים הנדרשים ומשכן קצר ביחס לתוכניות הקיימות בשוק הפרטי. המצאי הקיים בתחום ההכשרה המשטרתית בנושא זה אינו כולל את התכנים האלה בהיקף הנדרש: סביבות ענן; רשתות תקשורת; יישומונים חברתיים; רשתות ארגוניות, כתיבת סקריפט; OSINT (מודיעין ממקורות רשתיים גלוים); חקירת נוזקה (Malware). לשם השוואה, מבוא לקורס חוקר סייבר אורך 31 שעות הדרכה במכללה לשוטרים, ואילו קורס מקביל בשוק הפרטי הוא בהיקף של 120 שעות הדרכה; פורנזיקה בסביבת Windows נלמדת במכללה במשך תשע שעות הדרכה בלבד, בעוד בשוק הפרטי קורסים דומים הם בני 50 שעות הדרכה. יצוין כי מסלולי הכשרה מקובלים של חוקר עבירות סייבר נמשכים בין 800 ל-1,300 שעות הדרכה, בעוד שבמכללה לשוטרים ההכשרה הכוללת מסתכמת בפחות מ-200 שעות.

נדרשת אפוא הכשרה של החוקרים בכמה רבדים: רובד בסיסי - זיהוי סממני עבריינות במרחב המקוון המצריכים סיוע מקצועי בתחום הסייבר; רובד מתקדם - זיהוי האמצעים הטכנולוגיים שבהם התבצעו העבירות; רובד מחקרי - הבנת הדגם העסקי של פעולות ההונאה המתוחכמות.

2. בשנים 2016 עד 2020 פותחו תוכניות הכשרה לשוטרים ולחוקרים בתחום התקשוב והסייבר במטרה להשלים את פערי הידע במשטרה הנוגעים לפיתוחים טכנולוגיים ולחידושים בתחום העבריינות במרחב המקוון ולדרך להתמודד איתה. להלן רשימת ההכשרות שהתקיימו בנושאים האמורים:

לוח 16: **ההכשרות הפעילות בתחום התקשוב והסייבר במשטרת ישראל, 2016 - 2020**

שם ההכשרה	שנת פיתוח ההכשרה	בעלי התפקידים הרלוונטיים
CCPA	2016	חוקר מחשב מיומן
תיק"ן[99] ווביגט בסיסי	2013 (עודכן ב-2017)	שוטר צס"ם[100] בתפקיד תו"ם[101] / ווביגט[102] שוטרים ביחידות הסייבר במחוזות ובחטיבת הסיגינט-סייבר
חוקר מחשב מיומן מתקדם	2018	חוקר מחשב מיומן
השתלמות חומרת סלולר	2019	חוקר מחשב מיומן
מיצוי ראיות ומידע מחומר מחשב	2019	חוקרים, שוטרים ובעלי תפקידים מרשויות האכיפה ומהממשלה
חוקר סייבר	2019	חוקרי מחלקי סייבר במחוזות, ביחידת הסייבר הארצית ובחטיבת הסיגינט-סייבר והחקירות
תיק"ן ווביגט מתקדם	2019	שוטר המוגדר כתפקידן תו"ם/ווביגט בכל היחידות
הכשרת סייבר - עולם הרשת ותקשורת נתונים	2020	קצינים ושוטרים במערך סיגינט-סייבר
השתלמות על תוכנה פורנזית MA	לא נכתב	חוקר מחשב מיומן
מיומן ויזנט[103]	לא נכתב	חוקרים, בלשים, עובדי מעקב טכני ובוחני תנועה וכן בעלי תפקידים אחרים מרשויות האכיפה והממשלה

המקור: מסמך הכשרות בתחום הסיגינט והסייבר במכללה.

99 תקשורת נתונים.

100 צוות סיגינטי משולב.

101 תפיסה ומחשב.

102 Web Intelligence.

103 ויזנט - מודיעין המתמקד במידע חזותי.

לוח 17: **ההכשרות שהתקיימו במכללה בתחום התקשוב והסייבר, 2021 - 2020**

שם ההכשרה	מספר המשתתפים
חוקר פשיעה מקוונת	33
מיצוי ראיות ומידע מחומר מחשב	35
תיק"ן וובינט בסיסי	18
מפיקי תיק"ן מתקדם	12
הכשרת סייבר - עולם הרשת ותקשורת נתונים	130

על פי נתוני המכללה לשוטרים, בעיבוד משרד מבקר המדינה.

מן הנתונים שהוצגו עד כה עולה, כי בשנת 2019 החלה המכללה להפעיל את ההכשרה המקצועית המתקדמת של שוטרים במקצועות הסייבר. עוד עולה כי בשנים 2020 עד 2021 התקיימו רק מחצית מקורסי ההכשרה שפותחו בתחום הסייבר (חמישה מתוך עשרה). נוסף על כך בפרק זמן זה רק כ-38% ממצבת העובדים (228 מתוך 600) המועסקים ביחידות הסייבר השונות הוכשרו לעסוק בתחום זה.

מומלץ כי המכללה לשוטרים תגדיל ככל הניתן את מספר הקורסים המיועדים להכשרות בתחום הסייבר בהתאם לאמור בתוכניות ההכשרה. עוד מומלץ, כי המשטרה תפעל להגדיל באופן ניכר את מספר המשתתפים בקורסי ההכשרה כדי להשלים את הכשרתם של כלל השוטרים העוסקים במאבק בעבריינות במרחב המקוון, בהתאם לדרישות התפקיד ולמשימות שאותן הם נדרשים למלא.

נמצא, כי במכללה לשוטרים לא נקבע מערך סדור לשמירת הכשירות של העובדים בתחום הסייבר לאורך החיים המקצועיים שלהם.

על המכללה לשוטרים לבנות תוכנית סדורה לשמירת הכשירות של השוטרים המועסקים ביחידות הסייבר השונות ולשלב אותה במערך ההכשרות בתחום הסייבר.

בתגובתה ציינה המשטרה כי בכפוף להקצאת משאבים היא תבחן העברת חלק מהקורסים למגזרים נוספים במשטרה, ובכך תייעל את אופן הטיפול בתיקים.

3. דוח הצוות המשותף ציין את בעיית היעדר האוריינות של חוקרי עבירות כלכליות בנוגע לפעילות העבריינית שמתבצעת באמצעות נכסים וירטואליים ואמצעי תשלום מתקדמים מבוססי טכנולוגיה (FINTECH).

נוכח זאת המליץ דוח הצוות המשותף לפתח בקרב גורמי החקירה, המודיעין והתביעה הבנה רחבה של אופיים המגוון והמתפתח של הנכסים הווירטואליים, של אופן השימוש בהם ושל

אופן פעולת השווקים והשירותים הקשורים אליהם; של יכולות הניטור, האיתור, הניתוח והחקירה של הפעילות בנכסים הווירטואליים; של שיתופי הפעולה הבין-לאומיים הנדרשים בתחום זה; ושל הכלים הטכנולוגיים הדרושים לשם כך.

עוד המליץ הדוח כי הוועדה המתמדת תקים מרכז ידע להתמודדות עם העבריינות במרחב המקוון שירכז את פעילות המחקר והפיתוח של האמצעים הטכנולוגיים הנדרשים לשם אכיפה אפקטיבית נוכח האיומים הנוכחיים והעתידיים. המרכז יעמוד בקשר עם האקדמיה, עם מומחים מקצועיים ועם חברות המתמחות בתחומי הטכנולוגיה הרלוונטיים, ויכלול מעבדה טכנולוגית המשותפת לו ולגופי האכיפה והביטחון למחקר, פיתוח, סיוע מבצעי והטמעה של שיטות ויכולות, בדגש על חקר הנכסים הווירטואליים. זאת בדומה למעבדות שהוקמו באינטרפול, ביורופול ובארגונים נוספים בעולם.

מומלץ כי הוועדה המתמדת תבחן את החלופות המעשיות ליישום המלצת הצוות להקים מרכז ידע להתמודדות עם העבריינות במרחב המקוון כמפורט לעיל; זאת בין היתר, כדי לתכלל את ההכשרות הרב-ארגוניות והבין-ארגוניות הנדרשות בנושא הפשיעה הפיננסית, במיוחד עבור רשויות החקירה הנוגעות בדבר - במשטרה וברשות לאיסור הלבנת הון ומימון טרור.

4. ממסמכי יחידת הסייבר בלהב וחטיבת הסיגינט-סייבר עולה כי השימוש שעושים עבריינים בפיתוחים טכנולוגיים מתקדמים במרחב המקוון מצריך גיוס אנשי מקצוע מתחום מדעי המחשב, ניתוח מאגרי נתונים ואבטחת מידע בכלל ותקיפת מערכות סייבר בפרט, ולחלופין הכשרה מקצועית ייעודית של בעלי תפקידים במשטרה. הגיוס וההכשרה מותנים בהגדרה מדויקת של התפקידים הנדרשים בתחומים אלה במסגרת ענפי החקירות והמודיעין באמצעות מסמכים ייעודיים הקרויים "דפי מקצוע" שתנסח חטיבת הסיגינט-סייבר ויאשרו גורמי המטה הנוגעים בדבר באח"ם, באג"ת ובאגף משאבי אנוש (אמ"ש).

בעמ"ט הונאה שהוצג לפני המפכ"ל בפברואר 2021 נקבע כי במהלך אותה השנה יתקיימו קורסי הסמכה לתפקידים האלה: חוקר סייבר, בעל תפקיד מיומן מחשב, חוקר הונאה וחוקר מתקדם. עם זאת לא נקבע מועד להכשרת בעלי תפקידים במקצועות נוספים הנדרשים לתמיכה בחקירת עבירות במרחב המקוון שאותם אפיינה חטיבת הסיגינט-סייבר: מודיעין סייבר, מחקר ופיתוח, תוקפי סייבר, חוקרי תקשוב ומומחי המערך הטכנולוגי.

ממסמכי חטיבת הסיגינט-סייבר ניתן ללמוד כי החטיבה גיבשה את מתווה ההכשרה הנדרש לביצוע התפקידים האמורים ביחידה הארצית, אך עד מועד סיום הביקורת לא יושם מתווה ההכשרה האמור. בפועל, יחידת הסייבר בלהב מעסיקה עובדים בתפקידים הנדרשים, אך ללא תקינה סדורה הכוללת את תנאי הסף ואת דרישות התפקיד כאמור, ולכן לא ניתן לבצע מעקב ובקרה אחר מידת המועילות של תפקוד עובדים אלה בהשוואה לדרישות התקן המקצועי.

עולה מן הנתונים כי למשטרה אין כוח אדם מיומן במקצועות הסייבר בהיקף הנדרש לצרכים שהיא הגדירה, אך היא לא גייסה מומחים חיצוניים מחד גיסא, ולא הכשירה שוטרים מתאימים מאידך גיסא. בולט במיוחד החוסר במומחים במקצועות המודיעין במרחב המקוון לשם ביצוע התפקידים הנדרשים ביחידת הסייבר בלהב, כאמור.

מומלץ כי המשטרה תבחן את הדרכים להשלמת הפערים הנוגעים למומחיות הנדרשת בתחומי הסייבר לביצוע משימות מודיעין, חקירות ומבצעים במסגרת הטיפול בעבריינות במרחב המקוון.

הכשרת בעלי תפקידים במשרד המשפטים

כאמור לעיל, משרד המשפטים הוא שותף מלא ובעל תפקיד מרכזי בטיפול בעבריינות במרחב המקוון כחלק משרשרת האכיפה המתחילה במשטרה. פעילות המשרד מתבצעת הן בידי מייצגי המדינה בפרקליטות והן בידי היועצים המשפטיים במחלקות השונות.

הבנה טכנולוגית מעמיקה של המרחב המקוון היא חיונית לשם ניהול ההליך הפלילי, ובפרט לצורך גיבוש כתב אישום בביצוע עבירות במרחב המקוון ולצורך הייצוג בבתי המשפט בעניינים הכרוכים בראיות דיגיטליות, נדרשת הבנה טכנולוגית מעמיקה של מרחב זה. לימוד, הטמעה ויישום של תכנים מקצועיים אלה בקרב עובדי משרד המשפטים העוסקים בתחום האמור מצריכים הכשרה מקצועית מתאימה.

כאמור, ניהול תיקים שעניינם עבריינות במרחב המקוון נעשה הן ביחידות הפרקליטות במחוזות והן בפרקליטות המדינה, בהתאם למורכבות התיק, ולכן ההכשרות הנדרשות בתחום זה נוגעות, בשינויים המתחייבים, לכלל הפרקליטים העוסקים בתחום.

המכון להשתלמות פרקליטים ויועצים משפטיים במשרד המשפטים אמון על הקורסים וההשתלמויות העיתיות שעוברים המשפטנים בנושאים שונים. מנתוני משרד המשפטים עולה כי בשנים 2017 - 2019 השתתפו בהשתלמויות בתחום הסייבר והטכנולוגיה פרקליטים, משפטנים וסניגורים.

לוח 18: **השתלמויות לעובדי משרד המשפטים, ובפרט פרקליטים בתחום הסייבר והטכנולוגיה**

השנה	נושא ההשתלמות	מספר המשתתפים	כלל הפרקליטים (תחום פלילי)[104]
2018	סייבר וראיות דיגיטליות	130	652
	מבוא לסייבר	50	
2019	עבירות מחשב וראיות דיגיטליות	50	660
	ראיות שהופקו בדרך של חיפוש במחשב	80	
סה"כ		**310**	**1,312**

המקור: משרד המשפטים.

באוגוסט 2021 כתב משרד המשפטים למשרד מבקר המדינה כי בשנת 2020 לא התקיימו השתלמויות והכשרות לעובדים בשל הגבלות מגפת הקורונה, וכי בדצמבר 2021 מתוכננת השתלמות בנושא "חדשנות וטכנולוגיה בעולם המשפט", הפתוחה לפרקליטים וליועצים משפטיים מכלל משרדי הממשלה. בתגובתו על ממצאי הביקורת מינואר 2022 כתב משרד המשפטים כי באוקטובר 2021 התקיים קורס חוקר מחשב מיומן בהשתתפות עובדי הרשות להגנת הפרטיות, מח"ש, אגף האפוטרופוס הכללי ויחידת הסייבר בפרקליטות. כמו כן בשנים 2012 - 2021 השתתפו 9 פרקליטים וחוקרים בהשתלמויות של חוקר מחשב מיומן במשטרה.

הנתונים המפורטים בלוח מצביעים על הכשרה מקצועית בהיקף מצומצם שניתנת לעובדי משרד המשפטים בתחום המשפט והטכנולוגיה (לכ-23% מכלל הפרקליטים בתחום הפלילי), באופן שעלול להקשות על מילוי תפקידם בניהול תיקי עבריינות במרחב המקוון באופן מיטבי.

בדיון הוועדה המתמדת מיולי 2021 ביקש המשנה לפרקליט המדינה (עניינים פליליים) שבקורסי המשטרה בנושא סייבר ישוריינו מקומות לנציגים מהפרקליטות, וסוכם כי תתבצע חשיבה משותפת על התכנים המתאימים למשתתפים מכלל גופי האכיפה[105].

104 יצוין כי לא ניתן היה לפלח את כלל בעלי התפקידים במשרד המשפטים, למעט פרקליטים העוסקים בתחום הפלילי, שהשתלמויות בתחום הסייבר והטכנולוגיה הן רלוונטיות עבורם.

105 פרוטוקול הוועדה המתמדת (13.7.21).

מומלץ כי הפרקליטות תבחן את האפשרות להכשיר פרקליטים העוסקים במאבק בעבריינות במרחב המקוון, במסגרת קורסים ייעודיים נוסף על אלה שניתנים במשטרה.

בתשובת משרד המשפטים צוין כי ההמלצה מקובלת עליו, בכפוף לחלוקת המשאבים ביחס להכשרות השונות הנדרשות לפרקליטים. עוד צוין כי בימים אלו מגובשת תוכנית ההכשרה של המכון להשתלמות פרקליטים ויועצים משפטיים, וצפויות להיות הכשרות נוספות בנושאי סייבר וטכנולוגיה, ובהן למשל פורנזיקה דיגיטלית.

הכשרת שופטים

ההליך הפלילי מתקיים בניהולם ובפיקוחם של בתי המשפט, ולכן השופטים נדרשים להתמצא במידע הנוגע לראיות הדיגיטליות המוצגות לפניהם במסגרת ההליך כולו ולאמצעים הטכנולוגיים שמבקשות הרשויות לשם השגת הראיות.

הנהלת בתי המשפט (להלן - הב"ה) מופקדת בין היתר על הכשרתם המקצועית של השופטים באמצעות המרכז להכשרה ולהשתלמות שופטים שעל יד בית המשפט העליון. המרכז קיים בשנים 2019 ו-2021 השתלמויות בנושאים הקשורים להתמודדות עם העבריינות במרחב המקוון. בשנת 2020 לא קיים המרכז השתלמויות בנושאים אלה עקב מגפת הקורונה. יצוין כי בישראל כיהנו בשנת 2019 - 758 שופטים ו-79 רשמים, ובשנת 2021 - 745 שופטים ו-75 רשמים.

ממסמכי הב"ה עולה כי בשנת 2019 קיים המרכז שלוש השתלמויות ייעודיות ל-148 שופטים ורשמים אשר נמשכו במצטבר שבעה ימים, ובהן: (א) המשפט האזרחי במרחב הדיגיטלי (55 משתתפים בשלושה ימים); (ב) מטבעות דיגיטליים (44 משתתפים ביום עיון); (ג) ראיות מדעיות וטכנולוגיות (49 משתתפים בשלושה ימים). בשנת 2020 קיים המרכז שתי השתלמויות בנושאים: שוק ההון ומשפט מסחרי (יומיים), וטכנולוגיה, משפט, בינה מלאכותית ומה שביניהם (יומיים). במאי 2021 התקיים יום עיון לשופטים בנושא טכנולוגיה, אמצעי תשלום ומסחר בעידן הדיגיטלי. ההשתלמויות היו פתוחות לרישום לכלל השופטים והרשמים במערכת המשפט, ובסך הכול השתתפו בהשתלמויות האמורות בשנים 2020 – 2021, 160 נושאי משרה שיפוטית.

יצוין כי המלצת דוח הצוות המשותף בנוגע לקביעת "נכסים וירטואליים" כנושא לימוד מרכזי מתייחסת אף למערכת בתי המשפט ולהכשרת שופטים.

בתגובת הנהלת בתי המשפט מינואר 2022 נכתב כי המלצת דוח הצוות המשותף לא הועברה לידיעתה, וכי תוכנית ההשתלמויות של המרכז לשנת 2022 נקבעה ואינה ניתנת לשינוי בעת הזו.

בשנת 2019 התקיימו שבעה ימי השתלמות לשופטים בנוגע לסוגיות משפטיות בעידן הדיגיטלי, שהם כ-6% מכלל ימי ההשתלמות (111) שהתקיימו לשופטים ורשמים באותה שנה. בשנה זו השתתפו בהשתלמויות רק כ-18% מהשופטים והרשמים שכיהנו אותה עת בבתי המשפט בישראל, ואילו בשנת 2021 השתתפו ביום העיון היחיד שהתקיים בנושא - 5% מהשופטים והרשמים המכהנים (44).

נוכח אופייה הייחודי של העבריינות במרחב המקוון ומורכבותה, ובשים לב לפוטנציאל העלייה המתמדת בפשיעה במרחב זה, מומלץ כי המרכז להכשרה ולהשתלמות שופטים ישקול את הצורך הגובר להגדיל את היקף ההכשרות המקצועיות לשופטים בתחום האמור.

טיפול משרד המשפטים בעבריינות במרחב המקוון

פעילות יחידת הסייבר בפרקליטות המדינה

פרקליטות המדינה, בין כלל עיסוקיה, עוסקת בניהול ההליכים הפליליים שעניינם עבריינות במרחב המקוון בהתאם לסוג העבירה ולחומרתה. יחידות הפרקליטות במחוזות או יחידות חטיבת התביעות במשטרה[106] מגישות לבית המשפט את כתבי האישום בגין כלל העבירות שיש להן נגיעה ראייתית לזירה הדיגיטלית ובגין עבירות שבוצעו באמצעות תוכנות ויישומי מחשב (סחיטה, הונאה, מרמה, התחזות וכדומה). תיקים מורכבים ותקדימיים שעניינם פשיעה וטרור במרחב המקוון מטופלים ביחידת הסייבר בפרקליטות.

בשנים 2017 עד 2020 נפתחו ביחידות הפרקליטות 698 תיקים בגין אחת מהעבירות הכלולות בחוק המחשבים, התשנ"ה-1995 (להלן - חוק המחשבים), לפי הפירוט שלהלן[107]. יצוין כי על פי נתוני המשטרה בשנים 2017 עד 2020 נפתחו 3,132 תלונות שעניינן עבירות מכוח חוק המחשבים[108].

לוח 19: **מספר התיקים שבהם טיפלו יחידות הפרקליטות במחוזות, 2017 – 2020 (לפי יחידות)**

שם היחידה	יחידת הסייבר	יחידת מיסוי וכלכלה והמחלקה לחקירות שוטרים	מחוז דרום (פלילי)	מחוז חיפה (פלילי)	מחוז ירושלים (פלילי)	מחוז מרכז	מחוז צפון	מחוז תל אביב (פלילי)
מספר התיקים	77	2	79	62	160	147	42	129
סה"כ 698 תיקים								

106 בהתאם לחלוקת הסמכויות הקבועה בחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982.

107 תיקי פרקליטות שנפתחו בשנים 2017 - 2020 וכללו אחת מהעבירות בחוק המחשבים (1 - 6). הנתונים כוללים את התפלגות התיקים לפי יחידות וסטטוס התיקים. ב-317 מהתיקים סעיף העבירה החמור היה אחד מהסעיפים שבחוק המחשבים. הנתונים לא כוללים שמונה תיקים נוספים חסויים שלגביהם אין מידע.

108 משמדובר בנתונים שנאספו משני מאגרי מידע שונים (משרד המשפטים ומשטרת ישראל) יש לקחת בחשבון כי יתכן שהתיקים בהם טיפלו יחידות הפרקליטות בשנים 2017 - 2020 אינם בהכרח אותם תיקים שנפתחו כתלונות בשנים אלו במשטרה. כמו כן, סיווג התלונה עם פתיחתה כנוגעת לחוק המחשבים אינה מחייבת בהכרח שסיווגה לא ישונה במהלך הטיפול במשטרה או לאחר העברתה לפרקליטות.

מפילוח נתוני התיקים שטופלו בידי יחידות הפרקליטות בשנים 2017 עד 2020 התברר כי 457 מהם נגנזו[109] (כ-66%), ורק ב-86 תיקים (כ-12%), שהם כ-2% ממספר התלונות שעניינן חוק המחשבים הוגשו כתבי אישום.

מהנתונים שפרסמה הפרקליטות לשנים 2017 עד 2019[110] עולה כי ביחידת הסייבר נפתחו 170 תיקים והוגשו 65 כתבי אישום (כ-38% מהתיקים), כמתואר בלוח שלהלן.

לוח 20: **מספר התיקים שטופלו ביחידת הסייבר**

השנה	מספר התיקים שנפתחו	מספר התיקים שבהם הוגש כתב אישום	מספר התיקים שנגנזו
2017	49	14	13
2018	65	14	19
2019	56	37	-*

* בסיכום שנת 2019 לא פורטו נתוני גניזת התיקים.

פעולות האכיפה של יחידת הסייבר

1. כאמור, בשל מאפייני המרחב המקוון פחת באופן ניכר הסיכוי לזהות את העבריינים הפועלים במרחב זה ולהענישם, ובד בבד הצטמצמה הרתעתם שכן ההליכים הפליליים המקובלים במרחב הפיזי אינם תמיד מתאימים להתמודדות יעילה עם הפשיעה במרחב זה[111]. לפיכך, מאז הקמתה של יחידת הסייבר בשנת 2015 היא פועלת לצמצום הנזקים והסיכונים של העבריינות במרחב המקוון בשני נתיבים: (א) טיפול בתיקים פליליים כאמור; (ב) אכיפה חלופית - על פי רוב, במקרים שבהם לא ניתן להעמיד את העבריין לדין במאמץ סביר, ובייחוד בכל הנוגע לעבירות ביטוי, ובפרט הסתה לאלימות ואיומים[112]. יצוין כי במקרים מסוימים הפרקליטות מנהלת הליך פלילי לצד אכיפה חלופית.
2. על פי נוהלי יחידת הסייבר, האכיפה החלופית מתבצעת בשני מישורים - המישור הכופה והמישור הוולונטרי[113], כדלקמן:

109 גניזה היא סגירת תיק ללא העמדה לדין. יתר התיקים מנוהלים בפרקליטות או שנסגרו בתום הליך משפטי (12%); הועברו לטיפול גוף תובע אחר (13%); הוחזרו לגוף החוקר, נסגרו לאחר הליך מותנה ועוד (10%).

110 פרקליטות המדינה, סיכומי שנה 2017 - 2019.

111 ראו: אסף הרדוף, **הפשע המקוון** 24 (2010).

112 ראו: חיים ויסמונסקי, "אכיפה אלטרנטיבית של עבירות ביטוי במרחב הסייבר", בתוך: **משפט צדק? ההליך הפלילי בישראל - כשלים ואתגרים** (אלון הראל עורך, 2017).

113 פרקליטות המדינה - מחלקת הסייבר, **נוהל עבודה פנימי - טיפול בתכנים בלתי חוקיים שפורסמו במרחב המקוון.**

א. **המישור הכופה:** חוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט, התשע"ז-2017 (להלן - חוק הסמכויות), מסמיך את התובע לבקש מבית המשפט צו הגבלה המורה לספקי גישה למרשתת ולספקי שירות איתור ואחסון של תכנים במרשתת, להסיר או להגביל את הגישה לתכנים המופיעים באתרים הנוגעים לעבירות שונות, כגון הגרלה או הימור, פרסום תכנים פדופיליים, פרסום שירותי זנות, סחר בסמים, שימוש בחומרים מסוכנים ופעילות טרור. במקרים של חשד לביצוע עבירות כאמור, יחידת הסייבר מגישה לספקי השירות דרישה לחסימת האתר, להגבלת הגישה אליו או לסינונו מתוצאות החיפוש. יחידת הסייבר פועלת במישור הכופה גם בנוגע לפרסום בניגוד לצווי מניעה שנותן יו"ר ועדת הבחירות המרכזית[114]. אחת לשנה שר המשפטים מדווח לוועדת החוקה, חוק ומשפט של הכנסת על אודות יישום החוק[115].

משנת 2018 עד יולי 2021 קיבלה הפרקליטות פניות לבקשת צווי הגבלה שיפוטיים למניעת עבירות מכוח חוק הסמכויות לגבי 12,447 אתרי מרשתת. בפרק זמן זה הגישה הפרקליטות לבתי המשפט בקשות למתן צווים מכוח החוק האמור לאתרים במרשתת כמפורט בלוח שלהלן.

לוח 21: **מספר האתרים שלגביהם הגישה יחידת הסייבר בקשות לבתי המשפט מכוח חוק הסמכויות, 2018 - יולי 2021**

השנה	תוכני פדופיליה	פרסום זנות	אתרי הימורים	אתרי טרור	סך הכול
2018	83	46	3	3	146
2019	5,342	40	24	-	5,406
2020	3,591	16	17	-	3,642
המחצית הראשונה של 2021	3,243	-	10	-	3,253

המקור: פרקליטות המדינה.

114 סעיף 17ב לחוק הבחירות (דרכי תעמולה), התשי"ט-1959.

115 משרד המשפטים - ייעוץ וחקיקה (משפט פלילי), "דיווח לוועדת חוקה, חוק ומשפט לפי סעיף 15 לחוק סמכויות לשם מניעת ביצוע עבירות באמצעות אתר אינטרנט" (7.7.20).

מהלוח עולה כי בשנת 2019 הסתמנה עלייה תלולה במספר האתרים שלגביהם פעלה יחידת הסייבר במישור הכופה, מ-146 אתרים בשנת 2018 ל-5,406 בשנת 2019 (עלייה של כ-3,700%). עם זאת נמצא כי העלייה בפעילות יחידת הסייבר בתקופה האמורה נגעה לתכני פדופיליה, ואולם עלייה זו לא התקיימה בכל הנוגע לאתרים שפרסמו זנות, לאתרי הימורים ולאתרים של ארגוני טרור. במחצית הראשונה של 2021 הפעילה הפרקליטות את סמכותה רק לגבי עשרה אתרי הימורים.

ב. **המישור הוולונטרי:** לגבי יתר העבירות שאינן מנויות בחוק הסמכויות לעיל, אין בידי בתי המשפט הסמכות לתת צווי הגבלה כאמור. לכן, במקרים שיש בהם איום פוטנציאלי על ביטחון הגוף והרכוש של יחידים ושל קבוצות, העלול להגיע לכדי הפרעה לסדר הציבורי או פגיעה בשלומו של אדם, לרבות בריונות רשת ואלימות מילולית, נוהגת יחידת הסייבר לפנות למפעילי האתרים ולדווח להם שהתוכן הפוגעני שעלה לאתרם אינו חוקי, ושלכאורה מתבצעת בו עבירה פלילית. מפעילי האתרים מטפלים בפניית הפרקליטות באופן עצמאי ומחליטים על פי שיקול דעתם ובהתאם לתנאי השימוש של הפלטפורמה המקוונת אם להגביל את הגישה לתוכן הפוגעני, אם להסירו, אם לחסום את המשתמש שהעלה את התוכן או שלא לעשות דבר. הפרקליטות עוקבת אחר מצב היענות המפעילים לפניותיה ומתעדת את אופן טיפולם בתכנים הפוגעניים.

משנת 2018 עד יולי 2021 הגישה הפרקליטות 41,697 פניות למפעילי אתרים כמפורט בלוח שלהלן.

לוח 22: **פניות הפרקליטות למפעילי האתרים, 2018 - יולי 2021**

השנה	סך כל הפניות	אתר א'	אתר ב'	אתר ג'	אתר ד'	אתר ה'	שיעור ההיענות הכולל לפניות (באחוזים)
2018	14,238	12,426	1,143	285	429		92
2019	19,606	8,870	10,696	40			90
2020	4,458	4,249	54	255	272		81
מחצית 2021	3,395	2,292	889	609		888	62

מן הלוח עולה כי בתקופה האמורה הוסרו התכנים בממוצע בכ-88% מהפניות (2018 - 2019)[116]. מנתונים נוספים שנמסרו לביקורת עולה כי בשנת 2020 טיפלה הפרקליטות ב-4,458 מ-4,830 בקשות (92.3%).

(1) עתירה שהוגשה לבג"ץ נגד פעילות הפרקליטות במישור הוולונטרי, שעניינה אכיפה חלופית להסרת תכנים פוגעניים מהמרשתת[117], נדחתה בפסק דין שניתן באפריל 2021 (להלן - בג"ץ האכיפה הוולונטרית). עם זאת נפסק בעתירה האמורה כי על הפרקליטות "לשקול יוזמת חקיקה מסדירה ומפורטת לגבי מכלול האכיפה הוולונטרית, כמו שנעשה בחלק ממדינות המערב"[118].

> פעילות הפרקליטות במישור האכיפה הוולונטרי נעשית ללא הסמכה מפורשת בחוק, אלא מכוח הסמכות השיורית של הממשלה ומכוח סמכויות העזר של היועץ המשפטי לממשלה.
>
> לאור זאת ובעקבות פסיקת בג"ץ, על פיה יש לשקול יוזמת חקיקה מסדירה ומפורטת, מומלץ כי משרד המשפטים יפעל להסדרה ולהסמכה של פעילותה הוולונטרית של יחידת הסייבר בפרקליטות המדינה בנושא.

בתגובת משרד המשפטים על ממצאי הביקורת מינואר 2022 (להלן - תגובת משרד המשפטים) נכתב כי הוא בוחן את הדרך לעגן בחקיקה באופן מפורש את פעילות הפרקליטות במישור הוולונטרי להסרת תוכן מקוון, שפרסומו מהווה עבירה פלילית בישראל ונוגד את כללי השימוש של הפלטפורמה במרשתת, בתנאי שקיים צורך ממשי להסרת הפרסום האמור כדי להגן על אינטרס ציבורי משמעותי, וכל זאת תוך בחינה של הפגיעה בחופש הביטוי ושל הצורך בשקיפות.

(2) על פי נוהלי יחידת הסייבר, היא תפעל במישור הוולונטרי בעיקר בהתקיים חשד לביצוע עבירות אלה: גילוי הזדהות עם ארגון טרור והסתה לטרור; הסתה לאלימות; הסתה לגזענות; פגיעה בפרטיות; הטרדה מינית; סחיטה באיומים; איומים; התחזות כאחר; מידע כוזב או פלט כוזב. פניות למפעילי האתרים ייעשו גם לגבי תכנים במרחב המקוון שפרסומם נעשה בניגוד לחיקוקים שפורטו בחוק הסמכויות במקרים שבהם יחידת הסייבר סבורה שהפעלת צו הגבלה שיפוטי כנגדם עלולה לגרום להגבלה רחבה מדי שתביא לפגיעה עודפת בזכויות יסוד. השיקולים שתשקול הפרקליטות בפעולתה במישור הוולונטרי יכללו, בין היתר, גם את אלה: תפוצת הפרסום בפועל; קהל היעד; חומרת הפרסום; מועדו; פוטנציאל הוויראליות שלו; האופן שבו התפרסם בידי אלו שנחשפו אליו; האיזון הראוי בין האינטרס הציבורי, לרבות זכויות האדם לשם טוב, לפרטיות ולכבוד, מחד גיסא, לבין חופש הביטוי, הזכות לנגישות למידע וחופש השימוש במרשתת, מאידך גיסא.

---

116 פרקליטות המדינה, **סיכום שנה 2019**, עמ' 56.

117 בג"ץ 7846/19 **עדאלה - המרכז המשפטי לזכויות המיעוט הערבי בישראל ואח' נ' פרקליטות המדינה - יחידת הסייבר ואח'** (פורסם במאגר ממוחשב, 12.4.21).

118 **שם,** עמ' 45. מאידך גיסא נכתב בפסק הדין, כי לפחות במספר מדינות מערביות דמוקרטיות, הסמכות ליזום הסרת פרסומים פוגעניים באופן וולונטרי - "איננה מוקנית לרשויות המינהל מכוח הסמכה מפורשת לפעול בצורה האמורה".

על פי הנהלים האמורים, בקשה להסרת תכנים תופנה לאישורו האישי של מנהל יחידת הסייבר, בין היתר, במקרים אלה: (א) כל בקשה לגבי עובדי משרד המשפטים שנפגעו מפרסום המכוון נגדם; (ב) כל פנייה לגבי עובדי ציבור בכירים שנפגעו מפרסום המכוון נגדם.

בעניין זה העלתה הביקורת, כי הפרקליטות פועלת במישור האכיפה הוולונטרי לבקשת עובד ציבור שנפגע או גורם ממונה בהסכמה העובד. נמצא כי ההגנה במסגרת זו ניתנת לעובדי משרד הרווחה ולשוטרים, ולעתים לעובדי ציבור אחרים, בהם עובדי משרד המשפטים, אך הפרקליטות אינה פועלת במישור זה עבור נפגעים מקרב הציבור הרחב. מומלץ כי משרד המשפטים יבחן דרכים לקיום ההגנה הניתנת לעובדי ציבור בצורה שווה וישקול מתן מענה גם לנפגעים מקרב הציבור הרחב, בהתאם למשאביו.

(3) יחידת הסייבר פרסמה באתרה במרשתת מדריכים לציבור להגשת דיווח לספקיות התוכן במרחב המקוון על תוכן פוגעני המפר את תנאי השימוש של הספקיות. במסגרת זו הבהירה הפרקליטות לציבור, כי כאשר הנפגע סבור שמדובר בתוכן העולה כדי עבירה פלילית, מומלץ לו להגיש תלונה למשטרה.

באוגוסט 2015 מינתה שרת המשפטים דאז ועדה ציבורית בראשות השופטת בדימוס עדנה ארבל לגיבוש אמצעים להגנה על הציבור הרחב ועל נושאי משרה בשירות הציבור מפני פעילות ופרסומים פוגעניים במרשתת, לרבות בריונות[119]. בנובמבר 2020 סיכמה הוועדה את ממצאיה והמלצותיה בדוח שהוגש לשר המשפטים דאז (להלן - דוח ועדת ארבל[120]. על פי האמור בדוח הוועדה: בשנת 2018 התקבלו בפרקליטות 94 בקשות מעובדי ציבור להסרת תוכן פוגעני, 32 מהן הועברו לספקיות התוכן ולבסוף הוסרו 28 פרסומים הסרה מלאה, 2 פרסומים הוסרו חלקית ושתי בקשות נדחו.

עלה כי יחידת הסייבר ממליצה לציבור הרחב להגיש תלונות במשטרה במקרים שבהם התוכן הפוגעני עולה כדי עבירה פלילית, ואינה מפרסמת לציבור את האפשרות להגיש אליה בקשות מאת הציבור הרחב להסיר תכנים שונים מהמרשתת. מומלץ, כי משרד המשפטים ישקול להנגיש לכלל הציבור את שירותי האכיפה במישור הוולונטרי; בשים לב לכך שתיעוד ההליכים יהיה שקוף לציבור, ויתבצע התיעדוף הנדרש בהתאם לכלים ולמשאבים העומדים לרשותה.

3. ועדת ארבל המליצה מצד אחד להרחיב את ההגנה על עובדי ציבור ודומיהם החשופים לפגיעות במרשתת; אך מצד שני למקד את פעילות הפרקליטות בעובדי ציבור שפגיעים

119 כתב מינוי מ-5.8.15 בחתימת שרת המשפטים דאז בנושא "הוועדה לגיבוש אמצעים להגנה על הציבור ובהם נושאי משרה בשירות הציבור מפני פעילות ופרסומים פוגעניים כמו גם בריונות ברשת האינטרנט".

120 **דוח הוועדה לגיבוש אמצעים להגנה על הציבור ונושאי משרה בשירות הציבור מפני פעילות ופרסומים פוגעניים, כמו גם בריונות ברשת האינטרנט** (נובמבר 2020).

במיוחד לפגיעות מסוג זה, וזאת בשים לב לצורך בתיעוד ההליכים לשם השקיפות לציבור והפיקוח.

בבג"ץ האכיפה הוולונטרית שפורסם כאמור באפריל 2021, נקבע כי יחידת הסייבר אינה מקפידה על כל אלה: (א) תיעוד תוכן הביטויים שהיא מבקשת להסיר ופירוט מספק בדוחות השקיפות שלה[121]; (ב) פרסום נוהל עבודה שיפרט, בין היתר, את הרכיבים הנדרשים לשם ביצוע האכיפה הוולונטרית - סוג העבירה הפלילית הניצבת בבסיס הפנייה למפעילי האתר, העבירות שלכאורה קשורות לתוכן המבוקש להסרה, זהותו של האדם שהעלה את התוכן וזיקתו לישראל; (ג) שיקוף הסיכומים שבין יחידת הסייבר ובין ספקי השירות במרשתת. בפסק הדין הוצע גם לפרקליטות לשקול למסד מנגנון בקרה ופיקוח על פעילות יחידת הסייבר במסגרת האכיפה הוולונטרית.

עלה כי אין בפרקליטות תיעוד מלא בנוגע לפניות ששלחה למפעילות האתרים בשנים 2018 עד 2020, וכי אין בידה נתונים באשר לזהות המבקשים להסיר את התכנים.

מומלץ כי הפרקליטות תפעל ליישם את המלצות ועדת ארבל ופסיקת בג"ץ לאור ההערות שנכתבו בפסק הדין בנוגע לתיעוד החסר ולהשלמות הנדרשות בנוהלי היחידה בנוגע לרכיבים הרלוונטיים לפעילותה בנושא זה. הגברת השקיפות בנושא זה תתרום לאיזונים הנדרשים בפעילותה הוולונטרית של הפרקליטות למול ערכי חופש הביטוי והשימוש במרחב המקוון.

בתגובתה על ממצאי הביקורת מינואר 2022 כתבה פרקליטות המדינה כי היא שותפה לרצון להגביר את השקיפות בנוגע לפעילותה בתחום הסרת התכנים, וכבר החלה לפעול ברוח זו. כך, למשל, היא פרסמה באתר המרשתת שלה את נוהל העבודה להסרת תכנים מהרשת. כמו כן יחידת הסייבר החלה בעבודת מטה בנושא, בשים לב למורכבותו של התיעוד הנדרש "ולמשאבים הרבים שיידרשו".

פעילות הנהלת בתי המשפט להסרת תכנים הפוגעים בשופטים

עקרון שלטון החוק במשטר דמוקרטי חל על רשויות השלטון וממנו נגזר עקרון חוקיות המינהל. על פי עקרונות היסוד האמורים, על רשות שלטונית לפעול מכוחן של נורמות חקוקות. לכן ככלל, נקיטה בהפעלת כוח שלטוני ללא הסמכה סטטוטורית - אסורה[122]. יתרה מכך, במקרים מסוימים שבהם נוקטת הרשות בפעולה וולונטרית שהסירוב לציית לה אינו גורר בהכרח סנקציה כלשהי, הרי שלא ניתן לפטור אותה מהסמכה חוקית, היות שנמענים עשויים לפרש אותה

121 דוחות מטעם היחידה המפורסמים לציבור ובהם נתונים על פעילותה.

122 יצחק זמיר, **הסמכות המנהלית** כרך א' (2010).

כפעולה שלטונית בעלת משמעות כופה[123]. במיוחד אמורים הדברים במקרים שבהם פעילות שלטונית ללא הסמכה כאמור, עלולה לפגוע בזכויות אדם ובחירויות המוקנות לו בדין[124].

מנהל בתי המשפט הוסמך מכוח סעיף 82 לחוק בתי המשפט [נוסח משולב], התשמ"ד-1984 (להלן - חוק בתי המשפט), להיות אחראי בפני שר המשפטים על ביצוע סדרי המינהל של בתי המשפט.

בנובמבר 2015 פרסם מנהל בתי המשפט נוהל עבודה ובקרה לטיפול בפרסומים במרשתת כנגד שופטים ורשמים (להלן - שופטים) ובני משפחותיהם, שעל פי תוכנם הם עלולים לפגוע קרוב לוודאי באופן ממשי במעמד השופטים בעיני הציבור ובאופן שיש בו להביא לפגיעה משמעותית במערכת בתי המשפט; ובפרט במקרים שבהם הפרסום כולל אחת מהעבירות הפליליות שנמנו בנוהל[125]. הנוהל מסדיר את פעילותה של הב"ה בהתמודדות עם פרסומים אלה, בנפרד מפרסומים הנוגעים לכלל עובדי המדינה שבהם מטפלת יחידת הסייבר בפרקליטות המדינה כאמור[126]. על פי הנוהל, במקרים שבהם הב"ה פונה למפעילים בבקשה להסיר פרסום, היא מציינת כי הפרסום מהווה לכאורה עבירה פלילית שמנהל האתר צריך להסירו על פי חוק, אך אין היא מורה באופן מפורש על הסרת הפרסום.

בשנים 2015 עד 2020 פנתה הב"ה למפעילי האתרים לשם הסרת פרסומים פוגעניים כנגד שופטים, כמפורט בלוח שלהלן:

לוח 23: **פניות הב"ה למפעילי האתרים, 2015 - 2020**

השנה	מספר הפניות	מספר הפניות שנדחו
2015	17	1
2016	97	22
2017	85	32
2018	22	7
2019	3	1

המקור: הב"ה.

123 בג"ץ 3267/97 **אמנון רובינשטיין ואח' נ' שר הביטחון** (1998), פ"ד נב(5), 481; וראו גם: הנס קלינגהופר, **משפט מנהלי** (1957), 109-111, והלכת היסוד שנפסקה בעניין זה בשנים הראשונות שלאחר הקמת המדינה בבג"ץ 144/50 **ד"ר שייב נ' שר הביטחון** (1951), פ"ד ה 399.

124 בג"ץ 355/79 **קטלן ואח' נ' שירות בתי הסוהר ואח',** פ"ד לד(3) 294.

125 סעיפים 144ד2, 192 ו-144ב לחוק העונשין, התשל"ז-1977 (ובמקרים חריגים גם סעיף 255 לחוק); סעיף 3(א)(5א) לחוק למניעת הטרדה מינית, התשנ"ח-1998; וסעיפים 2(11) ו-5 לחוק הגנת הפרטיות, התשמ"א-1981.

126 הב"ה - הוראות נוהל של מנהל בתי המשפט מס' 3-2018, נוהל עבודה ובקרה לטיפול בפרסומים פוגעניים ברשת, 29.11.15.

בנובמבר 2018 מינה היועץ המשפטי לממשלה צוות ייעודי לבחינת נוהל הב"ה האמור. הרכב הצוות כלל את נציגי הב"ה, יחידת הסייבר בפרקליטות ומחלקת ייעוץ וחקיקה במשרד המשפטים. בספטמבר 2019 הגיש הצוות את המלצותיו ליועץ המשפטי לממשלה, שעיקרן עדכון הנוסח של נוהל הב"ה בהתאם לאופן שבו מתנהלת יחידת הסייבר בפרקליטות המדינה בנוגע להסרת תוכן פוגעני במרשתת (ראו לעיל), וכן סוכם כי הנוהל ויישומו ייבחנו מדי שנה בעצה אחת בין נציגי הב"ה ונציגי היועץ המשפטי לממשלה. על פי הנוסח המעודכן של נוהל הב"ה, הבחינה של הפרסום בנסיבות האמורות נעשית על ידי היועץ המשפטי למערכת בתי המשפט בהתייעצות עם המשנה לפרקליט המדינה (תפקידים מיוחדים), ובסופה הוא מעביר את המלצתו לגבי אופן הטיפול בפרסום, להחלטת מנהל בתי המשפט[127]. בעקבות המלצות הצוות כאמור, הודיע מנהל בתי המשפט בנובמבר 2019, כי הב"ה "מקבלת על עצמה שלא לפעול בניגוד לעמדת הפרקליטות אלא לאחר היוועצות עם היועץ המשפטי לממשלה". בדצמבר 2019 עודכן נוהל הב"ה בהתאם להמלצות הצוות.

בספטמבר 2020 קיימה ועדת חוקה, חוק ומשפט של הכנסת דיון בנושא. במסגרת הדיון העלו כמה מחברי הוועדה טענות שונות כנגד פעילות זו מטעמי פגיעה בזכויות יסוד של הפרט, בדגש על חופש הביטוי והיצירה, ופגיעה באמון הציבור במערכת המשפט. במענה לטענות אלה השיב היועץ המשפטי של הב"ה במהלך הדיון, כי היא לא פנתה לאמצעי התקשורת להסיר פרסום עיתונאי בעניינו של שופט, ולא עשתה שימוש "בסמכות דורסנית... אלא רק במקרים חריגים שזועקים לשמים"[128].

> מהלוח לעיל עולה כי החל בשנת 2015 הפעילה הב"ה אכיפה וולונטרית עצמאית לשם הסרת פרסומים נגד שופטים. פעילות זו, אשר לא נכללה במפורש במסגרת הסמכות המנהלית שהוקנתה בחוק בתי המשפט למנהל בתי המשפט, עוגנה בנוהל פנימי שעודכן בדצמבר 2019 באישור היועץ המשפטי לממשלה.

בתגובת הנהלת בתי המשפט על ממצאי הביקורת מינואר 2022 נכתב, כי בעשור האחרון מתמודדת הרשות השופטת עם תופעה הולכת וגוברת של ניסיונות לפגיעה בשופטים, רשמים ועובדי מערכת בתי המשפט, לרבות באמצעות הפצת מסרים שליליים במרשתת. מסרים אלה כוללים ביטויים שיש בהם השפלה, ביזוי ופגיעה בכבודם של נושאי המשרה האמורים בקשר למילוי תפקידם. בחלק מהמקרים מדובר בפרסומים אשר עלולים לפגוע באמון הציבור במערכת בתי המשפט וכתוצאה מכך בתפקוד הרשות השופטת, ואשר עולים לכאורה כדי עבירה פלילית באופן אשר מצדיק בחינת פעילות לשם הסרתם.

עוד ציינה בתגובתה האמורה הנהלת בתי המשפט כי היא מחילה על עצמה אמות מידה מחמירות בכל הקשור לפעילותה הוולונטרית להסרת פרסומים מהמרשתת; ולראיה משנת 2019 ועד ינואר 2022 היא עשתה זאת חמש פעמים בלבד.

---

127 בחינת כל פרסום תתבצע בשים לב לשיקולים הבאים, כדי לקבוע אם מתקיים אינטרס ציבורי המצדיק את הסרתו: הגנה מרבית על חופש הביטוי; חומרת הפרסום מבחינת תוכנו; מושא הפרסום; תוצאות הפרסום; פומביות הביטוי וצורת הפרסום.

128 https://main.knesset.gov.il/News/PressReleases/pages/press23092020c.aspx.

לאור פסיקת בג"ץ, הממליצה לשקול יוזמת חקיקה בנוגע לפעילותה הוולונטרית של יחידת הסייבר בפרקליטות המדינה[129], ובהינתן שהפעילות האמורה עלולה לפגוע בזכויות היסוד לחופש ביטוי ולמחאה, מומלץ כי בעת שתישקל ההסדרה בנוגע לפעילות הפרקליטות, תינתן הדעת גם על הסדרת סמכויות הנהלת בתי המשפט למנוע פגיעה בשופטים במרחב המקוון, בתנאים שייקבעו.

ההסדרה החוקית של המאבק בפשיעה המקוונת

החקיקה המרכיבה את דיני המחשבים והחיפוש בחומרי מחשב אינה תואמת את קצב השינויים המהיר של הזירה הטכנולוגית ואת התעצמות איומי הסייבר במרחב המקוון. כדי למנוע עבריינות במרחב זה ולצורך חקירת העבירות שכבר התבצעו בו, יש לפעול בפרק זמן קצר ככל האפשר כדי לקבל תמונה ברורה על מקום הראיות, היקפן ועקבותיהן בטרם יעלימו אותן העבריינים באמצעות הכלים הטכנולוגיים שברשותם. בשל הפערים הקיימים בין החקיקה הקיימת ובין נדיפותן של הראיות האלקטרוניות, התפתחה בקרב מערכת האכיפה פרקטיקה של הסדרה באמצעות נהלים של רשויות האכיפה שבהם עושות המשטרה והפרקליטות שימוש בסמכויות שיוריות או בסמכויות עזר כדי להתגבר על אותם פערים. יצוין כי במקרים מסוימים אושרה הפרקטיקה האמורה בפסיקת בתי המשפט.

המצב הנורמטיבי הקיים אינו נותן מענה מספק לזכויות האדם להגנה על חייו, על שמו הטוב ועל רכושו, הדורשות את הגברת יעילותה של האכיפה באמצעות מתן כלים וסמכויות לרשויות, מצד אחד. מצד שני, המצב הקיים אינו נותן מענה מאזן לאינטרס הציבור בשמירה כדבעי על זכויות האדם לפרטיות, לחופש ביטוי ויצירה ולחופש התארגנות, המחייבות פיקוח מועיל על התנהלותה של מערכת האכיפה במסגרת הפעלת סמכויותיה במאבק בעבריינות במרחב המקוון.

באוקטובר 2021 מינה שר המשפטים ועדה בראשות מנכ"ל משרד המשפטים במטרה לגבש אמצעים וצעדים שונים לצמצום הפער ההולך וגדל מדי יום בין ההתפתחויות הטכנולוגיות לבין ההסדרים הרגולטוריים והמשפטיים בישראל, ולהתמודדות עם השפעות חברתיות שליליות של תופעות שונות הכרוכות בפער האמור (להלן - הוועדה להתאמת המשפט לאתגרי החדשנות). הוועדה התבקשה למפות את הפערים בין משפט וטכנולוגיה המחייבים טיפול ולהציע דרכים אפקטיביות לצמצום הפער בין המשפט והרגולציה לבין ההתפתחות הטכנולוגית.

בבדיקת תיקוני החקיקה הנדרשים, מוצע כי הוועדה להתאמת המשפט לאתגרי החדשנות תיתן דעתה לפערים שבין החקיקה הקיימת ובין צורכי מערכת האכיפה בשנים האחרונות בטיפול בעבריינות במרחב המקוון, תוך שמירה על זכויות הנוגעים בדבר. להלן הממצאים:

129 **בג"ץ אכיפה וולונטרית**, בעמ' 57 לפסק הדין.

חוק המחשבים

חוק המחשבים מונה חמש עבירות בענייני מחשב וחומרי מחשב[130]: (א) שיבוש פעילות תקינה של מחשב או הפרעה לשימוש בו, ובכלל זה מחיקת חומר מחשב ושינוי חומר במחשב; (ב) עבירות באמצעות מחשב - העברת מידע כוזב או ביצוע פעולות שתוצאתן מידע כוזב; (ג) חדירה לחומר מחשב שלא כדין; (ד) חדירה לחומר מחשב שלא כדין כדי לבצע עבירה אחרת; (ה) עריכת תוכנה או ביצוע פעולות שעלולות להביא לידי שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו; פעולות שתוצאתן היא מידע כוזב; האזנת סתר[131] או פגיעה בפרטיות[132].

על ניסוחן הכללי והעמום של העבירות וחוסר העקביות שעלולה להיות בפרשנות של תכלית החוק נמתחה ביקורת בספרות המחקר, ובפרט בנוגע לאי-ההבחנה במדרג העבירות בין חדירה למחשב באמצעות גישה ללא הרשאה לבין חדירה באמצעות פצחנות או פריצה למחשב[133]. חוקרים באקדמיה מעירים גם על אי-התאמת החוק למציאות הקיימת, ולפיה המסגרת המושגית שיצר החוק התיישנה בעקבות הפיתוח הטכנולוגי המואץ של שנות האלפיים[134]. פער הזמנים בין החקיקה ובין הטכנולוגיה מקדם חוסר ודאות בנוגע לזכויות ומחויבויות משפטיות[135]. יצוין כי מאז חוקק חוק המחשבים בשנת 1995 הוא תוקן רק פעם אחת, בשנת 2012[136], אולם התיקון אינו נותן מענה לחידושים שחלו בעשור האחרון בייחוד במרחב המקוון, שבו קשה יותר להגדיר את עבירת החדירה למחשב או חדירה לחומר מחשב[137]. לדוגמה, במרשתת פועלים אתרים שאוספים מידע אישי על המשתמשים בהם - בעיקר לצורכי שיווק מוצרים; כמו כן, גולשים במרשתת עשויים ללקט מידע ממקורות שונים בלא קבלת רשות מבעלי זכויות הקניין הרוחני במידע זה. לשאלות משפטיות אלה עשויה להיות השלכה גם על יכולת של המשטרה לאסוף מידע באופן פעיל במרחב המקוון[138].

על פי עקרון ההלימה בדיני העונשין, הקובע שהעונש בגין ביצוע עבירה ישקף את חומרת המעשה הפלילי, נקבעו בחוק המחשבים עונשים של שלוש עד חמש שנות מאסר לאדם העושה אחת מהפעולות כאמור, באופן המשקף את הבנת הפשיעה המקוונת בתקופת חקיקת החוק אך אינו מתאים להבנתה היום. לדוגמה, החוק אינו מבחין בין חדירה למחשב פרטי לבין חדירה

130 סעיפים 2-6 לחוק המחשבים.

131 לפי חוק האזנת סתר, התשל"ט-1979.

132 לפי סעיף 2 לחוק הגנת הפרטיות, התשמ"א-1981.

133 אסף הרדוף, "חומר מחשב, חומר למחשבה: מבט תכליתי באיסור החדירה לחומר מחשב", **משפט חברה ותרבות**, 651-690 (2017).

134 נעמי אסיא ורחל אלקלעי, "עבירות מחשב בעשור החולף", **שערי משפט** ד(1) 397 (2006). המאמר סוקר, בין היתר, את החקיקה הענפה - המדינתית והפדרלית - בארה"ב, המותאמת לשינויי הטכנולוגיה התכופים. ראו שם, בעמ' 409-411: **Computer Fraud and Abuse Act 1986 (US) 18 U.S.C. 1030**, ופירוט נוסף בעניין החקיקה האמריקנית.

135 אסף הרדוף, **שם.**

136 חוק המחשבים (תיקון), התשע"ב-2012, ס"ח 2369 (17.7.12). התיקון עסק בהרחבת האיסור על פעולות אסורות בתוכנה בנוגע להחדרת נגיף מחשב לשם העתקת מידע ("סוס טרויאני") שאינו גורם בהכרח לנזק ישיר או לשיבוש פעילות המחשב. ראו בעניין זה את דברי ההסבר להצעת חוק המחשבים (תיקון) (פעולות אסורות בתוכנה - הרחבת האיסור), התשע"ב-2012, ה"ח 468 (23.5.2012).

137 זאת בניגוד לעילות הקבועות בחוק הפדרלי האוסטרלי: The Cybercrime Act 2001.

138 חיים ויסמונסקי, **חקירה פלילית במרחב הסייבר**, 145-150 (2015).

למחשב עסקי ובינן לבין חדירה למערכות ממוחשבות של תשתיות אזרחיות, לאומיות או ביטחוניות.

בעשור שחלף מאז תוקן חוק המחשבים, חלו שינויים רבים ומואצים בטכנולוגיות המשמשות לפשיעת סייבר[139] ולכן חמש העבירות המפורטות לעיל, הכלולות בחוק האמור, מהוות למעשה מסגרת משפטית לא מעודכנת לטיפול בהן.: (א) שיבוש פעילות תקינה של מחשב או הפרעה לשימוש בו; (ב) עבירות באמצעות מחשב; (ג) חדירה לחומר מחשב שלא כדין; (ד) חדירה לחומר מחשב שלא כדין כדי לבצע עבירה אחרת; (ה) עריכת תוכנה או ביצוע פעולות שעלולות להביא לידי שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו; פעולות שתוצאתן היא מידע כוזב; האזנת סתר או פגיעה בפרטיות.

על פי חוק המחשבים, שר המשפטים הוא הממונה על ביצוע החוק והוא רשאי באישור ועדת החוקה, חוק ומשפט של הכנסת להתקין תקנות מכוחו; אולם עד דצמבר 2021 לא הותקנו תקנות כאמור.

בשים לב להתפתחויות בתחום המידע והטכנולוגיות בעולם הפשיעה, השימוש לרעה במרחב המקוון, ופוטנציאל הפגיעה החמורה בציבור, מוצע למשרד המשפטים לבחון בשיתוף המשרד לבט"פ את הצורך בעדכון חוק המחשבים גם בהיבטי ענישה.

חוק איסור הלבנת הון

העבירות המופיעות בחוק המחשבים אינן מוגדרות "עבירות מקור" לפי חוק איסור הלבנת הון, התש"ס-2000[140] (להלן - חוק איסור הלבנת הון), אף כי במקרים מסוימים העבריינות במרחב המקוון חוסה בגדר הלבנת הון ומימון טרור על פי החוק, כגון ביצוע עבירות מחשב לצורך העברת נכסים וירטואליים בין מדינות, העלמת פעילות בלתי חוקית שנועדה לביצוע עבירות פיננסיות והסתרת זהות מבצעיהן באמצעות טכנולוגיות סייבר. יצוין כי ככלל, רף הענישה שנקבע בחוק איסור הלבנת הון על ביצוע עבירות הכלולות בו גבוה מהרף הקבוע בחוק המחשבים.

בספטמבר 2017 הציגה יחידת הסייבר למחלקת ייעוץ וחקיקה (משפט פלילי) את הצעתה בנוגע להוספת עבירת מקור לחוק איסור הלבנת הון. באפריל 2021 הגישה יחידת הסייבר השלמה להצעתה האמורה והציגה מחקרים ומסמכי מדיניות המעידים על עלייה בעבריינות במרחב המקוון המונעת ממניע כלכלי. על פי מסמכי המדיניות, אחד האתגרים המרכזיים העומדים לפני האיחוד האירופי הוא השוק ההולך וגדל של "שירותי פשיעה", המאפשר לאוכלוסיות, שבעבר עמד בפניהן מחסום טכנולוגי, לבצע עבירות. דוח הצוות המשותף אימץ את המלצות יחידת

139 ראו גם חיים ויסמונסקי "על תיקון סעיף 6 לחוק המחשבים", Law.co.il (17.7.12); https://www.law.co.il/articles/2012/07/28/amendments-to-the-israeli-computer-law

140 הלבנת הון היא ביצוע פעולה ברכוש שמקורו בפשיעה: עבירות המכונות "עבירות מקור" מפורטות בחוק איסור הלבנת הון וכוללות סחר בסמים, סחיטה, רצח, מעילות וגניבות, שוחד ועוד. הכול במטרה להסתיר או להסוות את מקורו של הרכוש, את זהות בעלי הזכויות בו, את מקומו, להטמיעו ברכוש לגיטימי ולהכינו לשימוש חוזר.

הסייבר כאמור[141]; ובדיון צוות המשנה לענייני חקיקה של הוועדה המתמדת מיולי 2021 החליטו כל גופי האכיפה הנוגעים בדבר לפעול לתיקון חקיקה שיכלול את עבירות המחשב כעבירת מקור בחוק איסור הלבנת הון.

עלה כי בחלוף ארבע שנים מהמועד שבו הציגה יחידת הסייבר את הצעתה לתיקון החוק לאיסור הלבנת הון, החליט צוות ייעודי של הוועדה המתמדת ביולי 2021 לפעול לתיקון חקיקה שיכלול את עבירות המחשב כעבירת מקור בחוק איסור הלבנת הון. עם זאת, התיקון טרם בוצע. נוכח האמור ולנוכח העובדה שפשיעת הסייבר הופכת עם השנים לכלי מרכזי בביצוע עבירות להשגת רווח כלכלי באמצעים פליליים, מוצע למחלקת ייעוץ וחקיקה במשרד המשפטים לפעול לקידום התיקון הנדרש לחוק איסור הלבנת הון, כפי שהוסכם והוחלט ביולי 2021[142].

פקודת סדר הדין הפלילי (מעצר וחיפוש)

1. פקודת סדר הדין הפלילי (מעצר וחיפוש) [נוסח חדש], התשכ"ט-1969 (להלן - פסד"פ), מסדירה היבטים שונים של חקירת עבירות פליליות, לרבות מעצר חשודים, חיפוש ראיות, תפיסת חפצים וחילוטם, וכן את האופן שבו רשויות החקירה רשאיות לבצע חדירה לחומר מחשב באמצעות קבלת צו שיפוטי, הקובע את מטרות החיפוש ואת תנאיו, באופן שלא יפגעו בפרטיות של אדם מעבר לנדרש[143].

במסגרת פסק דין בהליך שעניינו דיון בבקשה למתן צו חיפוש במחשב או בטלפון חכם, עלה כי בשנת 2019 ניתנו 24,000 צווי חיפוש בטלפונים ניידים (כ-8% מכלל תיקי החקירה שנפתחו באותה שנה), ובמקרים אחרים התקיימו חיפושים ללא קבלת צו כאמור אך בצירוף הסכמתו של הנחקר[144].

השתלשלות ההצעות לתיקוני חקיקה: בשנת 2014 התקבלה במליאת הכנסת בקריאה ראשונה הצעת חוק סדר הדין הפלילי (סמכויות אכיפה - המצאה, חיפוש ותפיסה), התשע"ד-2014 (להלן - הצעת חוק החיפוש), שנועדה לעדכן את דיני המצאת הראיות, חיפושן ותפיסתן, לרבות בנוגע לתוכנה ולחומר מחשב. בדברי ההסבר להצעת החוק נכתב כי החקיקה הקיימת לעניין חיפוש במחשבים אינה נותנת מענה מספק בכל הקשור לחדירה לחומר מחשב.

בדיונים פנימיים שהיו במחלקת ייעוץ וחקיקה במשרד המשפטים בשנים 2018 עד 2019 צוין כי עקב ההתפתחויות הטכנולוגיות, הצעת חוק החיפוש בנוסחה מ-2014 כבר התיישנה למעשה, ולכן אין בה מענה, בין היתר, לסוגיות אלה: (א) חדירה למחשב בסיוע גורם חיצוני - בעל תפקיד מיומן או תוכנה, שלא בנוכחות המחזיק במחשב; (ב) שימוש בכוח לפתיחת מכשירים סלולריים נעולים בהצפנה או בסיסמה; (ג) אי-קביעת עבירה עצמאית בהצעת

141 דוח הצוות המשותף, עמ' 30.

142 בעניין זה ראו גם את הפרק המתפרסם בדוח זה בנושא "משטר איסור הלבנת הון בישראל".

143 סעיף 23א(ב) לפסד"פ.

144 בש"פ 5105/20 **שמעון נ' מדינת ישראל**, עמ' 17 (פורסם במאגר ממוחשב, 25.5.21); מספר תיקי החקירה שנפתחו בשנת 2019 מתוך השנתון הסטטיסטי של משטרת ישראל לשנת 2019, 7.

החוק של סירוב למסור אמצעי פתיחה של מכשירים סלולריים וכניסה לחומרי מחשב, הגם שהיא נחוצה לשם מתן תמריץ למחזיק במחשב לאפשר את החיפוש בו.

בשלהי שנת 2018 הופצה בין הגורמים הרלוונטיים במשרד המשפטים טיוטה מתוקנת של הצעת חוק החיפוש, שבה הוטמעו שיקולים שבהם יתחשב בית המשפט בבואו להכריע בבקשות לצווי חיפוש בחומר מחשב, המאזנים בין צורכי רשויות אכיפת החוק והאינטרס הציבורי של חשיפת עבירות, מניעתן והבאת עבריינים לדין, ובין זכויות החשוד וצדדים שלישיים[145]. אולם הטיוטה טרם הוגשה לכנסת כהצעת חוק.

בתרשים להלן סיכום השינויים המוצעים בהצעת חוק החיפוש שעניינם תוספות מהותיות לסמכויות הקיימות בעניין חומר מחשב בפסד"פ אשר כלולות בפרק ו' להצעת החוק האמורה, כפי שהוצגו לפיקוד המשטרה על ידי חטיבת סיגינט-סייבר.

תרשים 17: **עדכון סמכויות החיפוש בפסד"פ לפי הצעת חוק החיפוש**

המקור: אח"ם - חטיבת הסיגינט-סייבר.

145 טיוטת הצעת חוק סדר הדין הפלילי (סמכויות אכיפה - המצאה, חיפוש ותפיסה), התשע"ט-2018.

הועלה כי עד מועד סיום הביקורת, ולאחר יותר משבע שנים, הליכי קידום הצעת חוק סדר הדין הפלילי (סמכויות אכיפה - המצאה, חיפוש ותפיסה), התשע"ד-2014, שנועדה לעדכן את דיני ההמצאה, החיפוש ותפיסת הראיות, לרבות בנוגע לתוכנה ולחומר מחשב, טרם הושלמו. משלא תוקנה החקיקה בנוגע לחיפוש בחומרי מחשב, המשטרה נדרשת לפעול במגבלות הדין הקיים לשם השגת ראיות פליליות.

בתגובת משרד המשפטים נכתב כי העבודה על עדכון הצעת החוק התעכבה במהלך השנתיים האחרונות בעקבות מגפת הקורונה ששאבה את מרב המשאבים לצורך מתן מענה משפטי לסוגיות שהתעוררו, וכי בחודשים האחרונים ריכזה מחלקת ייעוץ וחקיקה מאמץ להבשלת תזכיר החוק החדש. במסגרת זו היא ניהלה דיונים עם הגופים הנוגעים בדבר בקשר להסדרים הספציפיים שיש לקדמם.

2. בהיעדר הסדרה כאמור, התעוררו במשך השנים מחלוקות בין הגורמים השונים בקשר לסוגיות הנוגעות לחיפוש בחומר מחשב:

א. **חיפוש בהסכמה:** עמדת הסנגוריה הציבורית היא כי חיפוש בחומר מחשב על בסיס הסכמה של הנחקר, בלי לקבל צו שיפוטי, הוא מנוגד לחוק[146]. אולם על פי נוהלי המשטרה ניתן לבצע חיפוש כאמור ללא צו, בהינתן הסכמת החשוד ובנוכחותו במעמד החיפוש[147]. הנחת היסוד הקבועה בנוהל המשטרתי היא כי במקרה שבו מתבצע בהסכמה חיפוש במחשב, החוקר החודר לחומר המחשב בא בנעליו של המסכים לחדירה, והוא רשאי לבצע כל פעולה שבעל הרשאת הגישה רשאי לבצעה בעצמו, לרבות גישה לחומר האגור במחשבים מרוחקים בארץ ומחוצה לה, אם למסכים לחדירה הרשאה וגישה לחומר זה. עם זאת הנוהל קובע כי ככלל יש להעדיף חיפוש בחומר מחשב על סמך צו שיפוטי לפי סעיף 23א(ב) לפסד"פ. בפועל, לא ניתן לחדור לחומר מחשב שנתפס, לרבות כניסה למכשירי טלפון ניידים באמצעות סיסמה, קוד משתמש, טביעת אצבע או זיהוי פנים בלי לקבל את הסכמת הבעלים. ממסמכי המשטרה עולה כי חיפוש בחומר מחשב יכול להיעשות בהסכמה מדעת של החשוד[148], ואם החשוד מסרב לכניסת החוקרים למכשיר שבבעלותו, אין להפעיל כוח סביר כדי לגרום לו לפתוח את המכשיר ולהפיק ממנו ראיות, ואף אין לאלץ אותו למסור טביעת אצבע או שיקוף פנים.

יצוין לשם השוואה, במסגרת החקיקה למלחמה בטרור בבריטניה נקבע, כי גם רשויות אכיפת החוק רשאיות לערוך חיפוש במחשבים ובמכשירים שיש להם גישה למחשבים המצויים בשטחי המדינה, מבלי לקבל צו שיפוטי; וזאת לשם איסוף ראיות בחקירה

146 הסנגוריה הציבורית, "חיפוש בחומר מחשב על בסיס הסכמת הנחקר וללא צו שיפוטי - מיצוי הליכים לפני חקירה" (21.2.21).

147 נוהל אח"מ מס' 03.300.035 תפיסה וחיפוש במחשב (פברואר 2021).

148 נוהל תפיסה וחיפוש במחשב (פברואר 2021); הנחיית עבודה מ-5.11.17 - חיפוש בחומר מחשב כשלמחשב התפוס גישה אליו, סעיף 2.

פלילית. החוקרים רשאים לבצע זאת באמצעות פריצה למחשב מרחוק ללא צורך בתפיסת המחשב גופו[149].

ב. **שימוש בכוח:** על פי הפרשנות שניתנה בהנחיית המשנה ליועץ המשפטי לממשלה (משפט פלילי), הוראת סעיף 45 לפסד"פ המעגן סמכות כניסה למקום תוך שימוש בכוח, במקרה של סירוב, חלה גם על חדירה לחומר מחשב לפי סעיף 23א לפסד"פ, במקרים שבהם נדרשת טביעת אצבע של החשוד לצורך חדירה לחומר המחשב, וזה מסרב לבקשת המשטרה. כך גם קובע הנוהל המשטרתי בנושא תפיסת מחשב וחיפוש בו מפברואר 2021. אולם בסיכום דיון שנערך בנושא זה במשרד המשפטים בדצמבר 2019 נכתב כי עם קידום הצעת חוק החיפוש, יש לעגן סמכות זו במפורש בחוק בהתאם לנוסח שהציעה מחלקת ייעוץ וחקיקה. המתנגדים לעמדה זו טוענים כי מדובר בפגיעה בזכות לאי-הפללה עצמית, ולא ניתן לחייב את הנחקר לשתף פעולה עם רשויות החקירה[150].

> בהיעדר הוראת חוק ברורה בנושא, אין מענה לשאלות יסודיות שרשויות החקירה נדרשות אליהן בבואן לערוך חיפוש בחומר מחשב ולתפוס ראיות פליליות במרחב המקוון.

ג. **חיפוש בשרתים מרוחקים:** חסרה הסדרה מפורשת לגבי חיפוש וחדירה לחומר מחשב המצוי בשרתים מרוחקים. יצוין כי על פי הפסד"פ, אין הסמכה לבצע חיפוש במחשב שהמידע האגור בו שמור בשרתים שאינם בשטחה של מדינת ישראל. בנוסף, לא גובשה אמנה בין-לאומית המסדירה את התנאים לעריכת חיפוש ראיות בשרתים מרוחקים המצויים בשטחן של מדינות זרות[151]. בכנס של הוועדה המתמדת מאוקטובר 2018 דווח מפקד יחידת הסייבר בלהב, כי היא פועלת לחתום על אמנה כאמור. גם בדיון הוועדה המתמדת מיולי 2021 ציין המשנה לפרקליט המדינה (עניינים פליליים) כי נושא חיפוש בחומרי מחשב של שרתים הנמצאים בחו"ל הוא "קריטי" ומצוי על שולחנו של היועץ המשפטי לממשלה. יצוין כי מענה לנושא זה לא ניתן גם בהצעת החוק.

> במצב החוקי הקיים מתקשה המשטרה לחקור עבירות שהראיות לביצוען שמורות מחוץ לשטח המדינה וכך, למשל, לעקוב אחר ביצוע עסקאות בנכסים וירטואליים החשודים בשימוש למימון פעילות עבריינית.

בתגובת מחלקת ייעוץ וחקיקה (משפט פלילי) נכתב כי בעניין חיפוש בחומר מחשב מרוחק נעשה מאמץ משותף של כלל הגורמים לבחון את ההסדר הראוי שיהיה בו כדי

149 **The Investigatory Powers Act, 2016** (c. 25)

150 יגאל בלפור וגיל שפירא, "ונשמרתם לאצבעותיכם: חובתו של חשוד לסייע לחיפוש במכשיר סלולארי ושימוש בכוח לשם פתיחת מכשיר הנעול באמצעות טביעת אצבע", **הסנגור** 267 (2019).

151 יצוין כי בינואר 2021 אישר היועץ המשפטי לממשלה הנחיית עבודה של המשטרה (מנובמבר 2017) המאפשרת חדירה לשרתים מרוחקים בתנאים שנקבעו בהנחיה ובאישור היועץ המשפטי לממשלה. תוקף האישור פג במרץ 2022.

לתת מענה לצורכי גופי האכיפה, תוך איזון מול הפגיעה בזכויות הפרט ובחינת משפט משווה עדכני והתייחסות לאמנות ולתהליכים בין-לאומיים שונים.

בדיון שהיה ביולי 2020 בפורום ראשי מחלקי הסייבר במחוזות המשטרה, הוצע ליצור מנגנון שיתוף פעולה עם מדינות שמקיימות בשגרה חיפוש מרוחק בשרתים בישראל.

כפי שתואר לעיל, לא כל העבירות המתבצעות באמצעות מחשב או שניתן למצוא להן ראיות באמצעי תקשוב מוגדרות עבירות לפי חוק המחשבים. לכן אי-ההסדרה הסטטוטורית של סמכויות החיפוש של המשטרה בחומר מחשב עלולה לפגוע בזכויות יסוד של נחקרים שאינם חשודים בעבירה על חוק המחשבים, לדוגמה במקרים של תפיסת מכשיר סלולרי ופריקתו כדי לבדוק את נתוני מקום הנחקר ואת תוכן ההתכתבויות שלו בלי שניתן לכך צו שיפוטי מתאים; בשים לב לכך שלעיתים בקשה למתן צו כאמור נדונה במעמד התביעה בלבד, ולא ניתנת לנחקר זכות טיעון בגינו.

היעדרה של מסגרת חקיקתית מתאימה להתוויית שיקול הדעת של גורמי החקירה, התביעה והשפיטה בכל הנוגע לתפיסת מחשב ולחדירה אליו, וכן לחיפוש בחומר מחשב, פוגע ביכולת לבצע חקירה יעילה של פשעי סייבר ולמנוע אותם מחד גיסא, ובזכויות הפרט לכבוד האדם ולקניינו, להגנה על הפרטיות ולקבלת הליך הוגן מאידך גיסא.

בדצמבר 2021 עדכנה מחלקת ייעוץ וחקיקה את משרד מבקר המדינה כי לאחרונה גובשה הצעת חוק - תיקון לפקודת סדר הדין הפלילי (מעצר וחיפוש) (עילות חיפוש בלא צו בית משפט) (הוראת שעה), התשפ"ב-2021 שעניינה חיפוש ללא צו בית משפט, בהתאם להחלטת ממשלה שעניינה טיפול בפשיעה החמורה בחברה הערבית[152]. יצוין כי הצעת החוק מתייחסת לתפיסת חפץ, אולם כאשר נדרשת תפיסה של חומר מחשב האגור במצלמה או במחשב, יידרש צו שיפוטי כדי לחדור אליו. התיקון נועד להקנות למשטרה כלים לתפיסת ראיות לפשיעה חמורה, לרבות ראיות טכנולוגיות, שיש חשש שייעלמו או שישובשו, עד לקבלת צו בית משפט. על פי העדכון, עקב השגות שונות שהעלו גורמים הנוגעים בדבר בנוגע להצעת חוק החיפוש, הדיונים במשרד המשפטים בנושא צפויים להימשך עוד מספר חודשים.

מומלץ לגורמי משרד המשפטים להשלים את העדכונים הנדרשים בטיוטת הצעת חוק החיפוש, ולהפיץ לעיון הציבור תזכיר חוק המשקף את האיזונים הנדרשים בין צורכי רשויות האכיפה והבטחת יכולתן לקיים פעולות אכיפה יעילות לגילוי עבירות ומניעתן ובין זכויות היסוד של הנחקרים ושל צדדים שלישיים.

3. באוקטובר 2021 ריכזה חטיבת הסיגינט-סייבר באח"ם את כל השינויים העדכניים הנדרשים בהצעת החוק משנת 2014, שמטרתו הוגדרה "יצירת חקיקה מבוססת תכלית, שתהא גנרית דיה להכיל צרכים מבצעיים במציאות טכנולוגית ובסביבות איום משתנות". זאת בראי שלוש

152 החלטת ממשלה מס' 852, "מדיניות ממשלתית לטיפול בתופעות הפשיעה והאלימות בחברה הערבית בישראל ותיקון החלטות ממשלה" (1.3.21).

תכליות החדירה האלה: לצורכי מניעה ופעילות מבצעית; לצורכי איסוף ראייתי; ולסיכול במקרים דחופים.

בתגובתה על ממצאי הביקורת כתבה מחלקת ייעוץ וחקיקה (משפט פלילי) כי עמדת המשטרה בנושא כאמור הומצאה לה רק בדצמבר 2021, והיא מעוררת סוגיות משפטיות רגישות ומורכבות אשר טרם נבחנו, והזמן הדרוש לבחינתן עלול לגרום לעיכוב ניכר בקידום הצעת חוק החיפוש. לפיכך לא מן הנמנע כי סוגיות אלה ייבחנו בנפרד ולא ייכללו במסגרת העבודה המאומצת לקידום התיקון במתכונתו הקיימת. עם זאת, לאחר השלמת הדיונים המכריעים במהלך שנת 2022, בכוונת המחלקה להפיץ תזכיר חוק חדש באישור שר המשפטים.

הפערים בתחום סמכויות החיפוש שהעלתה המשטרה נוגעים בסוגיות מורכבות הדורשות ליבון ודיון מעמיק. משום כך, מומלץ שמשרד המשפטים יבחן את הסוגיות האמורות בשיתוף המשטרה, תוך איזון בין הצרכים המבצעיים של המשטרה לבין זכות היסוד לפרטיות.

חוק האזנת סתר

1. חוק האזנת סתר, התשל"ט-1979 (להלן - חוק האזנת סתר), נועד לקבוע מחד גיסא את האיסור הפלילי על ציתות לשיח תקשורתי, שהמצותת אינו צד לו (להלן - האזנת סתר), ומאידך גיסא את התנאים שבהם ניתן להתיר האזנת סתר ובראשם קבלת צו שיפוטי הקובע את תנאי ההיתר וגבולותיו, כאשר הדבר דרוש לגילוי, חקירה או מניעה של עבירות מסוג פשע בתנאים שפורטו בחוק. ככלל, התנאים לקבלת צו שיפוטי המתיר האזנת סתר על פי החוק האמור חמורים יותר מהתנאים שנקבעו בפסד"פ לקבלת צו חיפוש. יצוין כי הגדרת האזנת סתר בחוק האמור עשויה לכלול גם ציתות לתקשורת סינכרונית בין מחשבים, הגם שהעניין אינו מפורש בחוק שכן מדובר בהאזנה או קליטה של השיחה באמצעות מכשיר (בהתאם להגדרת המונח "האזנה" בחוק).

איסוף מודיעין במרחב המקוון, לרבות במהלך ביצוע חקירה סמויה ובמיוחד בנוגע לקריאת מסרים דיגיטליים והודעות טקסט המועברות באמצעות יישומונים ודואר אלקטרוני, עשוי להידרש לקבלת צו שיפוטי על פי חוק האזנת סתר. הוראת סעיף 23א בפסד"פ מחריגה מתחולת הוראות חוק האזנת סתר מקרים של קבלת מידע מתקשורת בין מחשבים אגב חיפוש שהותר מכוח צו שיפוטי. לכן חיפוש כדין של ראיות פליליות בחומר מחשב שנתפס ברשות חשוד או שהועתק, לרבות מכשיר סלולרי, מחשב לוח (טבלט), התקן נייד והתקן נייח, אינו בבחינת "האזנת סתר" לאור הוראות סעיף 23א(ג) לפסד"פ. אולם במקרים שבהם החיפוש הניב מידע שיורט משרתי האחסון קודם קליטתו במכשיר החשוד, אזי ייתכן שתחול עליו הגדרת האזנת סתר על פי החוק האמור, בהתאם לפסיקת בית המשפט המחוזי[153].

153 ת"פ (מחוזי ת"א) 40206/05 **מדינת ישראל נ' אליעזר פילוסוף ואח'** (פורסם במאגר ממוחשב), 5.2.2007.

בנסיבות אלה המידע לא יוכל לשמש ראיה קבילה במשפט, כל זמן שלא הוצא צו להאזנת סתר[154].

בעשור השלישי של המאה העשרים ואחת רבים מחומרי המחשב הדרושים לגורמי החקירה לצורכי החקירה הפלילית שמורים במרחב המקוון (ענני מידע במובחן מאובייקטים במרחב הפיזי) ולכן אינם ניתנים לתפיסה מוחשית. מוצע למחלקת ייעוץ וחקיקה לתת את הדעת על המענה החקיקתי הנדרש, בשים לב להשפעות שיש להבחנה בין המקרים שבהם קבלת מידע באמצעות תקשורת בין מחשבים נופלת להגדרת "האזנת סתר", אם לאו.

בתגובתה על ממצאי הביקורת כתבה מחלקת ייעוץ וחקיקה (משפט פלילי) כי חלק מההיבטים האמורים בנוגע לחוק האזנת סתר יוסדרו במסגרת הצעת חוק החיפוש, לרבות בנוגע לאופן החיפוש בחומר מחשב ולהיקפו.

2. ביולי 2017 הפנה המשנה לפרקליט המדינה (עניינים פליליים) את תשומת ליבם של הגורמים הרלוונטיים בפרקליטות ובמשטרה לקשיים הנורמטיביים בנוגע לדליית ראיות פליליות מחומר מחשב. במכתבו ציין כי היקפו העצום של חומר המחשב שנתפס מקשה מאוד על המשטרה לעיין בכל תכניו, וכי חשיפת מלוא החומר בפני החוקרים עלולה להביא לפגיעה של ממש בפרטיות החשודים ובזכויותיהם של צדדים שלישיים שאינם חשודים כלל. יצוין כי הנחיית פרקליט המדינה בנושא זה פורסמה בנובמבר 2020.

הועלה כי לא הוסדר בחקיקה היקף החיפוש המותר בחומר מחשב. כמו כן הנחיית פרקליט המדינה מנובמבר 2020, אינה מרפאת את הפגיעה האפשרית בפרטיותם של צדדים שלישיים שאינם נוגעים בדבר באמצעות החיפוש בחומרי מחשב שנמצאו ברשותם של חשודים ושל נאשמים.

אי-הסדרת הסוגיה של חיפוש הראיות בחומר מחשב משפיעה על היקף הפגיעה בזכות העיון המוקנית לנאשם בנוגע לחומר חקירה שנתפס בעניינו מכוח הוראת סעיף 74 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982 (להלן - החסד"פ)[155], לרבות בעקבות האזנת סתר. עמדת רשויות התביעה בהקשר זה היא שחדירה של התובעים למחשב וחיפושם בחומרי מחשב אינה בגדר "האזנת סתר" המטילה על מפיק השיחות להקשיב לכל השיחות המוקלטות ולסווג אותן. על פי מכתבו האמור של המשנה לפרקליט המדינה, נדרשת מתודולוגיית חיפוש סדורה שבמסגרתה ייעשה מאמץ לגלות את רוב חומרי החקירה המצויים במחשב, וזאת תוך תיעוד אופן החיפוש, לרבות מילות המפתח, שלבי החיפוש, הזמנים שבו בוצע וכיוצא באלה. בהתאם לזאת, זכות העיון לנאשם תחול רק על חומר מחשב שיסווג בתור חומר הנוגע לחקירה, במובחן מיתר החומרים שנתפסו אשר לא נערך בהם חיפוש לפי המתודולוגיה המוצעת.

154 ההבחנה שהוכרה בפסיקה לעניין זה היא בין מידע "נח" (in rest) שאינו בגדר "האזנת סתר" ובין מידע "נע" (in transition) שיחולו עליו הוראותיו המחמירות של החוק.

155 על פי סעיף 74(א) בחסד"פ, "חומר חקירה" הוא כל החומר שנאסף או שנרשם בידי הרשות החוקרת אשר נוגע לאישום.

מתודולוגיה זו עוגנה בהנחיית המשנה לפרקליט המדינה שגובשה בנובמבר 2020, ולפיה ניתן לבצע בחומרי מחשב "חיפוש מושכל" שבמהלכו יסונן החומר באמצעים ממוחשבים, בין היתר באמצעות מילות חיפוש מסוימות, בלי שעורך החיפוש מעיין בפועל בכל הקבצים המצויים במחשב[156]. נוסף על כך, ההנחיה קובעת רשימה של תנאים להיענות התביעה לבקשת חשוד או נאשם לבצע חיפושים מושכלים נוספים בחומר מחשב, וכי את החיפוש כאמור תעשה היחידה החוקרת ולא הפרקליטות.

בהעדר הסדרה מפורשת בחקיקה של היקף החיפוש המותר בחומר מחשב, עלולה להיפגע זכות הנאשם לעיון בחומרי החקירה הנוגעים לאישומו המצויים במחשב.

בתגובתו על ממצאי הביקורת הודיע משרד המשפטים כי אופן החיפוש והיקפו עתידים להיות מוסדרים בפסד"פ, וכי בכוונתו להציע הסדר חוקי להיבטים האמורים.

לאור הודעתו, מומלץ כי משרד המשפטים יכלול בהצעתו לשינויי חקיקה, בין היתר, את הנושאים האלה: הסדרת החיפוש בחומר מחשב הנוגע לחיפוש ראיות על ידי התביעה, וכן הסדרת החיפוש בחומר מחשב הנוגע למימוש זכויות היסוד של נחקרים ושל נאשמים בפלילים לעיין בחומר החקירה בעניינם ולהגן על פרטיותם ועל הפרטיות של צדדים שלישיים.

חוק הסמכויות

1. כאמור לעיל, חוק הסמכויות מאפשר הגבלה של גישה לאתרים במרשתת בתנאים מסוימים.

א. החוק קובע רשימה סגורה של עבירות שבגינן ניתן לאכוף על מפעילי אתרים במרשתת להסיר תכנים פוגעניים מאתרים במרשתת. רשימה זו אינה כוללת את העבירות המופיעות בחוק המחשבים. בספטמבר 2020 הגישה יחידת הסייבר ליועץ המשפטי לממשלה הצעה לתקן את חוק הסמכויות כך שיכלול גם אפשרות להוציא צווים לאתרי מרשתת שמתבצעת בהם פעילות אסורה לפי חוק המחשבים.

יצוין כי בדיון שהתקיים באוגוסט 2021 בנושא "אופן הטיפול באתרי אינטרנט המשמשים לביצוע הונאות פישינג (דיוג)", בהשתתפות גורמי מערכת אכיפת החוק במשטרה ובפרקליטות, נאמר כי חוק הסמכויות אינו מתייחס לאתרי דיוג. על רקע זה ובהיעדר מקורות הסמכה חלופיים בחוק, הרי שפעילות המשטרה בנוגע להסרת קישוריות דיוג לעמוד מתחזה של אתר במרשתת, בהסתמך על החוק האמור, מעוררת קושי משפטי.

עד מועד תום הביקורת טרם קודמה ההצעה האמורה לתיקון חוק הסמכויות לשלבי חקיקה. אולם בתגובתה על ממצאי הביקורת הודיעה מחלקת ייעוץ וחקיקה (משפט פלילי) כי ההצעה האמורה של יחידת הסייבר בפרקליטות תיבחן על ידה כחלק ממכלול תיקוני החקיקה בנושאים אלה.

156 הנחיית פרקליט המדינה מס' 7.15, "יישום הוראות סעיף 74 לחוק סדר הדין הפלילי [נוסח משולב], התשמ"ב-1982, על תוצרי חיפוש בחומרי מחשב - עבודת התובע" (24.3.21).

ב. בבג"ץ האכיפה הוולונטרית העיר בית המשפט[157] כי יש לשקול יוזמת חקיקה שתסדיר בפירוט את מכלול הפעולות שאותן נוקטת הפרקליטות במסגרת זו, כפי שנעשה בחלק ממדינות המערב[158]. יצוין כי הצעת החוק להסרת תוכן שפרסומו מהווה עבירה מרשת האינטרנט, התשע"ז-2016, והצעת החוק למניעת ביצוע עבירות באמצעות פרסום באינטרנט (הסרת תוכן), התשע"ח-2018 - לא הבשילו לכדי חקיקה.

בתגובת משרד המשפטים נכתב כי הוא החל בקידום מחדש של הצעת החוק, "עם שינויים מינוריים", שאושרה על ידי ועדת השרים לענייני חקיקה בדצמבר 2021 ומיועדת להנחה על שולחן הכנסת. על פי הצעת החוק, יידרשו שני תנאים מצטברים כדי ששופט בבית משפט מחוזי יורה על הסרת תוכן לבקשת תובע שהוסמך לכך על ידי היועץ המשפטי לממשלה: (א) פרסום התוכן במרשתת יהווה עבירה פלילית; (ב) קיימת אפשרות ממשית לכך שהמשך הפרסום יפגע בביטחונו של האדם, בביטחון הציבור או בביטחון המדינה. כמו כן, בהליך פלילי כאמור יוסמך השופט שדן בתיק, אחרי הרשעת המפרסם, להורות על הסרת התוכן שבשלו הורשע.

מומלץ כי במסגרת קידום הצעת החוק האמורה יוודא משרד המשפטים כי ההצעה משקפת את האיזון הדרוש בין חופש הביטוי ובין מתן מענה הולם לטיפול בעבירות שעניינן פרסום תוכן המסית לאלימות, לטרור, לגזענות או תכנים בלתי חוקיים אחרים. מומלץ גם כי משרד המשפטים יקיים בחינה בין-לאומית של החקיקה בנושא עובר להנחת הצעת החוק על שולחן הכנסת.

ג. החוק אינו מסמיך הגבלה או חסימה של אתר החשוד בהונאה. בהתאם לזאת, רשויות האכיפה מנועות מלבקש ולקבל צווים שיפוטיים ומלהפנותם לספקיות השירותים המקוונים במקרים הנדרשים.

בסיכום דיון בנושא הפשיעה המקוונת שהתקיים במטה הארצי באפריל 2021 ציין המפכ"ל כי העבירות בתחום ההונאה והסייבר פוגעות באזרחים רבים, בדגש על אוכלוסיות מוחלשות ובפרט קשישים וחסרי ישע. נוכח זאת הוא הנחה את גורמי הייעוץ המשפטי ואח"ם לבחון אפשרות לתיקוני חקיקה, תוך החמרת הענישה במקרים כאמור.

על פי חוק הסמכויות הקיים, חשד לביצוע מרמה והונאה במרחב המקוון אינו עילה להגבלת גישה או חסימת אתר במרשתת. נוכח העובדה שנפגעי עבירות אלה משתייכים לעיתים לאוכלוסיות מוחלשות, מומלץ שמשרד המשפטים יבחן את המענה הנדרש לשם הגנה על נפגעי עבירות אלה במרחב המקוון.

157 שם, בעמ' 57.

158 במסגרת הדיון בבג"ץ 7846/19 (שם, בעמ' 14) צוין כי פעילות וולונטרית ללא הסמכה סטטוטורית נוהגת בחלק ממדינות אירופה, כגון - בריטניה, צרפת, בלגיה, ספרד וגרמניה על בסיס הסדרים בין-לאומיים והנחיות רגולציה של האיחוד האירופי, לרבות מתווה שנחתם בין האיחוד ובין כמה בעלי פלטפורמות במרשתת בעניין הטיפול בפרסומי שנאה דרך מנגנוני הדיווח של הפלטפורמות. כמו כן צוין שם, כי בארה"ב לחלק ממפעילי הפלטפורמות המקוונות מוקנית חסינות בדין ולכן לא ניתן לפעול כנגדם במישור הכופה אלא רק במישור הוולונטרי.

מן הממצאים עולה כי אין בחקיקה בכלל ובהוראות חוק הסמכויות בפרט, סמכויות אכיפה המקנות לרשויות את הזכות לבקש צווי הגבלה שיפוטיים המחייבים את מפעילי האתרים במרחב המקוון להסיר תכנים ומסרים פוגעניים או לחסום את הגישה לאתרים מסוכנים במרשתת.

2. החלטת הממשלה אשר מכוחה הוקם בפברואר 2015 מערך הסייבר הלאומי (להלן - מס"ל) כגוף הממלכתי המופקד על הגנת המרחב המקוון של מדינת ישראל[159], לא עוגנה בחוק[160]. משום כך, סמכויותיו של מס"ל כלפי חלק ניכר מהגופים במשק[161], ניתנות להפעלה בהסכמת גופים אלו בלבד[162]. זאת בניגוד לרשויות אחרות העוסקות בהגנת סייבר ובמאבק בעבריינות במרחב המקוון, אשר החוק מקנה להן סמכויות אכיפה (ראו לעיל בפרק המבוא).

הועלה כי במצב הקיים אין בין מס"ל ובין מערכת האכיפה, חלוקת סמכויות ותפקידים ברורה. כמו כן, אין הגדרות מפורטות ומחייבות בנוגע לממשקי העבודה בין מס"ל ובין יתר הרשויות הנוגעות בדבר, ובפרט בנוגע לחובת שיתוף המידע בין מס"ל ובין המשטרה.

תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018, מאגם את החלטות הממשלה ואת מדיניותה בנוגע לסמכויות מס"ל והיקף אחריותו. עם זאת, תזכיר החוק טרם אושר ואינו אינו נוגע במישרין לפעילות מס"ל במקרים שיש בהם היבטי פשיעה ורכיבים פליליים המצריכים את התערבות המשטרה או את יידועה.

נוכח זאת, מומלץ שמשרד המשפטים יבחן עם מס"ל ועם המשטרה חלופות לקביעה בהצעת החוק המתגבשת של חלוקת התפקידים בין הגופים בטיפול במקרים שיש בהם היבטים משולבים של הגנת סייבר מחד גיסא ופשיעת סייבר מאידך גיסא.

במסגרת תגובתה על ממצאי הביקורת מינואר 2022 הודיעה מחלקת ייעוץ וחקיקה (משפט פלילי) כי הגורמים הנוגעים בדבר במשרדי הממשלה השונים עושים מאמצים להפיץ להערות הציבור את טיוטת תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי. לכשיושלמו מאמצי קידום תזכיר החוק, יינתן מענה מספק לצורך בהסדרת חלוקת התפקידים בין מס"ל ובין המשטרה בכל הנוגע לאירועי הגנת סייבר שבהם מתקיימים היבטי חפיפה בין הגופים, לרבות לעניין העברת המידע.

159 בתור יחידת סמך במשרד ראש הממשלה, ראו: החלטה מס' 2444 "קידום ההיערכות הלאומית להגנת הסייבר" והחלטה מס' 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר", 15.2.15. קדמה לכך, החלטת ממשלה מס' 3611 בנושא "קידום היכולת הלאומית במרחב הקיברנטי", 7.8.11.

160 זאת למעט סמכויות מסוימות שנקבעו בחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998 (להלן - החוק להסדרת הביטחון בגופים ציבוריים), כלפי הגופים המנויים בתוספת השנייה והתוספת החמישית לחוק זה.

161 שאינם מנויים בתוספת השנייה ובתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים.

162 בכפוף להוראות הדין הכללי, החלטות הממשלה ו"עקרונות ה-CERT הלאומי" שנקבעו בתיאום עם היועץ המשפטי לממשלה.

הממצאים העולים בפרק זה מצביעים על פערים שהצטברו לאורך שנים בשל הצורך בהסדרה עקב תיקוני חקיקה שלא הושלמו, ובשל הצורך במתן מענה שלם ומעשי לאיום במרחב המקוון בהתאם להתפתחות הטכנולוגית המהירה. מומלץ כי משרד המשפטים בשיתוף כלל הגורמים הרלוונטיים, יפעל לקדם את התיקונים הנדרשים בחקיקה הקיימת, תוך בחינת השפעתם על כלל זכויות הציבור באמצעות איזון בין צורכי מערכת אכיפת החוק ובין הזכויות המוקנות לפרט בדין.

בתגובתה מינואר 2022 על ממצאי הביקורת הודיעה פרקליטות המדינה כי היא שותפה לצורך בתיקוני החקיקה הנדרשים, כמפורט בפרק זה לעיל, וכי תהיה שותפה בעבודת המטה במשרד המשפטים לקידום תיקוני החקיקה, אם יהיה בכך צורך.

בתגובתו מינואר 2022 על ממצאי הביקורת הודיע המשרד לבט"פ כי הוא ומשרד המשפטים עובדים במשותף על כמה הצעות חוק אשר נוגעות לאכיפה של נושאי סייבר ומחשוב (לרבות חיפושים על כוננים, חיפוש בענן, תפיסת מחשבים, ראיות דיגיטליות ועוד). עוד ציין כי הוא סבור שהנושא מצוי באחריות משרד המשפטים, והוא ישמח לסייע ולהשתתף בכל תיקון חקיקה הנוגע לאכיפת החוק, לרבות חוקי הסייבר והדיגיטל.

מומלץ כי הממצאים העולים בפרק זה יובאו גם בפני הוועדה להתאמת המשפט לאתגרי החדשנות והאצת הטכנולוגיה, כדי שתבחן את הפערים שהוצגו ואת הצורך בתיקוני חקיקה נדרשים בהתאם.

סיכום

בשנים האחרונות מסתמנת עלייה תלולה של מאות אחוזים בהיקף העבריינות במרחב המקוון בישראל ובעולם, הכוללת עבירות באמצעות תוכנות מחשב המסתייעות בטכנולוגיה מתקדמת לצורך ביצוע פשיעה גם במרחב הפיזי. העבריינות במרחב המקוון מסכנת את הפרט, את הציבור הרחב, את המסחר המדינתי והגלובלי ואף את ביטחון המדינה; היא עלולה לאיים על חיי אדם, על שלומם של נשים, של גברים ושל ילדים והיא פוגעת בקניינם ובפרטיותם. בשנת 2020 נאמדו נזקיה הכוללים של פשיעת הסייבר ברחבי העולם בכ-6 טריליון דולר, והם צפויים לעלות מדי שנה בשנה. האתגרים הכרוכים בטיפול בנושא מורכבים והם מחייבים, בין השאר, שיתוף פעולה רציף בין מדינות ובין ארגונים בין-לאומיים העוסקים בכך.

בישראל, המשטרה היא הגורם המרכזי המופקד על הטיפול בעבריינות במרחב המקוון. הממצאים העולים בדוח זה מלמדים, כי המערך הקיים במשטרה אינו מגובה בתפיסת הפעלה עדכנית; אינו כולל כוח אדם מיומן במקצועות הסייבר בהיקף הנדרש לצרכים; ואינו מצטייד באמצעים הטכנולוגיים הנדרשים לביצוע עבודתו בשלמותה. על פי נתונים משנת 2019, קיימת תופעה של תת-דיווח למשטרה על פגיעות מעבריינות מקוונת.

ההערכות בדבר התגברות משמעותית של הפשיעה במרחב המקוון בשנים הקרובות מחייבות את גורמי האכיפה להגביר את ההיערכות שלהן באופן שיובטח המענה האכיפתי הדרוש. מוצע כי המשטרה תרכז מאמץ הן בבניין הכוח והן בהפעלתו למאבק בעבריינות במרחב המקוון בתמיכת המשרד לבט"פ בהתאם להמלצות המפורטות בדוח זה. לצד האמור, על המשטרה להקפיד כי כל פעולה הנעשית באמצעים הטכנולוגיים שברשותה, לרבות פריצה למערכות מחשב פרטיות ולמכשירים סלולריים, תיעשה תוך שמירה על זכויות הפרט ובהתאם לאישורים המשפטיים הדרושים.

על הפרקליטות והב"ה לפעול להסדרה ולהסמכה של חלק מפעולות האכיפה שהן נוקטות בהן. הסדרה זו נדרשת הן משום הצורך לאזן בין צרכי מערכת אכיפת החוק ובין הזכויות המוקנות לפרט בדין והן משום שהעתיד צופן עלייה באירועי עבריינות במרחב המקוון, אשר ידרשו פעולה מתואמת ומתוכננת.