התמודדות משטרת ישראל
עם פשיעת סייבר מתוחכמת

תקציר

רקע כללי

המרחב הקיברנטי הוא מרחב טכנולוגי המורכב ממחשבים, מרשתות מחשבים, מתוכנות, ממידע ממוחשב, מתוכן דיגיטלי ומבסיסי נתונים, שמתקיים בין היתר הודות לרשת האינטרנט ולטכנולוגיית ממשק בין מחשבים (להלן - מרחב הסייבר). המרחב מאופיין בהתפתחות טכנולוגית מהירה, החודרת לכל תחומי החיים ומעצבת את הפעילות החברתית, הכלכלית והמדינתית של האנושות.

יותר מ-2.5 מיליארד בני אדם בעולם צורכים מידע ומקבלים שירותים מגוונים במישרין או בעקיפין באמצעות מרחב הסייבר. אולם התועלת והרווחה החברתית הנובעות משימוש במרחב הסייבר עלולות להיפגע במקרים שבהם גורמים עבריינים מבקשים להשתמש ביכולות שמקנה הטכנולוגיה לצורכי פשיעה (להלן - פשיעת סייבר). המשרד לביטחון פנים (להלן - המשרד לבט"פ) ציין כבר בשנת 2012, כי פשיעת סייבר היא איום אסטרטגי על מדינת ישראל.

פשיעת סייבר גורמת נזקים כספיים הן ישירים כמו גניבת כספים ואובדן מידע בעל ערך כלכלי והן עקיפים היכולים להתבטא בהורדת דירוג אשראי של חברה בגין הפרצה באבטחת המידע שלה, באובדן הזדמנויות עסקיות, בירידה בביצוע פעולות מצד לקוחות עקב אובדן תחושת הביטחון במרחב הסייבר, וכן בהוצאות הכרוכות בהתגוננות מפני תקיפות עתידיות. נוסף על כך היא מסבה נזקים בלתי ממוניים כמו פגיעה בפרטיות.

קיים קושי לקבל מידע מלא לגבי היקף עבירות הסייבר, מפני שחלק ניכר מעבירות פשיעת הסייבר אינו מדווח. ממחקרים עולה כי: כ-34% ממשתמשי מרחב הסייבר בעולם בשנת 2015 נפלו קורבן לפשיעת סייבר פעם אחת לפחות; באנגליה בוצעו בשנת 2015 כשני מיליון אירועים מדווחים בגין פשיעת סייבר; בארצות הברית חל גידול של פי שניים בקירוב בנזק הכספי שנגרם בשל פשיעת סייבר מדווחת בשנים 2015-2012; בישראל, נפגעו בשנת 2015, כ-230,000 בני אדם מפשיעת סייבר. מנתוני משטרת ישראל (להלן - המשטרה) עולה כי מספר תיקי הסייבר שטופלו במשטרה בשנת 2015 כמעט שהוכפל לעומת שנת 2013. המשרד לבט"פ ציין כי שיעור הדיווח למשטרה על אירועים של פשיעת סייבר עומד על 9% בלבד לעומת 45% בעבירות אלימות. בסקר ביטחון אישי לשנת 2015, שערכה הלשכה המרכזית לסטטיסטיקה, עלה כי 90% מהמתלוננים למשטרה בגין פשיעת סייבר לא היו מרוצים מטיפול המשטרה בתלונתם.

פעולות הביקורת

בחודשים מרץ עד אוגוסט 2016 בדק משרד מבקר המדינה היבטים בהתמודדות המשטרה עם פשיעת סייבר מתוחכמת טכנולוגית. בין היתר נבדקו: מבנה מערך הסייבר, ניהולו והתאמתו להתמודדות עם פשיעה זו על מאפייניה המיוחדים; היבטים של כוח אדם ייחודי ושל המשאבים המוקצים לטיפול בפשיעה זו. הבדיקה נעשתה במשטרה ובמשרד לבט"פ. בירורי השלמה נעשו בפרקליטות המדינה ובמטה הסייבר הלאומי שבמשרד ראש הממשלה. במסגרת הביקורת נערכו גם בירורים בקרב גורמים באקדמיה ובתעשייה.

הליקויים העיקריים

מבנה מערך הסייבר במשטרה וניהולו

אי-הלימה בין תקן כוח האדם לצרכים: במועד הביקורת מנה תקן היחידה הארצית לטיפול בפשיעת סייבר כשליש בלבד מהיקף כוח האדם, שנדרש לצורך התמודדות עם הנושא על פי מסקנות והמלצות שגיבשה המשטרה במהלך עשר השנים האחרונות.

פיצול במבנה מערך הסייבר: מבנה מערך הסייבר אינו מותאם להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית. המבנה הקיים משקף את פריסת המערך המבוזרת (de-centralized) שהייתה קיימת במשטרה מאז שנת 2000, ובה יש פיצול והפרדה של חלקי המערך, שעוסקים בפשיעת סייבר מתוחכמת טכנולוגית, לכפיפויות פיקודיות שונות. מבנה מערך מבוזר זה אינו מתיישב עם הידע המקצועי שנצבר בעולם, והוא מנוגד למחקרים ולעמדה שהועלתה במשטרה, בדבר הצורך שמערך הסייבר במשטרה אשר מתמודד עם פשיעת סייבר מתוחכמת טכנולוגית, יהיה ריכוזי (centralized) ויכלול יחידה מרכזית שתרכז את כלל הפעילות בתחום זה.

הסטת עבודת מחלקי הסייבר: הרוב המוחלט של תשומות פעילות חוקרי מחלקי הסייבר במחוזות אינם מופנים לחקירת עבירות סייבר מתוחכמות טכנולוגית, שזהו ייעודם. פיקוד המחוז מְפַנה את מחלקי הסייבר לסייע לצוותי חקירה אחרים במחוז בטיפול בראיות שנתפסות במכשירים דיגיטליים כמו מחשב, טאבלט, טלפון חכם ומצלמה (להלן - ראיות דיגיטליות). מצב זה אינו מאפשר למחלקי הסייבר להקצות את משאביהם לטובת טיפול בתיקי פשיעת סייבר מורכבת שבתחומי אחריותם, ופוגע במקצועיותם ובמיומנותם של חוקרי מחלקי הסייבר במחוזות. אם המשטרה רואה צורך בתוספת חוקרים שיעסקו במיצוי ראיות דיגיטליות במחוזות בעבירות "קלאסיות", עליה לוודא שאין הדבר יבוא על חשבון התמקצעותם של חוקרי המחלקים שייעודם הוא עבירות סייבר מורכבות טכנולוגית.

אי-התאמת המערך למאפיין הגאוגרפי: תפיסת ההפעלה של מערך הסייבר קובעת כי זהות הגוף שיטפל בפשיעת סייבר תיקבע לפי השיוך הגאוגרפי (הטריטוריאלי) של העבירה. תפיסה זו עומדת בניגוד למאפייני פשיעה זו, שאינה תחומה בגבולות פיזיים והיא בעלת היבטים כלל-ארציים ובין-לאומיים.

חולשת מחלקי הסייבר: המאפיין הגאוגרפי מהווה חסם לפעילות אפקטיבית של המשטרה, בכך שהטיפול בפשיעת סייבר מתוחכמת טכנולוגית נעשה בלא שהובטח שהוקצו לטובת המשימה יכולות טכנולוגיות מתאימות, כוח אדם המסוגל להתמודד עם חשודים בכמה מחוזות, והיערכות לוגיסטית נאותה. כמו כן בעבר נוהלו תיקים ללא ראייה מערכתית של מספר המעורבים והנפגעים בתיק והיקף הפגיעה בהם וללא שיתוף בידע לגבי היבטים בין-לאומיים; לנוכח השיוך הגאוגרפי מתקיימות חקירות מקבילות באותו תיק ללא תיאום בין היחידות החוקרות.

טיפול בתיקי חקירה בהתאם למאפיין המורכבות הטכנולוגית: המשטרה לא פעלה ליצור דרך סדורה לאפיון מורכבותה הטכנולוגית של עבירת סייבר שתאפשר לקבוע את רמת התחכום הטכנולוגי של העבירה ולתת לה את המענה הטכנולוגי הנדרש לצורכי חקירה אפקטיבית של פשיעת סייבר. נמצא שכל מחלק סייבר בכל מחוז מגדיר בעצמו את מורכבות התיק, ופועל בהתאם לעקרונות שהתפתחו בו.

חוליית המטה של מערך הסייבר

תפקידה העיקרי של חוליית המטה הוא בניית הכוח של מערך הסייבר, ובין היתר: שיתוף המערך בכל הנוגע לתמונת המצב של פשיעת הסייבר ושיתוף הידע על אודות דרכי ההתמודדות עמה; הנחיה מקצועית, פיקוח ובקרה. כך יוכל מערך הסייבר להתמודד עם האתגרים הניצבים בפניו.

חוסר בשיתוף בידע: חוליית המטה לא מיצבה את עצמה כגוף מרכזי ומוסכם של שיתוף ידע מול כלל היחידות החוקרות במערך, ולא פעלה להבטחת ממשק רציף וקבוע של העברת ידע במערך. בעקבות זאת פעלו היחידות החוקרות במנותק זו מזו בלי להתעדכן בעניין יכולותיהן הטכנולוגיות או בעניין דרכי התמודדותן עם תיקי פשיעת סייבר.

הפרדת תחומי האחריות של גוף המטה: ההחלטה על הפרדת תחומי האחריות של גוף המטה למישור טכנולוגי נפרד מהמישור החקירתי אינה מביאה בחשבון את המאפיינים של פשיעת סייבר מתוחכמת טכנולוגית, שבה המישור הטכנולוגי והמישור החקירתי כרוכים זה בזה. החלטה כזו מנוגדת לידע מקצועי בין-לאומי הקיים בעולם.

חולשת חוליית המטה: חוליית המטה לא מיסדה תהליכי עבודה מוסדרים בין היחידות החוקרות במחוזות. לפיכך לא התקיימו ממשקי עבודה יעילים בין חוקרי פשיעת הסייבר בתחנות, בין מחלקי הסייבר ובין חוליית המטה. כתוצאה מכך

אירעו מקרים שבהם נגרם נזק לראיות דיגיטליות עד כדי איבוד ראיות ופגיעה בתיקי חקירה.

תקציב ורכש

תקציב: אף שבשנים 2015-2013 מספר תיקי פשיעת הסייבר כמעט שהוכפל, צמצמה המשטרה בשנת 2016 את תקציב ההצטיידות של מערך הסייבר בשליש, כך שהיקף התקציב לרכש אינו מספיק לנוכח הגידול הניכר בדרישות השטח.

היעדר אמצעים: ליחידות החוקרות חסרים אמצעים מסוימים שדרושים לחוקרים לצורך טיפול בראיות שנאספו; בתחנות קיים מחסור באמצעים טכנולוגיים שיאפשרו לאזרחים למסור ראיות דיגיטליות בעת הגשת תלונה בנוגע לפשיעת סייבר.

רכישה פרטית של ציוד: בשל חוסר בציוד טכנולוגי ולנוכח אי-הלימה בין הצרכים בשטח ובין הציוד הקיים, נאלצו חוקרי פשיעת סייבר בתחנות לרכוש מכספם האישי ציוד בסיסי במאות ש"ח, כדי שיוכלו לבצע את עבודתם.

גיוס כוח אדם טכנולוגי ושימורו

קושי בגיוס עובדים ובשימורם: קיים קושי לגייס כוח אדם למערך הסייבר בשל פערים בשכר שמוצע למועמדים למערך, בהשוואה לגופים מתחרים במגזר הציבורי והפרטי. בשל כך גיבשו המשטרה ומשרד האוצר בספטמבר 2015 טיוטת הסכם העסקה, ולפיו יוצע שכר גבוה בהרבה מהשכר המשולם כיום למועמדים "מומחים". אך עד ינואר 2017 לא הושג הסכם סופי. כמו כן, בהיעדר תמריצים מתאימים, יש קושי של ממש בשימור כוח האדם בעל מומחיות טכנולוגית גבוהה בתחום פשיעת הסייבר שנקלט ביחידה הארצית, וקיים חשש מעזיבת כוח האדם האיכותי, שהוא עמוד התווך של המערך.

היעדר ממשק בין המשטרה לבין מטה הסייבר הלאומי

כדי למצות את מלוא הפוטנציאל והמשאבים הלאומיים הקיימים יש לשלב מאמצים מצד כלל הארגונים הפועלים במרחב הסייבר במדינה, בייחוד לנוכח הקשר ההדוק שקיים בין תופעות פשיעה ובין איומי טרור ופגיעה במתקנים חיוניים. אף שהמשטרה הכירה בחשיבות הנושא, היא לא פעלה יחד עם מטה הסייבר הלאומי כדי לבסס את תפיסת ההפעלה של מערך הסייבר במשטרה באופן שיאפשר את התאמתה המיטבית למאפיינים המיוחדים של הפשיעה במרחב הסייבר.

ההמלצות העיקריות

מאחר שהמשטרה סבורה שיש צורך בהקצאת משאבים נוספים למערך הסייבר, מחובתה להעלות נושא זה בדיוני התקציב הנערכים בשיתוף המשרד לבט"פ ומשרד האוצר. במסגרת זו עליה להציג גם את המשמעויות ואת ההשלכות הנובעות מהקצאות תקציב חסרות לתחום זה, כדי שאפשר יהיה לבחון את הצורך בחיזוק מערך הסייבר בהשוואה לצרכים אחרים של המשטרה.

במסגרת עבודת המטה של המשטרה עליה יחד עם המשרד לבט"פ לבחון לאלתר את הצורך ביחידה מרכזית אחת שתתכלל את הנעשה בתחום פשיעת הסייבר המתוחכמת טכנולוגית תוך בחינת העוגנים המקצועיים המקובלים בעולם שנידונו בספרות המקצועית, זאת לצד פעילות המערך הפרוס בתחנות שמתמודד עם פשיעת סייבר שאינה מתוחכמת טכנולוגית ואשר זקוק ליכולות רלוונטיות. כמו כן יש לפעול להתאמת תפיסת ההפעלה של המערך למאפייני פשיעת הסייבר, שהם חציית גבולות מחוזיים ובין-לאומיים ומורכבות טכנולוגית. בנוסף על המשטרה ועל המשרד לבט"פ לבחון בשנית אם אכן הפרדת תחומי האחריות של גוף המטה במערך הסייבר תואם את הידע המקצועי הקיים בעולם, התומך בכך שבכל הנוגע לעבירות מתוחכמות טכנולוגית לא תהיה הפרדה מלאכותית בין המישור הטכנולוגי למישור החקירתי.

בחינות אלו נדרשות, שכן היערכות המשטרה והמשרד לבט"פ כיום לאתגרים ולסיכונים הלאומיים של פשיעת הסייבר המתוחכמת טכנולוגית, אינה מתבססת על התפיסות המקובלות בעולם ועל לקחי משטרות זרות, לגבי טיפול אפקטיבי בפשיעה זו וספק רב אם היא נותנת את המענה הדרוש לאיומים.

על המשטרה להסדיר ממשקי עבודה יעילים בין חוליית המטה שבמערך הסייבר לבין היחידות החוקרות, ובהם שיתוף מידע, הנחיה מקצועית ופיקוח ובקרה.

מרכזיותו של מערך הסייבר, ההתפתחות הטכנולוגית המהירה של הפשיעה והצורך במתן מענה לתלונות האזרחים, מחייבים את המשטרה ואת המשרד לבט"פ, לנתח את הצרכים הגדלים של מערך הסייבר אל מול יכולת ההתמודדות של המערך עם תיקים מורכבים טכנולוגית. לאור זאת עליהם לוודא שלרשות המערך המופקד על ההתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית יעמוד התקציב הדרוש להתמודדות אפקטיבית עם האתגרים שמציבה פשיעה זו, ובכלל זה תקציב לרכש ולהצטיידות, תקציב לגיוס כוח אדם בעל מומחיות טכנולוגית גבוהה ובעל ידע הדרוש להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית ותקציב לשימור כוח האדם שנקלט במערך מאז הוקם.

על המשרד לבט"פ, יחד עם המשטרה ובשיתוף מטה הסייבר הלאומי ומשרד האוצר, לפעול בהקדם למיצוי מלוא הפוטנציאל, הידע והמשאבים הלאומיים הקיימים, לטיפול מיטבי באיומי פשיעת הסייבר מתוך ראייה לאומית כוללת של האיומים. זאת בייחוד לנוכח הקשר ההדוק שקיים בין תופעות פשיעה ובין איומי טרור ופגיעה במתקנים חיוניים באמצעות מרחב הסייבר.

סיכום

ההתפתחויות במרחב הסייבר האיצו את התרחבות הפשיעה המתוחכמת טכנולוגית שכוללת עבירות נגד מחשבים, טלפונים חכמים, שרתים ורשתות מחשבים וכן שימוש הולך וגובר בתוכנות זדוניות, בחדירה לא חוקית למחשבים ולמאגרים ממוחשבים, בריגול עסקי וכדומה. פשיעה זו אינה תחומה בגבולות גאוגרפיים, והיא בעלת השלכות ברמה הלאומית וברמה הבין-לאומית. ממצאי דוח זה העלו שהמשטרה והמשרד לבט"פ הקימו אמנם מערך לטיפול בעבירות סייבר, אך לא התאימו את המערך לצרכים ולאתגרים של עבירות הסייבר מתוחכמות טכנולוגית שמתפתחות ומשתנות במהירות רבה. עבודת מערך הסייבר, שייעודו לטפל בעברות סייבר מתוחכמות טכנולוגית, מנותבת בעיקר לסיוע טכני ליחידות חקירה מחוזיות המטפלות בעבירות "קלאסיות" שאינן מתוחכמות טכנולוגית, על חשבון התמקצעות בלוחמה בפשיעת הסייבר.

ממצאיו של דוח זה מלמדים על כך שהמבנה הפיקודי המבוזר של מערך הסייבר, היעדרה של יחידה מרכזית והפרדת תחומי האחריות של גוף המטה למישור טכנולוגי נפרד מהמישור החקירתי - אין בהם כדי לתת מענה הולם לאתגרים שעמם נדרשת המשטרה להתמודד במסגרת הלחימה בפשיעה זו. תפיסת ההפעלה של המערך טעונה תיקון, שכן היא גובשה בהתאם למצב הפשיעה והאתגר הטכנולוגי שהיו בשנת 2000, ולא בהתאם למאפייניה הייחודיים של פשיעת סייבר שהתפתחו דרמתית מאז. אף על פי שחל גידול ניכר בהיקף פשיעת הסייבר המתוחכמת טכנולוגית בשנים האחרונות, חל קיצוץ של ממש במענה התקציבי שהופנה לתחום זה במשטרה, באופן שאינו עונה על הצורך הבסיסי של המערך. קיצוץ זה מונע את ההתעצמות הנדרשת לשם התמודדות עם פשיעה זו, ואף גורם ל"בריחת מוחות" מהמערך. לפיכך, במועד סיום הביקורת המשטרה אינה ערוכה להתמודדות עם עבירות פשיעת סייבר מורכבות טכנולוגית.

ממצאי הדוח מעידים כי המשטרה נמצאת בפיגור ניכר בהתמודדות עם פשיעת סייבר מורכבת טכנולוגית. המשך פעילות המשטרה במתכונתה הנוכחית עלול להרחיב את הפערים במענה הניתן לפשיעה זו. מתשובות המשטרה עולה אמנם כי קיימות תכניות עתידיות לחיזוק יכולותיה בתחום פשיעת הסייבר, תכניות שהינן בעלות השלכות רוחב מורכבות ושיבשילו לאורך זמן. יחד עם זאת נדרשת פעולה נוספת כדי לענות על הליקויים שהועלו בדוח זה. על המשטרה ועל המשרד לבט"פ לפעול לתיקון הליקויים וליישום ההמלצות שהועלו בדוח בהקדם וללא דיחוי כדי להתאים את פעילות מערך הסייבר במשטרה לעולם רווי טכנולוגיות מתקדמות ולאתגרים שבפניהם תעמוד המשטרה בשנים הקרובות.

התמודדות עם פשיעת הסייבר היא אתגר לאומי המחייב את המשטרה ואת המשרד לבט"פ לבסס תפיסה אסטרטגית רלוונטית למאפייני פשיעת הסייבר המתוחכמת טכנולוגית, ולהעצים במידה רבה את יכולותיה הטכנולוגיות של היחידה הארצית במשטרה. כל זאת בשיתוף מטה הסייבר הלאומי ותוך כדי בחינת הידע המקצועי בעולם.

מבוא

המרחב הקיברנטי הוא מרחב טכנולוגי המורכב ממחשבים, מרשתות מחשבים, מתוכנות, ממידע ממוחשב, מתוכן דיגיטלי ומבסיסי נתונים, וכולל גם את הגורם האנושי המורכב ממפתחים וממשתמשים בכל אלה (להלן - מרחב הסייבר)[1]. המרחב מתקיים בין היתר הודות לרשת האינטרנט ולטכנולוגיית ממשק בין מחשבים. המרחב מאופיין בהתפתחות טכנולוגית מהירה החודרת לכל תחום פעילות בחברה המודרנית ומעצבת את הפעילות החברתית, הכלכלית והמדינתית של האנושות.

יותר מ-2.5 מיליארד בני אדם בעולם צורכים מידע ומקבלים שירותים במישרין או בעקיפין במגוון תחומים כמו בנקאות, ביטוח, בריאות ותחבורה, וכן רוכשים באופן מקוון ומבצעים פעולות מקוונות לצורכי פנאי, תרבות ותקשורת באמצעות מרחב הסייבר. מרחב הסייבר משמש "כלי עבודה ראשון במעלה... ולארכיב כמעט אין סופי המאכסן בתוכו את זיכרונותיו ופרי עמלו של האדם"[2], ומהווה משאב בעל חשיבות מכרעת עבור מדינות, ארגונים, חברות, עסקים ואנשים פרטיים. לפיכך הפכה החברה המודרנית לתלויה בו ("dependence on it")[3].

בישראל ניכרת מגמה דומה למתרחש בעולם. לפי נתוני הלשכה המרכזית לסטטיסטיקה מאוקטובר 2015 לכ-96% ממשקי הבית יש טלפון נייד אחד לפחות; לכ-81% יש מחשב וכ-72% מחוברים לרשת האינטרנט. לפי הסקר החברתי של הלשכה המרכזית לסטטיסטיקה מספטמבר 2015, כ-42% ממשקי הבית השתמשו באינטרנט לצורכי קניות מקוונות.

התועלת והרווחה החברתית הנובעות מן השימוש במרחב הסייבר עלולות להיפגע במקרים שבהם מרחב זה אינו בטוח לשימוש. בית המשפט העליון ציין כי הקדמה הטכנולוגית והכלים שהיא מאפשרת אינם שמורים רק בידי רשויות המדינה ובידי החברה והמשק, "אלא נעשה באלו שימוש על ידי קבוצות עברייניות קטנות כגדולות, אשר הפנימו לפני זמן רב כי היתרונות הטמונים בהם מקדמים היטב את מטרותיהן". עוד ציין בית המשפט כי המציאות המודרנית והחידושים הטכנולוגיים הפכו ל"פלטפורמה נוחה לגורמים שליליים ועבריינים המבקשים לעשות שימוש ביכולות שמקנה הטכנולוגיה לצרכיהם"[4].

בית המשפט ציין כי המציאות המודרנית והחידושים הטכנולוגיים הפכו ל"פלטפורמה נוחה לגורמים שליליים ועבריינים המבקשים לעשות שימוש ביכולות שמקנה הטכנולוגיה לצרכיהם"

חוק המחשבים, התשנ"ה-1995 (להלן - חוק המחשבים) מבקש להגן על האינטרסים הרבים שמגלם מרחב הסייבר עבור החברה מפני ניצול לרעה של מרחב זה. חוק המחשבים מונה חמש עבירות בענייני מחשב וחומרי מחשב (להלן - עבירות סייבר או פשיעת סייבר): (א) שיבוש פעילות תקינה של מחשב, ובכלל זה מחיקת מידע מחשב ושינוי מידע במחשב; (ב) עבירות באמצעות מחשב שתוצאתן תהיה מידע כוזב שיש בו כדי להטעות; (ג) חדירה לחומר מחשב שלא כדין; (ד) חדירה לחומר מחשב שלא כדין כדי לבצע עבירה אחרת; (ה) עריכת תוכנה או ביצוע פעולות

1 מרחב הסייבר (Cyber) הוא קיצור של הביטוי המרחב הקיברנטי (Cybernetic).

2 רע"פ 8873/07 **היינץ ישראל בע"מ נ' מדינת ישראל** (פורסם במאגר ממוחשב, 2.1.11).

3 Nato Organization, **National Cyber Security, Framework Manual**, p. 3 (2012).

4 בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל ואח' נ' משטרת ישראל** (פורסם במאגר ממוחשב, 28.5.12), פסקאות 5, 42.

שעלולות להביא לידי שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו; פעולות שתוצאתן היא מידע כוזב; האזנת סתר[5] ופגיעה בפרטיות[6].

באוגוסט 2011 החליטה הממשלה[7] על הקמת מטה סייבר לאומי שישמש גוף מטה לראש הממשלה, לממשלה ולוועדותיה, ימליץ על מדיניות לאומית בתחום הסייבר ויקדם את יישומה. נקבע כי ההחלטה לא תחול על הגופים המיוחדים דוגמת המשטרה. עם זאת נקבע כי גם הגופים המיוחדים יהיו שותפים לגיבוש התפיסה הלאומית במרחב הסייבר[8].

המשטרה היא אחת מזרועותיו של המשרד לביטחון הפנים (להלן - המשרד לבט"פ) שאחראי על ביטחון הפנים של מדינת ישראל ואזרחיה. כבר בשנת 2012 ציין המשרד לבט"פ כי פשיעת הסייבר היא איום אסטרטגי ובמסמך מדיניות השר לשנת 2016 נקבע כי אחד מיעדי המשרד, הוא צמצום ממדי פשיעת הסייבר. בהערכת מצב שהכין המשרד לשנת 2016 צוין כי שיעור ההיפגעות מפשיעת סייבר בקרב בני עשרים ומעלה הוא הגבוה ביותר מבין העבירות ועומד על 5.8% - גבוה יותר משיעור הנפגעים בציבור זה בשל עבירות אלימות (3.3%). עוד צוין כי שיעור הדיווח למשטרה על אירועים של פשיעת סייבר עומד על 9% בלבד לעומת 45% בעבירות אלימות. בסקר ביטחון אישי לשנת 2015 שערכה הלשכה המרכזית לסטטיסטיקה עלה כי 90% מהמתלוננים למשטרה בגין פשיעת סייבר לא היו מרוצים מטיפול המשטרה בתלונתם.

כבר בשנת 2012 ציין המשרד לבט"פ כי פשיעת הסייבר היא איום אסטרטגי על מדינת ישראל

פעולות הביקורת

בחודשים מרץ עד אוגוסט 2016 בדק משרד מבקר המדינה היבטים בהתמודדות המשטרה עם פשיעת סייבר מתוחכמת טכנולוגית. בין היתר נבדקו: מבנה מערך הסייבר, ניהולו והתאמתו להתמודדות עם פשיעה זו על מאפייניה המיוחדים; היבטים של כוח אדם ייחודי ושל המשאבים המוקצים לטיפול בפשיעה זו. הבדיקה נעשתה במשטרה באגף חקירות ומודיעין (להלן - אח"ם), באגף תכנון וארגון (להלן - אג"ת), באגף משאבי אנוש, ביחידה הארצית לטיפול בפשעי סייבר ביחידת להב 433 ובמחוזות המשטרה. בדיקות נעשו גם במשרד לבט"פ, באגף ביטחון המידע וסייבר ובאגף תכנון תקצוב ובקרה. בירורי השלמה נעשו בפרקליטות המדינה ובמטה הסייבר הלאומי שבמשרד ראש הממשלה. במסגרת הביקורת נערכו גם בירורים בקרב גורמים באקדמיה ובתעשייה. בשנת 2015 בדק משרד מבקר המדינה את ה"היבטים בהיערכות המדינה להגנת המרחב הקיברנטי"[9].

5 לפי חוק האזנות סתר, התשל"ט-1979.

6 לפי חוק הגנת הפרטיות, התשמ"א-1981.

7 החלטת ממשלה מס' 3611 מיום 7.8.11 בנושא קידום היכולת הלאומית במרחב הקיברנטי.

8 גופים מיוחדים: צבא הגנה לישראל, משטרה, שירות הביטחון הכללי, המוסד למודיעין ותפקידים מיוחדים ומערכת הביטחון.

9 מבקר המדינה, **דוח שנתי 67א** (2016), עמ' 5. חלקו של הדוח נותר חסוי.

פשיעת סייבר

אירועים של פשיעת סייבר מתפתחים בקצב הולך וגובר תוך כדי ניצול החידושים הטכנולוגיים, פוגעים בקורבנות רבים ברחבי העולם ומסבים נזקים כלכליים עצומים. הפורום העולמי הכלכלי קבע בדוח הסיכונים שלו לשנת 2016 כי התקפות סייבר הן מבין חמשת הסיכונים הגלובליים הגדולים ביותר[10], והמרכז הבין-לאומי למניעת פשיעה (ICPC) הצביע כי ב-80% מאירועי פשיעת סייבר מעורבים ארגוני פשיעה.

פשיעת סייבר גורמת נזקים כספיים ישירים ועקיפים. דוגמאות לנזקים ישירים הן סכומי כסף שנגנבו, אובדן זמן, פיצויים שעסקים שנפגעו עלולים לשלם בגין נזקים שנגרמו ללקוחותיהם ואובדן מידע בעל ערך כלכלי (למשל רשימת לקוחות ופרטי אשראי). נזקים עקיפים יכולים להתבטא בהורדת דירוג אשראי של חברה בגין פְּרצה באבטחת המידע שלה, באובדן הזדמנויות עסקיות, בירידה בביצוע פעולות מצד לקוחות עקב אובדן תחושת הביטחון במרחב הסייבר, וכן בהוצאות הכרוכות בהתגוננות מפני תקיפות עתידיות[11]. נוסף על כך פשיעת הסייבר מסבה נזקים בלתי מָמוֹנִיים, כמו פגיעה בפרטיות.

שימוש בטכנולוגיה לביצוע עבירות

מגוון העבירות שמתרחשות במרחב הסייבר הוא רחב וכולל סוגי איומים רבים ומשתנים, הנבדלים ביניהם משמעותית במידת התחכום הטכנולוגי של העבירות, בסוגי העבריינים ובמניעיהם. מחקר של האו"ם משנת 2013 הצביע על מגוון העבירות במרחב הסייבר, וביניהן: עבירות ששיבשו פעולת מחשבים או הפריעו לה, עבירות פריצה וגישה לא חוקית למאגרי מידע ממוחשבים, עבירות שגרמו לשינויים במידע ממוחשב, עבירות של זיוף, הונאה, גניבת קניין רוחני, גניבת זהויות במרחב הסייבר, פשעי שנאה ופשעי פורנוגרפיה וטרור[12]. ארגון IC3 האמריקני[13] הרחיב את היקף התופעה המדווחת גם למקרים האלה: מניעת שימוש באתרים וגישה אליהם; פיתוח תוכנות זדוניות[14] והסוואתן, לדוגמה בפרסומות תמימות למראה שנועדו לסייע בגניבת כספים מחשבונות בנקים; החדרת וירוסים[15] למחשבים.

10 הפורום העולמי הכלכלי, **דוח הסיכונים הגלובליים לשנת 2016** (14.1.16).

11 חיים ויסמונסקי, **חקירה פלילית במרחב הסייבר** (הוצאת נבו, 2015) (להלן - ויסמונסקי), עמ' 55-54.

12 מחקר סוכנות האו"ם לסמים ופשיעה **Comprehensive Study on Cybercrime** (פברואר 2013) (להלן - מחקר סוכנות האו"ם לסמים ופשיעה).

13 ראו:
U.S. Department of Justice, Federal Bureau of Investigation, **2015, Internet Crime Report** (https://www.ic3.gov).

14 תוכנה זדונית היא תוכנה המשתמשת במרחב הסייבר לשם ביצוע פעולות לא חוקיות.

15 וירוס מחשב הוא תוכנה המוחדרת למחשב ומבצעת בו שינויים כגון במידע האגור בו.

פשיעת סייבר עושה שימוש נרחב ב"רשתות אפלות" ובפעולות טכנולוגיות מתוחכמות המשתמשות הן בטכנולוגיה מתקדמת המקשה את פענוח הפשעים והן בתוכנות זדוניות לשם השתלטות על מיליוני מחשבים

עברייני סייבר המומחים בטכנולוגיה ובמחשבים מבצעים עבירות כמו: פריצה למאגרים ממוחשבים; הפצת תוכנות ממוחשבות מתוחכמות לשם ריגול עסקי; גניבת מספרי כרטיסי אשראי; בניית מתקנים להעתקת מספרי כרטיסים מכספומטים; פרסום חוברות הדרכה בתחומים שונים של פשיעת סייבר. כל אלו תמורת תשלום המפורט במחירון מסודר. תופעה זו של "שירות לקוחות" מעידה על הזמינות, על הנגישות ועל הקלות בביצוע פשעי סייבר מתוחכמים טכנולוגית גם למי שאינו מיומן בכך.

פשיעת סייבר עושה שימוש נרחב ב"רשתות אפלות"[16] ובפעולות טכנולוגיות מתוחכמות המשתמשות הן בטכנולוגיה מתקדמת המקשה את פענוח הפשעים והן בתוכנות זדוניות לשם השתלטות על מיליוני מחשבים "מארחים" (hosts)[17] תמימים ברחבי העולם, שעל פי פקודה מבצעים פשעי סייבר במחשבים ובשרתים אחרים.

תוכנה זדונית שפעלה ברחבי העולם והתגלתה בשנת 2014 בין היתר על ידי האף.בי.איי, ממחישה את האמור לעיל באופן הזה: שרת מרכזי (master) שימש לבניית רשת מחשבים מארחים (ובכלל זה טלפונים חכמים), באמצעות הדבקתם בתוכנה זדונית ללא ידיעת בעליהם. אחת האפשרויות להדבקה היא באמצעות פתיחת קישור תמים למראה שנשלח בדואר אלקטרוני. כמיליון מחשבים שהודבקו בתוכנה הזדונית גויסו וביצעו יחד פעולות לא חוקיות כמו חדירה למחשב וגניבת מידע פרטי ועסקי, סחיטה על ידי הצפנת קובצי מחשב, הפצת וירוסי מחשב ומניעת גישה לאתרי אינטרנט. פעולות אלו נעשו בהתאם לפקודה שקיבלו מהשרת המרכזי ובלי שהוגבלו טריטוריאלית. בתרשים להלן המחשה לפעולה של תוכנה זדונית:

16 "רשתות אפלות" מתבססות על רשתות תקשורת אנונימיות המוצפנות ברמה גבוהה ועל אתרי אינטרנט שהגישה אליהם מוגבלת באופנים שונים, כך שהם נגישים רק לגורמים מסוימים ואינם מופיעים במנועי החיפוש המקובלים, בניגוד לצורת התקשורת הרגילה באינטרנט.

17 מחשב מארח בהקשר זה הוא מחשב שגורם עברייני משתלט עליו ללא ידיעת בעליו ומבצע באמצעותו פשעי סייבר. לדוגמה, אחת התקיפות שמתבצעת באמצעות מחשבים מארחים מטרתה לגרום לנפילת אתרים או שרתי מחשבי באופן המונע התחברות אליהם (מתקפת DDos).

תרשים 1: **המחשה לפעולה של תוכנה זדונית**

מקור: אתר האינטרנט של האף.בי.איי בעיבוד משרד מבקר המדינה.

התוכנה הזדונית גרמה בין היתר לנזקים האלה: מעל מיליון מחשבים הודבקו ושימשו תשתית לרשת המחשבים המארחים (שכינויה botnet) לביצוע פעולות ללא ידיעת בעליהם; נגרמו נזקים כספיים גלובליים שהוערכו במאות מיליוני דולרים, ובהם נזקי סחיטה שפגעו ב-234,000 קורבנות בקירוב; זוהו תשלומי כופר בסך של כ-30 מיליון דולר במהלך שנת 2013. כדי להשבית את פעילות התוכנה הזדונית נדרש שיתוף פעולה מצד עשר מדינות.

הגישה המובילה בעולם לטיפול יעיל בפשיעת סייבר מחלקת את העבירות לשלוש קטגוריות המושפעות בעיקר מרמת התחכום הטכנולוגי ששימש לביצוע העבירות[18]: (א) עבירות שהושלמו במרחב הפיזי שביצוען נעשה בסיוע מחשב; (ב) עבירות "קלאסיות" שבוצעו באמצעות מחשבים (cyber enabled crime); (ג) עבירות נגד מחשבים (cyber dependent crime). להלן בתרשים פירוט סוגי העבירות ורמת התחכום הטכנולוגי השלוב בהן.

תרשים 2: סוגי העבירות לפי רמת תחכום טכנולוגי

מקור: מידע מספרות מקצועית בעיבוד משרד מבקר המדינה.

18 ויסמונסקי, עמ' 32-35; מחקר סוכנות האו"ם לסמים ופשיעה; דוח הסוכנות המרכזית להתמודדות עם פשיעה באנגליה, National Crime Agency, NCA Strategic Cyber Industry Group, **Cyber Crime Assessment 2016** (July 2016).

היעדר נתונים

קיים קושי לקבל מידע מלא לגבי היקף עבירות הסייבר, מאחר שחלקן הגדול אינו מדווח, בין היתר, בגלל הגורמים האלה[19]: (א) פגיעה בקורבנות רבים בפיזור גאוגרפי נרחב, ומידת הנזק לכל קורבן לרוב אינה גבוהה במידה שמניעה אותו לדווח; (ב) בעליהם של המחשבים שבאמצעותם בוצעו תקיפות אוטומטיות על מחשבים אחרים לא היו מודעים לכך; (ג) קורבן העבירה (למשל קורבן גניבת מידע ממחשב וציתות לתקשורת באינטרנט) כלל לא היה מודע לפגיעה בו; (ד) הסתרה של ספקי שירות אינטרנט שהותקפו או של נותני שירותים מקוונים אחרים מחשש לבריחת לקוחות ולפרסום שלילי.

חרף הקושי בקבלת נתונים מלאים, להלן הנתונים הקיימים בעולם ובישראל:

1. כ-34% ממשתמשי מרחב הסייבר בעולם בשנת 2015 נפלו קורבן לפשיעת סייבר פעם אחת לפחות[20].
2. באנגליה בוצעו בשנת 2015 כשני מיליון אירועים מדווחים בגין פיתוח, הפצה ושימוש בווירוסים במרחב הסייבר וכ-400,000 אירועים מדווחים של חדירה אסורה למידע פרטי[21]; כן צוין באנגליה בסקר של איגוד הקמעונאים הבריטי לשנת 2013 כי כ-80% מהתאגידים במגזר הקמעונאי נפגעו מתוכנות זדוניות כולל תוכנות ריגול עסקי, כ-60% מהתאגידים נפגעו מחדירה אסורה למערכות המחשבים והמידע שלהם וכ-50% נפגעו מהתקפות מניעת שירות.
3. בארצות הברית חל גידול של פי שניים בקירוב (מעל 90%) בנזק הכספי שנגרם בגין פשיעת סייבר מדווחת, מ-525 מיליון דולר בשנת 2012 ל-1.007 מיליארד דולר בשנת 2015[22].
4. בישראל, לפי סקר ביטחון אישי של הלשכה המרכזית לסטטיסטיקה לשנת 2015, נפגעו כ-230,000 בני אדם מפשיעת סייבר, לעומת כ-195,000 בני אדם שנפגעו מעבירות אלימות או מעבירות של איום באלימות. לפי נתוני המשטרה בשנת 2015 דווחו למשטרה 5,089 אירועים.

מהסקירה לעיל עולה כי התחכום הטכנולוגי של פשעי סייבר מצריך היערכות מתאימה. רכיב יסודי בהיערכות ובמוכנות של גורמי אכיפת חוק להתמודדות עם פשיעת סייבר הוא יצירת מערכת מתודולוגית שתבטא את המגוון העצום של התופעות שנצפות במרחב הסייבר, ותותאם למידת תחכומן הטכנולוגי והתעדכנות בחידושים, מתוך חיזוק יכולות המשטרה לאיתור של נזקים ומזיקים[23]. בית המשפט העליון ציין כי "בקרב טכנולוגי זה שאנו מצויים עדיין בעיצומו... הרשויות... חייבות

> קיים קושי לקבל מידע מלא לגבי היקף עבירות הסייבר, מאחר שחלקן הגדול אינו מדווח. בישראל, לפי סקר של הלשכה המרכזית לסטטיסטיקה לשנת 2015, נפגעו כ-230,000 בני אדם מפשיעת סייבר

19 ויסמונסקי, עמ' 51-63.

20 "מגמות בעולם הסייבר לשנת 2015", בתוך משטרת ישראל, **תמונת פשיעת סייבר ארצית סיכום שנת 2015** (3.3.15).

21 סקר פשיעה של אנגליה ווילס: **CSEW Fraud and Cyber-crime Development: Field Trial**.

22 ראו:
U.S. Department of Justice, Federal Bureau of Investigation, **2015, Internet Crime Report** (https://www.ic3.gov).

23 אסף הרדוף, **פשיעת סייבר** (הוצאת נבו, 2010), עמ' 24-27, 171-172, 230-273.

להישאר עם היד על הדופק הטכנולוגי ולאמץ במהירות גדולה כלים ושיטות מתקדמים שיסייעו להן בביצוע מלאכתן"[24].

הגידול הניכר בעבירות במרחב הסייבר 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 (להלן - מערך הסייבר). משרד מבקר המדינה בדק את היערכות המשטרה לטיפול בפשיעה זו, להלן הממצאים.

24 בג"ץ 3809/08 **האגודה לזכויות האזרח בישראל ואח' נ' משטרת ישראל** (פורסם במאגר ממוחשב, 28.5.12), פסקה 5.

מבנה מערך הסייבר במשטרה וניהולו

הקמת היחידה הארצית: תקן כוח האדם

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 משטרת ישראל המוסמך לבצע את החיפוש אחר ראיות דיגיטליות (להלן - חוקר מיומן).

בעקבות חקיקת חוק המחשבים והעלייה בפשיעת הסייבר בעלת תחכום טכנולוגי בארץ ובעולם החליטה המשטרה באפריל 2000 על הקמת מפלג לעבירות מחשב (להלן - היחידה הארצית) ביחידה הארצית לחקירות הונאה. בין יתר תפקידיה הוטלו על היחידה המשימות האלה: לחקור עבירות העוסקות בחדירה למחשבים; לחקור עברות "קלאסיות" המתבצעות בסביבת מחשב; להעניק סיוע חקירתי בהפקת ראיות דיגיטליות ממחשבים; לאסוף מידע מודיעיני על עבירות המתבצעות בסביבת מחשב או באמצעות האינטרנט; לפתח תוכנות ושיטות חקירה ייחודיות הנוגעות לעבודת היחידה. כן הוטל על היחידה להכשיר חוקרים מיומנים. בפקודת ההקמה נקבע כי ביחידה הארצית יהיה מספר תקנים מועט.

בד בבד עם הקמת היחידה הארצית נקלטו במחוזות המשטרה חוקרים מיומנים שמשימתם העיקרית הייתה להפיק ראיות דיגיטליות ממחשבים עבור המחוזות. חוקרים אלו לא היו חלק מהיחידה הארצית. כך שמערך הסייבר של המשטרה כלל חוקרים מיומנים ביחידה הארצית וכן חוקרים מיומנים במחוזות.

במהלך השנים בחנו המשטרה והמשרד לבט"פ את היערכות המשטרה ומוכנותה להתמודדות עם פשיעת סייבר וכן נבחנו צרכיה המשתנים. להלן הפרטים:

1. **צוות הבדיקה משנת 2006**: בשנת 2006 הוקם במשטרה צוות לבדיקת הטיפול בעבירות מחשב. בבדיקתו העלה הצוות כי המשטרה מתקשה לנהל חקירות אפקטיביות, הן בשל אופי העבירות שהן חוצות גבולות גאוגרפיים והן בשל העלייה במורכבותה הטכנולוגית של פשיעת הסייבר והעלייה בהיקפי העבירות בארץ ובעולם.

   הצוות זיהה חולשות בעבודת המשטרה, ובהן: (א) תחום הטיפול של היחידה הארצית אינו מוגדר; (ב) היחידה אינה מסוגלת לתת מענה מספיק למגוון תפקידיה, ואין ביכולתה לחקור תיקים מורכבים רבים לאורך זמן; (ג) חשש לחקירות מקבילות שמבצעות יחידות חוקרות שונות בשל חוסר בגורם המרכז תיקים ברמה הארצית; (ד) אין הדרכה לכלל המשטרה לטיפול במתלוננים בנושא עבירות מחשב; (ה) עבודת החוקרים המיומנים במחוזות המשטרה בהפקת ראיות דיגיטליות נעשית כתפקיד הנוסף על תפקידם העיקרי במחוז (נע"ת); (ו) תחומי המודיעין, האיסוף וההערכה מכווני פשיעת סייבר לוקים בחסר.

   הצוות המליץ שהיחידה הארצית תכלול מטה שיעסוק, בין היתר, בהנחיות מקצועיות ובניהול הידע בתחום פשיעת הסייבר; תהיה בעלת יכולת מודיעינית וטכנולוגית משמעותית; תיתן מענה לכל עבירות המחשב בישראל; תהיה

כפופה לראש אח"ם. הוצע כי ליחידה הארצית יוקצו תקנים כדי שתוכל לעמוד ביעדיה, ושבכל מחוז במשטרה יוקם מערך של חוקרים מיומנים שיעסוק בהפקת ראיות דיגיטליות ממחשבים.

נמצא כי המלצות הצוות, לרבות ההמלצה שהתייחסה לכוח האדם הדרוש כדי שהיחידה הארצית תוכל לעמוד ביעדיה, לא יושמו.

2. **עבודת המטה משנת 2009:** בשנת 2009 נערכה עבודת מטה באח"ם שהוצגה בפני ראש אג"ת. המסקנה העיקרית מן העבודה הייתה כי תקינת כוח האדם, שלא השתנתה מאז שנת 2006, אינה מאפשרת טיפול הולם בפשיעת סייבר. באפריל 2009 הנחה ראש אג"ת דאז כי היחידה הארצית תתוגבר בשני שלבים. סוכם שהתקציב שיופנה לתגבור היחידה יסתכם ב-145 מיליוני ש"ח.

נמצא כי למרות עבודת המטה ולמרות הנחיית ראש אג"ת להגדיל במידה רבה את כוח האדם ביחידה הארצית, בשנים 2010-2009 לא נעשה שינוי של ממש במערך כוח האדם של היחידה הארצית.

3. במרץ 2011 הוצגו עקרונות עבודת המטה משנת 2009 שנערכה באח"ם לבכירי המשרד לבט"פ ולפיקוד המשטרה - אח"ם ואג"ת - ולפיהם תגדל היחידה הארצית בשני שלבים שכוללים בצדם תקציבים לצרכים טכנולוגיים, אמצעים יחידתיים וכלי רכב, ותכלול יחידות חקירה לצד גוף מטה שיעסוק בהנחיה מקצועית, בפיקוח, בהדרכה ובתכלול ידע.

4. **מסמך המדיניות משנת 2012:** במסמך מדיניות בנושא "המאבק בפשיעה במרחב הקיברנטי" של המשרד לבט"פ מיוני 2012 צוין, כי במשטרה טרם פותח מענה הולם לפשיעת סייבר, וכי היכולות הקיימות בתחום האכיפה של פשיעת סייבר הן "דלות ביותר", "זניחות" ו"מוגבלות מאוד". כן צוין כי המערך במשטרה אינו מפותח בכל הקשור לממד החדשנות הטומנת בחובה פשיעת סייבר, וכי בידי המשטרה אין את הידע המקצועי-טכנולוגי להתמודדות עם פשיעה מסוג זה.

המלצות מסמך המדיניות הדגישו במיוחד הן את הצורך לבנות "יכולת לנהל פרשיות חקירה מורכבות", והן את הצורך להגדיל במידה רבה את מספר החוקרים המקצועיים שעוסקים בפשיעת סייבר ולאייש את המערכים בחוקרים בעלי הכשרה אקדמאית ומקצועית רלוונטית. כמו כן התייחסו ההמלצות לצורך בחיזוק יכולות המשטרה להפיק ראיות דיגיטליות ממחשבים. ההמלצות קבעו כי "קיימת חשיבות קריטית למימוש המהלך להקמת יחידה גדולה ומקצועית יותר". המשרד לבט"פ הדגיש כי לנוכח אתגרי פשיעת הסייבר, תידרש הרחבה נוספת של המערך ב"תוך מספר שנים לא גדול". ההמלצות נכללו כחלק מיעדי המשרד לבט"פ לשנים 2013-2012.

5. **תכנית 2013:** בדיון שהתקיים בנובמבר 2012 במשרד לבט"פ בנושא "הקמת יחידה ללחימה בפשיעת סייבר" הוחלט על תכנית אופרטיבית לשנת 2013 שתכלול הקמת יחידה ארצית לחקירת פשעי סייבר וחיזוק יחידות ההונאה

במחוזות. תכנית זו הוגדרה "שלב ראשון בתכנית ארוכת טווח... שבסופה הן היחידה הארצית והן המחלקים במחוזות יחוזקו", זאת בשל היעדר מקורות למימוש התכנית המלאה משנת 2009.

כפועל יוצא, ביוני 2013 פרסם אג"ת את התכנית ל"הקמת המערך למאבק בפשיעת סייבר", שתהווה "קפיצת מדרגה" ותאפשר "לרכז את פעולות המשטרה בתחום הסייבר... מתוך שאיפה להיות צעד אחד לפני הפשיעה המתפתחת במרחב הסייבר". בחודש אוגוסט 2013 קיבלה התכנית אישור ארגוני מהמשרד לבט"פ.

אף שהצרכים הנדרשים להתמודדות עם פשיעת סייבר היו ידועים והועלו שוב ושוב, פעולות המשטרה והמשרד במהלך השנים מימשו רק חלק קטן מהתכנית המלאה להתמודדות עם התעצמות אתגרי הפשיעה בתחום זה

משרד מבקר המדינה מעיר למשרד לבט"פ ולמשטרה, כי אף שהצרכים הנדרשים להתמודדות עם פשיעת סייבר היו ידועים והועלו שוב ושוב במהלך עשר שנים מאז 2006, פעולות המשטרה והמשרד במהלך השנים מימשו רק חלק קטן מהתכנית המלאה להתמודדות עם התעצמות אתגרי הפשיעה בתחום זה.

במהלך השנים הללו נעשו בדיקות ועבודת מטה, גובשו המלצות ואושרו תכניות היערכות שכולן הצביעו על צורך ברור ומובהק להגדיל באורח ניכר את מספר התקנים ביחידה הארצית, ולאייש בשוטרים בעלי הכשרה מקצועית רלוונטית. למרות זאת נמצא כי רק בשנת 2016 היה התקן של היחידה הארצית בסדר גודל שלפי המלצת המשטרה היה אמור להיות כבר בשנת 2010 (השלב הראשון של התכנית המלאה). יצוין כי גם תקן זה הוא כשליש בלבד מהיקף כוח האדם הדרוש על פי המלצות המשטרה והמשרד לבט"פ בעבר.

בתשובת המשטרה למשרד מבקר המדינה מדצמבר 2016 (להלן - תשובת המשטרה) ציינה המשטרה כי תכנית 2013 מומשה בחלקה הן על ידי הקצאת משאבים חיצוניים ייעודיים למטרה זו והן באמצעות הקצאת משאבים ממקורות משטרתיים. לדברי המשטרה היא והמשרד לבט"פ פועלים להעלאת מודעותם של הגופים המתקצבים לצורך בהקצאת משאבים נוספים למערך הסייבר. בתשובתה הנוספת למשרד מבקר המדינה מפברואר 2017 (להלן - התשובה הנוספת) ציינה המשטרה כי עם זאת, אין לתלות את המענה לאיומי הסייבר רק בכמות כוח האדם הקיימת בפועל ביחידה הארצית, וכי אחריות המשטרה בתחום זה ממומשת גם באמצעות מערכים אחרים שלהם זיקה ישירה ועקיפה למימוש אחריות המשטרה בתחום הסייבר, ובהם מערך לאיסוף מידע במרחב הסייבר ומערך המאו"ר[25], שנועד לטפל בהיבטים של אלימות ופשיעה נגד ילדים ובני נוער ברשתות החברתיות. המשטרה הוסיפה כי כמו כן ייפרסו בתחנות המשטרה אמצעים טכנולוגיים להפקת ראיות דיגיטליות[26].

אגף התקציבים במשרד האוצר מסר בתשובתו למשרד מבקר המדינה מנובמבר 2016 כי הוא אינו מתנגד לתגבור יחידת הסייבר ומייחס חשיבות לטיפול בנושא במסגרת המשאבים הקיימים והעתידיים. לדבריו, במהלך דיוני התקציב קובעים המשרד לבט"פ והמשטרה את סדרי העדיפויות, ולפיהם מוקצה תקציב המדינה.

25 החלטות ממשלה מס' 1006 (17.1.16) ומס' 1972 (27.9.16).

26 ראו להלן בפרק "חוליית מטה - שיתוף בידע".

ואולם, נושא תקני כוח אדם למערך הסייבר לא נידון במהלך דיוני התקציב לשנים 2016-2015 ו-2017-2018.

משרד מבקר המדינה מעיר למשטרה כי מאחר שהיא סבורה שיש צורך בהקצאת משאבים נוספים למערך הסייבר, אך לטענתה הדבר נמנע ממנה בשל היעדר מקורות תקציביים, מחובתה להעלות נושא זה בדיוני התקציב הנערכים בשיתוף המשרד לבט"פ ומשרד האוצר. במסגרת זו עליה להציג גם את המשמעויות ואת ההשלכות הנובעות מהקצאות תקציב חסרות לתחום זה, כדי שאפשר יהיה לבחון את הצורך בחיזוק מערך הסייבר בהשוואה לצרכים אחרים של המשטרה.

עוד מעיר משרד מבקר המדינה כי בצד הפעולות שפירטה המשטרה בתשובתה הנוספת, עליה לתת מענה גם לפשיעת סייבר מתוחכמת העושה שימוש בטכנולוגיות מתקדמות ומגוונות שמשתנות במהירות רבה. מענה כזה מחייב כוח אדם מיומן וייעודי שיעסוק בכך, נוסף על המערכים המשלימים, שלא נועדו לטפל בפשיעת סייבר מתוחכמת טכנולוגית.

פיצול היכולות בתחום פשיעת הסייבר מבטל יתרונות רבים בהתמודדות יעילה עם פשיעת סייבר, הטמונים בקיומה של יחידה מרכזית גדולה וחזקה

מבנה מערך הסייבר

ממחקרים, מדוחות ומדיונים שעוסקים בהקמת מערכים משטרתיים עולה כי יש צורך מובהק בקיומה של יחידת פיקוד מרכזית שתהיה בעלת היכולות המקצועיות להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית וכן תשמש מוקד ידע, תיאום, ייעוץ והכוונה לכלל המשטרה בנושאי פשיעת סייבר. להלן דוגמאות:

1. במחקר של ארגון ה-NEIA[27] מפברואר 2012, שדן בחקירת פשעי סייבר ופשעי טכנולוגיה, צוינה החשיבות בדבר יחידה מרכזית שתפתח גישה אחודה להתמודדות עם פשיעת סייבר. הצורך ביחידה מרכזית גובר במיוחד לנוכח המעבר של פשיעת סייבר לפשיעה מתוחכמת טכנולוגית ולנוכח העובדה שפעמים רבות נדרשת התמודדות עם ראיות דיגיטליות מורכבות. לפי המחקר, טיפול מיטבי בפשיעת סייבר מתוחכמת טכנולוגית חייב להיות תחת יחידה מרכזית, כדי ליצור תיאום מירבי במערך שיביא לטיפול אחיד.

2. ממחקר שפרסמה בשנת 2014 מחלקת אסטרטגיה באג"ת[28] עולה כי פיצול היכולות בתחום פשיעת הסייבר מבטל יתרונות רבים בהתמודדות יעילה עם פשיעת סייבר, הטמונים בקיומה של יחידה מרכזית גדולה וחזקה. לפי המחקר ריכוז משאבים

27 National Executive Institute Associates (www.neiassociates.org/cybercrime-and-technology).

28 "יחידות סייבר ייעודיות בארגוני משטרה: סקירת מודלים ארגוניים ופרקטיקות מיטביות", **העיקר במחקר** (2013-2012). המחקר סקר מודלים ארגוניים ופרקטיקות מיטביות של יחידות סייבר משטרתיות, בהסתמכו בין היתר על עבודות מחקר של האיחוד האירופי שבחן 18 יחידות סייבר משטרתיות במדינות שונות באירופה (IPA, 2011), מחקר שנעשה באו"ם (UNAFEI, 2009), וכן על בחינת הפרקטיקות המומלצות של האף.בי.איי ושל משטרת דרום קוריאה.

מאפשר להתמודד באופן אפקטיבי יותר עם פשיעת סייבר רחבת היקף, לנוכח היותה פשיעה ברמה טכנית גבוהה וחוצת גבולות. כן צוין במחקר כי יחידה מרכזית אחת מביאה לידי תיאום טוב יותר בין כלל הגופים המעורבים בחקירות פשעי סייבר ולריכוז משאבים באופן שימנע כפילויות בחקירות, שכן עבריין סייבר יכול לתקוף בו בזמן כמה נקודות בכל רחבי המדינה.

3. בדוח ביקורת שהכין משרד המשפטים האמריקני על מערך האף.בי.איי לטיפול בפשיעת סייבר מיולי 2015[29], צוינה החשיבות בדבר יצירת מערך מרכזי מאוחד שיכלול את כלל כוח האדם המיועד להתמודדות ולטיפול באירועים במרחב הסייבר, כדי שיוכל לתאם ולתזמן את פעילותם של חוקרי המערך. צורך זה התעורר ביתר שאת בעקבות העובדה שאותן עבירות סייבר דווחו ליחידות שונות ברמה הארצית וברמה המקומית בארצות הברית[30]. מציאות זו פגעה הן ביכולת לטפל באירוע בצורה אחודה והן בתכלול הידע בתחום בין כל הכוחות הפועלים במרחב זה.

4. בדיון שנערך בינואר 2015, בהשתתפות פיקוד אח"ם ואג"ת, ציין סגן ראש אח"ם דאז כי "אופיין של העבירות בעולם הקיברנטי והאתגרים הטכנולוגיים **מחייבים איחוד כוחות ויכולות ברמה הארצית, על מנת להביא לשיפור יכולות האכיפה בתחום**" (ההדגשה אינה במקור).

במרץ 2015 הקים פיקוד אח"ם צוות עבודה לכתיבת תפיסת הפעלה של מערך הסייבר. ביוני 2015 הציגה חטיבת החקירות באח"ם את תפיסת ההפעלה בפני פיקוד אח"ם ואג"ת. לפי תפיסת ההפעלה, שבעקבותיה נקבע נוהל בנושא "הפעלת המערך לחקירת עבירות בסייבר, עבירות מחשב ומיצוי ראיות ממחשב" מחודש יוני 2015 (להלן - תפיסת ההפעלה), ובניגוד לעמדה המקצועית שהוצגה המלמדת על הצורך ביחידה מרכזית, הוחלט כי הטיפול בפשיעת סייבר יפוצל בין שלושה גופים, כדלהלן:

1. **חוליית סייבר:** תשמש יחידת מטה באח"ם בכפוף לראש חטיבת החקירות (להלן - חוליית המטה), ותבצע את התפקידים האלה: (א) תיאום פעילות היחידות החוקרות; (ב) הנחיה מקצועית וריכוז הדרכות והכשרות ליחידות החוקרות ולחוקרים המיומנים; (ג) פיקוח ובקרה על ניהול תיקי חקירה; (ד) איסוף מידע שוטף בהיבט הארצי והעולמי; (ה) רכישת ציוד מיוחד לטובת המערך.

2. **יחידה ארצית:** תרכז את פעולות המשטרה בתחום הסייבר, תהיה כפופה פיקודית למפקד יחידת להב 433 ותעסוק בתחומים האלה: (א) חקירת עבירות ברמה הארצית ועבירות חמורות ומורכבות ("עבירות מחשב איכותיות"), וכן עבירות המעוררות עניין ציבורי רב, עבירות בעלות היבטים ביטחוניים ועבירות הדורשות שיתוף פעולה עם גורמי חקירה בחו"ל; (ב) קבלת אחריות על הנחייתן המקצועית של יחידות חקירה אחרות במערך וסיוע לחוליית המטה בכל הקשור

29 **Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative** (July 2015) (להלן - דוח הביקורת על מערך האף.בי.איי).

30 כך לדוגמה תוכנה זדונית, שהדיווחים על אודות נזקיה התבטאו בתלונות הן לכוחות אכיפת חוק מדינתיים והן לכוחות מקומיים, בלי שהיה גורם מתכלל.

להדרכה ולהכשרה, ובכלל זה הכנת "קורס חוקר מיומן בסיסי" וקורס "חוקר מיומן מתקדם"; (ג) אחריות לכשירות החוקרים המיומנים, יצירת קשרים בין-לאומיים ואיסוף מודיעיני; (ד) הקמת מערך מחקר ופיתוח שיעניק פתרונות טכנולוגיים מתקדמים ליחידות החוקרות; (ה) מיצוי הראיות הדיגיטליות ממחשבים עבור יחידות החקירה בלהב 433, באמצעות הקמת מֶחְלק מיוחד בנושא.

3. **מערך חוקרי פשיעת סייבר במחוזות:**

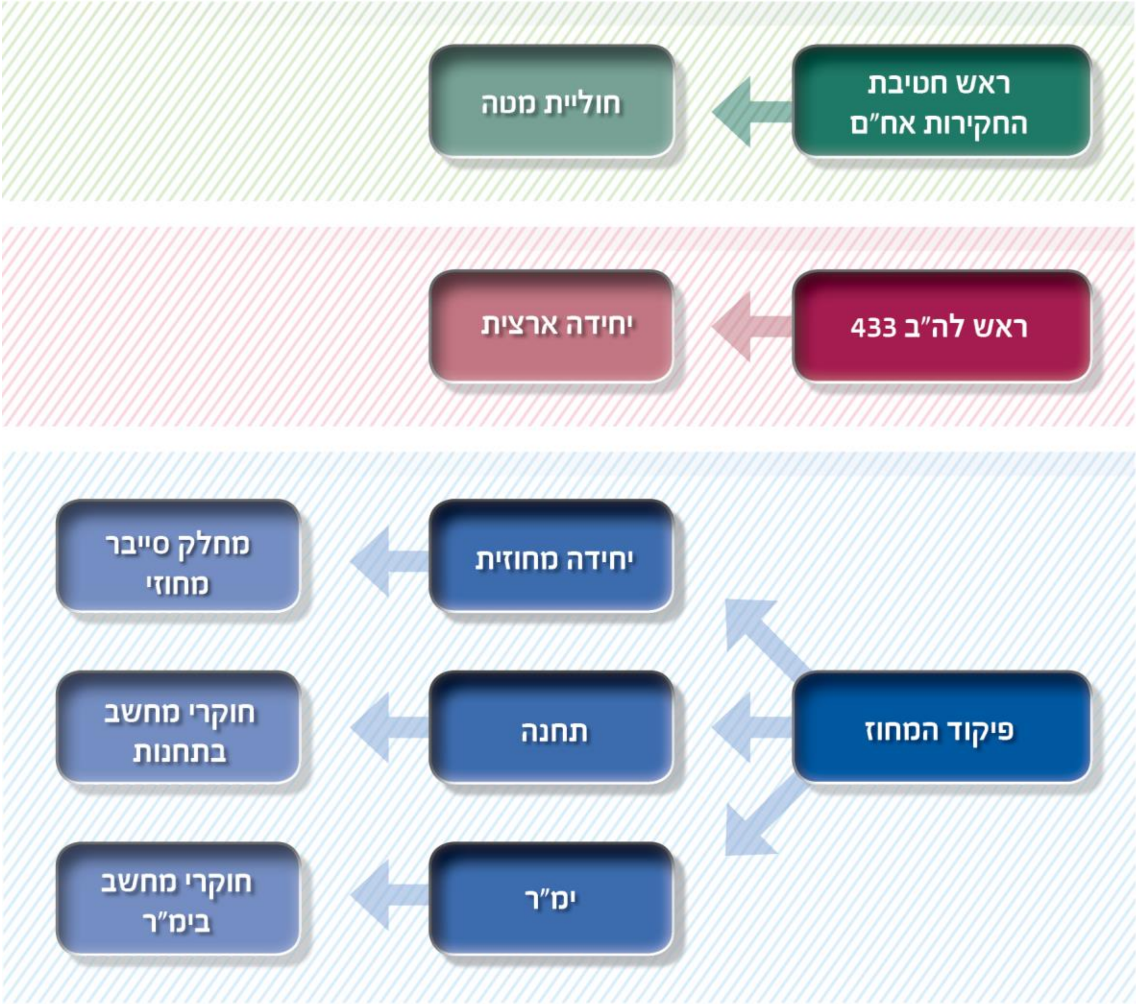
א. **יחידות סייבר מחוזיות:** יהיו כפופות למפקדי יחידות מחוזיות[31] (להלן - מחלקי סייבר). המחלקים יחקרו באופן בלעדי עבירות סייבר מתוחכמות שאירעו בתחומי המחוז שאליו הם כפופים פיקודית או תיקים שהיחידה הארצית העבירה אליהם "כאשר מקום ביצוע העבירה אותר במחוז". מחלקי הסייבר במחוזות יסייעו ליחידות החקירה האחרות במחוז לטפל בעבירות "קלאסיות" שבוצעו בתחומי המחוז, ובכלל זה הפקת ראיות דיגיטליות.

ב. **חוקרים שתפקידם להפיק ראיות דיגיטליות:** יהיו כפופים למפקדי התחנות או למפקדי היחידות המרכזיות במחוזות (להלן - ימ"ר) ותפקידם לסייע בכל הקשור להפקת ראיות דיגיטליות במסגרת טיפול המחוז בכלל תיקי החקירה.

בתרשים להלן מבנה מערך הסייבר שנגזר מתפיסת ההפעלה המפוצל לשלושה מערכים נפרדים:

31 במועד הביקורת מחלקי הסייבר המחוזיים היו כפופים ליחידות ההונאה המחוזיות.

תרשים 3: **מבנה מערך הסייבר וכפיפות היחידות**



מקור: נתוני המשטרה בעיבוד משרד מבקר המדינה.

ההמלצות שהובאו במחקרים בארץ ובעולם כאמור מייחסות חשיבות לכך שמערך הסייבר שעוסק בהתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית יהיה ריכוזי (centralized) ויכלול יחידה מרכזית שתרכז את כלל הפעילות בתחום זה, ואליה יהיו כפופים, פיקודית ומקצועית, כל מחלקי הסייבר המחוזיים. זאת לצד, חוקרי הסייבר הפרוסים בתחנות ובימ"רים שמתמודדים עם פשיעת סייבר שאינה מתוחכמת טכנולוגית ואשר זקוק ליכולות רלוונטיות.

ואולם, בניגוד להמלצות הללו ולעמדה שהביע סגן ראש אח"ם בינואר 2015, מבנה המערך שייעודו התמודדות עם פשיעת סייבר מתוחכמת טכנולוגית מבוזר (de-centralized) לכפיפויות פיקודיות שונות ואינו בעל מוטת שליטה מרכזית: היחידה הארצית פועלת בכפוף לפיקוד להב 433, וחוקרי מחלקי הסייבר כפופים כל אחד לפיקוד המחוז שבו הוא פועל, ועקב כך היחידה הארצית ומחלקי הסייבר עסקו בהתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית כל אחד בנפרד, באופן מבוזר שאינו אפקטיבי, כפי שיפורט להלן.

גם לאחר הקמת המערך הייתה מחלוקת לגבי יעילות מבנה המערך המפוצל שאימצה המשטרה ובעניין התאמתו להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית:

בדיון מיוני 2015, בנושא "תפיסת ההפעלה של מחלקי הסייבר במחוזות ושל היחידה הארצית", טען ראש חטיבת החקירות באח"ם דאז כי היחידה הארצית צריכה להיות בעלת מוטת שליטה - הן פיקודית והן מקצועית - על מחלקי הסייבר, וכי יהיה צורך לשנות את תפיסת ההפעלה שהוצגה. באוגוסט 2015 ציין ראש להב 433 בפני ראש אח"ם ש"כדי ליצר מדיניות וטיפול אחידים" יש להכפיף את מחלקי הסייבר ליחידה הארצית.

בסיכום ביקורת שערך אג"ת בנושא "היחידה הארצית לחקירת עבירות הסייבר בלהב 433" מאוגוסט 2015 נכתב כי למשטרה "אין עמדה חד-משמעית ברורה לגבי המבנה הרצוי של היחידה כיחידה ארצית אחת או ככזאת הכוללת גם שלוחות מחוזיות". בהמלצות דוח הביקורת נכתב כי יש "לבחון את מבנה היחידה לאור הצרכים שעלו מאז הקמתה".

המשטרה מסרה בתשובתה כי מבנה המערך הקיים נידון פעמים רבות, אך פריסתו נעשתה "בכפוף למבנים ארגונים [שהיו] קיימים" בשטח. לדבריה נושא הסייבר הוא תחום מתפתח, והיה ברור כי המערך יחייב מגוון שינויים והתאמות בתדירות גבוהה יחסית הן במבנה היחידה והן בשיטות ההפעלה. בתשובתה הנוספת מסרה המשטרה כי בשנה האחרונה היא פועלת למימוש תפיסת הפעלה מערכתית כוללת שאושרה על ידי פיקוד משטרת ישראל (להלן - תפיסת ההפעלה החדשה). במסגרת זו הוחלט, בתחילת שנת 2017, על הקמת מטה סייבר וטכנולוגיה כגוף מטה מקצועי שיהיה אחראי על בניין הכוח ועל התעצמות המערך על פי כמה עקרונות מנחים שנקבעו. לדברי המשטרה, אף שלמערך ריכוזי יש יתרונות, הוחלט בעקבות עבודת מטה שנעשתה ואימוץ תפיסת ההפעלה החדשה לחלק את האחריות והסמכות בטיפול בפשיעת סייבר באמצעות קביעת מדרגי הפעלה ויצירת הפרדה בין בניין הכוח לבין הפעלתו. זאת, תוך שמירה על הנחיה "ריכוזית" על ידי גורם מוביל במטה הסייבר, ותוך כדי השארת הטיפול בתחומי המחוז לאירועי סייבר במדרגי העבודה המחוזיים.

הלכה למעשה בפברואר 2017 עדיין לא הוחלה תפיסת ההפעלה החדשה, ומבנה המערך והפיצול בין יחידותיו שיקף אפוא את אותן כפיפויות פיקודיות עליהן הוחלט עוד בשנת 2000, ללא התאמה כמתחייב מן ההתפתחויות הטכנולוגיות ומהידע המקצועי המעודכן להתמודדות אפקטיבית עם פשיעת סייבר.

על המשטרה ועל המשרד לבט"פ לבחון את העוגנים המקצועיים המקובלים בעולם שנידונו בספרות המקצועית ונתמכות גם בפרקטיקות מקובלות[32] בכל הנוגע למבנה רצוי של יחידה אשר מתמודדת במובחן בפשיעת סייבר מתוחכמת טכנולוגית, ובד בבד עם הטיפול בעבירות קלאסיות המסתייעות במרחב הסייבר אולם אינן בגדר פשיעה כזאת.

הסטת עבודת מחלקי הסייבר לצורכי המחוז

כאמור, לפי מבנה המערך, מחלקי הסייבר כפופים מן הבחינה הפיקודית למחוזות, ומן הבחינה המקצועית לחוליית המטה. תפיסת ההפעלה קבעה כי החוקרים במחלקי הסייבר יעניקו סיוע טכני לחוקרים בתחנות ובימ"רים שאליו הם כפופים בטיפול במדיות דיגיטליות הקשורות לפשיעה "קלאסית" כמו: טלפון חכם, טאבלטים, מחשבים ודיסקים קשיחים, כרטיסי זיכרון וכרטיסי סים ומצלמות, ויפיקו מהם ראיות דיגיטליות לצורכי חקירה כמו תמונות, סרטונים, הודעות ותכתובות. יצוין כי פעולות אלה נעשות כסיוע לחקירת כלל תיקי המחוז, ואינן נעשות רק במסגרת חקירת תיקי פשיעת הסייבר.

בסיכום דיון מיוני 2015 בנושא "תפיסת ההפעלה של מחלקי הסייבר במחוזות" קבע סגן ראש אח"ם דאז שהחוקרים המיומנים במחוזות יעסקו בתחום הראיות הדיגיטליות של המחוז, והחוקרים המיומנים במחלקי הסייבר יטפלו "**בעבירות מורכבות מתחום העבירות בסביבה הרשתית** [סייבר]". כמו כן קבע כי "**סיוע [של המחלקים] למחוז במיצוי ראיות צריך להיות בשוליים**" (ההדגשות אינן במקור). לדבריו, באחריות מחלקי הסייבר להגדיר את גבולות הפעילות.

בדיקת משרד מבקר המדינה העלתה כי רובה המוחלט של עבודת מחלקי הסייבר במחוזות, מתמקדת בהפקת ראיות דיגיטליות (מיצוי) הנדרשות בחקירות תיקים שאינם פשיעת סייבר ונמצאים בטיפול התחנות ובטיפולן של היחידות המחוזיות שאליהן כפופים מחלקי הסייבר.

32 כך לדוגמה יחידת הסייבר בפרקליטות המדינה כוללת מערך אופרטיבי בצד מערך מטה תחת ניהול (פיקוד) אחד, כך שיתאפשר "טיפול הוליסטי באתגרי האכיפה הפלילית בזירת הסייבר". מבנה זה גובש לאחר התייעצות עם נציגי מטה הסייבר הלאומי במשרד ראש הממשלה.

הרוב המוחלט של תשומות פעילות חוקרי מחלקי הסייבר במחוזות לא הופנו לחקירת עבירות סייבר מתוחכמות טכנולוגית, אלא הכוונו על ידי פיקוד המחוז לסייע לצוותי חקירה אחרים לטיפול בראיות דיגיטליות, בעבירות "קלאסיות"

הבדיקה העלתה שבמחצית הראשונה של שנת 2016 הרוב המוחלט של תשומות פעילות חוקרי מחלקי הסייבר במחוזות לא הופנו לחקירת עבירות סייבר מתוחכמות טכנולוגית, אלא הוכוונו על ידי פיקוד המחוז לסייע לצוותי חקירה אחרים לטיפול בראיות דיגיטליות, בעבירות "קלאסיות", בניגוד להנחיית סגן ראש אח"ם מיוני 2015.

עוד עולה כי נכון למועד הביקורת, שיעור הטיפול בראיות דיגיטלית בתיקי חקירה של היחידות המחוזיות שאליהן כפופים מחלקי הסייבר (ההונאה) הוא גדול פי 4 משיעור הטיפול בראיות דיגיטליות בתיקי חקירה של מחלקי הסייבר. בולטים במיוחד שני מחוזות שבאחד מהם נבדקו פי 17.7 ראיות דיגיטליות בתיקי חקירה של יחידת ההונאה לעומת תיקי מחלק הסייבר, ובאחר נבדקו פי 6.6 ראיות דיגיטליות בתיקי הונאה לעומת תיקי סייבר.

מפקד מחלק סייבר באחד המחוזות ציין בדיון ממרץ 2015 כי המחלק מוסט על ידי המחוז "למשימות בתעדוף המחוז שאינו נוגע תמיד לתפקידי היחידה. זהו בזבוז משאבים". בדיון באותו החודש ציין סגן ראש אח"ם דאז כי "יתכן כי היה נכון להקים יחידה ארצית גדולה וחזקה ולא להפנות משאבים למחוזות... הניסיון מוכיח כי בשל מחסור במשאבים במחוזות קיים סיכון כי משאבים אלה יופנו למשימות אחרות".

במאי 2015 ציין מפקד מחלק סייבר באחד המחוזות כי "כדאי לשקול הוצאת חוליית סייבר מתוך מחלקי הונאה מחוזיים... זאת כדי למנוע הסטה של חוקרי סייבר לטיפול בתיקי הונאה". במסגרת הדיונים בדבר תפיסת ההפעלה של המערך במרץ וביוני 2015 התבטאו מפקדים במחלקי סייבר במחוזות בדיונים כי עבודתם העיקרית היא סיוע בתחום הפקת ראיות דיגיטליות למחוזות. נציגת אג"ת ציינה כי נושא מיצוי הראיות עבור המחוזות הוא "פער מרכזי שעולה מרמת השטח".

משרד מבקר המדינה מעיר למשטרה כי השלכות המבנה המפוצל של מערך הסייבר והכפיפות הפיקודית הישירה של מחלקי הסייבר ליחידות המחוזיות, הביאו לכך שרובה המכריע של עבודת המחלקים מוסטת למתן סיוע טכני למחוזות, ולא כפי שהנחה סגן ראש אח"ם שסיוע זה יהיה "בשוליים". התנהלות זו מגבילה את יכולתם של מחלקי הסייבר להקצות את משאביהם לטובת טיפול בתיקי פשיעת סייבר מורכבת שבתחומי אחריותם, ופוגעת במקצועיותם ובמיומנותם לטיפול בתיקים האלה.

בתשובתה מסרה המשטרה כי תיאור העובדות בדוח נכון, ואולם הסטת המחלקים לעבודות סיוע למחוזות לא נבעה בשל כפיפות המחלקים למחוז, אלא בשל היעדר אמצעים ייעודיים במחוזות לטיפול בראיות דיגיטליות. לדבריה, פיקוד אח"ם היה מודע לתופעה זו ופעל להרחיב את יכולותיהם של המחוזות לטפל במיצוי הראיות שבתחומם באופן שעתיד לצמצם במידה רבה את היקפי הסיוע של מחלקי הסייבר למחוזות עד סוף שנת 2017, ויאפשר למחלקי הסייבר להתפנות לטיפול בעבירות הסייבר שהן ייעודם העיקרי[33]. בתשובתה הנוספת מסרה המשטרה כי בעקבות עבודת

33 ראו להלן בפרק "חוליית המטה - הנחיה מקצועית, פיקוח ובקרה".

מטה שנעשתה ותפיסת ההפעלה החדשה ימוקמו מחלקי הסייבר ביחידה המרכזית בכל מחוז, וכי הכלים הטכנולוגיים המשמשים להפקת ראיות דיגיטליות יחולקו ליחידות במערך לפי תחומי האחריות והסמכות שלהן. עוד מסרה המשטרה כי תפיסת ההפעלה החדשה, שתבוא לידי ביטוי בתכנית דו-שנתית שלה, תיתן מענה מיטבי לסוגיית פיצולן של היחידות ולצורך בהגדרת האחריות של כל יחידה בהתמודדות עם פשיעת סייבר הרלוונטית לעיסוקם.

עולה החשש כי בשל מיקום מחלקי הסייבר במחוזות והכפפתם ליחידות המרכזיות במחוזות, לא יינתן מענה מספק לפשיעת סייבר מתוחכמת טכנולוגית

מתשובות המשטרה עולה כי המשטרה אמנם הייתה ערה לצורך של התחנות לטפל בעצמן בהפקת ראיות, אולם היא לא פתרה את הבעיה שבכפיפותם של מחלקי הסייבר ליחידות המחוזיות; כפיפות זו הביאה לכך שעבודת המחלקים מתמקדת בטיפול בצרכים השוטפים של היחידות המחוזיות שלהן הם כפופים, כלומר בעבירות פליליות "קלאסיות", במקום להתמקד בייעודם המקורי - טיפול בפשיעת סייבר מתוחכמת טכנולוגית. עקב אי-פתרון בעיה זו, תתקַבֵּע התופעה שלפיה ימשיכו מחלקי הסייבר להישאב לטיפול בתיקי המחוז בשל כפיפותם ליחידות המחוזיות, בניגוד לייעודם המקורי - עיסוק בפשיעת הסייבר המתוחכמת. כמו כן עולה החשש כי בשל מיקום מחלקי הסייבר במחוזות והכפפתם ליחידות המרכזיות במחוזות, לא יינתן מענה מספק לפשיעת סייבר מתוחכמת טכנולוגית.

על המשטרה ועל המשרד לבט"פ לבחון בדחיפות את התאמת מבנה מערך הסייבר להתפתחויות הטכנולוגיות בתחום, באופן שיעלה בקנה אחד עם הידע המקצועי והתפיסות שאומצו לאורו בעולם, התומכים ביחידה מרכזית שאליה כפופים גופי המטה והיחידות החוקרות, זאת גם אם המשטרה הצהירה על כוונתה לממש תפיסת הפעלה חדשה. יתר על כן, אם המשטרה רואה צורך בהוספת חוקרים שיעסקו בהפקת ראיות דיגיטליות במחוזות בעבירות "קלאסיות" או בחקירת עבירות קלאסיות שמסתייעות במרחב הסייבר המטופלות על ידי המחוזות, עליה לוודא שהדבר אינו יבוא על חשבון התמקצעותם של חוקרי המחלקים שייעודם הוא עבירות סייבר מורכבות טכנולוגית.

טיפול בתיקי חקירה בהתאם לשיוך גאוגרפי

נוהל המשטרה "הטיפול בתיקי חקירה בעבירות משותפות למספר יחידות" (משנת 2014), קובע כי בעבירות מחשב תתנהל החקירה בהתאם לנסיבות האלה: מקום גאוגרפי של ביצוע העבירה, מקום גאוגרפי שבו התקבלו התלונות הרבות ביותר, מקום מגוריו של החשוד, מיקומו הגאוגרפי של המחשב שבאמצעותו בוצעה העבירה, מקום מגוריהם של הנפגעים וכדומה. לפי תפיסת ההפעלה, כאשר מדובר בעבירה שאירעה בגבולות מחוז מסוים, יחקור אותה מחלק הסייבר שבאותו מחוז "באופן בלעדי". רק במקרים שבהם מדובר בעבירה שהיא חוצת גבולות יעבור התיק לטיפול היחידה הארצית.

המחקרים בתחום פשיעת הסייבר תומכים בגישה, ולפיה מאפיין המיקום הפיזי מאבד מחשיבותו ואינו מתאים לטיפול בפשיעה מסוג זה[34], מפני שאי-אפשר להבחין בין פשיעת הסייבר שנעשית במרחב גאוגרפי מסוים לבין מרחב גאוגרפי אחר, כיוון שמדובר בפשיעה המהווה מרחב נפרד בפני עצמה. פשיעת הסייבר אינה מוגבלת בהיקפה, והיא בעלת פוטנציאל לשכפל את עצמה ללא התערבות יד אדם[35]. פשיעת הסייבר יכולה להתבצע מכל מקום, בין השאר, בגלל טכנולוגיית קישוריות מרובה (כגון: Wi-fi) שזמינה בהיקף נרחב[36]. גם ממד האנונימיות אינו מאפשר לאפיין אזור גאוגרפי מסוים שממנו בוצעה העבירה. מדובר אפוא באירוע כלל-ארצי, ולרוב כלל-עולמי[37], שאינו ניתן לשיוך גאוגרפי.

בדיון שהתקיים במרץ 2015 ציין סגן ראש אח"ם דאז כי אין משמעות לחלוקה טריטוריאלית בפשיעת הסייבר. בהתייחסות אח"ם מפברואר 2016 צוין כי הפשיעה בעולם המודרני "**איננה נחתמת יותר על ידי גבולות טריטוריאליים אשר היטשטשו ללא היכר הודות לתופעת הגלובליזציה בכלל תחומי החיים**" (ההדגשה אינה במקור).

להלן דוגמאות לכתבי אישום, שהוגשו במהלך הביקורת, אשר משקפות את העובדה שפשיעת הסייבר חוצה אזורים גאוגרפיים, בשל העובדה שהעבירות בוצעו נגד קורבנות מכל רחבי הארץ:

1. ביוני 2016 הוגש כתב אישום נגד נאשם שנטען שפעל מכמה כתובות דוא"ל וחדר שלא כדין, תוך שימוש ברשת האינטרנט אל חשבונות בנק המוחזקים במחשבי הבנק בתל-אביב, בלוד ובמקומות נוספים. כן צוין כי הנאשם חדר לחשבונות של לקוחות בנקים שונים בישראל. בכתב האישום מפורטות עבירות נוספות שאין להן מיקום גאוגרפי מוגדר: חדירה וניסיון חדירה לאתרי אינטרנט במטרה להעתיק מידע; שליחת מסרונים כוזבים למספרי טלפון רבים של לקוחות בנקים שונים ברחבי ישראל כדי לדלות את פרטיהם האישיים ולהתחבר לחשבון הבנק שלהם באמצעות האינטרנט. באמצעות שיטה זו נטען כי הנאשם חדר לחשבונות בנק ללא הרשאה.

2. ביולי 2016 הוגש כתב אישום נוסף נגד נאשם אחר, ובו נטען כי הנאשם חדר באלפי הזדמנויות שונות, לחשבונות דואר אלקטרוני אישיים, ולחשבונות לשירותי 'ענן' שונים לאחסון וגיבוי קבצי מחשב של מעל 350 נשים ישראליות שונות. כן נטען בכתב האישום כי אותו נאשם ניסה לחדור לחשבונות נוספים בעוד מאות מקרים ברחבי ישראל.

34 ראו:
Susan W. Brenner, “Law, Dissonance, and Remote Computer Searches”, **North Carolina J. of Law & Technology** 14 (1) 43 (2012).

35 ראו:
Cameron S. D. Brown, “Investigation and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice”, **Inter. J. of Cyber Criminology** 9 (January-June 2015), pp. 58-62.

36 ראו מחקר סוכנות האו"ם לסמים ופשיעה.

37 באפריל 2016 חתמה ישראל על "אמנת בודפשט" (Convention on Cybercrime), המסייעת בין היתר, לכונן שיתוף פעולה בין גורמי אכיפת חוק ממדינות שונות כדי להתמודד ביעילות עם ההיבט הבין-לאומי של פשיעת סייבר.

למרות התובנות האמורות שהועלו במשטרה בשנים האחרונות וחרף העובדה שתובנות אלו נתמכות במאפייני הפשיעה המתבטאים בכתבי אישום שהוגשו לבית המשפט, תפיסת ההפעלה נותרה מבוססת על העיקרון שלפיו השיוך הגאוגרפי יקבע את זהות הגוף שיטפל בעבירה.

להלן מקרים של תיקי פשיעת סייבר חוצי גבולות שהטיפול בהם נעשה על ידי מחלקי הסייבר במחוזות לפי שיוך גאוגרפי:

1. בנובמבר 2015 נפתח באחד המחוזות תיק שהחל כחקירה בתחום עבירות הסמים. במסגרת החיפוש בביתו של החשוד בוצע חיפוש גם במחשבו של החשוד, ונמצאו ראיות הנוגעות לפשיעת סייבר בתחום ההונאה. במסגרת החקירה נמצאו ראיות לכך שהחשוד הוא "האקר" שמפתח סוסים טרויאניים[38] מסוגים שונים. כמו כן נמצא כי יש מעורבים נוספים השותפים למעשי החשוד.

   רק כעבור כמה חודשי חקירה של מחלק הסייבר באותו מחוז נוצר קשר בין מחלק זה לבין היחידה הארצית, ונחשף כי באותה העת ממש חקרה היחידה הארצית חשדות לגבי חלק מהמעורבים באותה פרשה.

   משרד מבקר המדינה מעיר כי החקירה בתיק טופלה על ידי שלושה מחלקי סייבר ללא מעורבותה של היחידה הארצית. רק משנעשתה פנייה ליחידה הארצית בעניין סיוע טכני, מסרה היחידה הארצית מידע בעל חשיבות גבוהה ביותר, ולפיו מתנהלת גם חקירה בין-לאומית לגבי חלק מהחשודים. מידע זה לא יכול היה להימסר קודם לכן למחלקי הסייבר מפני שהיחידה הארצית לא יודעה מלכתחילה על התיק, ולא הייתה שותפה להליכי החקירה בתיק.

   עוד מסרה המשטרה בתשובתה כי אכן רוב תיקי הסייבר הם חוצי מחוזות (ואפילו מדינות), וכי העבירות במרחב הקיברנטי מעצם טיבן חוצות גבולות פיזיים. לכן אין לדעת בשלב הראשון מהו היקף העבירות וכיצד מתקשר התיק למחוז מסוים.

38 סוס טרויאני (Trojan Horse) הוא כינוי לתוכנה תמימה למראה המוחדרת למחשב הקורבן, מפעילה בו קוד זדוני לביצוע פעולות לא חוקיות, ומאפשרת איסוף מידע ממחשב הקורבן. ראו בנושא זה ויסמונסקי, עמ' 21.

> המשטרה עוסקת בחקירת עבירות סייבר מתוחכמות טכנולוגית במחוזות המחולקים לפי גבולות גאוגרפיים, אף שהיא מכירה בכך שקיים קושי מובהק לשייך פשיעת סייבר למיקום גאוגרפי. מצב זה מביא לידי כפילות בטיפול, לידי שימוש לא יעיל בכלים הטכנולוגיים הקיימים ולהיעדר שיתוף בידע לגבי היבטים בין-לאומיים

מתשובת המשטרה עולה שהמשטרה עדיין עוסקת בחקירת עבירות סייבר מתוחכמות טכנולוגית במחוזות המחולקים לפי גבולות גאוגרפיים, אף שהיא מכירה בכך שקיים קושי מובהק לשייך פשיעת סייבר למיקום גאוגרפי. כך נוצר מצב שבו לעתים יחידות שונות חוקרות אותה פרשה ללא תיאום בין היחידות החוקרות. מצב זה מביא לידי כפילות בטיפול ולידי שימוש לא יעיל בכלים הטכנולוגיים הקיימים במשטרה. על כך מתווספת לעתים התופעה של היעדר שיתוף בידע לגבי היבטים בין-לאומיים, שנדרש כבר בשלבים מוקדמים של החקירה. כמו כן עולה חשש לפגיעה אפשרית בחקירה בשל אי-ראיית התמונה המלאה, היות שיחידה חוקרת אחת אינה מודעת לעבודת היחידה האחרת.

2. במחלק הסייבר של אחד המחוזות התנהל בשנים 2015-2014 תיק חקירה חוצה מחוזות שכלל נפגעים מכל רחבי הארץ. מיקומו הגאוגרפי של החשוד לא היה ידוע, אך נמצא כי הוא פועל מכתובות דוא"ל שונות, וכן נתפסו ראיות לביצוע עשרות העברות כספים לבנקים שונים ברחבי אירופה. מחלק הסייבר של אותו מחוז , שבו הוגשה התלונה הראשונה, טען כי "ככל שחלף הזמן והתקבלו עוד תיקי חקירה מהמחוזות השונים, התקבלה תמונת מצב בה מדובר בתופעה כלל ארצית". ממסמך של חטיבת החקירות באח"ם מדצמבר 2015 עולה כי המחוז פנה לחטיבת החקירות וביקש להעביר את תיק החקירה ליחידת הסייבר הארצית, בין היתר, מאחר "שאין עדיפות למחוז שכן התיקים הינם מכל הארץ". למרות העובדה כי מדובר בתיק ברמה הארצית, ראש חטיבת חקירות באח"ם קבע בדצמבר 2015 כי התיק יטופל ברמה המחוזית על ידי מחלק הסייבר במחוז האמור.

3. נמצא כי בשנת 2015 התנהל מבצע נגד חשודים בפדופיליה במרחב הסייבר, שהתגוררו בכתובות שונות ברחבי הארץ, שחייב שיתוף פעולה חוצה מחוזות. אף שמבצע זה חייב שיתוף פעולה מצד יחידות שונות, נוהל המבצע על ידי מחלק סייבר באחד המחוזות, וחלק מהחשודים נחקרו לא על ידי חוקרי מחלק הסייבר בלבד אלא גם על ידי חוקרי ההונאה במחוז, שאינם מיומנים בחקירת עבירות סייבר. בדומה נבחנו הראיות הדיגיטליות של החשודים על ידי חוקרי מחלק הסייבר של אותו מחוז, ולא ניכר כי נעשו שיתוף פעולה, תכלול ידע או ליווי חקירתי וטכנולוגי עם היחידה הארצית, אף שדובר במבצע ברמה הארצית.

4. מבדיקה שנערכה במהלך הביקורת באחד המחוזות, נמצאו תיקים שונים בטיפול מחלק הסייבר במחוז שבהם החשודים בביצוע עבירות הסייבר מתגוררים באותו המחוז, אך הקורבנות מתגוררים ביישובים במחוזות אחרים. כמו כן נמצא כי נפתח תיק שבו החשודים מתגוררים מחוץ למחוז, אולם הקורבן הוא מתוך המחוז.

דוגמאות אלו משקפות מצב שבו עקב השיוך הגאוגרפי, תיקי פשיעת סייבר מתוחכמת טכנולוגית וחוצי מחוזות וגבולות פיזיים, לא טופלו על ידי היחידה הארצית ולא נבחנו בראייה מערכתית על ידי גורם פיקודי אחד. לפיכך לא הובטח שהוקצו למשימות יכולות טכנולוגיות מתאימות וכוח אדם המסוגל להתמודד עם חשודים בכמה מחוזות בו-זמנית וכי הייתה היערכות לוגיסטית נאותה לביצוען. מאפיין השיוך הגאוגרפי מהווה אפוא חסם לפעילות אפקטיבית של המשטרה.

יחד עם זאת יצוין, כי ניכר שבמחלקי הסייבר נעשו מאמצים רבים להשגת התוצאות המיטביות בתיקי החקירה שהונחו לפתחם.

עקב השיוך הגאוגרפי, תיקי פשיעת סייבר מתוחכמת טכנולוגית וחוצי מחוזות וגבולות פיזיים, לא טופלו על ידי היחידה הארצית ולא נבחנו בראייה מערכתית על ידי גורם פיקודי אחד. יחד עם זאת ניכר שבמחלקי הסייבר נעשו מאמצים רבים להשגת התוצאות המיטביות בתיקי החקירה שהונחו לפתחם

המשטרה מסרה בתשובתה שההחלטה איזו יחידה חוקרת תטפל בתיק מתקבלת לאחר שקילת שיקולים מקצועיים הנוגעים לפן המקצועי ולעומסים ביחידות; יחידות החקירות הן המחליטות "היכן טובת ניהול התיק". לדבריה, "המבנה הארגוני של מערך הסייבר כיום נותן מענה למאפייני התופעה בהיבטים של טריטוריה גאוגרפית", והמענה לפשיעת הסייבר חוצת הגבולות יינתן על ידי היחידה הארצית.

על המשטרה ועל המשרד לבט"פ לבחון מחדש ולאלתר את המבנה הארגוני של המערך, כך שהטיפול בפשיעת סייבר, שהיא כאמור חוצת גבולות, יהיה באחריות גורם פיקוד מרכזי בניגוד למצב הקיים היום, כך שתתאפשר ראייה מערכתית בנושא היקף המעורבים, הנפגעים והנזקים בתיק.

המשטרה מסרה בתשובתה הנוספת כי תפיסת ההפעלה החדשה, שתבוא לידי ביטוי בתכנית דו-שנתית שלה, תיתן מענה מיטבי לסוגיית המאפיינים הטריטוריאליים של פשיעת הסייבר.

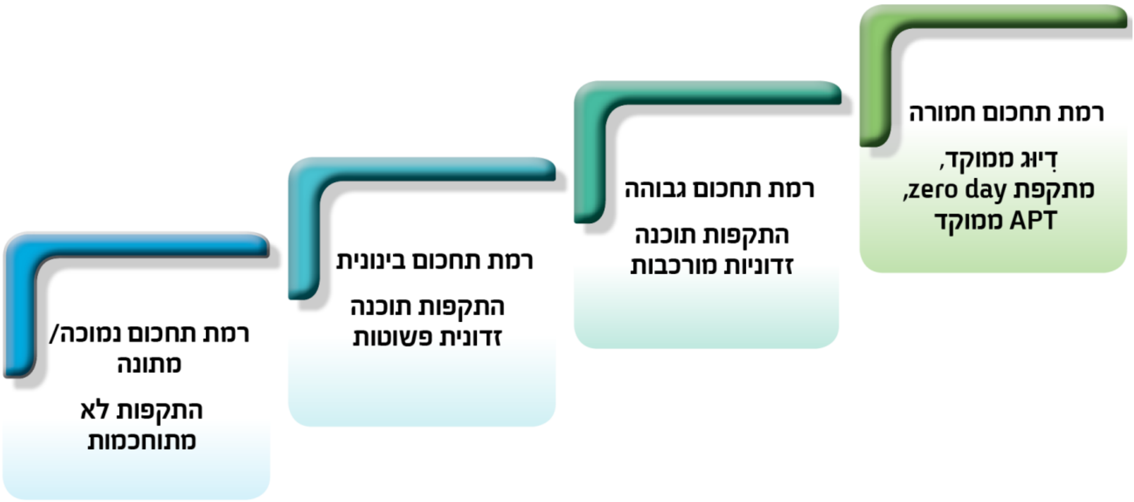
טיפול בתיקי חקירה בהתאם למאפיין המורכבות הטכנולוגית של העבירה

כדי לקדם מדיניות מותאמת למגוון התופעות שנכללות בהגדרת "פשיעת סייבר" יש צורך בהגדרת קטגוריות של פשיעה מסוג זה, לפי מידת מורכבותן הטכנולוגית של העבירות[39]. מיפוי איומים במרחב הסייבר מקובל בעולם, ומאפשר להתמודד בצורה טובה יותר עם פשיעה זו.

39 מחקר סוכנות האו"ם לסמים ופשיעה; המשרד לבט"פ, האגף למדיניות ותכנון אסטרטגי, יחידה מידע וידע, **סקירה בנושא מדידת פשיעה מקוונת** (2014).

ארגון ISACA[40] מציע למפות את מרחב האיומים על פי רמת תחכום טכנולוגי, מפשיעה בעלת רמת תחכום נמוכה שאינה מתמקדת בקורבן מסוים, עד לרמת תחכום גבוהה וחמורה המשתמשת בכלים מתוחכמים כלפי גורם ספציפי באופן מתמשך[41]. בתרשים להלן מומחשת החלוקה המוצעת כאמור במסמך ISACA:

תרשים 4: **רמת תחכום של סוגי איומי פשיעת סייבר**



מקור: ארגון ISACA.

תפיסת ההפעלה של המשטרה קובעת כי תיקי החקירה יפוצלו בין היחידה הארצית לבין מחלקי הסייבר לפי מורכבות העבירה, כך שהיחידה הארצית תחקור עבירות "הדורשות משאבי זמן, מומחיות ואמצעים מתוחכמים" (להלן - מאפיין מורכבות העבירה). נוהל המשטרה האמור בנושא "הטיפול בתיקי חקירה בעבירות משותפות למספר יחידות" מתייחס גם הוא למורכבותו של תיק נחקר כמאפיין הקובע שהיחידה הארצית תטפל בעבירות סייבר מורכבות.

40 ארגון בין-לאומי שנוסד בשנת 1969 ומרכז ידע מקצועי עולמי בדבר אבטחת מערכות מידע וטכנולוגיית מידע ומפתח תקנים בין-לאומיים בביקורת ובקרת מערכות מידע.

41 כגון: התקפות Zero Day- שימוש בטכנולוגיה מזיקה שטרם התגלתה וטרם ניתן לה פתרון על ידי חברות האנטי-וירוס; Advanced Persistent Threat (APT)- התקפות מתוחכמות ארוכות טווח באמצעות מגוון רחב של אמצעים מתקדמים על יעדים מוגדרים (כגון מערכות מידע מקוונות, שרתים) מתוך הכרתם לעומק. תחכום התקפות אלו מקשה על מערכות ההגנה של היעדים לזהות, לנטר ולמנוע את ההתקפה באמצעות "אמצעים אוטומטיים טיפוסיים", או בעזרת נהלים, "התנהגות נכונה" ושיגרת אבטחה של היעד בשל השימוש בכלים מונעי זיהוי ואיתור עקבות; דיוג ממוקד (פישינג)- שמאופיין כ"התקפה כללית" אשר מחפשת נקודת תורפה בסביבה הממוחשבת במטרה לגנוב מידע רגיש על ידי התחזות ברשת האינטרנט. ארגון ISACA, **מסמך התמרה לאבטחת סייבר** (2015), עמ' 17, 34.

מבדיקת משרד מבקר המדינה עולה כי היו מקרים שבהם טופלו תיקים מורכבים טכנולוגית במחלקים ולא הגיעו כלל לידיעת היחידה הארצית, עקב אפשרותם של המחלקים להגביל את גישת היחידה הארצית לתיקים אלה. יצוין כי פעמים רבות רמת המורכבות של עבירה מתגלה רק לאחר פרק זמן מסוים, בעיצומה של החקירה. יוצא אפוא שמחלק סייבר מחוזי, שיכולותיו הטכנולוגיות מוגבלות לעומת יכולות היחידה הארצית, מנסה לעתים להתמודד במשך תקופה ארוכה עם תיק חקירה שנפתח אצלו, ורק בשלב מאוחר יחסית בחקירה הוא פונה, בשל המורכבות הטכנולוגית של התיק, לקבלת סיוע מהיחידה הארצית.

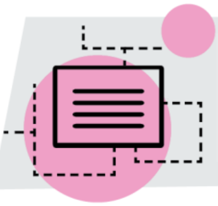
הפנייה של מחלק סייבר מחוזי ליחידה הארצית לשם קבלת סיוע טכנולוגי שנעשית בשלב מאוחר יחסית בחקירה, כפי שאירע בתיק שנידון לעיל, עלולה לשבש את החקירה עד כדי החמצת ראיות, מאחר שהטיפול שניתן לאותה עבירה טרם הפנייה לא תאם את רמת מורכבותה הטכנולוגית.

תיקי פשיעת סייבר יכולים להיות מוגדרים "מורכבים" בשל נסיבות שונות. בתרשים להלן דוגמה למסגרת אפשרית לתהליך עבודה שיטתי למיפוי רמת המורכבות הטכנולוגית של תיקי פשיעת סייבר בתחום המידע, כמו חדירה לא חוקית למאגרי מידע ממוחשבים פרטיים, מסחריים וציבוריים (computer data), על פי שיטות עבודה מקובלות בעולם[42]:

42 הסוכנות הלאומית לפשיעה באנגליה **Building a Response to CyberCrime** (April, 2016); ארגון היורופול משנת 2015 **The Internet Organised Crime Threat Assessment** (IOCTA), p. 27; מחקר סוכנות האו"ם לסמים ופשיעה (ראו לעיל הערת שוליים 12); ארגון ISACA **מסמך התמרה לאבטחת סייבר** (2015), עמ' 14-38.

תרשים 5: **שלבים למיפוי רמת המורכבות הטכנולוגית של תיקי פשיעת סייבר**

הפעולה שנעשתה



- גניבת מידע ממחשבים או ממאגרי מידע ממוחשבים
- נזק למידע או לנתונים ממוחשבים ושיבוש
- העברת מידע שנגנב לצד שלישי

סוג מידע

- מידע עסקי / תעשייתי / קניין רוחני
- מידע אישי (כגון תמונות פרטיות וחדירה לדוא"ל)
- מידע ציבורי (כגון מרשם אוכלוסין ורישומי עירייה)

רמת תחכום טכנולוגי

- התחזות: ניחוש מושכל של ססמאות
- פעולה שהצריכה גישה פיזית
- תוכנות מזיקות ווירוסים בעלי אופי גנרי
- שימוש בטכנולוגיה מתקדמת: הצפנה, Zero Day, APT, תוכנות לטשטוש עקבות של הכלים הטכנולוגיים וכדומה

מידע על התוקף

- ידע: ההשכלה הטכנולוגית של התוקף
- מאפייני העבריין: אדם בודד, קבוצה עבריינית, משפחת פשע; המניע לעבירה
- ממד בינלאומי: צורך בפנייה לגורמי אכיפת חוק זרים בשל כתובת IP זרה, שרת זר, חשבונות זרים בחו"ל (בישראל: ב-70% מהתיקים יש מעורבות של ממד זה)

מושא התקיפה

- חומרה / תשתיות
- מחשב אישי / טלפון חכם
- סביבת IT (כגון חוות שרתים, בסיסי נתונים גדולים ורשת מחשבים)
- דואר אלקטרוני ארגוני
- שירותי ענן

מקור: מידע מספרות מקצועית בעיבוד משרד מבקר המדינה.

מאחר שמאפיין מורכבות העבירה ורמת התחכום הטכנולוגי הוא גורם חשוב ומרכזי, שעל בסיסו אמורות להתקבל החלטות בדבר הפנייה לגורם החוקר וההתאמה של תשומות החקירה, הרי שיש מקום לקבוע הליך מקצועי סדור למיפוי טכנולוגי של סוגי האיומים של פשיעת הסייבר והיקפיהם.

בדיקת משרד מבקר המדינה העלתה כי מעבָר להגדרה הכללית שהובאה בתפיסת ההפעלה, ולפיה ינותב הטיפול בתיק לפי "מורכבותו", לא הגדירה התפיסה תהליך עבודה שיטתי ומוסדר שיאפשר לקבוע את רמת מורכבות התחכום הטכנולוגי של העבירה ולהעניק לה את הטיפול המיטבי מבחינת המענה הטכנולוגי הנדרש. לפיכך כל מחלק סייבר מגדיר בעצמו את מורכבות התיק ופועל בהתאם לעקרונות שהתפתחו בכל מחלק בנפרד.

המשטרה מסרה בתשובתה כי מורכבות פשיעת הסייבר משתנה וכי אי-אפשר לקבוע מסמרות להתמודדות עמה. כך למשל תופעת פשיעה שנראתה מורכבת בשנת 2013 הופכת לפשוטה שנה לאחר מכן לאחר פיתוח יכולות משטרתיות לטיפול. לאור זאת טוענת המשטרה שאי-אפשר להגדיר מראש מהי המורכבות הנדרשת, וראשי מחלקי הסייבר יודעים מתי ביכולתם לטפל בתיק ומתי יש להעבירו ליחידת הסייבר.

מתשובת המשטרה עולה כי בניגוד לפרקטיקות מקובלות בעולם, אשר נוקטות דרך סדורה לאִפיון המורכבות הטכנולוגית של פשיעת סייבר בראייה רחבה, ההחלטות שהתקבלו במשטרה לגבי מורכבות התיק נעשו אד-הוק בכל מחוז בנפרד, תוך התייחסות לתיק כפשיעה "קלאסית" ללא יד מתכללת וללא מעורבות חוליית המטה. על המשטרה לבחון את הגישות המקובלות בעולם בנושא זה, וכן לפנות למטה הסייבר הלאומי כדי לוודא שתפיסת ההפעלה נותנת מענה למאפיין המורכבות הטכנולוגית של פשיעת סייבר. כך יושג ניצול מיטבי ויעיל של המשאבים והידע הקיימים.

> תפיסת ההפעלה לא הגדירה תהליך עבודה שיטתי ומוסדר שיאפשר לקבוע את רמת מורכבות התחכום הטכנולוגי של העבירה. ההחלטות שהתקבלו במשטרה לגבי מורכבות התיק נעשו אד-הוק בכל מחוז בנפרד ללא יד מתכללת

חוליית המטה

תפקידה העיקרי של חוליית המטה הוא בניית הכוח של מערך הסייבר[43], לצורך קידומם ומימושם של מטרות הארגון וייעודו[44], ובין היתר: שיתוף המערך בכל הנוגע לתמונת המצב של הפשיעה ושיתוף הידע על אודות דרכי ההתמודדות עמה, הנחיה מקצועית, פיקוח ובקרה. כך יוכל מערך הסייבר להתמודד עם האתגרים הניצבים בפניו[45]. כאמור, במועד הביקורת הייתה חוליית המטה כפופה פיקודית לראש חטיבת החקירות באח"ם, וכללה מספר מצומצם של תקנים מאוישים. משרד מבקר המדינה בחן את פעילות חוליית המטה להשגת מטרות אלה, להלן הפרטים:

שיתוף בידע

1. אחד הקשיים לטיפול יעיל בפשיעת סייבר הוא היעדר שיתוף ידע מספיק בין הגופים במערך[46]. הצורך בשיתוף בידע בין כל הגופים החוקרים פשיעת סייבר מתעצם לאור אופייה שמשתנה בטווחי זמן קצרים מאוד ולנוכח עלייה מתמידה בתחכום הטכנולוגי. לפיכך, כדי שמערך הסייבר יפעל באופן מיטבי, על חוליית המטה להביא לשיתוף בין כלל גופי המערך ולחיזוק הקשרים המקצועיים ביניהם באופן מסודר ושיטתי, תוך כדי התעדכנות שוטפת ("keep up") בפעולות עברייני הסייבר ודרכי ההתמודדות במסגרת החקירות בעלות המאפיינים הטכנולוגיים[47].

החשיבות שנודעת לשיתוף הידע בין היחידות החוקרות - בינן לבין עצמן ובינן לבין חוליית המטה, מוצאת את ביטויה בהנחיות ובדגשים שניתנו לחוליית המטה במסגרת דיונים שנערכו בפיקוד המשטרה: בדיון משנת 2009 בנושא "פשיעה בעולם הסייבר" צוין שנושא שיתוף הידע חשוב מאוד; בדיון מדצמבר 2014 נקבע כי על חוליית המטה לקיים פורום חודשי עם מפקדי מחלקי הסייבר במחוזות "כדי לתאם... ולגבש המלצות ולקחים"; בדיון מיוני 2015 נקבע שיש לייצר שיתוף של ידע בדבר היכולות הקיימות ביחידות החוקרות; ובדצמבר 2015 ניתנה הנחייה באח"ם כי "חייבת להיות העברת מידע וידע", וכי החוקרים במחוזות יגיעו פעם בחודש ליחידה הארצית "לעדכונים ולימודים", ושנדרש ליצור פורום סייבר ארצי להעברת ידע בין כלל יחידות המערך.

43 גבי סיבוני ועופר אסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר** (אוקטובר 2015) (להלן - סיבוני ואסף), אוניברסיטת תל אביב, המכון למחקרי ביטחון לאומי, עמ' 22.

44 מחלקת התכנון/אגף התכנון והארגון משטרת ישראל, **המתודולוגיה של עבודת המטה לבניין הכוח במשטרת ישראל** (בהוצאת משטרת ישראל, אפריל 2016), עמ' 55, 78.

45 כפי שנקבע גם בתפיסת ההפעלה של מערך הסייבר.

46 דוח הביקורת על מערך האף.בי.איי. (ראו לעיל הערת שוליים 29).

47 מחקר סוכנות האו"ם לסמים ופשיעה ע"מ 143-144. (ראו לעיל הערת שוליים 12).

היחידות החוקרות פועלות במנותק זו מזו בלי שהוטמעו תהליכי עבודה המבטיחים ממשק רציף של העברת ידע, למעט קבוצת ווטסאפ פנימית בין חוקרי המערך

נמצא כי הוראות פיקוד אח"ם מהשנים 2014 ו-2015 העומדות על חשיבות התכלול ושיתוף הידע בין כל היחידות החוקרות לגבי התמודדות אפקטיבית עם פשיעת סייבר מתוחכמת טכנולוגית, לא יושמו, כמפורט להלן:

חוליית המטה לא יצרה פורום חודשי קבוע ומוסדר בהשתתפות נציגי היחידות החוקרות, ולעתים נדירות נערכו מפגשים בין חוקרים מיחידות שונות; לא נבנתה מסגרת קבועה לשיתוף ידע בין המחלקים, והחוקרים לא הגיעו פעם בחודש ליחידה הארצית לשם עדכונים כפי שהורה פיקוד אח"ם; למעט קבוצת ווטסאפ פנימית בין חוקרי המערך בה נעשה שיח מוגבל לצורך העברת ידע בין חוקרי המערך, לא נמצא כי מוסדו תהליכי העברת ידע בין כלל יחידות המערך.

כמו כן נמצא כי היחידה הארצית העבירה עדכון שבועי על אירועים שונים במרחב הסייבר, אולם חוליית המטה לא ערכה דיונים מקצועיים באירועים הללו, ולא הביאה ל"הנחלת הידע" במערך. לפיכך עדכון שבועי זה אינו משמש מסגרת מקצועית התואמת את הנחיות פיקוד אח"ם. יוצא אפוא כי הידע בתחום פשיעת סייבר מבוזר במערך, ואין זיכרון ארגוני להעשרת היחידות. כך לדוגמה נפגמת היכולת להצליב ידע באירועי סייבר שונים.

מציאות זו הביאה לידי כך שהיחידות החוקרות פועלות במנותק זו מזו בלי שהוטמעו תהליכי עבודה המבטיחים ממשק רציף וקבוע של העברת ידע, ובלי להיות מעודכנות בדבר יכולותיהן הטכנולוגיות של יחידות אחרות במערך או בדבר דרכי התמודדותן עם תיקי פשיעת סייבר שמאפייניהם עשויים להיות דומים. עולה אפוא שחוליית המטה לא הצליחה לממש את אחריותה, ואינה נתפסת כגוף מקצועי ומוסכם מול כלל היחידות החוקרות במערך.

המשטרה מסרה כי אכן לחוליית המטה יש קושי למלא את כלל משימותיה, אולם החוליה פעלה רבות להנחלת ידע לחוקרי הסייבר והקימה פורום לתמיכה טכנית ומקצועית המיועד לכלל החוקרים בתחום.

2. בשנים האחרונות מסתמנת עלייה ניכרת בפריסת מצלמות במרחב הציבורי, כמו מצלמות של רשויות, חברות ובתי עסק ומצלמות במכשירי הטלפון החכמים. בשל כך ראיות המופקות ממצלמות אלה הן רכיב מרכזי ביכולת פענוח תיקי חקירה. כדי להתמודד ביעילות עם מיצוי ראיות אלה החליטה המשטרה על הקצאת חדרים - "זירות טכנולוגיות" - ייעודיים בתחנות המשטרה (להלן - חדרי זי"ט), שבהם יוצבו חוקרים שיצוידו באמצעים טכנולוגיים למיצוי הראיות הללו.

נמצא כי אפיון חדרי הזי"ט מבחינת האמצעים הטכנולוגיים ושיטות ודרכי העבודה נעשה ללא מעורבות מקצועית מצד מחלקי הסייבר המחוזיים, למרות הידע שלהם בכל הקשור להתמודדות עם ראיות דיגיטליות.

יצוין כי בעניין זה פנה קצין אח"ם מאחד המחוזות באפריל 2016 בבקשה לשיתוף בתהליכי הקמת הזי"ט במחוז בכל הקשור לציוד, להדרכת חוקרי הזי"ט ולשיטות עבודה, אל פיקוד אח"ם, ואולם פניה מוקדמת זו לא נענתה על ידי חוליית המטה ואג"ת.

המשטרה מסרה בתשובתה כי אפיון הצרכים הטכנולוגיים לחדרי הזי"ט נעשה על ידי חוליית המטה שבחטיבת החקירות באח"ם יחד עם אג"ת. מטרת האפיון הייתה לתת כלים מתאימים לתחנה לטיפול באיסוף הראיות הייחודי לתחנות, בהתבסס על ידע מעשי שהצטבר בשטח בניסוי חלוץ (פיילוט) שבוצע לצורך כך באחת מתחנות המשטרה.

משרד מבקר המדינה מעיר כי אפיון חדרי הזי"ט היה צריך להתבצע תוך מעורבות מחלקי הסייבר במחוזות בשל ניסיונם הרב. העובדה כי לא נעשה כן, מלמדת על החסר בממשק מסודר בין מחלקי הסייבר לבין חוליית המטה, שאמורה לתכלל את פעילות כלל היחידות החוקרות במרחב הסייבר.

הנחיה מקצועית, פיקוח ובקרה

לפי תפיסת ההפעלה, על מחלקי הסייבר לסייע ליחידות החקירה בכל מחוז בטיפול בתיקי פשיעת סייבר ולהנחות מקצועית את החוקרים המיומנים. על חוליית המטה לפקח על עבודת מחלקי הסייבר ולוודא שמתקיימים ממשקי עבודה יעילים בין מחלק הסייבר, החוקרים המיומנים ושאר יחידות החקירה במחוז.

חוליית המטה, בהיותה גוף המטה שאמור לרכז את עבודת המערך, לא קבעה הנחיות מקצועיות, ונוהלי פיקוח ובקרה על עבודת המערך ועל שיתוף פעולה ותיאום בין היחידות החוקרות. עובדה זו פגעה ביעילות פעולתם של התחנות, החוקרים ומחלקי הסייבר במילוי משימותיהם בתחום אחריותם, להלן הפרטים:

1. במהלך 2016 ערכו שוטרי אחת התחנות חיפוש בביתו של חשוד בעקבות מידע מודיעיני. במהלך מעצרו של החשוד נגרם נזק בלתי הפיך לראיות הדיגיטליות ואי-אפשר היה להפיק שום ראיה כזו.

אף שהחשדות היו בתחום פשיעת סייבר, המעצר והחיפוש נעשו על ידי שוטרים שאינם מוסמכים בתחום הסייבר וללא ידיעת מחלק הסייבר במחוז. בכך הוסב נזק לראיות הדיגיטליות באופן שמאיין את יכולות המשטרה לחקור את התיק.

המשטרה מסרה בתשובתה כי השוטרים באירוע זה פעלו לפי נוהלי המשטרה המפרטים את תחומי האחריות והסמכות לטיפול בפשיעת סייבר ברמת המחוז, ואין אפשרות להקצות חוקרים מיומנים לכל חיפוש שנערך במחוז שכן טיפול בחומרי מחשב הפך לנפוץ בכל סוגי הפשיעה.

משרד מבקר המדינה מעיר למשטרה כי פרטי המקרה האמור מדגישים את החשיבות של הנחיה מקצועית בתחום הסייבר לכלל חוקרי המחוזות. כמו כן יש מקום ליידע את מחלק הסייבר בדבר הימצאות זירה דיגיטלית במהלך טיפול בתיק כדי למנוע תקלות, כפי שפורט לעיל.

2. בבקרות שנעשו בשנת 2013 במחלקי הסייבר בשני מחוזות ציינה חוליית המטה, כי תיקים אשר טופלו ביחידות השטח ולא הגיעו לטיפול מחלק הסייבר "לא טופלו בצורה מיטבית". על כן הומלץ להעביר את תיקי עבירות המחשב לטיפול מחלקי הסייבר במחוזות. בסיכום בקרה שערכה חוליית המטה במחוז אחר בשנת 2011 צוין כי על יחידות השטח להתייעץ עם מחלק הסייבר במחוז בכל הקשור לטיפול בתיקי פשיעת סייבר.

נמצא כי חוליית המטה לא פעלה מול פיקוד אח"ם במחוזות ומול מפקדי התחנות כדי לקבוע ממשקי עבודה יעילים בתחום הסייבר. כמו כן לא הוגדר אילו תיקי פשיעת סייבר יטופלו ברמת התחנה ואילו יועברו לטיפול של מחלקי הסייבר על אף ההמלצות האמורות בבקרות. לפיכך, פעלו התחנות נגד עברייני סייבר בלי שהתייעצו עם מחלקי הסייבר במחוזות, תוך כדי ניתוק מהידע ומהיכולות שהיו קיימות במחלקים, באופן שהביא למענה לקוי לפשיעת הסייבר.

3. בדיקת משרד מבקר המדינה, העלתה שבכ-20%-30% מן המקרים שבהם נעשה ניסיון לפרוק ראיות דיגיטליות, לא הצליחו חוקרי הסייבר בתחנות לעשות כן, בגלל היעדר ידע מקצועי-טכנולוגי והיעדר סיוע מקצועי שוטף מצד מחלקי הסייבר במחוזות, זאת מבלי שחוליית המטה פיקחה אחר הנעשה במחוזות. כך נוצרו מצבים של "איבוד ראיות" דיגיטליות.

המשטרה מסרה בתשובתה כי בתחום הפקת ראיות דיגיטליות אין הצלחה מוחלטת, והוסיפה כי הקושי הקיים בתחנות בתחום הפקת הראיות עתיד להיפתר עם הקמתם של חדרי הזי"ט בתחנות.

הקמת המעבדות בתחנות עשויה לשפר את היכולות בתחום הפקת הראיות הדיגיטליות. עם זאת, על המשטרה ועל המשרד לבט"פ לוודא כי יתקיים גם ממשק קרוב ורציף בין התחנות לבין מחלקי הסייבר.

✩

מהאמור לעיל עולה כי מערך הסייבר לוקה בחולשות של ממש בהיבטים של שיתוף ידע, פיקוח ובקרה ומתן סיוע טכנולוגי מצד מחלקי הסייבר שבאחריות חוליית המטה למחוזות. חולשות אלו נובעות מהמבנה המבוזר של מערך הסייבר שתוצאתו היא, היעדר ממשק ראוי בין חוליית המטה לבין היחידות החוקרות של המערך. מציאות זו משקפת היעדר "יד מכוונת" של גוף מטה כלפי היחידות החוקרות במערך.

מערך הסייבר לוקה בחולשות של ממש בהיבטים של שיתוף ידע, פיקוח ובקרה ומתן סיוע טכנולוגי מצד מחלקי הסייבר שבאחריות חוליית המטה למחוזות

המשטרה מסרה בתשובותיה כי השינוי במבנה המערך בעקבות עבודת המטה הנעשית בעת מסירת התשובה ותפיסת ההפעלה החדשה עתידים להפחית במידה ניכרת את היעדר התיאום המתואר בביקורת, וכן להביא לתיאום בין כלל המערכים בהיבטים המקצועיים והאופרטיביים ולביצוע פיקוח עִתי. כמו כן מסרה המשטרה כי חלק מהתקלות ייפתרו עם חלוקת תחומי האחריות של חוליית המטה בין שתי חטיבות מקצועיות: האחת, תהיה אחראית להיבטים הטכנולוגיים, והשנייה תהיה אחראית להיבטי חקירה קלאסיים, תוך שיתוף פעולה ביניהן וזאת לפי מדיניות מטה הסייבר במשטרה.

משרד מבקר המדינה מעיר כי על המשטרה לבחון בשנית את כוונתה ליישם את השינוי המבני האמור, שאינו עולה בקנה אחד עם התובנות והפרקטיקה המקובלות בעולם. כך לדוגמה, לפי מסמך שהכינה הסוכנות המרכזית להתמודדות עם פשיעת סייבר באנגליה, מאפריל 2016 שכותרתו "Building a Response to Cyber Crime"[48], נדרש שבעבירות סייבר מתוחכמות טכנולוגית, כלל פעילות המטה תתבצע בצורה הוליסטית תחת יחידה מרכזית ותקיף את הצרכים החקירתיים והטכנולוגיים, תשתף את הידע במערך ותספק תמונת מצב של הפשיעה והאסטרטגיה, ולא תפוצל בין מערכים נפרדים באופן מלאכותי.

עוד מעיר משרד מבקר המדינה כי הפרדת תחומי האחריות של חוליית המטה בין המישור הטכנולוגי למישור החקירתי נוסף על המבנה המפוצל הקיים של כלל מערך הסייבר, אינה מביאה בחשבון את המאפיינים של פשיעת סייבר מתוחכמת טכנולוגית, שבה שני המישורים כרוכים זה בזה. במציאות זו אין מענה לחולשותיו של המערך המבוזר כפי שפורטו בדוח זה, ובכללן החולשה בתחום שיתוף הידע בין כלל הגורמים העוסקים בנושא. על המשטרה ועל המשרד לבט"פ לוודא כי הידע המקצועי הקיים בעולם לטיפול בפשיעת סייבר מתוחכמת טכנולוגית נבחן ומיושם.

48 National Crime Agency, (April 2016).

על המשטרה ועל המשרד לבט"פ לוודא שעבודת המטה המתקיימת כיום תיתן מענה לצרכים הייחודיים של המלחמה בפשיעת סייבר מתוחכמת טכנולוגית. במסגרת זו עליהם לבחון לעומק את מבנה המערך ואת שאלת הכפפתו הטכנולוגית והחקירתית, ובכלל זה את הכפפת מחלקי הסייבר למחוזות. בחינה זו נדרשת, שכן היערכות המשטרה והמשרד לבט"פ כיום לאתגרים ולסיכונים הלאומיים הקשורים לפשיעת סייבר מתוחכמת טכנולוגית אינה מתבססת על התפיסות המקובלות בעולם ועל לקחי משטרות זרות לגבי טיפול אפקטיבי בפשיעה כאמור, וספק רב אם היא נותנת את המענה הדרוש לאיומים.

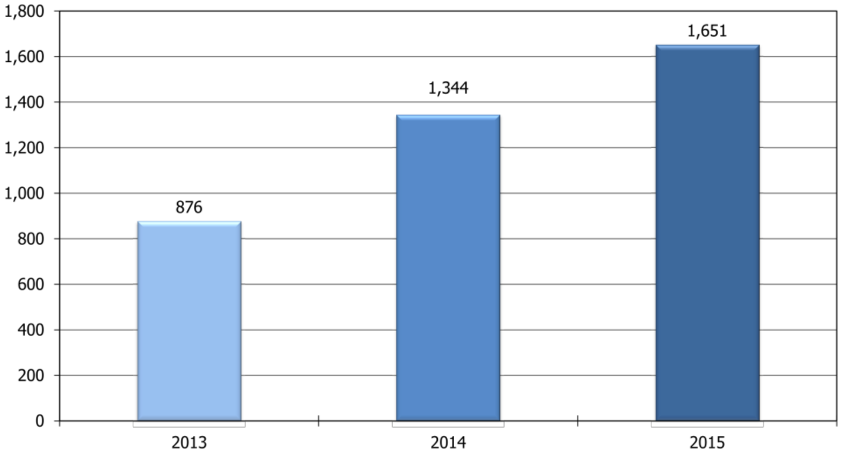
הפרדת תחומי האחריות של חוליית המטה בין המישור הטכנולוגי למישור החקירתי אינה מביאה בחשבון את המאפיינים של פשיעת סייבר מתוחכמת טכנולוגית, שבה שני המישורים כרוכים זה בזה

תקציב ורכש

תקצוב מערך הסייבר

בתרשים להלן מספר תיקי פשיעת סייבר שטופלו במערך הסייבר בשנים 2015-2013:

תרשים 6: **מספר תיקי פשיעת סייבר 2015-2013**



מקור: נתוני המשטרה. נתונים אלו כוללים את הטיפול בעבירות פדופיליה והטרדה מינית שטופלו על ידי חוקרי מערך הסייבר.

מהנתונים לעיל עולה כי מספר התיקים שבהם טיפל מערך הסייבר כמעט שהוכפל בשנים 2015-2013. בחלק מתיקי פשיעת הסייבר מאופיינים ככאלה המחייבים מאמץ מתמשך[49], ולעתים כפי שעולה מביקורת אג"ת מאוגוסט 2015 "פרשיות הופכות מורכבות יותר ונדרשת כחצי שנת אדם לעבודה על פרשיה מורכבת". זאת בשל התמודדות החקירות עם מורכבות טכנולוגית הכרוכה בחילוץ ראיות דיגיטליות, ובפענוחן. חלק מהתיקים שנחקרים כוללים בחינת מדיות דיגיטליות רבות בו זמנית. המורכבות הטכנולוגית שעמה מתמודד מערך הסייבר ממחישה את ההיקף ההולך וגדל של פעילות החוקרים, הדורש מענה טכנולוגי ותקציבי הולם.

תכנית הרכש להצטיידות ולהכשרות של מערך הסייבר לשנת 2016 הייתה אמורה "לתת למערך להמשיך להתקדם בהכשרות, תוכנות, ציוד וכלים חדשים אשר נדרשים לתחום שמתפתח במהירות רבה".

49 מסמך ארגון היורופול; **The Internet Organized Crime Threat Assessment** (IOCTA) Pp. 12 (2015). במסמך מצוין הצורך ב"חקירה מקיפה לטווח רחוק" (long-term comprehensive investigation”).

לפי מסמכי אח"ם, התקציב עבור הצטיידות ותפעול מערך הסייבר לשנת 2015 היה 9 מיליון ש"ח, ובשנת 2016 עמד תקציב זה על 6 מיליון ש"ח בלבד.

מהאמור עולה כי למרות שבשנים 2015-2013 כמעט שהוכפל מספר תיקי פשיעת הסייבר, בשנת 2016 צמצמה המשטרה בשליש את תקציב ההצטיידות והתפעול של המערך. מצב זה משקף חוסר הלימה לנוכח הגידול הניכר בהיקף הפעילות הנדרש ממערך הסייבר.

המשטרה מסרה בתשובתה כי תכנית הרכש נקבעה תחילה לצורך הצטיידות באמצעים, ובהמשך נועד התקציב בעיקר לתמיכה ולחידוש רישיונות. לדבריה, לא הייתה הפחתה מכוונת של תקציב ההצטיידות למערך הסייבר אלא הוא התכנס למסגרות שוטפות, אשר קבעו מראש הגורמים המתקצבים במשטרה.

בדיקת משרד מבקר המדינה העלתה כי מתוך הסכום שאושר בסך של 6 מיליון ש"ח, 1.6 מיליון ש"ח יועדו להעסקת כוח אדם אזרחי, 1.5 מיליון ש"ח יועדו לתשלום עבור התחייבויות קודמות עוד משנת 2015 וסכום של כ-190,000 ש"ח יועד להוצאות נסיעה. יוצא אפוא שלרכש נטו לשנת 2016 נותר סכום של 2.7 מיליון ש"ח בלבד לכלל המערך.

סכום זה (2.7 מיליון ש"ח) מיועד הן להתמודדות עם פשיעת הסייבר, המתוחכמת טכנולוגית, והן לצרכים של המחוזות לצורך הפקת ראיות דיגיטליות שאינן מתוחכמות. ליחידה הארצית הוקצו 1.6 מיליון ש"ח, ולשאר המערך - הכולל הן את המחלקים והן את החוקרים המיומנים בתחנות - הוקצו כ-1.1 מיליון ש"ח. מתוך הסכום של 2.7 מיליון ש"ח, 80% יועדו לחידוש רישיונות לשלוש תוכנות ו-20% ממנו יועדו להדרכות שוטפות. ממסמכי אח"ם עולה שתקציב המשטרה המפורט לעיל אינו נותן מענה להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית, ואינו מאפשר הצטיידות בכלים חדשים הנדרשים לתחום זה שמתפתח במהירות רבה.

תקציב המשטרה אינו נותן מענה להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית, ואינו מאפשר הצטיידות בכלים חדשים הנדרשים לתחום זה שמתפתח במהירות רבה

ועדת המשנה להגנה בסייבר של ועדת החוץ והביטחון של הכנסת פרסמה באוגוסט 2016 דוח שעסק ב"בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל". גם בדוח זה צוין כי "**הוועדה התרשמה מחולשתה של המשטרה**" בין היתר בשל "**היעדר משאבים מספקים להתמודדות עם פשעי סייבר בעלי השלכות חמורות** (כל ההדגשות אינן במקור).

יצוין כי המשטרה מודעת לחסרים התקציביים לרכש במערך הסייבר. במסמך נוסף של אח"ם מיוני 2016 צוין כי "לנוכח גידול משמעותי בדרישות של השטח, היקף התקציב לרכש לא מספיק... יש צורך בתגבור תקציבי הרכש של מערך הסייבר, הנמצא כיום בין הנושאים המרכזיים המקודמים על ידי פיקוד המשטרה".

המשטרה מסרה בתשובתה כי פיקוד המשטרה ער לצרכים הגדלים בהצטיידות למערך הסייבר ומקצה לכך תקציב ממקורותיו השונים. לדבריה תוקצבו 14.8 מיליוני ש"ח באופן חד-פעמי במסגרת הקמת חדרי זי"ט בתחנות.

משרד מבקר המדינה מעיר למשטרה כי תקציב זה נותן מענה רק לסוגיית מיצוי ראיות מחשב וראיות פורנזיות עבור התחנות, ולא נותן מענה להתמודדות האפקטיבית עם פשיעת סייבר מתוחכמת טכנולוגית.

בתשובתה הנוספת ציינה המשטרה כי אין מקום לראות את הנתח התקציבי הניתן לפעילות השוטפת של יחידת הסייבר הארצית בנפרד משאר התקציב המופנה לתשתיות, רכש ופיתוח מהם נהנים כלל המערכים המקצועיים של המשטרה לרבות יחידת הסייבר הארצית.

משרד מבקר המדינה מכיר בכך שנעשו פרויקטים שמשיקים למרחב הסייבר, ובכלל זה פרויקטים חדשניים כמו שיתוף פעולה עם מעבדות הסייבר של מוסד אקדמי. עם זאת, על המשטרה והמשרד לבט"פ, לוודא שלרשות המערך המופקד על ההתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית יעמוד התקציב הדרוש לשם התמודדות אפקטיבית עם האתגרים שמציבה פשיעה זו.

פערי הצטיידות במערך הסייבר

1. **אמצעים מסוימים:** בתפיסת ההפעלה נקבע כי ביחידה הארצית ימוקם אמצעי שדרוש לחוקרי היחידה לצורך התמודדות עם מערכות נתונים מורכבות.

   ביוני 2015 אושרה תכנית רכש שכללה הצטיידות באמצעי האמור, בסכום של כ-2 מיליון ש"ח. היחידה הארצית דרשה להפעיל את האמצעי בעצמה, ואילו מנהל הטכנולוגיות במשטרה דרש לנהל בעצמו את האמצעי.

   המשטרה מסרה בתשובתה כי עדיין מתקיימים דיונים בנושא.

   לנוכח המחלוקת, במועד סיכום הביקורת ינואר 2017, לא היה במערך הסייבר האמצעי האמור. משרד מבקר המדינה מעיר כי נדרש שיתנהל שיח מקצועי בין הגורמים הרלוונטיים במשטרה כדי לקדם את הנושא באופן שיענה על הצרכים הטכנולוגיים של מערך הסייבר וימנע פגיעה ביעילות תפקוד המערך.

2. **כלי רכב:** ממסמך של אח"ם עולה כי חוקרי הסייבר במחוזות נדרשים לבצע פעולות חקירה רבות הדורשות כלי רכב לרבות חיפוש ותפיסת מחשבים. פעולות אלו נעשות בשטח הטריטוריאלי של המחוז ואף מחוץ לו. כמו כן נדרש כלי רכב לצורך העברת מוצגים לבדיקה במעבדת הסייבר במחוז או לבדיקה ביחידה הארצית.

בדיקת משרד מבקר המדינה העלתה כי עם הקמת מחלקי הסייבר במחוזות לא הוקצו להם כלי רכב[50], כך שהחוקרים מסתמכים על כלי רכב של המחוז. לפי אח"ם, כאשר אין כלי רכב פנוי בנמצא "נפגמות חקירות המבוצעות על ידם".

המשטרה מסרה בתשובתה כי הקצאת משאבים, כגון כלי רכב, נעשית לפי מפתחות סדורים. במסגרת התקציב העומד לרשות המשטרה לא אושרו בקשות אח"ם לתקנון כלי רכב למחלקי הסייבר, משיקולי תקציב.

משרד מבקר המדינה מעיר למשטרה ולמשרד לבט"פ כי עליהם לעקוב מעת לעת אם צורכי המערך וההיקפים ההולכים וגוברים של זירות פשיעה רוויות ראיות דיגיטליות מחייבים בחינה מחודשת של המפתח בדבר תקנון כלי רכב ליחידות העוסקות בפשיעת סייבר על רבדיה השונים.

3. **רכש ישירות מחו"ל:** בשל העובדה כי מערך הסייבר נדרש להגיב בזריזות יחסית לאירועים ולהתפתחויות הטכנולוגיות נדרשת אפשרות לרכישת תוכנות ושירותים מקוונים ישירות מחברות בחו"ל דרך אתר אינטרנט, וזאת באמצעות כרטיס אשראי בין-לאומי. יצוין כי רכישה באמצעות כרטיס אשראי בין-לאומי עשויה לחסוך למשטרה כספים המשולמים לחברות מתווכות.

ביולי 2015 אישרה עקרונית יחידת החשב הכללי במשרד האוצר הקצאת שני כרטיסים נטענים במסגרת שנתית בסך של 10,000 ש"ח עבור "רכש ותשלומים באינטרנט", במענה לבקשת חשבות המשטרה בפברואר אותה שנה.

עד מועד סיום הביקורת לא הונפקו כרטיסי אשראי בין-לאומיים למערך הסייבר למרות הצורך והיתרונות הגלומים בשימוש בכרטיסים מסוג זה ברכישות מקוונות.

בתשובתה ציינה המשטרה כי עד פברואר 2017, אח"ם בשיתוף פעולה עם הגורמים המקצועיים ביחידה הארצית בחשבות, יגבשו נוהל עבודה להקצאת כרטיס נטען לצורך רכש מחו"ל ולשימוש בכרטיס זה.

50 למעט במחוז ירושלים.

4. **רכישה פרטית של ציוד:** בבדיקת משרד מבקר המדינה נמצא כי בשל חוסר בציוד טכנולוגי ולנוכח אי-הלימה בין הצרכים בשטח ובין הציוד הקיים, נאלצו חוקרי פשיעת סייבר בתחנות לרכוש מכספם האישי ציוד בסיסי במאות ש"ח כדי שיוכלו לבצע את עבודתם, כמו: דיסקים און קי ואמצעי אחסון נוספים, מסכים קטנים, סוללות נטענות, כבלים מתאימים, עכברים אלחוטיים, שנאים, ערכות מברגים וכדומה. הציוד שנרכש מסייע לחוקרים המיומנים להתמודד ביתר יעילות עם הקושי של זירות עמוסות ראיות דיגיטליות בלא שניתן מענה מערכתי עקרוני על ידי פיקוד מערך הסייבר.

בשל חוסר בציוד טכנולוגי ולנוכח אי-הלימה בין הצרכים בשטח ובין הציוד הקיים, נאלצו חוקרי פשיעת סייבר בתחנות לרכוש מכספם האישי ציוד בסיסי

מתשובת המשטרה עולה כי היא מכירה בתופעת רכישה פרטית של ציוד. לדבריה, תהליכי הרכש המשטרתיים ארוכים ולעתים מסורבלים, ולכן אושר לפתוח קופה קטנה לסיוע לצורכי השטח. עם זאת, הבהירה המשטרה כי לא כל הציוד שנרכש באופן פרטי אושר על ידי אח"ם לרכש בשל אילוצי התקציב.

על המשטרה לפעול כדי למצוא פתרון הולם לצורכי השטח כך שהשוטרים לא ייאלצו לרכוש באופן פרטי ציוד חיוני הנדרש להם בעבודתם.

5. **אמצעים להגשת ראיות דיגיטליות בתחנות:** תלונות מצד אזרחים על עבירות סייבר מוגשות לחוקרים במרכזי שירות לאזרח בתחנות.

נמצא כי יש מחסור באמצעים טכנולוגיים בתחנות שיאפשרו לאזרחים למסור ראיות דיגיטליות בעת הגשת תלונה בנוגע לפשיעת סייבר. האמצעים החסרים הם: מחשב ייעודי המחובר לאינטרנט לצורך קבלת חומרים ממדיות דיגיטליות (כגון דיסק און קי); כתובת דואר אלקטרוני אזרחי שאליה יוכלו אזרחים לצרף חומרים דיגיטליים לתלונותיהם; מדפסת שתאפשר הדפסה מידית או סריקת הראיות הדיגיטליות.

המחסור באמצעים לקבלת תלונות הועלה כבר במסמך ממרץ 2015 בדיון באג"ת, ובו צוין כי "ישנו צורך להקצות לכל הפחות גישה לאינטרנט/מכשור + הדפסה ככל שרלוונטי".

משרד מבקר המדינה מעיר כי למרות הפערים באמצעים, שהיו ידועים למשטרה למעלה משנה וחצי, לא פעל פיקוד המשטרה למתן מענה לצרכים הטכניים בתחנות.

המשטרה מסרה בתשובתה כי פתרון חלקי לבעיה יינתן עם המשך פריסת חדרי הזי"ט המתוכננת בתחנות המשטרה. לחדרים הללו תינתן כתובת דואר אלקטרוני אזרחית שתאפשר לאזרחים להעביר חומרים דיגיטליים. כמו כן

מתוכנן כי בכל תחנה יוצב חוקר שיסייע בקבלת ראיות דיגיטליות מאזרחים, ויעניק ייעוץ בנושא תלונות בהקשר של מרחב הסייבר. הכשרה מתאימה לחוקרים האלה נמצאת בשלבי אישור.

משרד מבקר המדינה מעיר כי על המשטרה לוודא שמתקיים ממשק בין מרכזי השירות, בין האזרחים, בין חדרי הזי"ט ובין החוקרים שאמורים לסייע בקבלת ראיות דיגיטליות מאזרחים. כמו כן מעיר משרד מבקר המדינה כי עד השלמת המהלך כאמור בתשובת המשטרה, יש לוודא שהאזרחים מקבלים את המענה הדרוש לצורך הגשת ראיות דיגיטליות במסגרת הגשת תלונות על פשיעה במרחב הסייבר ובכלל.

✯

ההתפתחות הטכנולוגית המהירה של פשיעת הסייבר בצד הצורך במתן מענה לתלונות האזרחים, מחייבים את המשטרה ואת המשרד לבט"פ, לנתח את הצרכים הגדלים של מערך הסייבר אל מול יכולת ההתמודדות של המערך עם תיקים מורכבים טכנולוגית. לאור תוצאות הניתוח עליהם, יחד עם משרד האוצר, להתאים את התקציב לצורכי הרכש וההצטיידות כך שתתאפשר התמודדות עם פשיעת סייבר מתוחכמת טכנולוגית; כמו כן על התקציב להיות מותאם לכלל הצרכים השוטפים של המערך, כדי לגשר על הפערים שהוצגו לעיל.

גיוס כוח אדם טכנולוגי ושימורו

1. **גיוס עובדים:** החיבור הקיים בין עולם עתיר טכנולוגיה ובין עבריינות על כל גווניה מציב בפני המשטרה אתגר מורכב. פרופיל כוח האדם שביכולתו להתמודד עם אתגר זה שונה מפרופיל כוח האדם הנדרש משוטרים העוסקים במשימות משטרתיות מסורתיות. השכר והתנאים הנלווים המוצעים לאוכלוסייה בפרופיל הנדרש הם נמוכים ולוקים בחסר בהשוואה למצופה ולמוצע לה במגזרים אחרים במשק. ממסמכי המשטרה עולה כי המשטרה ומערך הסייבר "כלל לא נמצאות במרחק קרוב לתחרות ואטרקטיביות גיוס המועמדים הרלבנטיים... סוגיית השכר הינה החסם המשמעותי ואבן נגף אסטרטגית ביכולת הארגון [המשטרה] לגייס... כוח-אדם מתאים באיכות ובכמות".

להלן בלוח פרטים של שלושה מועמדים לגיוס ליחידה הארצית שמשקפים את פערי השכר האמורים, כפי שמסרה המשטרה:

לוח 1: **פערי שכר חודשיים (ברוטו) של מועמדים לגיוס ליחידה הארצית**

תפקיד	שכר שהוצע במשטרה בש"ח	שכר במקום עבודה אזרחי בש"ח	פער באחוזים
קצין חקירות	13,250	28,000	111%
נגד טכנולוגיות סייבר	10,190	19,000	86%
נגד טכנולוגיות סייבר, האקר	7,630	25,000	228%

מקור: נתוני המשטרה.

מהנתונים בלוח עולה כי פערי השכר מגיעים לאלפי ש"ח ואף יותר בחודש ומקשים על מערך הסייבר לגייס כוח אדם מתאים מן הבחינה הטכנולוגית.

במסמך שהכינה לשכת ראש אח"ם צוין, שכדי לסייע למשטרה לעמוד בתחרות על כוח אדם איכותי ומיומן מול השוק הפרטי נדרש לפתח כלים מגוונים לשיפור השכר הבסיסי וכלים לגיוס כוח אדם איכותי ושימורו.

המשטרה יחד עם משרד האוצר גיבשו במהלך שנת 2016 טיוטת הסכם העסקה ייחודי. טיוטת ההסכם הציעה מסגרת לשכר ייחודי לשוטרים במעמד זמני, ולפיה יוצע למספר מצומצם של מועמדים "מומחים" שיגויסו למערכים הטכנולוגיים באח"ם, וביניהם מערך הסייבר שכר גבוה משמעותית מהשכר המשולם כיום. כוח האדם שיגויס במתווה זה יועסק לתקופה קצובה של חמש שנים ברמות שכר שונות, בהתאם לתפקיד ולידע של המועמדים.

במאי 2016 פנה השר לבט"פ במכתב אל שר האוצר בנושא "בקשה לאישור תנאי העסקה ייחודיים ביחידות הסייבר... במשטרה", וציין כי "במודל השכר

הקיים במשטרה כיום, לא ניתן להציע שכר אטרקטיבי למועמדים פוטנציאליים בשל התחרות מול גופים ביטחוניים מקבילים וגופים אזרחיים/עסקיים, ומשטרת ישראל נתקלת בקושי גדול לגייס ולשמר אוכלוסייה זו".

עד ינואר 2017, לא אושר הסכם ההעסקה הייחודי, והיעדרו מקשה על מערך הסייבר לגייס כוח אדם.

מתשובת המשרד לבט"פ מדצמבר 2016 עולה כי טרם הושגה הסכמה סופית בינו לבין משרד האוצר לגבי מתווה ההסכם הסופי, וכי המשרד ממתין לתשובת משרד האוצר.

מתשובת אגף השכר והסכמי עבודה במשרד האוצר מינואר 2017 עולה כי בחודשים האחרונים לובנו הסוגיות העיקריות, ומשרד האוצר פועל לגיבוש טיוטת הסכם סופית. עוד ציין האגף כי משרד האוצר מאשר למשטרת ישראל לגייס מועמדים ליחידת הסייבר בהתאם לתנאי השכר שגובשו בטיוטת ההסכם, וכי אושר להכיר ביחידה הארצית כיחידה המזכה בתוספת של דירוג מחקר למגויסים, בכפוף לעמידה בקריטריונים הרלוונטיים.

על המשרד לבט"פ ועל משרד האוצר לסיים את התהליך שנמצא על המדוכה במהלך כשנה וחצי, באופן שיסייע בגיוס כוח אדם מתאים שיעניק את המענה המקצועי הדרוש למילוי המשימות בתחום זה.

2. **שימור כוח אדם:** במסמך בנושא "הצעה לתגמול שכר למערך הסייבר" של אגף משאבי אנוש מיוני 2014, הוצעו פתרונות לטובת שימור כוח אדם במערך הסייבר, לדוגמה מתן מענקים חד-פעמיים, רכב, לימודים וכדומה.

במסמך מנובמבר 2014 שהכין ראש היחידה הארצית עבור ראש היחידה לתכנון שכר, צוין כי חלק מהשוטרים שכבר גויסו "בעלי ניסיון עשיר בתחום הסייבר... אולם השכר הנמוך מקשה עליהם להישאר בארגון". בספטמבר 2015 כתב ראש היחידה הארצית כי "אנשים מוכשרים מאוד שכבר הגיעו ליחידה מוצאים עצמם מועסקים בשכר מאוד נמוך כבר תקופה ארוכה מאוד". בדצמבר 2015 כתב ראש חוליית המטה כי החוקרים הטכנולוגיים במערך הסייבר "חווים שחיקה גדולה בעבודתם עקב עומסי העבודה בתחום ולכן **חוקרים רבים שאינם מתוגמלים מבקשים לעזוב את המערך, ובכך אנו מפסידים חוקרים אשר השקענו בהם כסף רב בהכשרות**" (ההדגשה אינה במקור).

במאי 2016 ציין ראש היחידה הארצית כי "הבעיה החמורה היא שיש כבר עזיבה של שוטרים מתוך היחידה".

למרות הצורך הברור שעלה בנושא תגמול כוח האדם הקיים בעל המומחיות הטכנולוגית הגבוהה ובעל הידע להתמודדות עם פשיעת סייבר מתוחכמת טכנולוגית, שנקלט במערך הסייבר מאז הקמתו, נמצא כי טרם הושלם הטיפול בהצעות שהועלו למתן מענה על צורך זה. על המשטרה, המשרד לבט"פ ומשרד האוצר לתת את הדעת לחשש שהיחידה הארצית עומדת בפני מגמה של עזיבת כוח אדם מיומן ואיכותי המהווה את עמוד התווך של המערך, בהיעדר תמריצים מתאימים לשימורו. במצב זה פעילות מערך הסייבר צפויה להיפגע קשות, ועליהם למצוא בהקדם פתרון לבעיה זו.

משרד מבקר המדינה מעיר למשטרה כי בתשובתה היא פירטה כי היא מטפלת בנושא תגמול השכר לגיוס כוח אדם טכנולוגי, וכי צעדיה ייתנו מענה לצורך האמור. ואולם, תשובתה אינה נותנת מענה לצורך בשימור השוטרים המשרתים כיום במערך ולמניעת עזיבתם.

קיים חשש שהיחידה הארצית עומדת בפני מגמה של עזיבת כוח אדם מיומן ואיכותי המהווה את עמוד התווך של המערך, בהיעדר תמריצים מתאימים לשימורו

✯

בעולם הטכנולוגי יש חשיבות רבה מאוד לסביבת עבודה מתקדמת. מהביקורת עלה כי מערך הסייבר במשטרה מצטייר בעולם התעסוקה כחסר אמצעים ובעל תקציב זעום, שאינו מקבל די קשב מצד פיקוד המשטרה, שאינו מעניק סביבת עבודה הולמת להתמודדות עם פשיעת הסייבר המתוחכמת ושאין בו כוח אדם בהיקף משמעותי בעל רמה טכנולוגית גבוהה. מציאות זו פוגעת בשמו המקצועי של מערך הסייבר ובפרט בשמה של היחידה הארצית באופן שמקשה לשמר את כוח האדם הקיים ביחידה הארצית, ושמשפיע על גיוס מועמדים ברמה מקצועית וטכנולוגית גבוהה.

הממצאים שהועלו בפרק זה מלמדים שהמשטרה והמשרד לבט"פ טרם ענו על הצורך הדחוף בחיזוק המערך הקיים ובבניית שלד מקצועי של כוח אדם טכנולוגי מיומן בעל הכשרה מקצועית מתקדמת ומגוונת, המתאימה לדינמיות ולהתפתחות הטכנולוגית של פשיעת סייבר, כך שיהיה אבן שואבת לגיוס מועמדים נוספים ברמה הולמת ולשימורם בארגון לאורך זמן.

תפיסת ההפעלה של המשטרה ומערך הסייבר הלאומי

הספרות המקצועית התייחסה למענה המערכתי הנדרש להתמודדות עם פשיעת סייבר בראייה לאומית מתכללת[51]. כדי למצות את מלוא הפוטנציאל והמשאבים הלאומיים הקיימים יש לשלב מאמצים מצד כלל הארגונים הפועלים במרחב הסייבר במדינה. יש לפעול לכך בתחומים של פיתוח הון אנושי ושל פיתוח טכנולוגי ובאמצעות הקמת מערכים אפקטיביים. בסופו של התהליך יפעלו כל הארגונים בשיתוף הדדי ובהיזון חוזר[52], בייחוד לנוכח הקשר הקיים במרחב הסייבר בין תופעות פשיעה ובין איומי טרור ולנוכח הסיכון לפגיעה במתקנים חיוניים[53].

כאמור, בהחלטת הממשלה על הקמת מטה הסייבר הלאומי נקבע כי היא לא תחול על הגופים המיוחדים, ובהם המשטרה. בדיון ביולי 2012 בהשתתפות המפכ"ל דאז[54], קבע ראש אח"ם דאז כי "מטה הסייבר הלאומי משמש היום גוף ידע שחובה על המשטרה להתחבר אליו וללמוד ממנו", והוסיף כי יש להקים את מערך הסייבר במשטרה "כחלק ממערך הסייבר הלאומי". בדצמבר 2014 הורה המפכ"ל דאז על הקמת צוות באחריות ראש אג"ת דאז "שיוביל עבודת מטה בתחום הסייבר, האיומים והדרכים להתמודדות בשותפות עם מטה הסייבר".

בדוח של ועדת המשנה להגנה בסייבר של ועדת החוץ והביטחון של הכנסת מאוגוסט 2016, שעסק ב"בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל", נקבע כי קיים צורך לחבר "נכונה" בין הידע והיכולות הלאומיות ובין אחריות המשטרה להתמודד עם פשיעת סייבר וכי "הוועדה סבורה שנכון יהיה לדון בנושא בוועדות הכנסת הרלוונטיות".

לא נמצא כי המשטרה פעלה יחד עם מטה הסייבר הלאומי כדי לבסס את תפיסת ההפעלה של מערך הסייבר במשטרה באופן שיאפשר את התאמתו המיטבית למאפיינים המיוחדים של הפשיעה במרחב הסייבר.

המשטרה מסרה בתשובתה כי בהתייחסותה של משטרת ישראל לדוח ועדת חוץ וביטחון צוין כי בולט היעדר חלקה של משטרת ישראל, בייחוד בנושא הטיפול באירועי סייבר. לדעת המשטרה, אין ספק כי תפיסת ההפעלה המדינתית בנושא

51 Singapore's Cyber Security Strategy (2016).

52 סיבוני ואסף, עמ' 22-23.

53 ראו:
Charles Mclellan, "Cybercrime and cyberwar: A Spotter's Guide to The Groups That Are Out to Get you", **Special Report, Cyber war and The Future of Cybersecurity** (September 2016), p. 4; Lior Tabansky, "Cybercrime: A National Security Issue", **Military and Strategic Affairs**, 4, no. 3 (December 2012).

54 רב-ניצב (בדימוס) יוחנן דנינו.

צריכה להתייחס גם לאירועי סייבר פליליים, במיוחד נוכח העובדה כי גם אירועים מדינתיים, יטופלו ברוב המקרים כאירוע פלילי. יתרה מזו, אירועים רבים הנוגעים לחוסנה של מדינת ישראל בתחום הסייבר הם אירועים פליליים. על הרשות הלאומית להגנת הסייבר לתת לאירועים הללו מענה בתחום ההגנה, ועל המשטרה לפעול לאיתור העבריינים מחוללי האירועים - כך שמדובר אפוא בשני צדדיו של אותו מטבע.

עוד מסרה המשטרה כי היא תפנה למטה הסייבר הלאומי כדי ללמוד את תפיסתו בנוגע לפעילות מערך הסייבר שלה ולממשקים בינה לבין המטה.

בתשובתו למשרד מבקר המדינה מסר המשרד לבט"פ, כי הוא "רואה בחיוב יצירת מאמץ משולב בתחום הסייבר - וימשיך לקדם ולהעמיק את שיתופי הפעולה עם כלל הגורמים הרלוונטיים, לרבות משטרת ישראל, משרד האוצר ומערך הסייבר הלאומי". מטה הסייבר הלאומי מסר בתשובתו למשרד מבקר המדינה מדצמבר 2016 כי במסגרת חיזוק יכולות ההתמודדות עם פשיעת סייבר, הוא היה שותף לעבודת מטה שמטרתה לתמוך ביכולות אכיפת החוק. כך לדוגמה, פעל מטה הסייבר הלאומי לבניית הכוח של יחידת הסייבר בפרקליטות המדינה ולהגדרת תפקידיה וממשקיה.

משרד מבקר המדינה מעיר למשטרה ולמשרד לבט"פ כי ראוי שעבודת המטה שמבצעת המשטרה ויישומה בכל הקשור למבנה המערך, להפרדת תחומי האחריות של גוף המטה ולתפיסת ההפעלה - ייעשו לאחר בחינת הידע המקצועי הקיים במטה הסייבר הלאומי, ואחרי שיוודאו כי השינויים המתוכננים נעשים בהתאם למאפייני פשיעת הסייבר המתוחכמת טכנולוגית.

משרד מבקר המדינה מעיר כי על המשרד לבט"פ יחד עם המשטרה ובשיתוף מטה הסייבר הלאומי ומשרד האוצר, לפעול בהקדם כדי למצות את מלוא הפוטנציאל, הידע והמשאבים הלאומיים הקיימים, לטיפול מיטבי באיומי פשיעת הסייבר, מתוך ראייה לאומית כוללת של האיומים.

סיכום

ההתפתחויות במרחב הסייבר האיצו את התרחבות הפשיעה המתוחכמת טכנולוגית שכוללת עבירות נגד מחשבים, טלפונים חכמים, שרתים ורשתות מחשבים וכן שימוש הולך וגובר בתוכנות זדוניות, בחדירה לא חוקית למחשבים ולמאגרים ממוחשבים, בריגול עסקי וכדומה. פשיעה זו אינה תחומה בגבולות גאוגרפיים, והיא בעלת השלכות ברמה הלאומית וברמה הבין-לאומית. ממצאי דוח זה העלו שהמשטרה והמשרד לבט"פ הקימו אמנם מערך לטיפול בעבירות סייבר, אך לא התאימו את המערך לצרכים ולאתגרים של עבירות הסייבר מתוחכמות טכנולוגית שמתפתחות ומשתנות במהירות רבה. עבודת מערך הסייבר, שייעודו לטפל בעברות סייבר מתוחכמות טכנולוגית, מנותבת בעיקר לסיוע טכני ליחידות חקירה מחוזיות המטפלות בעבירות "קלאסיות" שאינן מתוחכמות טכנולוגית, על חשבון התמקצעות בלוחמה בפשיעת הסייבר.

ממצאיו של דוח זה מלמדים על כך שהמבנה הפיקודי המבוזר של מערך הסייבר, היעדרה של יחידה מרכזית והפרדת תחומי האחריות של גוף המטה למישור טכנולוגי נפרד מהמישור החקירתי - אין בהם כדי לתת מענה הולם לאתגרים שעמם נדרשת המשטרה להתמודד במסגרת הלחימה בפשיעה זו. תפיסת ההפעלה של המערך טעונה תיקון, שכן היא גובשה בהתאם למצב הפשיעה והאתגר הטכנולוגי שהיו בשנת 2000, ולא בהתאם למאפייניה הייחודיים של פשיעת סייבר שהתפתחו דרמתית מאז. אף על פי שחל גידול ניכר בהיקף פשיעת הסייבר המתוחכמת טכנולוגית בשנים האחרונות, חל קיצוץ של ממש במענה התקציבי שהופנה לתחום זה במשטרה, באופן שאינו עונה על הצורך הבסיסי של המערך. קיצוץ זה מונע את ההתעצמות הנדרשת לשם התמודדות עם פשיעה זו, ואף גורם ל"בריחת מוחות" מהמערך. לפיכך, במועד סיום הביקורת המשטרה אינה ערוכה להתמודדות עם עבירות פשיעת סייבר מורכבות טכנולוגית.

ממצאי הדוח מעידים כי המשטרה נמצאת בפיגור ניכר בהתמודדות עם פשיעת סייבר מורכבת טכנולוגית. המשך פעילות המשטרה במתכונתה הנוכחית עלול להרחיב את הפערים במענה הניתן לפשיעה זו. מתשובות המשטרה עולה אמנם כי קיימות תכניות עתידיות לחיזוק יכולותיה בתחום פשיעת הסייבר, תכניות שהינן בעלות השלכות רוחב מורכבות ושיבשילו לאורך זמן. יחד עם זאת נדרשת פעולה נוספת כדי לענות על הליקויים שהועלו בדוח זה. על המשטרה ועל המשרד לבט"פ לפעול לתיקון הליקויים וליישום ההמלצות שהועלו בדוח בהקדם וללא דיחוי כדי להתאים את פעילות מערך הסייבר במשטרה לעולם רווי טכנולוגיות מתקדמות ולאתגרים שבפניהם תעמוד המשטרה בשנים הקרובות.

התמודדות עם פשיעת הסייבר היא אתגר לאומי המחייב את המשטרה ואת המשרד לבט"פ לבסס תפיסה אסטרטגית רלוונטית למאפייני פשיעת הסייבר המתוחכמת טכנולוגית, ולהעצים במידה רבה את יכולותיה הטכנולוגיות של היחידה הארצית במשטרה. כל זאת בשיתוף מטה הסייבר הלאומי ותוך כדי בחינת הידע המקצועי בעולם.