

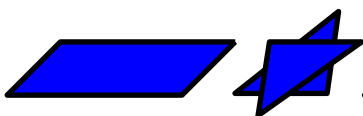


המכללה לביטחון לאומי
מחזור מ"ו, 2018-2019

קורס משפט ציבורי –
מטלת סיום
חוק הסייבר במדינת ישראל

מגיש: אל"ם יהודה אלמקייס
מנחה אקדמי: פרופ' סוזי נבות

פברואר 2018



תוכן עניינים

עמוד

1.....	מבוא
1.....	פרק ראשון - הסייבר במרחב הלאומי – רקע
2-3.....	פרק שני - הבסיס המשפטי לפעילות מערך הסייבר הלאומי
3-10.....	פרק שלישי - תזכיר חוק הסייבר (20.6.18)
11-12.....	פרק רביעי - ביקורת ציבורית על חוק הסייבר הישראלי
13.....	סיכום
14-15.....	רשימת מקורות

עבודה זו תתמקד בעיקרה בסקירת תזכיר חוק הסייבר הישראלי לצורכי היכרות ולמידה. בסופה תנסה להביא עמדות מנוגדות המבקרות את תזכיר החוק והטוענות לחוסר מידתיות ולפגיעה בזכות הפרט לשם איזון ההסתכלות על החוק ובעיקר משום שסביר להניח כי מתח זה רק צפוי להתגבר ככל שהדיגיטציה תתפוס מקום נרחב יותר בחיינו.

הסקירה תתייחס לתזכיר החוק מיוני 2018, זה הנמצא בשיח ציבורי ער ובסבב הערות והתייחסויות טרם אישור ועדת השרים לחקיקה והצבעה בכנסת. תזכיר חוק זה, עורר ומעורר שיח ציבורי ביקורתי ונרחב, העשוי להפוך את הדיון בעבודה זו לרלוונטי יותר.

תזכיר החוק נועד לממש את החלטות הממשלה שנצטברו בנושא היערכות הסייבר הלאומית תחת חוק בחקיקה ראשית. החלטות אלו, אשר התקבלו בתהליך הדרגתי וכחלק מבניית ועיצוב מתמשך של המעורבות המדינתית בתחום הסייבר בעשור האחרון מהוות חלק מתהליך הלמידה וההתמודדות, המתרחשים במדינות המערב והממוקדים בחקיקה פנימית.

יש לציין, כי מתנהלים ויכוח ומאבק דיפלומטי בינלאומי באשר לגיבוש הסכמים וחקיקה בינלאומית בתחום הסייבר. מדינות המערב מתנגדות לחקיקה בינלאומית, שמא זו תכובד רק מצדם ותצר את צעדיהם ומדינות המזרח ובראשן רוסיה וסין פועלות, ככל יכולתן, כדי לקדם הסכמים בינלאומיים וחקיקה בנושא זה. על כן, מתקיימים שיתופי פעולה במסגרת התארגנויות בינלאומיות ממוקדות, אך לא כלליות, בהן שותפה על פי רוב גם מדינת ישראל. בדו"ח הפורום הכלכלי העולמי לשנת 2018 נקבע כי סייבר הוא אחד מחמשת הסיכונים הגדולים בעולם (פורום הכלכלי, 2018).

פרק ראשון - הסייבר במרחב הלאומי – רקע

לתחום הסייבר נודעים הקשרים מדינתיים - הן אזרחיים והן צבאיים. **חוק הסייבר מתמקד בהיבטיו האזרחיים של החוק** כאשר לצה"ל מערך הגנת סייבר עצמאי, הממוקד במערך איומים נפרד ובעל אתגרים ודרכי התמודדות המתאימים לו.

על כן, מתמקד חוק הסייבר במרחב האזרחי – הפרטי והממשלתי והם אלו הנמצאים במוקד **תפיסת ההגנה**. רוב רובו המכריע של המרחב מבוסס על תשתיות, מערכות טכנולוגיות אזרחיות, המופעלות על ידי ארגונים אזרחיים.

ניהול הסב"ר (הסביבה הרשתית) עומד בבסיס תהליכי הליבה של הארגון האזרחי, הן התהליכים העסקיים והן התפעוליים ורק הארגון יכול לשאת באחריות להגנה על עצמו. עם זאת, **הנחת העבודה הלאומית הבסיסית היא כי אין בכוחו של הארגון הבודד להעמיד את המומחיות והמשאבים הנדרשים כדי להתמודד עם מגוון האיומים האפשריים** ובפרט כאשר מדובר בתוקף מתוחכם ובדגש על תוקף מדינתי.

הנחת עבודה זו, מהווה בסיס להבנה היסודית כי נדרש **שיתוף פעולה וסיוע של הממשלה לארגונים במשק ובין הארגונים כמרכיב מרכזי בהגנה על מרחב הסייבר**. זוהי גישה רווחת בקרב מרבית המדינות המפותחות.

פרק שני - הבסיס המשפטי לפעילות מערך הסייבר הלאומי

1) הבסיס המשפטי לפעילות מערך הסייבר הלאומי מבוסס על **התוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים** התשנ"ח-1988 ועל החלטות הממשלה בנושא.

2) תזכיר החוק שפורסם נועד **לממש את החלטות הממשלה ולהשלים את מהלך הקמתו של מערך הסייבר הלאומי כחלק מתהליך התפתחות הידע והרגולציה בתחום**, בארץ ובעולם, בשנים האחרונות.

3) **החלטות ממשלה קודמות בנושא :**

- החלטה מספר 3611, מיום 07.08.11, בנושא "קידום היכולת הלאומית במרחב הקיברנטי" בה הוחלט על **הקמת המטה הקיברנטי הלאומי במשרד ראש הממשלה**. על המטה הוטל לקדם היערכות לאומית להגנת הסייבר ולגבש תפיסת הגנה לאומית במרחב הסייבר.

- החלטה מספר 2443, מיום 15.02.15, בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".

ההחלטה עוסקת בקידום **מדיניות אחידה ומסונכרנת בתחום רגולציה בהגנת הסייבר** וכן ריכוז המאמצים הממשלתיים להגן על הממשלה עצמה.

- החלטה מספר 2444, מיום 15.02.15, נושא "קידום ההיערכות הלאומית להגנת הסייבר".
 ההחלטה עוסקת בהקמה של מערך הסייבר הלאומי לצדם של גופי הביטחון והרגולציה הקיימים, כפועל יוצא של שני עקרונות בתפיסה שאישרה הממשלה :
 - הצורך בפיתוח דיסציפלינה חדשה, העוסקת בממשקים שבין המדינה לבין ארגונים בתחום הגנת הסייבר כדיסציפלינה ייחודית.
 - הצורך לייחד מאמץ לטיפול בתקיפת סייבר, הכללתה ומניעת התפשטותה מחד גיסא וטיפול בגורם התוקף מאידך גיסא.
- החלטה מספר 3279, מיום 17.12.17, בנושא "איחוד מטה הסייבר והרשות הלאומית להגנת הסייבר לגוף אחד – "מערך הסייבר הלאומי".

(4) הכוונה בהחלטות הממשלה

- החלטות הממשלה כוונו לקביעת מענה לאומי, אינטגרטיבי לשיפור מוכנותם של הארגונים במשק להגנה בסייבר באמצעות הפעילויות הבאות :
- אסדרה, תימרוץ, רישוי, הסמכה, תקינה, הסברה ותרגול.
 - היתוך מידע ומודיעין מהסכמים מסחריים, מגופי הביטחון ומהארגונים עצמם, לטובת גילוי וזיהוי של איומי סייבר טרם התממשותם וגיבוש תמונת מצב לאומית.
 - התמודדות עם אירוע סייבר בזמן אמת תוך סיוע מדינתי לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו.
 - הפעלת יכולות ביטחוניות.
 - עבודה שוטפת עם גופים מקבילים בעולם.
 - פיתוח והטמעה של תהליכים ומנגנונים רוחביים לשיתוף מידע.

פרק שלישי - תזכיר חוק הסייבר (20.6.18)

תזכיר החוק מבקש להסדיר בחקיקה את הממשקים בין מערך הסייבר הלאומי למרחב האזרחי, את הסמכויות והממשקים של מערך הסייבר עם הגורמים הביטחוניים וגם רשויות האסדרה. בתזכיר החוק חמישה חלקים :

- **הגדרות ומונחים** בתחום הסייבר.
- **פרק ארגוני** – שמטרתו לאפשר הסדרים ארגוניים ייחודיים של מערך הסייבר הלאומי כגוף ביטחוני-מבצעי-טכנולוגי בשירות הציבורי.
- **פרק אופרטיבי** – העוסק בסמכויות הנדרשות למערך לשם איתור תקיפות סייבר והתמודדות איתן.
- **פרק רגולטורי** – העוסק באסדרה לאומית ומגזרית לצורך העלאת רמת החוסן של מגזרי המשק וקובע את תפקידו של מערך הסייבר הלאומי כמאסדר הלאומי בתחום הגנת הסייבר.
- **פרק הוראות שונות** – שמטרתו הבהרות של המצב המשפטי בעניין הערכות הסייבר בארגונים, תוך התייחסות ליחס שבין הגנת הסייבר לפרטיות בארגון.

הפרק ראשון – הגדרת מונחים בתחום הגנת הסייבר

- תכלית הגדרת המונחים הייעודיים לתחום הגנת הסייבר מאפשרת את יצירתה של מסגרת משפטית לתחום הסמכויות הנדרשות באופן מוגדר.
- נתמקד בסקירת מונחי הליבה הייעודיים לתחום ההגנה הלאומית הסייבר.
- **"הגנת הסייבר"** מוגדרת בתזכיר החוק כמכלול הפעילויות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות **אבטחת מידע**.

בסיפא של הגדרת "הגנת הסייבר" נכלל גם הביטוי **"אבטחת מידע"**. זאת, על מנת לשקף את ההתפתחות של תחום הידע המקצועי בנושא זה. בעולם אבטחת המידע, הערך המוגן המרכזי היה שמירת סודיות המידע, אשר מנהל אבטחת המידע היה צריך לוודא שלא יגיע לידיים לא נכונות או למנוע את שיבושו של המידע. כיום פוטנציאל האיומים והנזק התרחב מאוד בהינתן קישוריות מפותחת. מגוון מטרות התקיפה התרחב וגם מושאי ההגנה ועל כן יש לפעול למניעת שיבוש שירותים חיוניים ופגיעה בתשתיות חיוניות (רפואה, מים, חשמל, תחבורה ועוד), ואינטרסים נוספים הנשענים היום יותר מבעבר על מערכות טכנולוגיות.

כתוצאה מכך מחייבת תפיסת ההגנה שינוי משמעותי של ניהול הסיכונים באופן שלצד קיום עקרונות אבטחת המידע המקובלים (הגנה פיזית, הגנה לוגית, הרשאות, מדיניות וכדומה) נדרש טיפול כולל וחוצה ארגון, הכולל ניטור רציף ומעמיק יותר של מערכות המידע ושל מרחב הסיכונים. זאת, על מנת לאפשר את מניעת התקיפה אם ניתן ובהינתן תקיפה לאפשר להנהלת הארגון **קבלת החלטות מושכלת ובמינימום אי-ודאות** תוך יכולת אבחון של היקף הנזק וגיבוש

משמעויות לנקיטת צעדים לצמצום הנזק ולהתאוששות מהירה ככל הניתן. שינוי זה נתפס כשינוי איכותי של הרחבת תכולת השדה המקצועי ל"הגנת הסייבר" ולא רק "אבטחת מידע", באופן שהגנת הסייבר כוללת את אבטחת המידע.

ההגדרות הנוספות בפרק נשענות בעיקרן על ההגדרות המצויות בחוק המחשבים, התשמ"ו – 1997 שהוא החוק התשתיתי במדינת ישראל העוסק במחשבים. במסגרת זו כולל חוק המחשבים את ההגדרות "חומר מחשב", חומר השמור במחשבים, וכולל רכיבי תוכנה ומידע, וכן "מחשב" (הכולל גם התקן תקשורת או רכיב נתיק שניתן לחבר למחשב) בנוסף כולל החוק את ההגדרה "שפה קריאת מחשב", קרי שפה הניתנת לקריאה וביצוע על ידי מחשבים. את המידע המצוי במחשבים וברשתות, "חומר המחשב", ניתן לחלק לשלושה סוגים מרכזיים:

סוג מידע ראשון – מידע טכנולוגי טהור שלא ניתן להסיק ממנו מסקנות על אדם – מידע אשר משקף פעילות מחשובית תפקודית בין אלמנטים שונים הנדרשים לתפקודה של מערכת המידע. ברובד זה מצוי מרחב פעולה של תוקפים לשם שיבוש הפעילות המחשובית, אך איננו מכיל בהכרח מידע או נתונים אודות אדם או גוף מזוהה או ניתן לזיהוי.

סוג מידע שני – מידע טכנולוגי טהור שניתן להסיק ממנו במישרין או בצירוף מידע אחר, מידע על אדם – מדובר במידע, אשר ניתן לגזור ממנו מסקנות או מידע אודות אדם או גוף מזוהה או ניתן לזיהוי.

סוג מידע שלישי – מידע טכנולוגי המתעד מסרים אנושיים – מסרים אנושיים חזותיים או קוליים שניתנים לפענוח בלתי אמצעי בידי בני אדם, כלומר זהו הרובד שבו אנשים מתקשרים ומתבטאים.

טרם עידן הסייבר "אבטחת המידע" עסקה בעיקר בשני סוגי המידע האחרונים. כיום, בעידן הסייבר, נוסף גם סוג המידע הראשון שהרי הגעה לכל סוג מידע משמעה השגת נגישות למערכת הארגונית ונגישות זו מגלמת פוטנציאל תקיפה וחדירה לנכסי הארגון. על כן, המשגת "ההגנה בסייבר" יש בה משום הרחבת ההגדרה הקיימת בנושא "אבטחת המידע" ומבלי לגרוע ממנה. הדבר מביא אותנו אל המושג המרכזי הבא.

• **"מידע בעל ערך אבטחתי"** - מידע שיש בו כדי לסייע לאיתור תקיפת סייבר, התמודדות עמה או מניעתה ובכלל זה אחד מאלה:

- (1) **סממנים** (indicators) - נתונים המצביעים על תקיפת סייבר או איום סייבר.
- (2) מידע על **חולשות** במערכות ממוחשבות, ברכיביהן, בנהלים הקשורים במערכות אלה או בתהליכים הקשורים אליהן, אשר ניתן לנצל כדי לייצר תקיפת סייבר.
- (3) מידע על תוכנות או **נוזקות** שמטרתן יצירת תקיפת סייבר או גרימת נזק.
- (4) מידע על **שיטות ואמצעים** לביצוע תקיפת סייבר.
- (5) מידע על **שיטות ואמצעים** להתמודדות עם תקיפות סייבר.

מדובר בהגדרה מרכזית, העומדת במרכז **איסוף ועיבוד המידע** הנדרש בעת פעילות הגנת הסייבר. הגדרה זו שואפת לכלול את כלל המידע הקיים הקשור לתקיפה אפשרית, מתהווה, בהתרחשות או שאירעה וכן ביחס לקיום שיטות תקיפה, זיהוין ואופן ההתמודדות עם תקיפות בפועל.

הגדרה זו תשמש אותנו בפרק האופרטיבי באשר לתכלית איסוף המידע לצורך הגנה על הארגון שבו נמצא המידע ולא לצורך איסוף מידע עליו לצרכי פיקוח או אכיפה. סביב סוגיה זו נסוב ויכוח באשר להיקף סמכויות הרשות להגנה בסייבר, שיוצג בהמשך.

במסגרת תזכיר חוק הסייבר המושג **"תקיפת סייבר"** איננו מוגדר על אף שימוש מרובה בו בגוף החוק (24 פעמים) ולצורך העניין והמשך העבודה נציע את ההגדרה הבאה: **"תקיפת סייבר** נועדה לבטא את טווח המעשים של ניצול לרעה של מחשב או מידע ממוחשב באמצעות מחשב".

הפרק השני – פרק ארגוני

מטרתו לאפשר הסדרים ארגוניים יחודיים של מערך הסייבר הלאומי כגוף ביטחוני-מבצעי-טכנולוגי בשירות הציבורי הכפוף לראש הממשלה. פרק זה מגדיר את ייעודו ותפקידיו של מערך הסייבר הלאומי ואת מנגנוני הפיקוח והבקרה הפנימיים.

מערך הסייבר הלאומי הינו גוף ממשלתי, ביטחוני שייעודו להגנה לאומית בתחום הסייבר תוך ביצוע פעולות **ביטחוניות, אופרטיביות ורגולטוריות** שתכליתן למנוע מהאיום להתרחש, ובהינתן התממשות האיום למזער את הנזק ולאפשר התאוששות יעילה ומהירה. מערך הסייבר הוא גוף ביטחוני-מבצעי, ולכן עובדי המערך נדרשים לזמינות למענה לטיפול בתקיפות סייבר העשויות להתרחש בכל שעה ומקום במרחב האזרחי ולקיים ממשקים גם עם ארגוני הביטחון האחרים בשגרה ובחירום. **תפקידי מערך הסייבר הלאומי כפי שמופיעים בחוק :**

(1) לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים האופרטיביים כנגד תקיפות סייבר.

(2) לקדם את יכולת ההתמודדות של ישראל עם תקיפות סייבר.

(3) לקדם מדיניות ומובילות ישראלית בתחום הסייבר בהתאם למדיניות הממשלה ולהחלטותיה.

(4) לקדם שיתופי פעולה בתחום הסייבר במישור הבינלאומי ולערוך הסכמי שיתוף פעולה בתחום הסייבר.

(5) לייעץ לממשלה וועדותיה בתחום הסייבר.

(6) לבצע כל תפקיד אחר בתחום הגנת הסייבר שיקבע ראש הממשלה.

על מנת, לממש את ייעודו ואחריותו מפעיל מערך הסייבר הלאומי את **המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר** (CERT – Computer Security Response Team) הפועל באופן רציף 24/7/365 למול כלל הארגונים במדינת ישראל ממשלתיים ופרטיים, מול ארגוני הביטחון הרלוונטיים ולמול שותפים ותעשיות בעולם. ה-CERT מוגדר כמתקן המחויב ב"רציפות תפקודית" מלאה בשגרה ובחירום שכן זמינותו מתחייבת ביתר שאת וביחס ישר למתיחות הביטחונית.

במסגרת פרק זה מוגדרים אופן מינוי ראש מערך הסייבר הלאומי ותפקידיו ושאר המועסקים במערך הסייבר. ניתנת **החרגה** במסגרת החוק להעסקת בעלי תפקידים נדרשים על פי תקנות אחרות מאלו החלות בשירות המדינה לאור **צורך במומחיות מיוחדת** (סעיפים 5א,ב). כמו כן, מוגדרת גם חובת הסודיות החלה על עובדי המערך הן משיקולי **הגנה בסייבר** והן **כהגנה על פרטיות** מידע אליו נחשף העובד במסגרת עבודתו.

כדי להתמודד עם המתח הקיים בין הצורך בהגנה ונגישות ל"מידע בעל ערך אבטחתי" אשר הוגדר קודם, חויב ראש מערך הסייבר במסגרת החוק במינוי **מפקח פרטיות פנימי** במערך האחראי על יישום הוראות **חוק הגנת הפרטיות** במערך והמחויב בביצוע תהליכי איכות המוגדרים בחוק בהקשר לביצוע תפקידו כגון: הכנת תכנית עבודה, ביצוע הכשרות, בירור הפרות, הגשת דוחות שנתיים ועוד וכן מוגדרות בחוק סמכויותיו המוגדרות לפי סעיף 15 לחוק הסדרת הביטחון בגופים ציבוריים, תשנ"ח-1988 (סעיף 12). המפקח יזכה להגנה תעסוקתית ולא ניתן להפסיק את כהונתו ללא התייעצות עם רשם מאגרי המידע על פי חוק הפרטיות, הוא יונחה מקצועיות על ידי הרשם ותובטח אי העמדתו של המפקח בניגוד עניינים.

ראש הממשלה, שהינו השר הממונה על מערך הסייבר הלאומי מחויב על פי תזכיר החוק במינוי **ועדה מפקחת לעניין השפעת הפעילות על הזכות לפרטיות** במערך הסייבר הלאומי. בראש הוועדה יעמוד **שופט בדימוס**, נציג היועץ המשפטי לממשלה, נציג ציבור בעל מומחיות בנושא הגנת הסייבר וביטחון מדינת ישראל, נציג ציבור בעל מומחיות וניסיון מובהקים בתחומי זכויות אדם והגנת הפרטיות, מזכיר הוועדה הינו ראש מערך הסייבר הלאומי. הוועדה תגיש **דין וחשבון שנתי** לראש הממשלה באשר לאירועים שבהם עלה **חשש להפרת הוראות החוק** בתחום הפרטיות בידי עובד המערך או מטעמו וכן ממצאים באשר לקיומן ומימושן של הנחיות פנימיות בתחום ההגנה על הפרטיות ועצם מימושן. לוועדה יש סמכויות נרחבות באיסוף מידע ומסמכים, זימון כל אדם רלוונטי להופיע בפניה וכן במקרה של חשש להפרת דין בסמכותה של הוועדה להעביר את המשך הטיפול לגורם המוסמך לכך.

פרק שלישי – פרק אופרטיבי

פרק זה עוסק בסמכויות, הנדרשות למערך, לשם איתור תקיפות סייבר והתמודדות איתן. הבסיס התפיסתי להבניית הפרק האופרטיבי נעוץ בהבנה כי נדרשת מעורבות של המדינה באיתור תקיפות סייבר בארגונים במרחב האזרחי והכלתן הן לשם הגנה על הארגון הנתקף, צמצום הנזק והמשך תפקודו אך גם בכדי להפיק לקחים ולצמצם את הסיכון לאינטרס הציבורי.

הפרק מתבסס על פעילויות הגנת סייבר מקובלות בעת חשש או איתור תקיפה. במקרה כזה, פעילויות האיתור וההגנה נדרשות להתבצע ברשת הארגון שבו מתרחשת התקיפה משום שתקיפה בסייבר מתאפיינת ביצירת תשתית נגישות ברשת הנתקפת. בתקיפה אופיינית, התוקף משתמש בתקשורת המקשרת את הארגון אל החוץ או בקישור לא תקני אל תוך רשת הארגון ופועל לניצול חולשה לצורכי חדירה והשגת נגישות. תקיפות סייבר מבוססות על ניצול חולשות טכנולוגיות, חלקן אופייניות לכלים הסטנדרטיים בהם משתמש הארגון וחלק מהחולשות נובעות מטעות הנעשית ברשת הארגון אותה מנצל התוקף. באמצעות הנגישות שהשיג התוקף (Lockheed Martin, 2010), מתקין התוקף את כלי השליטה הזדוני המאפשר לו שליטה והפעלה מרחוק אם בתצורת "כפתור אדום" עליו ילחץ ביום פקודה ואם בתצורת איסוף מידע על הארגון.

התוקף נוהג להסוות את ערוץ הנגישות שבנה בינו לבין התקשורת התקנית של הארגון כך שלא יתגלה. שתי פעולות חיוניות הנגזרות מהמתואר לעיל : הראשונה, הארגון נדרש לניטור מערכותיו ולעדכון כלי ההגנה שברשותו כל העת כך שיוכל לאתר תוקף ולסכל תקיפה הן מבעוד מועד או בהתרחשותה והשנייה היא הצורך בקיומו של גוף סיוע חיצוני מקצועי לאור המצאו של תוקף מתוחכם, שכבר הצליח או מנסה לעבור דרך מערכי ההגנה של הארגון. הגוף החיצוני לא רק יסייע בהתאוששות, אלא יוכל לנהל חקירה פורנזית באשר לסיבות לחולשה שנוצרה בכלי או בתשתית הארגונית וכן לפעול לטיפול בחולשה וחיסון הארגון מפניה. כמו כן, יפעל להערכת הנזק בהקשרי דלף מידע אישי והפקת לקחים לאומית להמשך בכדי להבטיח מניעת הישנות המקרה בגופים נוספים.

פעילות המדינה, באמצעות מערך הסייבר הלאומי ברשתות הארגון הינה מהות ההסדרה המבוצעת בפרק זה במסגרת תזכיר החוק להגנת הסייבר ומערך הסייבר הלאומי. פונקציית המטרה של הפרק האופרטיבי היא טיפול בתקיפה ממוחשבת, בשונה מהקשרים אחרים בהם המדינה מפעילה סמכות כנגד ארגונים במקרה זה המדינה הופכת לגורם פעיל המסייע לארגון. בכדי לסייע לארגון, המדינה נדרשת לגישה לרשתות הארגון ועשויה להיחשף למידע אחר כנזק אגבי אפשרי ולא כמטרה הגנתית. בכך שונה פעולת מערך הסייבר מפעולת רשויות האכיפה והביטחון, במקרה זה הראיות הינן ראיות טכנולוגיות פורנזיות העומדות בהגדרה של "מידע בעל ערך אבטחתי".

על הרקע המדובר, עוסק הפרק בעקרונות כלליים המסדירים את הפעלת הסמכות ושיקול הדעת לעניין פעולות ההגנה הנדרשות. הפעלת הסמכות מוסדרת בהתאם לעקרונות המיידיות: קרי –

1. לאחר בחינה כי האמצעי אכן נדרש.
 2. ננקט האמצעי שפגיעתו היא הפחותה ביותר ביחס לטיפול בתקיפה.
 3. הסיכון לזכות לפרטיות ולתפקודו של הארגון נמוך מהתועלת שבפעולה.
- מרכיב מרסן נוסף בהקשרי המיידיות הוא עקרון פעולה שמעורבות המערך כמעורבות חיצונית תבוצע אך ורק במקרה בו הארגון אינו מסוגל בעצמו, לאתר את התקיפה במדויק או להתמודד עמה, להכיל את הנזק, קרי לצמצם או למנוע אותו ולהתאושש תוך יכולת הפקת לקחים. למול אמירה זו חשוב להבין את האינטרס הציבורי והלאומי. גופים מסוגים לא מעטים, בנקים כדוגמא, עשויים לשאוף שלא לדווח על אירוע אלא להכיל אותו גם במחיר של תשלום כופר לתוקף או נזק כלכלי שאיננו מבוטל על מנת שלא לאבד את אמון לקוחותיהם. במקרה כזה התוקף וכלי התקיפה עשויים להישאר רלוונטיים ולעבור לבנק הבא. על כן, לא ניתן להגדיר מרכיב זה כעקרון פעולה קבוע ומחייב ולכל מקרה דרוש עיון כשלעצמו.
- לאור האמור, קיימת חשיבות לאיתור מהיר של שיטת התקיפה וכן שיתוף מידע לאומי ובין-לאומי למול שותפים בדבר סוגי התקיפות והטיפול בהן למול איתורן המוקדם ככל הניתן (NIST, 2018). שיתוף זה בונה את החוסן הלאומי ואת החוסן הבינלאומי בין שותפים, שיתוף זה מוכיח עצמו כיעיל (ENIS, 2016).

שלב חיוני לבניית החוסן והחיסון הלאומי בסייבר הוא שילוב המידע המצטבר עם גופי הביטחון ליצירת תמונת מצב לאומית לשם מתן דוח שנתי לראש הממשלה בנושא הגנת הסייבר הלאומית המהווה בסיס לקביעת המדיניות הלאומית (פרק ב', סעיף 4ה') וכן לפיתוח ולהטמעה של תהליכים ומנגנונים שיטתיים ורוחביים לשמירת ולחיזוק החוסן הלאומי בתחום ההגנה למול התחזקות קבועה של התוקפים.

במטרה לממש מדיניות זו, המהווה מגמה משותפת בקרב המדינות המפותחות (OECD, 2015) המהווה חלק מחוסן הלאומי, הביטחוני והכלכלי של מדינות אלו, מחוייבת כל מדינה באירופה להקים מרכז CERT (CERT – Computer Security Response Team), מרכז פיקוח לאומי, המרכז מידע אודות חולשות, תקיפות ושיטות התמודדות בזמן-אמת, תוך שיתוף במידע זה בהקדם האפשרי עם המרחב האזרחי (NIST, 2018 עדכון).

על כן, התקבלה החלטת ממשלה 2444 משנת 2015 על הקמת CERT הלאומי (הרשות להגנת הסייבר, 2015). פעילותו החוקית הוסדרה בהתאם למסגרת משפטית שגובשה עם היועץ המשפטי (הרשות הלאומית להגנה בסייבר, 2015) לממשלה בכדי להבטיח מידתיות בהקשרי זכויות הפרט והגנה על עקרונות "אבטחת המידע" בעידן הסייבר. בהחלטה הוגדרו עקרונות אשר מופיעים כיום בתזכיר החוק, על כן משונה בעיני התרעומת האזרחית עם פרסום תזכיר

החוק שהרי אינני מזהה רגרסיה כלשהי במידתיות בהקשרי זכויות הפרט (קנין, פרטיות) בין החלטות הממשלה ובין תזכיר החוק. להלן ארבעת העקרונות המובילים בהחלטת הממשלה :

1. **אבחנת סוג המידע** הנאסף ובידולו ממידע אודות אדם או גוף.
 2. הגבלה על השימוש במידע **לצרכי הגנת הסייבר**.
 3. הבניית **שיקול דעת מנהלי** בעת איסוף מידע, שמירתו, עיבודו והפצתו תוך שמירה על חוק הפרטיות (התשמ"א – 1981).
 4. מינוי **מפקח פרטיות פנימי וועדה מפקחת** לעניין השפעת הפעילות על הזכות לפרטיות (מופיעים גם בתזכיר החוק, פרק ב' סעיף 10, 13).
- עיקר פעילות המערך מבוססת על ההנחה בדבר קיומה של **זהות אינטרסים** בין הרשות הלאומית להגנה בסייבר והארגון הנתקף, אך לא ניתן לומר זאת באופן גורף כפי שפירטתי מעלה בדוגמא על תקיפת בנק ועל כן בתזכיר החוק חויבו גופים מפוקחים אשר יוגדרו בפרק הרגולציה **בחובת דיווח** לרשות הלאומית להגנה בסייבר (תזכיר החוק, סעיף 52, סעיף 6/45).

הפרק רביעי – פרק רגולטיבי

מטרת הפרק היא הסדרת התחום תוך קביעת מדיניות אחידה ואיזון בין עוצמת האיום בתחום הסייבר ובין האינטרסים הציבוריים והמשקיים, על פי רוח זו נקבעו באסדרה **4 עקרונות** על (סעיף 42):

1. התאמה לתקינה בינלאומית מקובלת או נהוגה במדינות מפותחות.
2. התאמה ייחודית לישראל רק במידת הצדקה.
3. באסדרה מגזרית – התאמה למאפייני המגזר והארגונים השונים בו.
4. הלימה בין האיום לארגון לאופן ההסדרה.

כפי שניתן לראות מעקרונות העל, מתקיים רצון לרגולציה הכרחית בלבד בכדי לאפשר את הפחתתו של **הנטל הרגולטורי** ולייצר מסגרת התמודדות אפקטיבית ומאוזנת. ניכר, כי מתקיימת פתיחות רגולטיבית ויכולת **ערעור על החלטות** בכדי למנוע מצבים של פגיעה לא בארגון כזה או אחר במשק (סעיף 44ג).

הרגולציה מתבצעת בפועל באמצעות הנחיות מחייבות בתחום ההגנה בסייבר שמפרסמת הרשות הלאומית להגנה בסייבר למגזרים השונים ומתעדכנות מעת לעת בהתאם להפקת לקחים והתפתחות תחום התקיפה בסייבר וכן תחום ההגנה בסייבר. במסגרת הנחיות אלו מפורסמת **מדיניות ונהלי התמודדות, שימוש באמצעים מקובלים** תוך זהירות מקידום עסקי של כלי הגנה פרטי כזה או אחר, **מצבי הכוונות** המהווים שפה משותפת בין הרשות לבין הארגונים השונים באשר ל-"גובה החומות" ההגנתיות תחת התראה בעלת חומרה וסבירות המוערכות ברשות, **אופן**

ותדירות בדיקה עצמית של רמת ההגנה הארגון באמצעות 'בדיקת חדירות' ואופן הדיווח על תקיפות או איומי סייבר.

במסגרת הרגולציה מחויבת הרשות הלאומית להגנה בסייבר לבצע **מיפוי של המרחב האזרחי** כדי להעריך את **חומרת הפגיעה** באינטרסים חיוניים למול קריטריונים אשר הוגדרו בחוק – היקף פגיעה אפשרית בחיי אדם, גודל הציבור המשתמש בשירותי הארגון, נזק כלכלי צפוי, היקף המידע בידי הארגון ורגישותו, השפעה על תפקוד שירותי המחשוב והאינטרנט בישראל והשפעה על גורמי ייצור, משאבים, שירותים החיוניים לקיום האוכלוסייה ולכלכלת המדינה **בשגרה בחירום**.

נקודה ראויה לציון, כי בניגוד ליחסי הגומלין בין צה"ל למשרד התקשורת בו צה"ל מעורב בניהול התקשורת במדינת ישראל ובעל סמכויות גוברות במצב חירום בהקשרים מסוימים. בנושא הסייבר צה"ל איננו גורם המוזכר בחוק ולהערכת נתפס בעיני הרשות כמשאב מסייע, 'כוח התערבות' וכגורם דומיננטי בהערכת המצב המודיעינית במקרה הצורך. זהו שינוי משמעותי ביחסי צבא-חברה המעידים על תחושת מסוגלות טובה ביחס ליכולת ההתמודדות העצמאית של הרשות להגנה בסייבר בחירום.

כדי לוודא את מימושו של החוק על ידי הארגונים מגדיר תזכיר החוק (סעיף 54) את **התניית מתן או חידוש רישיון לארגון** ביכולתו להראות יישום אפקטיבי של המדיניות והנהלים באמצעות הצהרה עצמית, חוות דעת מקצועית או סקר אבטחה מקצועי. כמו כן, לרשות סמכות פיקוח לצורך אכיפת ביצוע ההוראות בחוק ובמסגרת זו מוסמכת הרשות להתלות, להגביל או לבטל רישיון בגין הפרת הוראות.

החוק מגדיר את **הארגונים המפוקחים ומונחים באופן ישיר** על ידי הרשות להגנה בסייבר בכפוף לשלושה קריטריונים ברורים :

1. הארגון חשוף לתקיפות העשויות לגרום לפגיעה באינטרס חיוני.
2. אין רשות מאסדרת בעלת סמכות, משאבים ויכולת להנחות את הארגון.
3. מתקיים חשש סביר (למול סעיף 1).

סמכויות הפיקוח על ארגונים המפוקחים באופן ישיר הינה נרחבת ביחס למידע על כל אדם בארגון, מסירת כל ידיעה ומידע **הרלוונטי לעניין ההגנה בסייבר** ואפשרות כניסה לכל מקום בארגון הרלוונטי לתחום.

לסיכום, הפרק עוסק במכלול **הפעילות הממוקדת במניעה ובהיערכות למתקפות סייבר** על יסוד מנגנוני הנחיה **ישירה ועקיפה** ברמה הלאומית והמגזרית, בכדי לאפשר למדינה את שמירת וחיזוק חוסנה המשקי. לאסדרה בתחום הסייבר ממד מובהק של **ביטחון לאומי** והצורך במסגרת רגולטיבית, גמישה להתאמות בהתאם לנסיבות המשתנות במהירות הינו מובהק למול צורך מובהק לא פחות באי הכבדה על הפעילות הכלכלית והעסקית במדינת ישראל.

ההיצמדות לשיטות פעולה ונהלים בינלאומיים הנהוגים חלקם במדינות ה-OECD, באירופה ובארצות הברית מהווה גורם מאזן, מרסן ומידתי למניעת חוסר איזון בין האיום לחוק ההגנה.

פרק רביעי - הביקורת הציבורית על חוק הסייבר הישראלי

פרסום תזכיר חוק הסייבר עורר גל של תגובות הנוגעות לפגיעה בזכות הפרטיות תוך הצפת טענות שונות. הטענות משקפות חשש ליברלי טיפוסי ומקובל במדינה דמוקרטית, אך בעבודה זו משמעותי לנסות להצדיק או להפריך טענות אלו מתוך נקודת מבט חיצונית על טענות אלו תוך חיפוש האיזון בין חשיבות ההגנה, המגבלות המקצועיות ומעל לכל הזכות לפרטיות. ראשית, רוב תחילתו של הגל, דווקא עם פרסומו של תזכיר החוק. תזכיר החוק מצוי בהלימה מלאה להחלטות הממשלה, אשר התקבלו בשנים האחרונות ואין בו כדי להחמיר את המתח בין ההגנה לזכות לפרטיות, אך כנראה בחברה המעבר מהחלטת ממשלה לחוק נתפסת בציבור כמהלך משמעותי.

טענת, תהילה שורץ מהמכון הישראלי לדמוקרטיה היא ש-"(...) אין מגבלות מספקות על השימוש במידע שנלקח – לכמה זמן מותר לשמור אותו? האם אפשר להעביר אותו אל המשטרה? אל גורמים נוספים?".

ניתן לומר על כן, שאיסוף המידע הוא הכרחי לצורכי חיסון מפני פוגעני סייבר וביצוע תחקור פורנזי של הראיות כפי שמבוצע בכל זירת פשע, ממד הסייבר הינו ממד יציר אדם אך עדיין כזה שמתקיימת בו התרחשות כמו התקפה, הגנה, אינטראקציות עסקיות ופשעים. תזכיר חוק הסייבר מניח מספר הגבלות כדי לוודא עמידה בטענות אלו:

1. מינוי **מפקח פרטיות פנימי** ליישום חוק הגנת הפרטיות במערך לרבות הגדרת תפקידיו וסמכויותיו.
2. מינוי **וועדה מפקחת** על מערך הסייבר הלאומי לעניין השפעת הפעילות על הזכות לפרטיות ובראשות שופט בדימוס.
3. מתן **סמכות** לוועדה המפקחת להעברת מידע להמשך טיפול במידה ועולה חשש להפרת הדין.
4. הגדרת **עקרונות מידתיות** להתערבות רק במקרה של: חיוניות האמצעי, נקיטה באמצעי שפגיעתו הפחותה ביותר ושהסיכון לזכות הפרטיות נמוך מהתועלת שבפעולה.
5. הוגדר איסופו של **מידע בעל ערך אבטחתי** בלבד (סעיף 17ג').
6. דרישת מידע ומסמכים **הוגבלה** רק לנדרש לצורך איתור תקיפת הסייבר או מניעתה (סעיף 20).
7. אין לתפוס חפץ מבלי לתת למחזיק בו **הזדמנות להשמיע טענותיו** ורק במידה ויש סכנה ממשית ומידית לשלום הציבור או בטחונו אזי רשאית הרשות להגנה בסייבר לתפוס את החפץ (סעיף 23ב')

8. במידה ונתפס החפץ יש להחזירו בתום בדיקה ולא יאוחר **מחמישה עשר ימים**, הארכת תקופה זו הינה רק בסמכות בית המשפט(סעיף 23ד).
9. "המידע שנמסר למערך ההגנה בהסכמה **לא ישמש כראיה** כנגד מוסרו בהליך אזרחי, מנהלי או פלילי" (סעיף 41א').
10. על המידע אודות ארגון שנמסר למערך ההגנה בסייבר יחול סעיף 9(א) לחוק חופש המידע תשנ"ח-1988 ויראו אותו **כמידע שאין למוסרו** לפי אותו סעיף.
11. כמו כן, נקבעו נהלים מחמירים ביחס **לאופן שמירתו של מידע** המשמש כראיות לחקירה.

ניתן להביא טיעונים נוספים לניסיונות ליצירת מידתיות ואיזון בין הזכות לפרטיות, חופש המידע ובין הצורך בהגנה, אך הדבר המרכזי הינו קיום **מנגנוני הפיקוח** ובראשם הוועדה לפיקוח על מימוש חוק הפרטיות, שנבנתה באופן מרשים ויושבים בה מומחים משפטיים לתחום הפרטיות לצד מומחים בתחום הסייבר ובראשם שופט בדימוס בעל שיקול דעת רחב. בראייתי המנגנון הינו מחולל האיזונים והבלמים העתידי, המרסן ובעל הפוטנציאל לתקן חריגה או עבירה באם זו התרחשה. בכל פעולה של כניסה חיצונית לארגון והוצאת חפץ או חומר יש מידה של פגיעה בקניין ובפרטיות בראיית האזרח גם אם תתבצע על פי חוק ועקרונות המידתיות המחייבים שבו על כן, נדרש **שיקול דעת מנהלי ומערכתי בכל פעולה**.

טענות דומות נשמעות גם מאיגוד האינטרנט הישראלי, הטוען להיעדר מנגנוני פיקוח ופוטנציאל לפגיעה בזכויות אזרח ועל הקמתו של ארגון ביון חדש תחת השם רשות הסייבר הלאומית. אכן, אין לי ספק כי קיים **פוטנציאל** בסוג פעילות מסוג זה לפגיעה בזכויות אזרחי וכי פעילות הגנתית-ביטחונית-מבצעית אזרחית הינה בעלת אלמנטים של ביון ומודיעין לאור הפעילות למול יריב. מאפיין זה הינו אינהרנטי וגלום בפעילות זו, אך הוא נכון בכל מדינה ובכל נקודת זמן. למרות זאת, התרשמותי על פי החוק נראה כי ישנו ניסיון כן למתן מענה ראוי לחששות אלו במסגרת החוק. על כן נדרשים רגישות מיוחדת ותהליך הפקת לקחים מתמשך ברשות להגנת הסייבר בתקופת המעצבת שבה אנו נמצאים תוך פתיחות לביקורת והעצמת מנגנוני הפיקוח.


סיכום

מרחב הסייבר מתעצב ומשתנה במהירות ואיתו גם מתודות ההגנה בממד הסייבר. לאחר מספר שנים, בהן הרשות להגנה בסייבר התגבשה ושינתה את צורתה עד למבנה הנוכחי בו היא פועלת היום וכן פעלה מתוקף החלטות ממשלה אשר התגבשו כחלק ממגמה מתואמת ומושכלת במדינות העולם המערבי הוחלט על חקיקת חוק הסייבר בחקיקה ראשית.

חשוב לציין כי ניתן להתרשם לחיוב מהפתיחות בתהליך ההתייחסות הציבורית לתזכיר חוק הסייבר והדיאלוג הענייני המתנהל לעיני כל (הרשות הלאומית להגנה בסייבר, 2018), מעיון בהתייחסות להערות ניכר כי מתבצע דיאלוג פרודוקטיבי ויסודי. לאורך תזכיר החוק, ניכר הרצון במציאת נקודת איזון נכונה הן בהקשר האופרטיבי והן בהקשר הרגולטיבי לרבות מנגנונים מרסנים ותבחינים בכל מקום בו ניתן לקיימם.

משיח בלתי אמצעי עם גורם ברשות להגנה בסייבר, עולה כי, האינטראקציה מול הארגונים הינה כזו שהרשות הלאומית להגנה נתפסת כגורם מסייע וככתובת אפקטיבית ורצויה.

החוק משיק למספר לא מבוטל של חוקים – החוק להגנת הפרטיות התשמ"א-1981, חוק חופש המידע התשנ"ח-1998 וחוק המחשבים תשנ"ה-1995 כחוקים ישראליים ומנגד מאמץ רגולציות ותפיסות ממדינות ליברליות כאלמנט מידתי המאזן בין המתחים שנסקרו בעבודה. נראה כי, רוח תזכיר החוק, המנגנונים המרסנים והשיח הציבורי יש בהם משום נקודת פתיחה טובה למימוש החוק באופן מאוזן.

1. **The Global Risks Report 2018, World Economic Forum** .1
<https://www.weforum.org/reports/the-global-risks-report-2018>
2. מערך הסייבר הלאומי, "תזכיר חוק הגנת הסייבר", 2018.
3. מערך הסייבר הלאומי, "החלטות הממשלה והחוק להסדרת הביטחון בגופים ציבוריים", 2018.
4. Lockheed Martin, Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intursion Kill chains.
<https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
5. **NIST**, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>
6. **ENISA**, <https://www.enisa.europa.eu/publications/actionable-information-for-security>
7. ENISA, A Flair for Sharing, <https://www.enisa.europa.eu/publications/legal-information-sharing-1>
8. **OECD Digital Security Risk Management for Economic and Social Prosperity**, <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>, B.1. (iii), p. 12.
9. NIS Directive, article 9 .8
<https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
10. הרשות הלאומית להגנת הסייבר, "עקרונות הפעולה של המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר", 2015.
<https://www.gov.il/he/Departments/Policies/principles>
11. המכון הישראלי לדמוקרטיה – ד"ר תהילה שוורץ אלטשולר, "מאמר דעה – חוק הסייבר", 2018.
<https://www.idi.org.il/articles/23988>
12. ארגון האינטרנט הישראלי – עומר כביר, "איגוד האינטרנט הישראלי יוצא למלחמה נגד חוקר הסייבר החדש", 2018.
<https://www.calcalist.co.il/internet/articles/0,7340,L-3744696,00.html>
13. תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018.
14. תזכיר חוק הגנת הסייבר, התשע"ח-2018, docx.

15. החלטת ממשלה מספר 3611, מיום 07.08.11, בנושא "קידום היכולת הלאומית במרחב הקיברנטי".
https://www.gov.il/he/departments/policies/2011_des3611
16. החלטת ממשלה מספר 2443, מיום 15.02.15, בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".
https://www.gov.il/he/Departments/policies/resolution_2443
17. החלטת ממשלה מספר 2444, מיום 15.02.15, נושא "קידום ההיערכות הלאומית להגנת הסייבר".
<https://www.gov.il/BlobFolder/news/govdecisions/he/2444.pdf>
18. עקרונות הפעולה של ה-CERT הלאומי.

<https://www.gov.il/BlobFolder/policy/principles/he/principles.pdf>

17. הסבר החוק להגנת הפרטיות התשמ"א-1981.

<http://www.moin.gov.il/arabic/NationalSupervision/Documents/law-haganat-privet.pdf>

18. חוק חופש המידע, התשנ"ח-1998.

<http://cms.education.gov.il/EducationCMS/Units/Hofesh/NosachHachoch/ck>

19. חוק המחשבים, תשנ"ה-1995.

<https://law.co.il/media/computer-law/computers law nevo.pdf>

20. הערות והתייחסויות גופים וארגונים לתזכיר החוק, 2018.

[#https://www.gov.il/he/departments/news/cyberlawpublic](https://www.gov.il/he/departments/news/cyberlawpublic)