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

א. שם החוק המוצע

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

ב. מטרת החוק המוצע והצורך בו

תזכיר החוק המוצע נועד לממש את החלטות הממשלה[1] (להלן – החלטות הממשלה) ומדיניותה בתחום הגנת הסייבר, ובהתאם לכך גם את ההיבטים הקשורים במערך הסייבר הלאומי וסמכויותיו. החלטות הממשלה, התפיסה שעומדת בבסיסן והניסיון שנצבר מאז קבלתן, מהווים ביחד את נקודת המוצא להוראות התזכיר.

היווצרות מרחב הסייבר היא תולדה של ההתפתחות הטכנולוגית המואצת של העשורים האחרונים, ותרומתו להתפתחות האנושית אינה ניתנת לערעור. מרחב זה מאפשר זרימה חופשית של ידע, הון ושירותים עם חסמי כניסה נמוכים מאד, ובכך הוא משפר את הרווחה החברתית ומעודד חדשנות. התבססותן של פעילויות מסורתיות רבות על מרחב הסייבר הולכת ועולה (דוגמת תשלומים דיגיטליים או שליטה ובקרה בתהליכי ייצור ותפעול), במקביל לפיתוח מתמשך של פעילויות מרכזיות חדשות באמצעותו. מהפכת המידע והתקשורת מובילה לשגשוג והתייעלות בכל תחומי החברה, החל בייצור תעשייתי, צרכנות, תיירות, תקשורת, הפצה של מידע ומסחר מקוון. כתוצאה מכך ונוכח השפעתו הנרחבת על פעילותם של פרטים, ארגונים ומדינות, הופך מרחב הסייבר לבעל חשיבות אסטרטגית.

בשנים האחרונות ניכרת עלייה משמעותית בשכיחותם של איומי סייבר ובחומרתם, בעולם כולו. מגמה זו מיוחסת במידה רבה למאפיינים הייחודיים של המרחב אשר מקלים על הפעילות העוינת בתוכו: קבועי הזמן הקצרים המאפיינים את השתנות המרחב ואת הנעשה בו, חוסר הרלוונטיות של המרחק הפיזי לפעילות במרחב, וכתוצאה מכך חשיפה לאיומים מכל העולם בסבירות דומה, האנונימיות היחסית המתאפשרת בו, היעדר כוח ביטחוני החוצץ בין התוקף לנתקף, עלות נמוכה לפיתוח יכולות פעולה במרחב ועליית "שטח הפנים" לתקיפה כתוצאה מהתרחבותו המהירה של מרחב זה. איומים אלו עלולים להוביל לפגיעה בתוך המרחב (למשל במידע או בתפקוד), לפגיעה בעולם הפיסי (למשל פגיעה במערכות רפואיות או בתשתיות אנרגיה), לפגיעה תפקודית משקית קשה, ואף לפגיעה בחיי אדם. תקיפות הסייבר הולכות והופכות מתוחכמות יותר, ותוצאותיהן קשות יותר ומורכבות יותר לטיפול. כתוצאה מכך עולה הסיכון לפגיעה בביטחון האישי, בפעילות המשק ובביטחון המדינה, באופן המחייב התייחסות ברמה הלאומית.

---

[1] בהחלטת ממשלה מספר 3611 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" מיום 07.08.2011 (להלן – החלטה 3611), הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה) והוטל עליו, בין היתר, לגבש תפיסת הגנה לאומית למרחב הסייבר. בהחלטות הממשלה מספר 2443 ("קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר") ו- 2444 ("קידום ההיערכות הלאומית להגנת הסייבר") מיום 15.02.2015 אישרה הממשלה את התפיסה שגיבש המטה.

עוד יצויין כי ביום 17.12.17 קיבלה הממשלה החלטה מספר 3270 שבה נקבע כי המטה והרשות יאוחדו לגוף אחד – מערך הסייבר הלאומי (להלן - המערך).

החלטות הממשלה משקפות תפיסת הגנה לאומית חדשה במרחב הסייבר.

העובדה כי הסייבר הוא מרחב אזרחי במהותו היא במוקד תפיסת ההגנה. רובו המכריע של המרחב מבוסס על תשתיות, מערכות וטכנולוגיות אזרחיות, המופעלות על-ידי פרטים וארגונים אזרחיים, ומכאן שמרבית האיומים במרחב זה מופנים כלפי המגזר האזרחי שברשותו מצוי גם רוב המידע על אודות המתרחש במרחב. לאור זאת ומאחר שניהול הרשתות עומד בבסיס תהליכי הליבה של הארגון (עסקיים, תפעוליים או אחרים) – רק הארגון יכול לשאת באחריות להגנה על עצמו. מנגד, מובן כי אין בכוחו של הארגון הבודד להעמיד את המומחיות והמשאבים הנדרשים להתמודדות עם מלוא מגוון האיומים שתוארו לעיל, בפרט כאשר הוא מודע רק למתרחש בגבולותיו.

מצב עניינים מורכב זה עמד בבסיס ההבנה היסודית כי שיתוף פעולה, בין הממשלה לבין הארגונים במשק ובין הארגונים לבין עצמם, יהווה מרכיב מרכזי בהגנה על מרחב הסייבר, וזו גם הגישה הרווחת בקרב רובן המוחלט של המדינות המפותחות.

בהתאם לכך, בהחלטות הממשלה נקבע מענה אינטגרטיבי: שיפור רמת הכשירות והמוכנות של הארגונים במשק באמצעות פעילויות 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 בזמן אמת עם אירועי סייבר, לרבות סיוע לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו; הפעלת יכולות ביטחוניות; עבודה שוטפת עם גופים מקבילים בעולם; פיתוח והטמעה של תהליכים ומנגנונים רוחביים לשיתוף מידע.

גם במדינות המערב מקודמת מדיניות הגנת סייבר לאומית. בשנת 2015 המליץ ה-OECD למדינות הארגון לגבש מדיניות הגנת סייבר הכוללת התמודדות עם הסיכונים למרחב הדיגיטלי[2]. באיחוד האירופי חוקקה בשנת 2016 (בתוקף החל מיום 10.5.2018)[3] חקיקה המחייבת את חברות האיחוד לגבש מדיניות הגנת סייבר, לקבוע אסדרה לתשתיות קריטיות ולהקים מרכז טיפול לאומי באירועי סייבר. בדו״ח לשנת 2018, קבע הפורום הכלכלי העולמי כי הסייבר הוא אחד מחמשת הסיכונים הגדולים בעולם[4] והמליץ להגביר את ההיערכות לאירועי סייבר.

הקמת מערך הסייבר הלאומי, לצדם של גופי הביטחון והרגולציה הקיימים, היא פועל יוצא של שתי עמדות יסוד בתפיסה שאישרה הממשלה: הצורך בפיתוח דיסציפלינה חדשה, העוסקת בממשקים שבין המדינה לבין ארגונים בתחום הגנת הסייבר, אשר אינה קיימת ככזו בגופים אחרים, והצורך לייחד מאמץ לטיפול בתקיפה ובמכלול פעילות האיתור וההכלה שלה ושל התפשטותה בארגוני המרחב האזרחי, מעבר ולצד הטיפול בתוקף. כך, התזכיר המוצע לא נועד לשנות את ייעודם או סמכויותיהם של גופים נוספים המפעילים סמכויות במרחב הסייבר בישראל בהתאם למסגרת המשפטית החלה עליהם ובכלל זה שב״כ, הממונה על הביטחון במערכת הביטחון ומשטרת ישראל.

---

[2] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

[3] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
ליישום באנגליה ראו: https://www.ncsc.gov.uk/guidance/introduction-nis-directive

[4] The Global Risks Report 2018, World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2018

מטרת התזכיר המוצע להסדיר את ייעודו, תפקידיו וסמכויותיו של מערך הסייבר למימוש מדיניות הממשלה, בהתאם לעיקרון החוקיות, תוך שילוב בין תפיסות יסוד של המשפט החוקתי בנושאים המוסדרים בתזכיר החוק לבין תפיסות של משפט וטכנולוגיית מידע.

התזכיר כולל פרק ארגוני המסדיר את מאפייניו הייחודיים של מערך הסייבר הלאומי, פרק העוסק בסמכויות הנדרשות לאיתור תקיפות ולהתמודדות עמן, ופרק העוסק באסדרה לאומית ומגזרית לצורך העלאת רמת החוסן של מגזרי המשק.

בפרק הטיפול בתקיפות סייבר, הכולל סמכויות טיפול של המערך בתקיפות סייבר, קבועות הוראות העוסקות בכלים הנדרשים לטיפול בתקיפות סייבר בארגונים ובשיתוף מידע ביחס אליהן. הפרק כולל עקרונות להבניית שיקול הדעת המנהלי בעת הפעלת הסמכות, כגון חובת מסירת מידע לארגון שבו מופעלות הסמכויות, וכן במדרג סמכויות מאשרות.

הפרק הרגולטורי קובע את תפקידו של מערך הסייבר הלאומי כמאסדר הלאומי בתחום הגנת הסייבר, בהתאם להחלטות הממשלה. כיום כל רשות מאסדרת קובעת תקני סייבר לפי שיקול דעתה ובאופן שאינו בהכרח אחיד. בהתאם, מוצע כי מערך הסייבר הלאומי יהא מופקד על תוכן האסדרה באופן שיחייב את כל הרשויות.

בנוסף, מוצעים עקרונות להבניית שיקול הדעת האסדרתי באופן המביא בחשבון את התקינה המקובלת במדינות המפותחות וכן היבטי נטל משקי, השפעה על תחרות ורווחת צרכנים. בפרק הרגולטורי נכללת גם הסמכה "שיורית" שמטרתה הסמכה של המערך, באישור ראש הממשלה, לקבוע דרישות בתחום הגנת הסייבר אשר יחולו על פעילויות משקיות, ככל שאינן מוסדרות בדין אחר ושיש בהן סיכוני סייבר משמעותיים.

להשלמה יצוין כי כבר בשנת 2002 קיבלה ועדת השרים לענייני ביטחון לאומי החלטה מספר ב/84 בנושא "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" משנת 2002 (להלן – החלטה ב/84), שבה הוסדר הטיפול בהגנת מערכות ממוחשבות חיוניות מפני תקיפות סייבר– מערכות שהפגיעה בהן עלולה לגרום לנזק פיזי או כלכלי משמעותי מאד, לפגיעה בחיי אדם או לפגיעה באספקת שירות ציבורי חיוני. האחריות להנחיית תשתיות קריטיות הוטלה על שירות הביטחון הכללי, בהתאם לחוק להסדרת הביטחון בגופים ציבורים, תשנ"ח – 1998[5]. בשנת 2016, במסגרת מימוש החלטות הממשלה בדבר גורם לאומי בתחום הגנת הסייבר, הוסדרה העברת האחריות להנחיית התשתיות הקריטיות למערך הסייבר הלאומי, למעט לעניין גופי תקשורת כמוגדר בחוק. העברת האחריות הוסדרה במסגרת הוראת שעה,[6] ובוצעה במהלך 2017. בהתאם להחלטות הממשלה יש לקבעה כהוראת קבע, ולכן במקביל להפצת תזכיר זה יש כוונה להפיץ תזכיר משלים לקביעת הסמכת מערך הסייבר לעניין תשתיות קריטיות כהוראת קבע.

ג. __עיקרי החוק המוצע__

עיקר 1 – הגדרת מונחים בתחום הגנת הסייבר

היבט מרכזי בתזכיר המוצע הוא הגדרת מונחים ייעודים לתחום הגנת הסייבר. המיקוד בתחום הגנת הסייבר מאפשר ליצור מסגרת משפטית לתחום הסמכויות הנדרשות באופן מוגדר ומידתי.

"הגנת הסייבר" מוגדרת בתזכיר בשים לב למכלול הפעילויות הנדרשות לכך, ועל מנת לשמור על תיאום עם מופעים אחרים בחקיקה. בסיפא של הגדרת "הגנת הסייבר" נכלל גם הביטוי "אבטחת מידע". זאת על מנת לשקף את

[5] ס"ח התשנ"ח, עמ' 348; התשע"ז, עמ' 494.

[6] חוק להסדרת הבטחון בגופים ציבורים החוק להסדרת הביטחון בגופים ציבוריים (הוראת שעה), התשע"ו–2016.

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. כיום פוטנציאל הנזק התרחב מאוד שכן ניתן באמצעות תקיפת מחשב לשבש פעילויות. מגוון מטרות התקיפה התרחב וכך גם מושאי ההגנה ועל כן יש לפעול למניעת שיבוש שירותים חיוניים (כגון שירותים רפואיים), פגיעה בתשתיות (כגון חשמל, מים, תחבורה), מניעת נזק לאדם ולסביבה (כגון זיהום אוויר) ואינטרסים נוספים הנשענים היום, שלא כמו בעבר, על מערכות טכנולוגיות.

כתוצאה מכך תפיסת ההגנה מחייבת שינוי משמעותי של ניהול הסיכונים באופן שלצד קיום עקרונות תפיסות אבטחת המידע המקובלות (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 להנהלת הארגון קבלת החלטות רציפה לגבי המתח שבין התפקוד התקין של הארגון ושמירה על נכסיו לבין מניעת תקיפות, וכן הבנת היקף פוטנציאל הנזק והמשמעויות לנקיטת אמצעים למניעת הנזק, בעת שיש חשש לתקיפה. שינוי זה נתפס כשינוי איכותי של הרחבת תכולת השדה המקצועי ל"הגנת הסייבר" ולא רק "אבטחת מידע", באופן שהגנת הסייבר כוללת את אבטחת המידע.

יתר ההגדרות בפרק נשענות בעיקרן על ההגדרות המצויות בחוק המחשבים, התשנ"ו-1996[7] (להלן – חוק המחשבים), שהוא החוק התשתיתי 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" המלמדת על סימנים או אותות שנועדו לקריאה וביצוע בידי מחשבים, וכן

את המידע המצוי במחשבים וברשתות, "חומר המחשב", ניתן לחלק **לשלושה סוגים מרכזיים:**

מידע טכנולוגי טהור שלא ניתן להסיק ממנו מסקנות על אדם - מידע טכנולוגי אשר משקף פעילות מיחשובית סטנדרטית, כגון תקשורת בין מחשב לנתב, בין מחשב למדפסת, בין מחשב לשרת וכן אוסף של פעילויות שגרתיות הקשורות בהפעלת המחשב. ברובד זה מבוצעת פעילות מיחשובית רבה במסגרת התפעול השוטף והתפקוד של מערכות המידע. ברובד זה גם מצוי מרחב פעולה משמעותי של תוקפים, תוך הסטה או שינוי של הפעילות המיחשובית, והכוונתה מרחוק בידי התוקף. מידע זה אינו מכיל נתונים או מידע אודות אדם מזוהה או ניתן לזיהוי, משום שזהו מידע טכני כפשוטו.

מידע טכנולוגי טהור שניתן להסיק ממנו במישרין או בצירוף מידע אחר, מידע על אדם – זהו "תיעוד" של פעילות מיחשובית אשר ניתן לגזור ממנו מסקנות או מידע על אודות אדם מזוהה או ניתן לזיהוי. רובד זה כולל "סדרות" מידע כגון נתונים אודות תקשורת בין מחשבים או Metadata,[8] ונתונים אחרים שנועדו לתעד פעילות של מערכות מחשב. באופן כללי מידע זה דומה למידע טכנולוגי טהור שתואר לעיל, אך במידה שמידע זה כולל מידע המאפשר לזהות אדם מסוים, ניתן להסיק ממנו מסקנות על אודות התנהגות אדם.

מידע טכנולוגי המתעד מסרים אנושיים - מסרים אנושיים ישירים חזותיים או קוליים שניתנים לפענוח בלתי אמצעי בידי אדם, כלומר זהו הרובד שבו אנשים מתקשרים ומתבטאים.

באופן כללי, פעילות הגנת הסייבר ממוקדת בשתי קבוצות המידע הראשונות. לעיתים נדרש עיסוק גם בשכבת התוכן, לדוגמה כאשר שיטת התקיפה היא שיטוי של עובד בארגון ללחוץ על קישור זדוני, אולם המיקוד בשכבת התוכן נועד לאתר תוכן זדוני בשפת מחשב. במימד המשפטי חשוב להדגיש, כי תכלית איסוף המידע בפרק האופרטיבי היא לצורך הגנת הארגון שבו נמצא המידע, ולא לצורך איסוף מידע עליו לצרכי פיקוח או אכיפה.

[7] ס"ח התשנ"ה, עמ' 366 ; התשע"ב, עמ' 514

[8] ראו הגדרת "נתוני על" בתזכיר חוק לתיקון פקודת הראיות (מקור והעתק כראיה), התשע"ח-2017.

איסוף ועיבוד של מידע זה נדרש כדי לקיים את תכלית הגנת הסייבר, כשם שנדרשת נגישות של טכנאי מחשבים לרשת כדי להפעילה באופן תקין.

בהתאם לכך, רכיב מרכזי בהגדרות הוא הביטוי **"מידע בעל ערך אבטחתי"**, העומד במרכז איסוף ועיבוד המידע הנדרש בעת פעילות בתחום הגנת הסייבר. רכיב זה נועד לבטא מידע על תקיפות ושיטות תקיפה ואופן זיהויין, וכן דרכי התמודדות עם תקיפות סייבר.

הביטוי "תקיפת סייבר" נועד לבטא את טווח המעשים של ניצול לרעה של מחשב או מידע ממוחשב באמצעות מחשב.

הביטוי "אינטרס חיוני" נועד להגדיר את האינטרסים החברתיים החשובים שיש להגן עליהם מפני תקיפות סייבר. הוא נועד לכלול את סוגי האיומים והתקיפות שעלולים לגרום לפגיעה בחיי אדם, לנזק כלכלי, לדלף מידע, לפגיעה סביבתית ועוד, כמפורט בסעיף. לצד נזקן של פגיעות אלה עלולה גם להיגרם פגיעה תודעתית שיש בה סיכון להשפעה על אמון הציבור במערכות השלטוניות ובתפקודן התקין של מערכות חיוניות.

הביטוי "אינטרס חיוני" מהווה נקודת מוצא עקרונית להכוונת שיקול הדעת המנהלי הן בעת הפעלת סמכויות לטיפול בתקיפה כמפורט להלן בפרק העוסק בסמכויות טיפול באירועים, והן בעת מיפוי המרחב הישראלי לצורכי קביעה של תפיסת הגנה ואסדרה.

עיקר 2 (פרק ב') - מערך הסייבר הלאומי ייעודו ותפקידיו

מערך הסייבר הלאומי הוא גוף ממשלתי שמשימתו הגנה לאומית בתחום הסייבר המבוססת על תחום טכנולוגיית המידע (מחשבים, רשתות והגנת הסייבר) תוך ביצוע פעילויות ביטחוניות, אופרטיביות ורגולטוריות, שתכליתן למנוע מהאיום להתממש.

בדומה לארגונים ביטחוניים אחרים, מאפיינים אלה מחייבים שינויים מסוימים בהיבטים ארגוניים ובמסגרת שבה מערך הסייבר פועל. מסגרת זו צריכה להיקבע תוך שמירה על עקרונות היסוד של המנהל הציבורי, ובזיקה לגורמים המופקדים על תחומים אלה בממשלה ובמרכזם נציבות שירות המדינה. קביעתה של מסגרת משפטית בהתאם להוראות חוק זה משקפת את המאפיינים הייחודיים של פעילות מערך הסייבר, ולצד זאת את החשיבות הרבה לקיומה של מסגרת נורמטיבית סדורה.

מוצע להסדיר את הסמכות של ראש הממשלה לקבוע הוראות מתאימות שיאפשרו לממש את הצרכים הארגוניים של מערך הסייבר הלאומי.

מנגנוני פיקוח ובקרה פנימיים –

לראש המערך ולבעלי תפקידים בכירים בו אחריות לפקח על קיום החוק ועקרונותיו בזמן אמת או סמוך ככל הניתן לזמן אמת. כמפורט להלן, לצורך בניית מסגרת מאוזנת ומידתית של הפעלת סמכות, התזכיר כולל עקרונות מנחים, הבנייה של שיקול הדעת המנהלי, וכן צורך באישור בית משפט. עקרונות אלה מנחים את בעלי התפקידים השונים בעת הפעלת הסמכות ופרשנותה.
לצד מנגנונים אלה, מוצעים שני מנגנוני פיקוח נוספים.

מנגנון פיקוח מרכזי הוא "מפקח פרטיות פנימי", וזאת בהתאם לעבודת מטה שבוצעה במשרד המשפטים וברשות להגנת הפרטיות למול גופים ביטחוניים, ובאה לידי ביטוי בהצעת חוק הגנת הפרטיות (סמכויות אכיפה), תיקון מספר 13, התשע"ח-2018[9]. מפקח הפרטיות הפנימי הוא עובד המערך, שתפקידו לפקח על

[9] ה"ח התשע"ח, עמ' 1206.

ההגנה על הזכות לפרטיות בפעילות המערך. נוכח החובה לאזן בין הצורך התפעולי מבצעי באיסוף המידע ועיבודו לבין הסיכון לפגיעה בפרטיות, מוצע להקים גורם פיקוח פנימי ייעודי. לצד הבקרה בדיעבד, יהיה למפקח הפרטיות תפקיד גם בסיוע לעיצוב מערכות המידע השונות המשמשות את המערך, כדי לצמצם את סיכוני הפרטיות הכרוכים בהם.

מנגנון פיקוח נוסף הוא מינוי ועדה מפקחת, חיצונית למערך, שתשמש כגורם מפקח על פעילות המערך. מאחר שהמערך הוא יחידת סמך במשרד ראש הממשלה, השר הממונה עליו הוא ראש הממשלה, וזאת בדומה לגופים ביטחוניים נוספים הפועלים במשרד ראש הממשלה כיחידות סמך. ראש מערך הסייבר הלאומי מדווח ישירות לראש הממשלה. לצד מנגנוני הפיקוח והבקרה המקובלים במערכת הממשלתית ובגופים ביטחוניים, מוצע להקנות לראש הממשלה כלי בקרה חיצוני על מערך הסייבר הלאומי, ועדה מפקחת עצמאית, שממוקדת בתחום הסיכונים לפרטיות.

הוועדה המפקחת נועדה לחזק את מנגנוני הבקרה לנוכח ייחודיותו של תחום זה. מוצע למנות ועדה אשר בראשה יעמוד משפטן בכיר, נציג היועץ המשפטי לממשלה, ושלושה נציגי ציבור בעלי כשירות רלבנטית. מוצע כי השלד מקצועי התפעולי יתבסס על מערך הסייבר. מוצע להטיל על הוועדה לדווח לראש הממשלה אחת לשנה לפחות על פעילות המערך. לצורך כך מוצע כי הוועדה תקבל מהמערך דיווחים עיתיים בפורמט שייקבע, וכן להסמיך אותה לקבל מידע ומסמכים מגורמים רלוונטיים לצורך ביצוע תפקידיה ביעילות.

עיקר 3 (פרק ג') –סמכויות המערך להתמודדות עם תקיפות סייבר

הפרק המוצע מסדיר מסגרת משפטית להפעלת סמכויות לצורך התמודדות עם תקיפת סייבר.

בהתאם לתפיסה מתקדמת של הגנת הסייבר, כמפורט להלן, בעת קיומה של תקיפה או חשש לתקיפה כזו נדרש לבצע פעולות שמטרתן לאתר את היקף הימצאותה של התקיפה ברשת הארגונית, להבין אילו פעולות ניתן לבצע באמצעות קבצי התקיפה או הנגישות לרשת הארגונית, למנוע את התרחשותן או להכיל את הנזק ולסלק את התקיפה, על מנת למנוע פגיעה או פגיעה נוספת במערכות הארגון או במרחב הסייבר.

תכלית הפעילות לפי הפרק, קרי הגנת הסייבר ומניעת פגיעה בתהליכים ארגוניים או במידע ארגוני, שונה מהקשרים אחרים שבהם המדינה מפעילה סמכות כלפי ארגונים. פונקציית המטרה של הפרק האופרטיבי היא טיפול **בתקיפה ממוחשבת**, שנעשית באמצעות "שפה קריאת מחשב" (כהגדרת הביטוי בחוק המחשבים) והאינדיקציות לקיומה באות לידי ביטוי בשפה זו. חשיפה למידע אחר, ככל שקיימת חשיפה כזו, היא תוצאת לוואי ולא מטרה עיקרית. בכך שונה פעולת מערך הסייבר מפעולת רשויות האכיפה והביטחון, אשר יעד לגיטימי בפעילותן הוא איסוף ראיות או מודיעין על אנשים ממחשבים ומתקשורת במסגרת פעולות חקירה ומודיעין. הסמכויות לפי פרק זה אינן ממוקדות בפעילות אכיפה או פיקוח כלפי הארגון, כי אם בהגנה. עקב כך יש הבדל עקרוני בין הפרק האופרטיבי לבין חקיקה אחרת העוסקת ומסדירה את הסמכויות של רשויות המדינה בכל הנוגע לפעילות הקשורה למידע המצוי במחשבים ובתקשורת.

התפיסה שבבסיס הפרק היא כי נדרשת מעורבות של המדינה **באיתור תקיפות סייבר בארגוני המרחב האזרחי ובטיפול בהן**, בשל הצורך במסגרת "על ארגונית" לכך. זוהי מסגרת חדשה שנועדה לאפשר למדינה לבצע פעילות הגנה שמטרתה הגנה על תפקודו התקין של מרחב הסייבר ומניעת תקיפות שיש בהן כדי ליצור סיכון משמעותי לאינטרס הציבורי.

על מנת להסדיר מבחינה משפטית את הסמכות של המערך וכן לתת ודאות לגבי הסמכות ואופן הפעלתה למערך ולגורמים במרחב האזרחי שמולם הוא פועל, הפרק מבוסס על פעילויות הגנת סייבר מקובלות בעת איתור תקיפה והתמודדות עמה, כמפורט להלן.

ביצוע פעילות הגנה ואיתור תקיפה ברשת ארגון מחייבת עבודה ברובד הממוחשב שבו מתרחשת התקיפה, וזאת על בסיס תובנות מקובלות בתחום הגנת הסייבר. בהתאם לתובנות אלה מהלך ראשוני בתקיפת סייבר הוא יצירת "ראש גשר" ברשת הארגון הנתקף על ידי התוקף. התוקף משתמש **בתקשורת הממוחשבת הנכנסת והיוצאת** מהארגון כדי לנצל חולשה במערכות הארגון ולחדור פנימה. תקיפות סייבר מבוססות על ניצול חולשות טכנולוגיות, על שימוש באותן שיטות תקיפה או כלי תקיפה, וכי תקיפות מתקדמות לעומת זאת, מבוססות על שיטות תקיפה או כלי תקיפה לא מוכרים. לאחר מכן, באמצעות ראש הגשר, מתקין התוקף ברשת הארגון את התוכנות הזדוניות המאפשרות לו שליטה והפעלה מרחוק.[10] תוקף מתקדם מסווה את פעילותו ברשת הארגון, כדי להגן על עצמו מפני איתור פעילותו על ידי מערכות ההגנה הארגוניות. הוא מסווה את **התקשורת בינו לבין התוכנות שהתקין בארגון במסגרת הפעילות הממוחשבת השגרתית ברשת הארגון**. פועל יוצא מהמתואר לעיל הוא שלצורך איתור התקיפה ברשת הארגונית ארגונים נדרשים לניטור רציף של מערכותיהם, שכן באמצעות ניטור זה ניתן לאתר במקרים רבים את התקיפה, גם אם היא לא היתה מוכרת קודם. פעילות זו נדרשת פעמים רבות גם כדי לעמוד בהוראות חוק הקשורות בטיפול במידע, כגון איתור ומניעת דלף של מידע אישי.[11]

על רקע זה הפרק כולל עקרונות כלליים המסדירים את הפעלת הסמכות ושיקול הדעת לעניין פעולות ההגנה הנדרשות. הפעלת הסמכות מוסדרת בהתאם לעקרון המידתיות, קרי - לאחר בחינה כי האמצעי אכן נדרש, כי ננקט האמצעי שפגיעתו היא הפחותה ביותר ביחס לצורך בטיפול בתקיפה, וכי הסיכון לזכות לפרטיות ולתפקודו של הארגון נמוך מהתועלת בפעולה. הפרק כולל מדרג של סמכויות מאשרות בהתאם לסוג הפעולה ולהיקף המעורבות שלה בפעילות הארגון.

הנחת העבודה המקצועית היא שמעורבות פעילה של המערך בתחומים אלה תידרש כאשר הארגון אינו מסוגל בעצמו, כחלק מניהול שגרת מערכות המידע שלו או שגרת ההגנה שלו, לאתר את התקיפה במדויק או להתמודד עמה ולמנוע את הנזק מהאירוע, וזאת, בדומה לתפקיד של מערך הרפואה הדחופה או מערך הכיבוי במרחב הפיזי. הקישוריות הגבוהה והאינטנסיבית במרחב הסייבר מגבירה את הסיכון הכולל ומייצרת אתגרים משמעותיים וצורך בזמני תגובה מהירים.

בנוסף, לנוכח הקישוריות במרחב הסייבר וקלות השכפול של שיטות תקיפה והדבקה, נדרש שיתוף מידע בדבר סוגי התקיפות והטיפול בהן, וכן נדרש לאתר, מוקדם ככל הניתן, פעילות זדונית.[12] החוסן המערכתי הנדרש מחייב יכולת איתור, גילוי וזיהוי של תקיפות באמצעות שיתוף מידע על אודות תקיפות וניסיונות תקיפה, מידע הנמצא כיום במערכות הארגונים ויש תועלת רבה בשיתופו.[13] נוסף על כך מתחייב ניתוח של המידע האמור, תוך כדי שילוב עם מידע ממקורות נוספים ובכלל זה של גופי הביטחון, לטובת גילוי וזיהוי של איומי סייבר וגיבוש תמונת מצב לאומית. בנוסף נדרשים פיתוח והטמעה של תהליכים ומנגנונים רוחביים לשיתוף מידע וכן יכולת התמודדות בזמן אמת עם אירועי סייבר, לרבות סיוע לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו.

---

[10] ראו את החיבור: Lockheed Martin, Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intursion Kill chains, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[11] Andrew Cormack, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTed
A Journal of Law, Technology & Society, Volume 13, Issue 3, December 2016, https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/

[12] NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
ENISA, https://www.enisa.europa.eu/publications/actionable-information-for-security

[13] ENISA, A Flair for Sharing, https://www.enisa.europa.eu/publications/legal-information-sharing-1

מדיניות זו דומה למגמה מרכזית זו של המדינות המפותחות להקים מרכז לאומי אשר תפקידו לרכז מידע על אודות חולשות, תקיפות ושיטות התמודדות, תוך שיתוף במידע זה בהקדם האפשרי עם המרחב האזרחי.[14] בהתאם לדין החל באירופה, נדרשות כל מדינות האיחוד האירופי להקים מרכז לאומי כזה.[15] לצד הפעילות החשובה של שוק חברות הגנת הסייבר, נדרשת מסגרת ארגונית ייעודית ממשלתית על-ארגונית כדי לתת מענה הולם ואינטנסיבי בקצב ובהיקף הנדרשים להתמודדות עם האיומים.

למדינה יתרונות נוספים בתחום זה ובהם היכולת למקד את ההתראות והמידע בתוך הקשר המאפשר פעילות, היכולת לרכז כוח אדם בניתוח האירועים, וכן היכולת לשלב מידע ותובנות על אודות איומים מדינתיים, שאינם מצויים בידי השוק הפרטי. זאת נוסף על יתרונותיה בסגירת הפער התשתיתי באמצעות שיתוף, העברת מידע והתראות.

בישראל החל לפעול בשנת 2017 אגף ה-CERT הלאומי, מכוח החלטת הממשלה 2444 משנת 2015, ובהתאם למסגרת משפטית שתואמה עם היועץ המשפטי לממשלה.[16]

ההסדרה של פעילות מערך הסייבר באיסוף ובטיפול במידע לשם איתור וטיפול בתקיפות סייבר מוסדר בחוק בהתאם לעקרונות האלה:

1. הגדרה ייעודית לסוג המידע שנאסף ומעובד בהקשר זה, תוך ניסיון לבדלו ולהפרידו ככל הניתן, ממידע על אודות אדם או על אודות ארגון מזוהה.
2. הגבלה של מטרת השימוש במידע לצרכי הגנת הסייבר.
3. הבניית שיקול הדעת המנהלי בעת איסוף מידע ושמירתו.
4. קביעת כללים לעיבוד המידע בידי גורמים מוסמכים, באופן שמצמצם את החשש לשימוש בו לרעה, וזאת בהמשך ובדומה למסמך "עקרונות ה-CERT הלאומי" אשר תואם עם היועץ המשפטי לממשלה.[17]
5. קביעת מסגרות בקרה ארגוניות הכוללות מינוי ממונה פרטיות וכן מינוי ועדה מפקחת.

עיקר פעולת המערך מבוססת על ההנחה שיש זהות אינטרסים בין הארגון הנפגע ובין המערך עצמו בדבר הצורך לתת מענה מידי ומתאים בקרות אירוע. זה המקום להדגיש כי נשוא הטיפול של המערך הוא **התקיפה** המתרחשת בארגון, בעוד שהטיפול **בתוקף** יובל בידי הגורמים האחראים לכך.

[14] 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.

[15] NIS Directive, article 9.

[16] https://www.gov.il/he/Departments/Policies/principles

[17] https://www.gov.il/he/Departments/Policies/principles

עיקר 4 (פרק ד׳) – אסדרה לאומית בתחום הגנת הסייבר

פרק זה מבוסס על המסגרת החוקתית החלה על אסדרה שלטונית, על מאפייני תחום אבטחת המידע – הגנת הסייבר, וכן על ההוראות החלות בהתאם להחלטת הממשלה 2118 בעניין הפחתת נטל רגולטורי.[18] על מנת לאפשר מסגרת התמודדות אפקטיבית עם סיכוני הסייבר, הפרק כולל מצד אחד הסמכה לפתח שיטה ותפיסות להגנה, ומצד שני עקרונות שמטרתם הבניית שיקול הדעת המנהלי בעת פיתוח ומימוש כאמור כדי להתחשב בהשפעות של אסדרה זו על הפעילות המשקית.

פרק האסדרה בחוק המוצע עוסק במכלול פעילות הממוקדת במניעה ובהיערכות למתקפות סייבר, על יסוד מנגנוני הנחיה ברמה הלאומית והמגזרית, אשר יאפשרו למדינה לחזק את החוסן המשקי.

בהקשר זה למדינה תפקיד משמעותי, השונה מהקשרים אחרים שבהם המדינה מפעילה סמכויות אסדרה, בכך שמדובר בהגנה על תפקודו התקין של מרחב הסייבר ועל אינטרסים לאומים חיוניים בעלי היבטים בטחוניים.

בנוסף להשפעה שיש לאיום הסייבר על המשק האזרחי, יש לו גם מימד מובהק של ביטחון לאומי. זהו רובד שיקולים נוסף מעבר לשיקולי רגולציה משקית כלכלית הנשקלים בדרך כלל. האינטרס הביטחוני אינו ניתן לכימות כספי בלבד ויש לו השפעות רוחב וקשרי גומלין. על כן, הצורך לייצר מסגרת רגולטורית גמישה, בעלת יכולת התאמה לנסיבות המשתנות במהירות, מקבל משנה תוקף.

רכיב מרכזי בהחלטות הממשלה, כמפורט גם בתפיסת האסדרה שאישרה הממשלה, הוא פיתוח האסדרה ופריסתה באופן מידתי, תוך התחשבות במשמעויות ובהשפעות של העלאת רמת החוסן לפעילות הארגונית. על המדינה לסייע בקביעת אופן ההגנה על הארגונים האזרחיים וכן לנקוט אמצעים להבטחת הפנמה של הוראות אלה בקרב ארגונים אלה, באמצעות תהליכי רישוי, פיקוח ובמידת הצורך - אכיפה.

פרק הרגולציה נועד לייצר מסגרת מידתית להפעלת שיקול דעת רגולטורי, תוך שימוש בעקרונות תוכן, ובעקרונות תהליכיים שמטרתם מימוש תפיסה זו. לצד זאת, ולנוכח אתגרי האיומים המשתנים תדיר במרחב הסייבר וההתמודדות עמם, נדרשת מסגרת משפטית שתאפשר הפעלה גמישה של סמכות.

בין היתר, מתבטא האיזון בין צרכי הגנת הסייבר וההשפעה על פעילות הארגונים -

א. בקביעת מסגרת שיקולים שיש להתחשב בהם בעת קביעת הוראות רגולטוריות;
ב. בקביעת תהליך מבוסס עובדות הנשען על תקינה בינלאומית;
ג. בהתבססות על תהליכי איתור נכסים ותהליכים לאומיים ברמה הלאומית (כגון זה של רשות החירום הלאומית) וברמה המגזרית (בהתבסס על רשויות האסדרה המגזריות);
ד. בקביעת מודל אסדרה מבוזר המבוסס כברירת מחדל על רשויות אסדרה מגזריות קיימות.

גיבוש מודל האסדרה המוצע נעשה תוך הכרה בצורך לאזן בין מספר אינטרסים ציבוריים, ובכללם, הצורך מצד אחד להגן על מגוון אינטרסים ציבוריים אשר מרחב הסייבר מציב בפניהם סיכונים חדשים שמולם המדינה חייבת להיערך, ומנגד, הרצון להימנע מסיכונים לנטל רגולטורי עודף על המשק ומפגיעה בחדשנות ובתמריצים חיוביים, בהקשר הסייבר ובכלל.

---

[18] http://www.pmo.gov.il/policyplanning/Regulation/Pages/RegulationA.aspx

המודל הרגולטורי המשולב שמוצע בתזכיר מאזן בין ריכוזיות וביזוריות. מודל זה מתאים את עוצמת המענה הרגולטורי הנדרש לרמות הסיכון השונות, באופן אשר שואב את המירב מהניסיון המקומי והבינלאומי בתחום.

ככל שבמגזרים מסוימים יימצא כי הארגונים אינם בעלי מוכנות מתאימה בתחום הגנת הסייבר - תידרש רגולציה. עם זאת, הנחת העבודה היא כי לארגונים אינטרס טבעי להגן על פעילותם ונכסיהם הממוחשבים. השקעה אפקטיבית בהגנת סייבר, בשל היותה רכיב תשתיתי לפעילות תקינה של ארגונים, מגוננת על הפעילות הכלכלית ומהווה מעין "ביטוח" מפני התרחשות אירועי סייבר עתידיים. עקב כך, הזיקה בין הצורך בהשקעה בהגנת הסייבר לבין האינטרסים הפנימיים של הפירמות או הארגונים היא הדוקה יותר, ובהתאמה לכך מוצדקת יותר. בנספח לתזכיר ובהתאם להחלטה 2118 מסמך "הערכת השפעות רגולציה" של פרק זה.

ד. __השפעת החוק המוצע על תקציב המדינה__

להוראות חוק זה אין השפעה ישירה על תקציב המדינה.

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

פרק א': פרשנות

הגדרות 1. בחוק זה -

" איום סייבר" - סיכון להתרחשות תקיפת סייבר;

" אינטרס חיוני" – כל אחד מאלה:

(1) ביטחון המדינה, ביטחון הציבור או בטיחותו;

(2) חיי אדם;

(3) כלכלת המדינה;

(4) תפקודן התקין של תשתיות, מערכות או שירותים חיוניים בשגרה או בחירום ובכלל זה שירותי האינטרנט והתקשורת;

(5) תפקודם התקין של ארגונים המספקים שירותים בהיקף משמעותי;

(6) מניעת סכנה ניכרת לסביבה או לבריאות הציבור;

(7) מניעת פגיעה משמעותית בפרטיות בהיקף שקבע שר המשפטים או בנכס מידע משמעותי;

(8) אינטרס שקבע ראש הממשלה בצו לאחר התייעצות עם השר הנוגע בדבר.

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות;

"ארגון מפוקח" – ארגון הפועל בתחום שמפוקח על ידי רשות מאסדרת כמשמעותה בסעיף 47, או על ידי המערך לפי סעיף 57 או 61;

"גוף מיוחד" – כל אחד מאלה:

(1) צבא ההגנה לישראל;

(2) שירות הביטחון הכללי;

(3) משטרת ישראל;

(4) המוסד למודיעין ולתפקידים מיוחדים;

(5) הממונה על הביטחון במערכת הביטחון;

"גורם אחראי במערך" – עובד מערך בכיר שהוסמך לפי חוק זה לבצע את הפעולות הקבועות בחוק זה או לפיו;

"הגנת הסייבר" - מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע;

"חומר מחשב, מחשב, פלט, שפה קריאת מחשב, תוכנה" – כהגדרתם בחוק המחשבים;

"חוק האזנת סתר" – חוק האזנת סתר, התשל"ט-1979;[1]

"חוק הגנת הפרטיות" – חוק הגנת הפרטיות, התשמ"א-1981;[2]

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995;[3]

"חוק התקשורת" – חוק התקשורת (בזק ושידורים), התשמ"ב -1982;[4]

" 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.

"מידע בעל ערך אבטחתי רגיש" – מידע בעל ערך אבטחתי אשר עובד המערך סימן הגבלות על הפצתו, וכל עוד המידע לא פורסם לרבים כדין;

" מידע לא מזוהה" – מידע שלא מאפשר זיהוי של יחיד או ארגון באמצעים סבירים;

" מידע מוגן" – כל אחד מאלה:

(1) מידע שחוק הגנת הפרטיות חל עליו;

---

1 ס"ח התשל"ט, עמ' 118; התשע"ז, עמ' 1060
2 ס"ח התשמ"א, עמ' 128; תשע"ז, עמ' 986
3 ס"ח התשנ"ה, עמ' 366; התשע"ב עמ' 514
4 ס"ח התשמ"ב, עמ' 218; התשע"ו, עמ' 1177

(2) תוכן שיחה כהגדרתה לפי חוק האזנת סתר, למעט מידע בשפה קריאת מחשב או כתב שלא נועד לפענוח חזותי בידי אדם;

(3) מידע שהוא סוד מקצועי או סוד שהוא בעל ערך כלכלי, לרבות סוד מסחרי שפרסומו עלול לפגוע פגיעה ממשית בערכו, וכן מידע הנוגע לעניין מסחרי או מקצועי הקשור לעסקו של אדם, שגילויו עלול לפגוע פגיעה ממשית באינטרס מקצועי, מסחרי או כלכלי.

"עובד מוסמך" – עובד המערך שהוסמך לפי חוק זה לביצוע פעולה בחומר מחשב או פעולות אחרות לפי חוק זה, לאחר שעבר הכשרה מתאימה מהסוג שקבע ראש המערך בכללי המערך;

"פעולה בחומר מחשב" – הפעולות המנויות להלן:

(1) חדירה לחומר מחשב;

(2) העתקה של חומר מחשב;

(3) הקלטה או ניטור של תקשורת בין מחשבים;

(4) מתן הוראות למחשב בשפה קריאת מחשב;

(5) שינוי חומר מחשב ובלבד שאין בו שינוי של מידע שהוא רשומה מוסדית או מידע הניתן לפענוח חזותי בידי אדם; לעניין זה, "רשומה מוסדית" - כהגדרתה בסעיף 35 לפקודת הראיות;

(6) דיווח למערך בשפה קריאת מחשב על איתור סממנים ומאפייניהם;

(7) התקנת מחשב או התקן אחר ברשת תקשורת או במחשב של ארגון לשם ביצוע הפעולות המנויות בסעיפים (1) עד (6).

"פקודת הראיות" – פקודת הראיות [נוסח חדש], התשל"א-1971;[5]

"תקיפת סייבר" - פעילות שנועדה לפגוע בשימוש במחשב או בחומר מחשב השמור בו, ובין היתר:

(1) שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;

(2) מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו;

(3) אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;

(4) חדירה שלא כדין לחומר מחשב כמשמעותה בחוק המחשבים;

(5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר;

---

[5] דיני מדינת ישראל, נוסח חדש 18 ,עמ' 421; ס"ח תשע"ז, עמ' 388

(6) גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הדלפתו של מידע כאמור;

(7) הפרעה או מניעת נגישות של מחשב לרשת תקשורת.

פרק ב': מערך הסייבר הלאומי ייעודו ותפקידיו

מערך הסייבר הלאומי וייעודו 2. (א) מערך הסייבר הלאומי הוא גוף בטחוני מבצעי הפועל במשרד ראש הממשלה לפי הוראות חוק זה והחלטות הממשלה (להלן בחוק זה - המערך);

(ב) ייעוד המערך הוא הגנת מרחב הסייבר וקידום ישראל כמובילה עולמית בתחום הסייבר;

(ג) ראש הממשלה הוא השר הממונה על מערך הסייבר הלאומי.

תפקידי המערך 3. תפקידי המערך הם:

(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 והחלטותיה;

(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.

ראש המערך 4. (א) הממשלה, לפי הצעת ראש הממשלה, תמנה את ראש המערך, בהתאם להוראות חוק שירות המדינה (מינויים), התשי"ט- 1959[6] (להלן – חוק המינויים).

(ב) ראש המערך יהיה מופקד על ניהול המערך ועל ביצוע תפקידיו לפי חוק זה.

(ג) לראש המערך יהיו כל הסמכויות הנתונות לפי חוק זה לעובדי המערך.

(ד) ראש המערך רשאי לאצול סמכות שניתנה לו לפי חוק זה, לעובד בכיר במערך.

---

[6] ס"ח התשי"ט, עמ' 86; התשע"ה עמ' 105

(ה) אחת לשנה ימסור ראש המערך לראש הממשלה, דוח מצב הגנת הסייבר הלאומית שיכלול סקירה וניתוח לגבי מצב הגנת הסייבר בישראל, פעילויות שננקטו בשנה החולפת ופעילויות שנדרש לנקוט בעתיד.

היבטים ארגוניים של המערך

5. (א) על אף האמור בחוק המינויים, רשאי ראש הממשלה, לאחר התייעצות עם שר האוצר ועם נציב שירות המדינה, לקבוע בתקנות או בכללים הוראות אחרות מאלה החלות בשירות המדינה, לעניין ארגון וניהול כוח אדם במערך, והכל בכפוף להוראות חוק יסודות התקציב, התשמ"ה-1985[7] (להלן – חוק יסודות התקציב) ולהוראות חוק התקציב השנתי.

(ב) ראש הממשלה רשאי לקבוע בכללים משרות או תפקידים במערך אשר נדרשת בהם מומחיות מיוחדת ועקב כך, על אף האמור בכל דין, ניתן להעסיק בהם גם מי שאינו עובד המדינה, לתקופה קצובה.

(ג) מבלי לגרוע מהוראות חוק שירות המדינה (משמעת), התשכ"ג-1963[8], רשאי ראש הממשלה לקבוע בתקנות הוראות נוספות בדבר משטר ומשמעת שיחולו במערך.

(ד) ראש המערך יקבע בנהלי המערך הוראות לעניין כשירות והכשרה של גורם אחראי ועובד מוסמך כתנאי להפעלת סמכויות לפי חוק זה.

סודיות

6. (א) עובד המערך וכן הפועל מטעם המערך לפי הוראות חוק זה, בעבר או בהווה, לא ימסור מידע מוגן שהגיע אליו בתוקף תפקידו או במסגרת פעילותו במערך, למי שאינו רשאי לקבלו, אלא אם כן נדרש לכך כדין או קיבל היתר לכך בכתב בהתאם להוראות שקבע ראש המערך לפי חוק זה;

(ב) עובד המערך וכן הפועל מטעם המערך לפי הוראות חוק זה, בעבר או בהווה המגלה או המפרסם מידע מוגן לפי חוק זה שהגיע אליו בתוקף תפקידו או במסגרת פעילותו במערך, למי שאינו רשאי לקבלו, בלא היתר לפי סעיף (א), דינו - מאסר שלוש שנים; הביא אדם לגילוי או לפרסום כאמור ברשלנות, דינו - מאסר שנה;

(ג) אין בסעיף זה כדי לגרוע מסמכות שר לפי סעיפים 44 ו-45 לפקודת הראיות, או מסמכויות הצנזור לפי תקנות ההגנה (שעת חירום), 1945, או מכל סמכות אחרת למניעת פרסום לפי כל דין;

(ד) אין בהוראות סעיף זה כדי לגרוע מתחולת הוראות פרק ז' בחלק ב' לחוק העונשין, התשל"ז-1977.[9]

---

[7] ס"ח התשמ"ה, עמ' 60; התשע"ד עמ' 300

[8] ס"ח התשכ"ג, עמ' 50; התשע"ה, עמ' 105

[9] ס"ח התשל"ז, עמ' 226; התשע"א, עמ' 80

הגבלות על עובדי המערך

7. (א) ראש הממשלה רשאי לקבוע בתקנות הגבלות על עובדי המערך בתקופת עבודתם במערך ולאחריה, ככל שהדבר דרוש לשם מילוי תפקידי המערך, להבטחת טוהר המידות במערך, ולהבטחת אמון הציבור במערך.

(ב) עובד המערך לא יהיה חבר בארגון עובדים ולא ייטול חלק בפעולות להקמתו, לקיומו או לניהולו של ארגון עובדים; עבירה על הוראת סעיף זה תיחשב כעבירת משמעת; בסעיף קטן זה, "ארגון עובדים" - כל התארגנות או נציגות, בין קבועה ובין ארעית, שבין מטרותיה או פעולותיה נמנה הטיפול בארגון המערך, בניהולו, במשטר ובמשמעת ובתנאי השירות של עובדי המערך, או ייצוג של עובד המערך בנושאים אלה.

סייג לאחריות

8. עובד המערך או הפועל מטעם המערך בתפקידים שקבע ראש הממשלה לא יישא באחריות פלילית או אזרחית למעשה או למחדל שעשה בתום לב ובאופן סביר במסגרת תפקידו ולשם מילויו; ואולם אין בהוראות סעיף זה כדי לגרוע מאחריות משמעתית לפי כל דין.

ממונה הגנת הסייבר במערך

9. (א) ראש המערך ימנה מבין עובדי המערך, עובד שיפקח על קיום הגנת הסייבר במערך הסייבר שיהיה ממונה הגנת הסייבר.

(ב) ראש המערך יוודא כי לממונה יש את האמצעים הנדרשים למילוי תפקידו.

(ג) ממונה הגנת הסייבר לא ימלא תפקיד אחר אשר עלול להעמידו בניגוד עניינים במילוי תפקידו לפי סעיף זה.

מפקח פרטיות פנימי במערך

10. (א) ראש המערך, בהתייעצות עם רשם מאגרי מידע לפי חוק הגנת הפרטיות (להלן – הרשם), ימנה מבין עובדי המערך מפקח פרטיות פנימי (להלן – המפקח הפנימי), בהתאם לתנאי כשירות והכשרה שיורה עליהם הרשם, בהתייעצות עם ראש המערך.

(ב) המפקח הפנימי ימונה לתקופת כהונה אחת שלא תעלה על שבע שנים.

(ג) לא תופסק כהונתו של המפקח הפנימי והוא לא יועבר מתפקידו אלא בהתייעצות עם הרשם.

(ד) המפקח הפנימי יהיה עובד המערך הכפוף ישירות לראש המערך או לעובד בכיר במערך הכפוף ישירות לראש המערך, והוא יונחה מקצועית בידי הרשם.

(ה) המפקח הפנימי לא ימלא תפקיד נוסף ולא יעסוק בעיסוק נוסף העלולים להעמיד אותו בחשש לניגוד עניינים במילוי תפקידו לפי סעיף זה ולפי סעיף 11.

תפקידי מפקח הפרטיות הפנימי

11. המפקח הפנימי יפקח על יישום הוראות חוק הגנת הפרטיות במערך, יקיים בקרה על ביצוען ובכלל זאת -

(1) יכין תכנית עבודה שנתית שתובא לאישור ראש המערך, הרשם והוועדה המפקחת לפי סעיף 13 לפיקוח על קיום הוראות חוק הגנת הפרטיות, ולבירור הפרות חוק הגנת הפרטיות במערך;

(2) יבדוק את נהלי המערך בתחום הפרטיות ועמידתם בהוראות חוק הגנת הפרטיות;

(3) יברר הפרות בתחום הוראות חוק הגנת הפרטיות, בהתאם להנחיות הרשם;

(4) ידווח לרשם בלא דיחוי, בכפוף להוראות ההתאמה הביטחונית והמידור החלות על המערך, על ממצאים של פעולות הפיקוח הבדיקה והבירור שביצע;

(5) יקיים בקרה על אופן תיקון ליקויים שהתגלו בממצאי הפיקוח והבירור;

(6) יקיים הכשרה והדרכה של עובדי המערך בנושאי פרטיות;

(7) יגיש לראש המערך, לוועדה המפקחת ולרשם דין וחשבון שנתי על אופן ביצוע תכנית הפיקוח ועל קיום הוראות החוק במערך.

(8) יסייע לראש המערך בקיום הוראות סעיפים 17(ג) ו – 38.

סמכויות המפקח הפנימי

12. לצורך מילוי תפקידו יהיו למפקח הפנימי הסמכויות לפי סעיף 15 לחוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח – 1998[10] (להלן – החוק להסדרת הביטחון)

ועדה מפקחת על מערך הסייבר הלאומי

13. (א) ראש הממשלה ימנה ועדה שתפקח על פעילות המערך לפי הוראות פרק ג' לחוק זה לעניין השפעת הפעילות על הזכות לפרטיות (להלן – הוועדה).

(ב) נציג ראש מערך הסייבר הלאומי ישמש כמזכיר הוועדה.

(ג) הרכב הוועדה יהיה כדלקמן:

(1) שופט בדימוס או משפטן בכיר אחר בעל כשירות לכהן כשופט מחוזי – יו"ר;

(2) נציג היועץ המשפטי לממשלה;

(3) נציג מקרב הציבור בעל מומחיות, רקע וניסיון בתחומים הנוגעים לענייני הגנת הסייבר והביטחון של מדינת ישראל;

---
[10] ס"ח התשנ"ח, עמ' 348; התשע"ז, עמ' 494

(4) נציג מקרב הציבור בעל ידע וניסיון מובהקים בתחומי זכויות האדם והגנת הפרטיות;

(5) נציג מקרב הציבור בעל מומחיות רקע וניסיון בתחומי טכנולוגית המידע;

(ד) חבר הוועדה יהיה בעל התאמה בטחונית.

(ה) לא יגלה אדם דבר מדיוני הוועדה או מכל חומר שנמסר לה, אלא אם הסמיך אותו לכך ראש הממשלה, או באישור היועץ המשפטי לממשלה או נציגו.

(ו) חבר ועדה במילוי תפקידיו לפי חוק זה לא יהא נתון לכל מרות זולת מרות החוק ויפעיל שיקול דעת עצמאי.

תפקידי הוועדה 14. (א) הוועדה תגיש לראש הממשלה אחת לשנה, וכן בכל עת אחרת שלדעתה הדבר נדרש, דין וחשבון מטעמה על פעילות המערך בהתאם להוראות חוק זה.

(ב) לצורך ביצוע תפקידיה תקבל הוועדה דיווחים עיתיים על פעילות המערך וביצוע תפקידיו שיאפשרו לעמוד על ההשפעה של פעילות המערך על הזכות לפרטיות בפעילות המערך, ובכלל זה:

(1) נתונים על שימוש בסעיפי הסמכות לפי החוק;

(2) נתונים על פעילות מערך הגילוי והזיהוי לפי סעיף 17;

(3) אירועים שבהם עלה חשש להפרת הוראות החוק בתחום הפרטיות בידי עובד המערך או מטעמו;

(4) הנחיות פנימיות בתחום ההגנה על הפרטיות ואופן מימושן;

(5) תוכנית העבודה והדוח השנתי של מפקח הפרטיות הפנימי של המערך.

סמכויות הוועדה 15. (א) לצורך ביצוע תפקידיה לפי חוק זה רשאית הוועדה לאסוף מידע ומסמכים, ויהיו ליו"ר הוועדה, הסמכויות הבאות:

(1) להזמין אדם לבוא בפניה ולמסור מידע או מסמכים שברשותו; מי שהוזמן להעיד או להציג מסמך או מוצג אחר בפני הוועדה, חייב להתייצב בפני הוועדה ולמסור לה מידע או מסמך.

(2) להסמיך אדם הכשיר לכך לדעת הוועדה, ובלבד שהוא בעל התאמה בטחונית, לאסוף חומר הדרוש לביצוע תפקידיה ויהיו נתונות לו הסמכויות לפי פסקה (1).

(ב) ראתה הוועדה במסגרת פעילותה שעולה חשש להפרת הדין בידי גורם או אדם מסוים, תחדל מטיפול לגביו ותעביר את המשך הטיפול לגורם המוסמך לכך.

פרק ג׳: סמכויות המערך

סימן א׳: כללי

סמכויות המערך 16. (א) לצורך מילוי תפקידיו מוסמך המערך, לבצע את הפעולות המנויות להלן, בין היתר באמצעות המרכז הלאומי לסיוע בהתמודדות עם איומי סייבר:

(1) לקבל ולאסוף מידע בעל ערך אבטחתי ומידע שעשוי לשמש להפקת מידע בעל ערך אבטחתי;

(2) לעבד מידע לצורך הפקת מידע בעל ערך אבטחתי בהתאם להוראות חוק זה;

(3) להעביר, לשתף ולהפיץ מידע בעל ערך אבטחתי לכלל המשק ולארגונים הפועלים בו בהתאם להוראות חוק זה;

(4) לסייע לארגונים להתמודד עם אירועי סייבר בהתאם להוראות חוק זה.

(ב) ראש הממשלה בהסכמת שר המשפטים יקבע בתקנות הוראות לעניין איסוף מידע, עיבודו, העברתו, שיתופו והפצתו לפי פסקאות (1) עד (3).

מערך גילוי וזיהוי 17. (א) המערך יפעיל מערך גילוי וזיהוי בתחום הגנת הסייבר לצורך גילוי מוקדם של תקיפות סייבר וסיוע בהתמודדות עמן; המידע שייאסף ויעובד במערך הגילוי והזיהוי ישמש למטרה זו בלבד.

(ב) מערך הגילוי והזיהוי יאסוף מידע בזמן אמת מהגופים המנויים בסעיף 18 (להלן בסעיף זה – הארגונים) לשם עיבודו למידע בעל ערך אבטחתי;

(ג) מערך הגילוי והזיהוי יפעל בהתאם לעקרונות האלה:

(1) איסוף מידע מהארגונים ימוקד במידע בעל ערך אבטחתי;

(2) עיבוד המידע למידע בעל ערך אבטחתי יבוצע ככל הניתן בזמן אמת, באופן ממוחשב אוטומטי;

(3) איסוף המידע ועיבודו ייעשה בהתאם להוראות סעיף 38.

(ד) מערך הסייבר הלאומי יפרסם המלצות לעניין אופן מסירת הודעה ללקוחות ועובדי הארגונים בדבר פעילות מערך הגילוי והזיהוי;

(ה) ראש הממשלה ושר המשפטים יקבעו בתקנות הוראות לעניין אופן איסוף, עיבוד, שמירה וביעור של המידע במערך הגילוי והזיהוי והשימוש בו, וכן רשאים הם לקבוע בכללים הוראות נוספות לעניין מערך הגילוי והזיהוי אשר פרסומם יהיה חסוי משיקולי הגנה על סודיות, שיטות ואמצעים.

ארגונים שייכללו במערך הגילוי וזיהוי

18. מערך הגילוי והזיהוי יכלול את הארגונים האלה:

(1) משרדי הממשלה;

(2) גוף מבוקר כהגדרתו בסעיף 9 לחוק מבקר המדינה (נוסח משולב), התשי"ח-1958,[11] שראש המערך קבע ששיתופו יתרום תרומה של ממש לגילוי תקיפות סייבר ולהתמודדות עמן ולמעט הגופים המיוחדים;

(3) ארגון המנוי בתוספת החמישית לחוק להסדרת הביטחון.

(4) בעל רישיון כהגדרתו בחוק התקשורת; ואולם היה בעל רישיון מנוי בתוספת הרביעית לחוק להסדרת הביטחון, לא יחולו עליו הוראות סימן זה אלא באישור הקצין המוסמך לפי אותו חוק; ניתן לבעל הרישיון צו לפי סעיף 13(ב) לחוק התקשורת, לא יחולו עליו הוראות סימן זה אלא לאחר אישור הגורם המוסמך לפי אותו סעיף ולאחר שראש המערך התייעץ עם ראש שירות הביטחון הכללי לפי חוק שירות הביטחון הכללי, התשנ"ב-2002,[12] (להלן – חוק שירות הביטחון הכללי);

(5) ארגון אחר שביקש להצטרף למערך הגילוי והזיהוי וראש מערך הסייבר אישר את הצטרפותו; ראש הממשלה בהתייעצות עם שר המשפטים יקבע בתקנות את אופן הגשת הבקשה, וכן הוראות בדבר מסירת הודעה ללקוחות ועובדי הארגון אודות פעילות מערך הגילוי והזיהוי.

(6) ארגון אחר מהמנויים לעיל, שקבעו ראש הממשלה ושר המשפטים, לאחר שראש המערך חיווה דעתו כי הארגון מספק שירותים בהיקף משמעותי בישראל ושיתופו במערך הגילוי והזיהוי יתרום תרומה של ממש לגילוי ולזיהוי של תקיפות סייבר ולהתמודדות עמן במסגרת הגנת הסייבר בישראל.

סימן ב': סמכויות לטיפול בתקיפות ובאיומי סייבר

הוראות כלליות

19. (א) הפעלת הסמכויות לפי פרק זה תיעשה רק בידי מי שהוסמך לביצוע הפעולה לפי הוראות חוק זה או שנקבעו לפיו.

[11] ס"ח התשי"ח, עמ' 92; התשנ"ח, עמ' 352
[12] ס"ח התשס"ב, עמ' 179, התשע"ד, עמ' 667

(ב) הפעלת סמכויות תיעשה לאחר שבעל הסמכות מסר לארגון מידע על אודות הצורך בפעולה והשפעותיה על הארגון.

(ג) הפעלת סמכויות כלפי ארגון תיעשה אם התקיים האמור להלן -

(1) יש יסוד סביר להניח שמתרחשת או עשויה להתרחש תקיפת סייבר שעלולה לגרום לפגיעה באינטרס חיוני.

(2) הפעלת הסמכות נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה;

(3) בעל הסמכות שקל את השפעת הפעלת הסמכויות על הארגון ועל הזכות לפרטיות;

(4) בעל הסמכות נוכח כי הפעלת הסמכות אין בה כדי לפגוע בפעילות הארגון או בזכות לפרטיות במידה העולה על הנדרש בנסיבות העניין.

(ד) הופעלה סמכות לפי פרק זה וחלפו תשעים ימים מעת שהופעלה הסמכות האמורה – לא תופעל הסמכות או סמכות נוספת לפי פרק זה בארגון אלא אם נוכח ראש המערך כי יש יסוד סביר להניח שתקיפת הסייבר עדיין מאיימת על אינטרס חיוני והפעלת הסמכויות בארגון נדרשת להתמודדות עמה או לאיסוף מידע עליה;

(ה) הוראות סעיפים (ג) ו- (ד) יחולו בשינויים המחויבים אם הפעולה בארגון נעשית לבקשת הארגון, והוראות סעיף 35 יחולו בשינויים המחויבים ולפי ההקשר.

דרישת מידע ומסמכים

20. עובד מוסמך רשאי לדרוש מכל ארגון הנוגע בדבר למסור לו כל ידיעה או מסמך, ובכלל זה עותק של חומר מחשב, הנדרשים לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה.

מינוי איש קשר בארגון שיש בו תקיפת סייבר

21. עובד מוסמך רשאי להורות לארגון למנות איש קשר שיקבל הוראות מהמערך ויעביר את המידע הנדרש אל המערך או אל מי שהוסמך לכך מטעמו לפי הוראות סימן זה.

כניסה למקום

22. (א) גורם אחראי במערך רשאי להיכנס למקום או להורות לעובד מוסמך להיכנס למקום, אם היה לו יסוד סביר להניח שבמקום נמצא מחשב או חומר מחשב שבו מידע בעל ערך אבטחתי הדרוש לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה;

(ב) על אף האמור בסעיף קטן (א) לא ייכנס גורם אחראי במערך או עובד מוסמך למקום המשמש למגורים אלא בהסכמת המחזיק במקום או על פי צו של בית משפט השלום; אולם רשאי ראש המערך להורות לגורם אחראי או לעובד מוסמך להיכנס למקום המשמש למגורים גם בלא צו מאת בית משפט, אם היה לו יסוד סביר להניח שבמקום נמצא מחשב או חומר מחשב שבו מידע בעל ערך אבטחתי כאמור בסעיף קטן (א) שנדרש למניעת סכנה ממשית ומידית לשלום הציבור או ביטחונו, ואין דרך אחרת להשיגו בנסיבות העניין.

23. תפיסת חפץ לצורך טיפול בתקיפה

(א) עובד מוסמך רשאי לתפוס חפץ שיש לו יסוד סביר להניח שיש בו מידע בעל ערך אבטחתי, שבדיקתו המידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה.

(ב) לא יתפוס עובד מוסמך חפץ כאמור בסעיף קטן (א) אלא לאחר שנתן למחזיק בו הזדמנות להשמיע טענותיו. סבר הגורם האחראי כי הדבר יביא לפגיעה משמעותית ביכולת לאתר תקיפת סייבר, להתמודד עמה או למנוע אותה, ויש סכנה ממשית ומידית לשלום הציבור או ביטחונו, רשאי הוא לתפוס את החפץ ולתת למחזיק להשמיע טענותיו בפניו בהזדמנות הראשונה.

(ג) נתפס חפץ לפי סעיף זה, יחזירו העובד המוסמך לארגון שממנו נתפס לאחר שביצע בו את הבדיקה, בהקדם האפשרי ולא יאוחר מחמישה עשר ימים מיום שנתפס.

(ד) בית משפט השלום רשאי להורות -

(1) כי החפץ יוחזר לארגון, לבקשתו;

(2) על הארכת תקופת ההחזקה של החפץ מעבר לאמור בסעיף קטן (ג), לבקשת העובד המוסמך, אם סבר כי בנסיבות העניין קיים צורך בהארכת התקופה לשם איתור תקיפת הסייבר, טיפול בה או מניעתה.

24. המצאת חפץ לבדיקה

היה לעובד מוסמך יסוד סביר להניח שחפץ שנמצא בחזקתו או בשליטתו של ארגון מכיל מידע בעל ערך אבטחתי ובדיקתו המידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה, רשאי הוא להורות על הצגתו או המצאתו בשעה, במקום ובאופן הנקובים בהוראה; לעניין זה, יראו חפץ כנמצא בשליטתו של ארגון - אם הארגון יכול להשיגו במאמץ סביר.

25. הסתייעות במומחה

לצורך ביצוע פעולות ובדיקות לפי פרק זה, רשאי עובד מוסמך להסתייע במומחה שהוא בעל ניסיון, ידע או אמצעים הדרושים לביצוע הפעולות והבדיקות האמורות, ובלבד שהעובד המוסמך יהיה נוכח במקום ביצוע הפעולות והבדיקות בידי המומחה, בעת ביצוען, ויפקח עליו. בסעיף זה "מומחה" – גם מי שאינו עובד ציבור.

סמכות מתן הוראות

26. (א) עובד מוסמך רשאי לתת לארגון הוראות, ובכלל זה הוראות לגבי ביצוע פעולות בחומר מחשב של הארגון, לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה.

(ב) בהוראה שייתן, יפרט העובד המוסמך את התמצית העובדתית והמקצועית להחלטתו ליתן את ההוראה לפי סעיף קטן (א) ככל שאין בכך כדי לפגוע או לעכב את הטיפול בתקיפה, לחשוף מקורות מידע, שיטות או אמצעים.

(ג) נתקבלה הוראה מעובד מוסמך כאמור בסעיף קטן (א) יבצע אותה הארגון במועד הקבוע בה וידווח על אופן ביצועה לעובד המוסמך.

(ד) לא יגלה אדם תוכן הוראה שניתנה לארגון, פרטים הקשורים בתקיפה או בטיפול בה שנמסרו לארגון, אלא אם התיר זאת העובד המוסמך ובתנאים שיקבע ובכפוף לכל דין; העובד המוסמך רשאי להנחות את הארגון בדבר אופן ההגנה על סודיות הפעילות לפי פרק זה כלפי עובדיו ואחרים.

צו לפעולות למניעת תקיפת סייבר או לטיפול בה

27. (א) שופט בית משפט השלום רשאי להתיר בצו לעובד מוסמך לבצע פעולה במחשב או בחומר מחשב, אם שוכנע כי יש יסוד סביר להניח כי מתרחשת תקיפת סייבר או שיש איום סייבר שכתוצאה מהם עלולה להיגרם פגיעה באינטרס חיוני (להלן בסעיף זה – "צו ביצוע פעולות");

(ב) בהחלטה למתן צו ביצוע פעולות, יתחשב בית משפט השלום, בין השאר, באלה:

(1) חומרת הנזק אשר עלול להיגרם בשל תקיפת הסייבר אשר בקשר אליה מתבקש הצו וההסתברות להתרחשותה;

(2) השפעת הפעולות המבוקשות על הארגון שהצו חל עליו ועל גורמים נוספים שעשויים להיות מושפעים מהצו, ככל שישנם;

(3) מידת הפגיעה בפרטיות כתוצאה מביצוע הפעולות המבוקשות ומידת פגיעה אחרת בארגון או באדם.

בקשת הצו

28. (א) בקשה לצו ביצוע פעולות כאמור בסעיף 27 תוגש בכתב על ידי גורם אחראי במערך (להלן - המבקש), ויפורטו בה הפעולות השונות שנדרש לבצע במחשב או בחומר מחשב; הבקשה תיתמך בתצהיר של הגורם האחראי במערך.

(ב) המשיב בבקשה הינו הארגון שבמחשביו מבקשים לבצע פעולות כאמור; הדיון במתן הצו יתקיים במעמד הצדדים שזומנו לדיון, ואולם רשאי בית המשפט לתת צו לביצוע פעולות במעמד צד אחד אם הוא סבור שהמשיב הוזמן כדין ולא התייצב לדיון.

הדיון בבקשה 29. (א) בדיון בבקשה למתן צו לפי סעיף 27 או 32, רשאי המבקש לבקש לפרט או להציג בפני בית המשפט בלבד עובדות או מידע שעליהם הוא מבסס את בקשתו (להלן בסעיף זה – חומר חסוי); בקשה כאמור תוגש בכתב בצירוף נימוקים.

(ב) בית המשפט רשאי להיענות לבקשה כאמור בסעיף קטן (א) ולהסתמך על החומר החסוי אם מצא כי חשיפת החומר החסוי עלולה לפגוע או לסכל את אפשרות איתור תקיפת הסייבר, התמודדות עמה, או לפגוע באינטרס בטחוני או אינטרס ציבורי אחר; החומר החסוי יסומן, יוחזר למבקש לאחר העיון והדבר יירשם בפרוטוקול.

(ג) בית המשפט יודיע למבקש ולמשיב על החלטתו בבקשה לפי סעיף קטן (א), ורשאי הוא לקבוע שנימוקי ההחלטה, כולם או מקצתם, יהיו חסויים.

(ד) החליט בית המשפט שלא להיעתר לבקשה בדבר אי-גילויו של החומר החסוי לפי סעיף קטן (א), רשאי המבקש להודיע כי הוא חוזר בו מהגשת החומר החסוי, ומשעשה כן לא יועמד החומר לעיון המשיב והשופט יתעלם ממנו לצורך החלטותיו.

(ה) החליט בית המשפט שלא להיעתר לבקשה בדבר אי-גילויו של החומר החסוי לפי סעיף קטן (א), רשאי המבקש לערער על החלטת בית המשפט בעניין זה בתוך חמישה עשר ימים ממועד מתן ההחלטה, לפני בית משפט של ערעור אשר ידון בערעור בשופט אחד.

(ו) הודיע המבקש לבית המשפט שהחליט כאמור בסעיף קטן (ה), כי הוא שוקל להגיש ערעור כאמור באותו סעיף קטן, לא יעביר בית המשפט את החומר החסוי למשיב עד להכרעה בערעור.

(ז) בדיון בערעור לפי סעיף קטן (ו), רשאי בית המשפט לעיין בחומר החסוי ולקבל פרטים נוספים מהמבקש בלי לגלותם למשיב.

(ח) ראש הממשלה ושר המשפטים רשאים לקבוע הוראות נוספות בתקנות לעניין סדרי הדין לפי פרק זה.

ערעור על החלטת בית משפט 30. מי שהיה צד להליך למתן צו לפי סעיף 27 רשאי לערער על החלטת בית המשפט בתוך שלושים ימים ממועד מתן ההחלטה, לפני בית משפט שלערעור אשר ידון בערעור בשופט אחד, שיהיה מוסמך לבטלו או לשנות תנאים בו.

ביצוע הצו 31. ניתן צו לפי סעיפים 27 או 32, יבצע העובד המוסמך את הפעולות המנויות בצו לאחר שמסר על כך הודעה לאיש קשר מטעם הארגון, וככל הניתן בנוכחותו.

32. **צו לביצוע פעולות בחומר מחשב לצורך בקרה מדגמית**

(א) שופט בית המשפט השלום רשאי להתיר בצו, לצורך בקרה מדגמית, ביצוע פעולה במחשב או בחומר מחשב של ארגון אם סבר כי יש סיכוי של ממש לאתר באמצעותן תקיפת סייבר בארגון, בשים לב למאפייני הפעילות בארגון (להלן בסעיף זה – צו פעולות לצורך בקרה מדגמית).

(ב) בהחלטה למתן צו פעולות לצורך בקרה מדגמית, יתחשב בית משפט השלום, בין השאר, באלה:

(1) נחיצות הצו והפעולות מכוחו לצורכי הגנת הסייבר;

(2) השפעת הפעולות המבוקשות על הארגון שהצו חל עליו ועל גורמים נוספים שעשויים להיות מושפעים מהצו, ככל שישנם;

(3) מידת הפגיעה בפרטיות כתוצאה מביצוע הפעולות המבוקשות והאפשרות לפגיעה אחרת בארגון או באדם.

33. **בקשת הצו והדיון בה**

(א) בקשה לצו פעולות לבקרה מדגמית תוגש בכתב על ידי גורם אחראי במערך ויפורטו בה הפעולות המבוקשות והקשר בינן לבין תכלית הבקרה המדגמית בהתאם לסעיף 32; הבקשה תיתמך בתצהיר של גורם אחראי במערך;

(ב) המשיב בבקשה הינו הארגון שבמחשביו מבקשים לבצע פעולות כאמור; הדיון במתן הצו יתקיים במעמד הצדדים שזומנו לדיון , ואולם רשאי בית המשפט לתת צו לביצוע פעולות במעמד צד אחד אם הוא סבור שהמשיב הוזמן כדין ולא התייצב לדיון.

(ג) בית המשפט ידון בבקשה לפי סעיף זה בדלתיים סגורות, אלא אם הורה אחרת.

(ד) גילוי הוראות לפי סעיף זה או פרטים הקשורים בפעילות לפיו אשר נמסרו לארגון אסור אלא אם התיר זאת הגורם האחראי.

34. **פעולה בחומר מחשב אינה האזנת סתר או חדירה שלא כדין**

פעולה שנעשתה לפי הוראות סעיפים 26 ,17, 27, 35 או 36 לא תיחשב כהאזנת סתר או כחדירה שלא כדין לחומר מחשב כמשמעותן בחוק האזנת סתר או בחוק המחשבים, בהתאמה.

35. **ביצוע פעולה בהסכמה**

(א) גורם אחראי במערך רשאי להורות על ביצוע פעולה בארגון הדורשת אישור בית המשפט לפי סימן זה אף בלא צו כאמור, אם הארגון הסכים לביצוע הפעולה והתקיים האמור להלן:

(1) נותן ההסכמה הוא גורם מוסמך מטעם הנהלת הארגון;

(2) לפני מתן ההסכמה הסביר הגורם האחראי לנותן ההסכמה, בלשון המובנת לו, את כל אלה -

(א) הנסיבות המצדיקות את ביצוע הפעולה;

(ב) השפעת ביצוע הפעולה על הארגון ועל ארגונים נוספים ככל שישנם;

(ג) מידת הפגיעה בפרטיות או אפשרות לפגיעה אחרת באדם או בארגון כתוצאה מביצוע הפעולה, קיומה של אפשרות לצמצום הפגיעה והדרכים לכך;

(ד) את זכותו של הארגון שלא להסכים לביצוע הפעולה;

(ב) ארגון שנתן הסכמה לביצוע פעולה לפי סעיף זה רשאי לחזור בו מהסכמתו; אין בחזרה מהסכמה כדי לפגוע בחוקיות הפעולות שנעשו עד לחזרה מההסכמה.

סימן ג׳: סמכויות נוספות

פעולה דחופה בחומר מחשב להגנת סייבר

36. (א) ראש המערך רשאי להורות על הפעלת סמכות המנויה בסימן ב׳, שלשם הפעלתה נדרש צו בית משפט, ללא צו כאמור, לתקופה שלא תעלה על עשרים וארבע שעות, ובלבד שהתקיימו כל אלה:

(1) הפעלת הסמכות נדרשת בדחיפות לשם מניעת נזק ממשי לאינטרס חיוני כתוצאה מתקיפת סייבר, אין דרך אחרת למניעת הנזק האמור, ואין שהות לבקש מבית המשפט צו;

(2) התקיימו יתר דרישות הסעיפים האמורים בפרק זה, ככל שהדבר אינו מסכל את ביצוע הפעולה.

(ב) ראש המערך ידווח באופן מיידי ליועץ המשפטי לממשלה על הסמכויות שהורה להפעילן לפי סעיף קטן (א) לא יאוחר משש שעות ממועד הפעלתן.

(ג) גורם אחראי יפנה לבית המשפט באופן מיידי ולא יאוחר מעשרים וארבע שעות ממועד הפעלת סמכות לפי סעיף זה בבקשה למתן צו לפי הוראות פרק זה, אשר תכלול דיווח על הפעלת הסמכות ופירוט הפעולות שבוצעו במסגרתה לפי סעיף זה.

ממשקים עם רשויות אחרות ורשויות מאסדרות בעת טיפול בתקיפה

37. נוכח ראש מערך הסייבר בעת טיפול בתקיפת סייבר לפי פרק זה שמניעת הפגיעה באינטרס החיוני או צמצומה מחייב פעולה של בעל סמכות נוסף, יודיע על כך ללא דיחוי לאותו בעל סמכות; בעל הסמכות יקבע איש קשר לסיוע למניעת הפגיעה האמורה ולהיערכות להתמודדות עמה.

סימן ד׳: הגנה על הפרטיות ומידע מוגן שנאסף לפי פרק זה

עיצוב לפרטיות והגנה על מידע מוגן

38. (א) לצורך הגנה על הפרטיות ושמירה על מידע מוגן ראש המערך אחראי ליישום העקרונות המנויים להלן במערכות המחשב המשמשות לפעילות המערך (להלן בסעיף זה – המערכות):

(1) עיצוב טכנולוגי של המערכות באופן שנאסף ונשמר המידע המוגן המינימלי הנדרש לקיום ייעוד המערך, והוא מעובד ככל הניתן באופן שהוא מידע לא מזוהה;

(2) עיצוב טכנולוגי של המערכות באופן שעיבוד מידע למידע בעל ערך אבטחתי נעשה ככל הניתן באופן אוטומטי או ללא שהוא חשוף לאדם;

(3) שילוב בקרות טכנולוגיות במערכות המאפשרות פיקוח על העמידה בהוראות החוק לעניין איסוף שימוש ועיון במידע מוגן.

(ב) ראש הממשלה ושר המשפטים יקבעו תקנות לעניין הוראות סעיף זה.

סודיות ואי גילוי

39. (א) לא יגלה אדם או ארגון מידע שנמסר לו אודות הוראה או מידע אחר הקשור בפעילות המערך אשר סומן בידי גורם אחראי כמידע מוגן, מידע בעל ערך אבטחתי רגיש או מידע בעל סיווג בטחוני.

(ב) בית המשפט רשאי להורות, לבקשת אדם הנוגע בדבר, על גילוי מלא או חלקי של מידע כאמור, לאחר ששמע את עמדת המערך ושקל את האינטרס הציבורי בגילוי המידע למול החשש לפגיעה בפעילות המערך או בהגנת הסייבר.

מסירת מידע

40. ראש המערך, עובד הכפוף לו, או מי שפועל מטעמו, לא יגלה ידיעה או מסמך שנמסרו לו מכוח תפקידו או סמכויותיו לפי פרק זה, אלא בהתאם להוראות חוק זה, או לצורך הליך פלילי בשל עבירה חמורה או בשל הפרעה לעובד ציבור.

שימוש במידע שנמסר למערך

41. (א) מידע שנמסר למערך בהסכמה לפי הוראות פרק זה לא ישמש כראיה כנגד מוסרו בהליך אזרחי, מנהלי או פלילי למעט בעבירות שקבע שר המשפטים בתוספת הראשונה לחוק.

(ב) על מידע מוגן ועל מידע אודות ארגון שנמסר למערך בידי ארגון יחול סעיף 9(א) לחוק חופש המידע התשנ"ח-1998[13] (להלן- חוק חופש המידע) ויראו אותו כמידע שאין למוסרו לפי אותו סעיף.

(ג) ראש הממשלה יקבע כללים לעניין העברת מידע בעל ערך אבטחתי לגופים המיוחדים לצורך מימוש הוראות חוק זה.

פרק ד': אסדרה לאומית בתחום הגנת הסייבר

מטרות הפרק

42. מטרות פרק זה הן:

[13] ס"ח התשנ"ח עמ' 226; התשע"ו עמ' 1223

(1) העלאת העמידות והחוסן של ארגונים במגזרי המשק לתקיפות סייבר, בין היתר באמצעות הנחייתם להיערכות ושמירה על כשירות מתאימה להתמודדות עם איומי סייבר ותקיפות סייבר;

(2) להסדיר את ההנחיה בתחום הגנת הסייבר תוך קביעת מדיניות אחידה והתחשבות באינטרסים ציבוריים ומשקיים אחרים.

עקרונות על לאסדרה

43. (א) בעת קביעת תקנות, צווים והוראות בתחום הגנת הסייבר בידי ראש מערך הסייבר הלאומי או בעל סמכות אסדרה (להלן – האסדרה) ישקלו השיקולים האלה:

(1) התאמת האסדרה לתקינה בינלאומית או תקינה מקובלת ונוהגת במדינות מפותחות בעלות שווקים משמעותיים;

(2) התאמת האסדרה לאיומי הגנת הסייבר בישראל המצדיקים שינויים ייעודיים;

(3) באסדרה מגזרית - התאמת האסדרה למאפייני המגזר ולמאפייני פעילותם של הארגונים השונים במגזר;

(4) קיום יחס הולם בין היקף ואופן האסדרה לסוגי הארגונים איומי הסייבר שלהם הם חשופים והסתברות התרחשותם.

(ב) קביעת אסדרה תיעשה לאחר בחינת מידע על העלויות הישירות הנובעות ממנה והשפעתה על פעילות עסקית, תחרות הוגנת ורווחת צרכנים; ראש הממשלה רשאי לקבוע תקנות לעניין אופן ביצוע סעיף זה.

המערך – גורם מסדיר לאומי

44. (א) ראש המערך ינחה את הרשויות המאסדרות לעניין אופן יישום הוראות חוק זה בתחום הגנת הסייבר ביחס לתחום הנתון לסמכותם.

(ב) אסדרה בתחום הגנת הסייבר תיקבע בהתאם לעקרונות לפי סעיף 43, ובאישור ראש מערך הסייבר הלאומי.

(ג) מי שרואה עצמו נפגע כתוצאה מהחלטה של מאסדר בתחום אסדרת הגנת הסייבר, רשאי לפנות בבקשה לבחינה חוזרת של ההחלטה לראש מערך הסייבר הלאומי; בחינה חוזרת כאמור תעסוק רק בהיבטי הגנת הסייבר של ההחלטה ולא בעמדתו של מאסדר לגבי עניינים אחרים שבסמכותו; ראש הממשלה יקבע בתקנות הוראות לעניין הגשת בקשה לבחינה חוזרת כאמור וסדרי הדיון בבקשה.

הנחיות בתחום הגנת הסייבר

45. המערך יפרסם הנחיות בתחום הגנת הסייבר שיגובשו בהתאם לעקרונות המנויים בסעיף 43 ובכלל זה:

(1) מדיניות ונהלים לצורכי התמודדות עם איומי הסייבר בידי ארגון או עבורו;

(2) אמצעים מקובלים הנדרשים לצרכי הגנת הסייבר והתמודדות עם איומי סייבר;

(3) מצבי כוננות ודרישות הגנת הסייבר הנגזרות מהן בארגון;

(4) אופן הבדיקה של קיום הנחיות בתחום הגנת הסייבר בידי ארגון או עבורו;

(5) תהליכי הזדהות;

(6) אופן הדיווח למערך על תקיפות או איומי סייבר;

מיפוי המרחב האזרחי – המערך

46. (א) ראש המערך יורה על שיטה למיפוי חשיפת המשק לתקיפות סייבר שיש בהן כדי לפגוע באינטרס חיוני (להלן – השיטה).

(ב) השיטה תכלול התייחסות להיקף הפגיעה האפשרית באינטרס חיוני בשל תקיפת סייבר (להלן – תרחיש הנזק) בהתבסס, בין היתר, על שיקולים אלה:

(1) לעניין חומרת הפגיעה באינטרס חיוני -

(א) רמת השירות הנדרשת מסוגי ארגונים בשגרה ובחירום וטיב השירות ובכלל זה כפי שהוגדרו בידי רשות החירום הלאומית שהוקמה לפי החלטות הממשלה;

(ב) היקף הפגיעה האפשרית בחיי אדם;

(ג) גודל הציבור המשתמש בשירותי הארגון;

(ד) הנזק הכלכלי הצפוי;

(ה) היקף המידע המצוי בארגון, ורגישותו;

(ו) היקף הפגיעה בסביבה;

(ז) פגיעה משמעותית בפרטיות;

(ח) השפעה של תקיפת סייבר בארגון על תפקודם התקין של שירותי המיחשוב והאינטרנט בישראל;

(ט) השפעה של תקיפת סייבר בארגון על גורמי ייצור, משאבים, שירותים, תהליכים ומוצרים החיוניים לקיום האוכלוסייה, לכלכלת המדינה ולפעילות הגורמים המיוחדים בשגרה ובחירום.

(י) עמדת רשות מאסדרת לעניין איומי סייבר בארגונים מפוקחים על ידה;

(2) לעניין החשיפה לתקיפות סייבר – סוגים של איומי סייבר ביחס לפעילות ולהסתברות התרחשותם.

(ג) ראש המערך ידווח לראש הממשלה על השיטה;

(ד) ראש המערך יפרסם את עיקרי השיטה, באופן שאין בו, להנחת דעתו, כדי לסכן אינטרס חיוני.

הגדרת רשות מאסדרת

47. (א) בפרק זה, "רשות מאסדרת" – שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים משקיים המופיעים בתוספת השנייה; ראש הממשלה רשאי להוסיף בצו תחומים משקיים לתוספת השנייה לאחר שהתייעץ עם השר הממונה על התחום, ככל שיש כזה.

(ב) במקרים שבהם בתחום מתחומי הפעילות המנויים לעיל יש יותר מרשות מאסדרת אחת אשר יש לה סמכות הנחיה בתחום הגנת הסייבר, רשאי ראש הממשלה לקבוע בתוספת השנייה, לאחר שהתייעץ עם השרים הנוגעים בדבר, את הרשות המאסדרת האחראית למימוש הוראות פרק זה באותו תחום (להלן – רשות מאסדרת מובילה).

(ג) הרשות המאסדרת המובילה תפעל בתיאום עם הרשות המאסדרת האחרת בעלת הסמכות באותו תחום פעילות כאמור בסעיף קטן (ב).

תפקיד הרשות המאסדרת - מיפוי בתחום פעילותה

48. (א) רשות מאסדרת, בהתייעצות עם ראש המערך, תגדיר תרחישי נזק בשל תקיפות סייבר בתחום הפעילות שעליו היא אחראית ואת מידת חומרתם בהתאם לשיטה.

(ב) רשות מאסדרת תסווג את הארגונים המפוקחים על ידה לפי חומרת תרחישי הנזק והקשר של הארגונים אליהם.

אסדרה מגזרית למניעה והתמודדות עם תקיפות סייבר

49. (א) רשות מאסדרת בהתייעצות עם ראש המערך, תבחן את הצורך בקביעה או במתן הוראות בתחום הגנת הסייבר לארגונים המפוקחים על ידה, ככל שהדבר נדרש לצורך התמודדות עם תרחישי נזק שהוגדרו לפי סעיפים 46 או 48.

(ב) קביעת הוראות בתחום הגנת הסייבר בידי רשות מאסדרת תיעשה בהסכמה של ראש מערך הסייבר הלאומי.

(ג) נקבעה רשות מאסדרת מובילה לפי סעיף 47(ב) תבחן הרשות המאסדרת המובילה את הצורך בהוראות ביחס לארגונים מפוקחים במגזר שצוין בצו האמור.

הוראות למניעת תקיפות סייבר ולהתמודדות עמן

50. הוראות והנחיות לפי פרק זה יכללו את הדרישות האלה:

(1) דרישות המבוססות על ההנחיות לפי סעיף 45;

(2) דרישה כי ארגון מפוקח יהיה מסוגל להראות יישום אפקטיבי של המדיניות והנהלים, באמצעות הצהרה עצמית, חוות דעת מקצועית או סקר אבטחה מקצועי שבוצע על ידי גוף חיצוני; דרישות כאמור ייקבעו על פי אמות מידה שתקבע הרשות המאסדרת בהסכמת המערך, ובהתאם לרמת הסיכון;

(3) דרישה כי ארגון מפוקח יחזיק תיעוד מעודכן אודות מערכות המחשב המשמשות את הארגון ואבטחתן באופן המאפשר קבלת סיוע חיצוני במידת הצורך.

דרישות ארגוניות בתחום הגנת הסייבר – ממונה סייבר

51. (א) רשות מאסדרת רשאית להורות לארגון מפוקח, שרמת הנזק לפי תרחיש הנזק שאליו הוא חשוף היא גבוהה, למנות ממונה הגנת סייבר.

(ב) רשות מאסדרת, בהתייעצות עם ראש המערך, רשאית לקבוע כי ממונה הגנת הסייבר כאמור בסעיף קטן (א) יהיה בעל התאמה ביטחונית.

(ג) ראש הממשלה רשאי לקבוע בתקנות תנאים לגבי כשירותו, חובותיו ותפקידו של ממונה הגנת הסייבר בארגון.

דיווחים תקופתיים

52. רשות מאסדרת רשאית להורות לגבי ארגון מפוקח חובת דיווח תקופתי על אופן העמידה בהוראות לפי פרק זה.

יחידות הכוונה מגזריות

53. (א) לצורך מימוש האמור בחוק זה תהיה ברשות מאסדרת יחידת הכוונה להגנת סייבר.

(ב) ראש הממשלה יקבע תקנות לעניין תפקידים והכשרה הנדרשת ממי שמפעיל או מסייע להפעלת סמכויות אסדרה בתחום הגנת הסייבר ברשות מאסדרת.

(ג) על אף האמור בחוק המינויים, רשאי ראש הממשלה, לאחר התייעצות עם שר האוצר ועם נציב שירות המדינה, לקבוע בתקנות או בכללים הוראות אחרות מאלה החלות בשירות המדינה, לעניין ארגון וניהול כוח אדם הנדרש למימוש תפקידי יחידת הכוונה להגנת סייבר הפועלת ברשות מאסדרת, והכל בכפוף להוראות חוק יסודות התקציב, ולהוראות חוק התקציב השנתי.

(ד) לא ימונה עובד או יועץ בתחום הגנת הסייבר ליחידת הכוונה מגזרית אלא בהסכמת הגורם האחראי במערך.

54. **קיום הוראות הגנת סייבר כתנאי למתן היתר או רישיון וחידושו**

(א) רשות מאסדרת שמוסמכת להעניק לארגון היתר, רישיון, תעודה או כיוצא באלה (להלן - רישיון) , לפעילות לפי דין, רשאית להתנות מתן הרישיון כאמור או חידושו בקיום ההוראות שניתנו לפי סעיף 50, ורשאית היא לקבוע ברישיון כאמור תנאים שעל הארגון לקיים כתנאי לשימוש בזכויות לפי הרישיון.

(ב) הרשות המאסדרת רשאית לדרוש כי ארגון שהיא נתנה לו הוראות לפי סעיף 50, יוכיח עמידה בדרישות הוראות אלה באמצעות חוות דעת של מומחה מתאים; הרשות המאסדרת, בהסכמה של ראש המערך, רשאית להורות על אמות מידה לגבי מומחה ולגבי חוות דעת כאמור.

55. **סמכויות פיקוח**

הוסמך אדם כמפקח ברשות מאסדרת והוקנו לו סמכויות פיקוח לפי אותו דין, רשאי הוא להפעיל את סמכויות הפיקוח שהוקנו לו כאמור לשם פיקוח על ביצוע ההוראות לפי חוק זה.

56. **סמכות להתלות רישיון, להגבילו או לבטלו**

הוסמכה רשות מאסדרת בדין להתלות רישיון, לבטלו או להגבילו בשל הפרת תנאי הרישיון שניתן לפי דין או בשל הפרת הוראות הדין, יחולו סמכויות אלה, בשינויים המחויבים, גם בשל הפרת הוראות שנקבעו ברישיון או שניתנו לפי חוק זה.

57. **הנחייה ופיקוח ישירים של המערך על ארגונים**

(א) המערך יפקח במישרין לפי הוראות פרק זה על מגזר משקי המוגדר בתוספת השלישית; ראש הממשלה רשאי לתקן את התוספת השלישית בצו ולהורות על פיקוח והנחייה ישירים בידי המערך על פעילות במגזר משקי שקבע, ובלבד שהתקיימו כל אלה:

(1) המגזר כולל ארגונים המקיימים פעילות החשופה לתקיפות סייבר שפגיעה בה יכולה לגרום לפגיעה באינטרס חיוני;

(2) אין רשות מאסדרת בעלת סמכות, משאבים ויכולת ארגונית להנחות בתחום הגנת הסייבר בארגונים השייכים למגזר האמור;

(3) יש חשש סביר שלנוכח העדרה של רשות מאסדרת כאמור בפסקה (2), תתממש הפגיעה באינטרס החיוני המנוי בפסקה (1).

(ב) בסעיף זה "מגזר משקי" – ארגון או קבוצת ארגונים, שהפעילות העיקרית שלהם בעלת מאפיינים או צביון דומה.

58. **סמכות מתן הוראות במסגרת הנחיה ישירה**

הורה ראש הממשלה על הנחיה ופיקוח ישירים על ידי המערך, כאמור בסעיף 57, יחולו הוראות סעיפים 49 עד 52 על המערך כמפורט להלן:

(1) המערך ימפה את המגזר שבו עליו לבצע הנחייה ופיקוח ישירים בהתאם לשיטה.

(2) ראש המערך רשאי לתת הוראות לשם יישום הגנת הסייבר לארגונים במגזר האמור, ובכלל זה הוא רשאי להורות על מינוי ממונה הגנת סייבר וקבלת דיווחים תקופתיים.

סמכויות פיקוח במסגרת הנחיה ישירה

59. לשם פיקוח על קיום הוראות לפי סעיף 58 יהיו לעובד מוסמך שמונה לכך סמכויות אלה:

(1) לדרוש מכל אדם למסור לו את שמו ומענו ולהציג בפניו תעודת זהות או תעודה רשמית אחרת המזהה אותו;

(2) לדרוש מכל אדם הנוגע בדבר למסור לו כל ידיעה או מסמך שיש בהם כדי להבטיח או להקל על ביצוע הוראות פרק זה; בפסקה זו, "מסמך" - לרבות פלט, כהגדרתו בחוק המחשבים.

(3) להיכנס למקום, ובלבד שלא ייכנס למקום המשמש למגורים אלא על פי צו של בית משפט.

מתן הוראות לארגון במגזר שמצוי בהנחיה ישירה של המערך

60. נוכח עובד מוסמך כי ארגון לא קיים הוראות ליישום הגנת הסייבר שניתנו לפי סעיף 58(2) רשאי הוא להורות לארגון לנקוט את הפעולות הנדרשות לשם כך.

מתן סמכויות לרשות מאסדרת לשם הנחיית ארגון ברמת סיכון גבוהה

61. (א) ראש הממשלה רשאי להורות בצו על הוספת רשות מאסדרת לתוספת הרביעית, אם נוכח, בהתייעצות עם השר הממונה וראש המערך, כי התקיימו שני אלה:

(1) תחת פיקוחה של הרשות המאסדרת נמצא ארגון שתקיפת סייבר בו עלולה לגרום לנזק חמור לאינטרס חיוני בהתאם למיפוי שנערך לפי סעיף 48;

(2) אין לרשות המאסדרת סמכויות על פי דין להורות לארגון ליישם הוראות הגנה בסייבר, ולפקח על ישומן, בהיקף הנדרש להתמודדות עם הסיכון.

(ב) לרשות מאסדרת המנויה בתוספת הרביעית יהיו נתונות הסמכויות המנויות בסעיפים 58, 59 ו – 60 לצורך קיום הוראות חוק זה.

הנחייה ישירה זמנית בידי המערך

62. (א) נוכח ראש המערך כי לעניין ארגון מסוים מתקיימים התנאים הבאים, רשאי הוא להכריז כי הארגון יהיה נתון להנחיה זמנית על ידי המערך:

(1) הארגון מקיים פעילות שחשופה לתקיפות סייבר שעלולות לגרום לפגיעה חמורה באינטרס חיוני;

(2) הארגון אינו כפוף להנחיה ופיקוח על פי דין של רשות מאסדרת, ועקב כך עלולה להתממש הפגיעה באינטרס החיוני המנוי בפסקה (1).

(ב) קבע ראש המערך כאמור, יהיו נתונות לעובד מוסמך הסמכויות לפי סעיפים 58, 59 ו – 60 כלפי הארגון.

(ג) הנחייה לפי סעיף זה תהיה לפרק זמן שלא יעלה על שלושה חודשים מהכרזה לפי סעיף (א).

פרק ה׳: הוראות שונות

הארגון והדירקטוריון

63. דירקטוריון חברה מסוג שקבע ראש הממשלה בהתייעצות עם שר המשפטים (להלן – החברה), ידון לפחות אחת לשנה באלה:

(1) איומי הסייבר לפעילות החברה;

(2) הנזק שעלול להיגרם לתפקודה, לנכסיה, ללקוחותיה או לספקיה של החברה כתוצאה מהתרחשות תקיפת סייבר והסתברות התרחשות הנזק בשל תקיפת סייבר;

(3) משאבים שהוקצו לצורך צמצום החשיפה האמורה;

(4) הגורם האחראי בחברה על הגנת הסייבר, הסמכויות והמשאבים שניתנו לו לשם כך;

(5) אופן והיקף היישום של ההנחיות לפי סעיף 45;

פעילות מותרת לצורכי הגנת סייבר – הארגון

64. לא יראו פעולה שמבצע ארגון למטרת הגנת הסייבר של מחשבי הארגון כפגיעה בפרטיות, האזנת סתר, חדירה אסורה לחומר מחשב, אם מתקיימים בה כל אלה:

(1) לארגון יש מדיניות הגנת סייבר בהתאם להוראות או תקן מקובל ביחס לצרכי הגנת סייבר בארגון, בשים לב לאיומי הסייבר שלהם הוא חשוף;

(2) לארגון יש מדיניות גישה ושימוש במידע המעובד לצורכי הגנת הסייבר, המגבילה את האיסוף, השימוש ועיבוד המידע להיקף הנדרש לצורכי הגנת הסייבר;

(3) הארגון הודיע לעובדיו, ללקוחותיו ולגורמים אחרים שמידע עליהם עשוי להיאסף במסגרת פעילות זו, פרטים על הפעילות, על מטרותיה, ועל השימוש במידע;

בסעיף זה, ״מחשבי הארגון״ - מחשבים המצויים ברשותו כדין או בשימושו בהתאם לחוזה.

פעילות מותרת לצרכי הגנת הסייבר

65. (א) לא יראו שיתוף של מידע שנאסף בארגון, עם ארגון נוסף או יותר, או עם מערך הסייבר הלאומי כפגיעה בפרטיות לפי חוק הגנת הפרטיות, אם מתקיימים כל אלה:

(1) המידע הוא מידע בעל ערך אבטחתי;

(2) הארגון מסר פרטים על הפעילות, על מטרותיה, ועל השימוש במידע במסגרתה לעובדיו ולקוחותיו;

(3) השימוש במידע הוא למטרת הגנת הסייבר.

(ב) עובד המערך או מי שפועל מטעמו לא יישאו באחריות לפי חוק הגנת הפרטיות על פגיעה בפרטיות לפי חוק הגנת הפרטיות, שנעשתה באופן סביר במסגרת תפקידם ולשם מילויו.

שיתוף מידע לצורכי הגנה – פעולה מותרת

66. לא יראו שיתוף מידע בעל ערך אבטחתי בין שני ארגונים או יותר למטרת הגנת סייבר, כהפרה של הוראות חוק ההגבלים העסקיים, התשמ"ח-1988,[14] בתנאי שיתקיימו כל אלה:

(1) המידע אינו כולל נתונים על לקוחות, ספקים, כמויות או מחירים של הארגונים;

(2) המידע אינו כולל מידע על איכות מוצר או שירות המסופק על ידי אחד הארגונים.

תחולת החוק על גופים נוספים

67. סמכויות מכוח חוק זה לא יופעלו לגבי הגופים המנויים להלן, אלא בהסכמת הגורמים המנויים לצדם –

(1) לשכת נשיא המדינה – בהסכמת מנהל הלשכה;

(2) הכנסת – בהסכמת יושב ראש הכנסת;

(3) משרד מבקר המדינה – בהסכמת מבקר המדינה;

(4) ועדת הבחירות המרכזית לכנסת – בהסכמת יושב ראש הוועדה;

(5) הגופים המיוחדים – בהסכמת ראש הגוף;

(6) מערכת הביטחון והגופים המנויים בצו שר הביטחון לפי החוק להסדרת הביטחון – בהסכמת הממונה על הביטחון במערכת הביטחון.

סקרים משקיים ומגזריים

68. (א) ראש המערך או מי שהוא הסמיכו לכך, רשאי לערוך סקרים לאומיים או מגזריים על מנת לאתר פערים ברמת הגנת הסייבר ולבירור רמת ההגנה במרחב הסייבר במרחב האזרחי.

---

[14] ס"ח התשמ"ח, עמ' 128; התשע"ו, עמ' 126

(ב) כל אדם חייב, לפי דרישתו של ראש המערך, או מי שהוא הסמיך לכך מבין עובדי המערך, למסור לו את המידע, המסמכים, ושאר התעודות שלדעת ראש המערך יש בהם כדי להבטיח או להקל את ביצועו של סעיף זה.

הסדרים הסכמיים בתחום הגנת הסייבר

69. אין באמור בהוראות חוק זה כדי למנוע הסדרה של פעולות הקבועות בו באמצעות הסכמים, ובכלל זה במסגרת הסכמים שבין הגופים המיוחדים או משרד הביטחון לבין ספקיהם.

התקשרות עם גורמים מקבילים

70. (א) ראש המערך רשאי לחתום עם גוף בינלאומי הסכם לשיתוף פעולה ועזרה הדדית לשם התמודדות עם תקיפות סייבר או היערכות לקראתן, או לקידום שיתופי פעולה בתחום הסייבר במישור הבינלאומי; בסעיף זה - "גוף בינלאומי" – גוף העוסק בהגנת הסייבר במדינת חוץ, בין אם הוא רשות ממשלתית ציבורית או ארגון בינלאומי; ראש הממשלה יקבע בכללים הוראות לעניין פעילות לפי סעיף זה.

(ב) לא יועבר מידע מוגן לגוף בינלאומי אלא אם כן מדובר במידע בעל ערך אבטחתי ושוכנע ראש המערך, לאחר שנועץ במפקח הפנימי על הפרטיות, כי הוא ישמש אך ורק למטרה שלשמה נמסר.

הסמכה לביצוע פעולות לסיכול תקיפת סייבר הנמנית בין יעדי שירות הביטחון הכללי

71. (א) לצורך סיכול איומי טרור וריגול, כמשמעותם בסעיף 7 לחוק שירות הביטחון הכללי, רשאי ראש שירות הביטחון הכללי (להלן – ראש שב"כ), להסמיך בעלי תפקידים מבין עובדי שירות הביטחון הכללי (להלן – שב"כ) בסמכויות הנתונות לעובד מוסמך או גורם אחראי לפי סעיפים 19 עד 36 לחוק.

(ב) הפעלת סמכויות לפי סעיף (א) תיעשה לאחר שהתקיימו כל אלה:

(1) ראש שב"כ השתכנע כי יש תקיפת סייבר והתקיימו יתר התנאים הקבועים בסעיף 19 לחוק (להלן – התקיפה);

(2) ראש שב"כ השתכנע כי הפעלת הסמכות נדרשת לצורך סיכול איומי טרור או ריגול כמשמעותם בסעיף 7 לחוק שירות הביטחון הכללי, הנובעים מהתקיפה;

(3) ראש שב"כ או עובד בכיר שהוא מינה לכך התייעץ עם ראש מערך הסייבר הלאומי או עובד בכיר שהוא מינה לכך לעניין הפעלת הסמכות לפי סעיף זה;

(ג) יתר הוראות החוק למעט סעיפים 13 עד 15 יחולו על הפעלת סמכויות לפי סעיף קטן (א) ומידע שנאסף באמצעותן.

איסור על גילוי מידע על פעילות המערך
72. פעילות מערך הסייבר לפי חוק זה אסורה בגילוי אלא בהתאם להוראות חוק זה או להוראות שיקבעו ראש הממשלה ושר המשפטים.

תקנות
73. ראש הממשלה ממונה על ביצועו של חוק זה, והוא רשאי להתקין תקנות לביצועו.

תוספת ראשונה (סעיף 41)

תוספת שנייה (סעיף 47)

שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים המשקיים האלה:

(1) שירותים פיננסיים;

(2) שירותי בריאות ורפואה;

(3) תחבורה, תחבורה ציבורית, תובלה, תעופה, ושייט;

(4) הגנת הסביבה;

(5) ייצור אנרגיה והולכתה;

(6) מים וביוב;

(7) שירותי דואר ותקשורת, שירותי בזק ושידורים מסחריים

תוספת שלישית (סעיף 57)

תוספת רביעית (סעיף 61)

דברי הסבר

כללי כתוצאה מהיקף האיומים במרחב הסייבר וחומרתם, עלול להיגרם נזק לרציפות במתן שירותים חיוניים, לחיי אדם, לפעילות המשק ולאינטרסים לאומיים חיוניים אחרים, ועל כן החליטה הממשלה על הקמת מערך הסייבר הלאומי. לשם מימוש ייעודו להגנת מרחב הסייבר ולצורך מילוי תפקידיו, מוצע להעניק למערך סמכויות שונות במרחב הסייבר, כמפורט להלן.

פרק ב׳: מערך הסייבר הלאומי ייעודו ותפקידיו

סעיף 2 מוצע להסדיר בחקיקה את פעילותו של מערך הסייבר הלאומי הפועל במשרד ראש הממשלה, בכפיפות לראש הממשלה, בהתאם להחלטות הממשלה.[15] המערך פועל כיום בתחום הגנת הסייבר בהתאם להחלטות הממשלה בנושא זה, וכן בהתאם לחוק להסדרת הביטחון בגופים ציבורים, התשע״ו–2016 (הוראת שעה). מערך הסייבר הלאומי הוא גוף בטחוני מבצעי שמשימתו הגנה לאומית בתחום הסייבר המבוססת על תחום טכנולוגיית המידע (מחשבים, רשתות ואבטחת מידע) תוך ביצוע פעילויות בטחוניות אופרטיביות ורגולטוריות, שתכליתן למנוע מהאיום להתממש.

סעיף 3 התפקידים מגדירים את משימותיו העיקריות של מערך הסייבר הלאומי. בפרקי החוק הוסדרו הסמכויות הנדרשות למימוש משימות ההגנה של מערך הסייבר. סעיפי הסמכות כוללים הסדרים ותנאים מפורטים יותר באשר לאופן מימוש התפקידים והפעלת הסמכויות.

סעיף 4 ראש המערך הוא הסמכות המנהלית והמבצעית הבכירה במערך, והוא מתמנה בהתאם לכללים החלים על משרות בטחוניות בכירות. כיום מופיעה משרתו של ראש המערך בתוספת השנייה לחוק שירות המדינה (מינויים), התשי״ט-1959. מוצע כי ראש המערך יידרש למסור לראש הממשלה אחת לשנה דוח על מצב הגנת הסייבר.

סעיף 5 מערך הסייבר הוא גוף בטחוני מבצעי ולכן עובדי המערך נדרשים להיות זמינים למענה לטיפול בתקיפות סייבר וממשקים עם הארגונים במרחב האזרחי ועם גורמי מערכת הביטחון, בשגרה ובחירום.

מאפיינים אלה מחייבים שינויים מסוימים בהיבטים ארגוניים ובמסגרת הארגונית שבה הוא פועל, בדומה לארגונים בטחונים וארגונים רגולטוריים אחרים במנהל הציבורי הישראלי. מסגרת זאת צריכה להיקבע תוך שמירה על עקרונות היסוד של המנהל הציבורי, ובזיקה לגורמים המופקדים על תחומים אלה בממשלה ובמרכזם נציבות שירות המדינה. קביעתה של מסגרת משפטית בהתאם להוראות חוק זה משקפת את המאפיינים הייחודים של פעילות זו, ולצד זאת את החשיבות הרבה של קיום מסגרת נורמטיבית סדורה.

מוצע להסדיר את הסמכות של ראש הממשלה לקבוע הוראות מתאימות שיאפשרו לממש את הצרכים הארגוניים של מערך הסייבר הלאומי.

סעיף 6 לנוכח המידע הרגיש אודות גופים אזרחיים שנתקפים, וכן אודות שיטות הגנה עליהם, מוצע שעובדי המערך יהיו תחת חובת סודיות ייעודית.

סעיף 7 ייעוד מערך הסייבר הוא הגנה על הביטחון הלאומי בתחום הסייבר. מעצם טיבה תקיפת סייבר היא תקיפה

---

[15] בהחלטת ממשלה מספר 3611 בנושא ״קידום היכולת הלאומית במרחב הקיברנטי״ מיום 07.08.2011 (להלן – החלטה 3611), הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה) והוטל עליו, בין היתר, לגבש תפיסת הגנה לאומית למרחב הסייבר. בהחלטות הממשלה מספר 2443 (״קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר״) ו- 2444 (״קידום ההיערכות הלאומית להגנת הסייבר״) מיום 15.02.2015 אישרה הממשלה את התפיסה שגיבש המטה.

עוד יצויין כי ביום 17.12.17 קיבלה הממשלה החלטה מספר 3270 שבה נקבע כי המטה והרשות יאוחדו לגוף אחד – מערך הסייבר הלאומי (להלן - המערך).

המצויה בקרב המערכות ועלולה להתפרץ וליצור סיכון משמעותי לאינטרסים ציבורים חיוניים. ככל עובדי המערך על עתודותיו נדרשים לזמינות שתאפשר להם לאתר את האיום מבעוד מועד ולטפל בו ככל שהוא מתממש, תוך דאגה לטיפול לאלתר במניעת הנזק או במזעורו. תקיפות סייבר משמעותיות שהתפרצו בעולם חייבו התגייסות מיידית של מערכי הטיפול באירועי סייבר ותגבור הפעילות השגרתית.

מכל הטעמים הללו נבנה בימים אלו מערך הסייבר הלאומי כגוף הירכי מבצעי המופקד על תפעול אירועי סייבר ומתן הנחיות התגוננות בשגרה ובחירום ברמה הלאומית.

על מנת להגשים את ייעודו כבר כיום מפעיל מערך הסייבר הלאומי, את המרכז הלאומי לסיוע בהתמודדות עם אירועי סייבר (להלן – ה- CERT הלאומי) במתכונת עבודה רציפה בכל ימות השבוע ושעות היממה. פעילות זו מבוצעת באופן רציף הן מול שותפי משימות ההגנה שבקהיליית הביטחון, והן עם גורמים אזרחיים נוספים הפעילים בכל ימי השבוע.

עקב הצורך והחשיבות בקיום גורם מומחה טכנולוגי מבצעי לאומי בזמינות מלאה לטיפול בתקיפות סייבר, מוצע לקבוע איסור על התאגדות של עובדי המערך, על מנת למנוע אפשרות של שביתה שבה תיפגע הרציפות התפקודית של המערך. המערך כגוף מבצעי בטחוני המטפל באיומים ובסיכונים לאינטרסים חיוניים במרחב האזרחי, דומה לגופים בטחוניים אחרים שבהם לא ניתן לאפשר הפסקת פעילות בשל שביתה. רוחב המשימה מחייב ביתר שאת זמינות מלאה של עובדי המערך בהתאם לצורך. תפקידי המערך מחייבים "רציפות תפקודית" מלאה שלו בשגרה ובחירום, שכן ההגנה על מרחב הסייבר נעשית כל העת, והפסקת הפעילות השוטפת או יכולת התגובה לאירועים עלולה ליצור פערים ברמת ההגנה וחשיפה לניצול חולשות. בהתאם לכך, ניתן גם לראות בעובדי המערך כמי שחלים עליהם הוראות סעיף 30(א) לחוק שעות עבודה ומנוחה התשי"א-1951.[16]

סעיף 8 הסעיף נועד להקנות הגנה לעובדי המערך והפועלים מטעמו על מנת לאפשר ביצוע המשימות הטכנולוגיות והבטחוניות אשר נעשו בתום לב ובאופן סביר במסגרת התפקיד ולשם מילויו.

סעיף 9 מערך הסייבר נדרש להגן על עצמו מפני תקיפות סייבר, ובהתאם לכך מוצע כי המערך יקבע תפקיד ברור של ממונה הגנת הסייבר. הסדר זה הולם גם את העצמאות האבטחתית של מערך הסייבר הלאומי בהתאם לחוק להסדרת הביטחון בגופים ציבורים, התשמ"ח-1998.

סעיפים 10-12 בהתאם לעבודת המטה שבוצעה בין משרד המשפטים והרשות להגנת הפרטיות לבין גופי הביטחון, הוצע בהצעת חוק הגנת הפרטיות (סמכויות אכיפה) (תיקון מספר 13), התשע"ח-2018[17] לקבוע מפקח פרטיות פנימי אשר תפקידו לפקח על קיום הוראות חוק הגנת הפרטיות במסגרת פעילות המערך, תוך שמירה על מאפייניה המסווגים והרגישים של הפעילות. להקמה של פונקציה פנימית חשיבות להפנמה של עקרונות הגנת הפרטיות בפעילות המערך, ולצד פעילות הפיקוח מוצע כי למפקח הפרטיות הפנימי יהיה מעמד בעת מימוש עקרונות הפרטיות ועיצוב לפרטיות הקבועים בחוק ולפיו.

סעיפים 13-15 מוצע להקים ועדה חיצונית מפקחת בראשות שופט בדימוס או משפטן בכיר אחר אשר תפקידה לפקח על היבטי הפרטיות של פעילות מערך הסייבר, ולדווח על כך לראש הממשלה. חברי הוועדה צריכים להיות בעלי רקע רלבנטי ובכלל זה היכרות עם תחום הפרטיות, הביטחון והטכנולוגיה. על מנת להקנות לוועדה יכולת פיקוח עצמאית מוצע להסמיך אותה בסמכויות קבלת מידע.

פרק ג' סמכויות המערך

סעיף 16 מוצע לקבוע כי המערך מוסמך, בין השאר, לקבל ולאסוף מידע בעל ערך אבטחתי ומידע שעשוי לשמש

[16] ס"ח התשי"א, עמ' 204; התשע"ח, עמ' 284
[17] ה"ח התשע"ח, עמ' 1206

להפקת מידע כאמור; לעבד את המידע האמור כך שיוכל לשמש לטובת העלאת חוסן הארגונים במשק מפני תקיפות סייבר ויסייע לארגונים בהתמודדות עמם.

כמפורט במבוא, הקמה של גוף לאומי לאיסוף ושיתוף מידע בעל ערך אבטחתי הוא רכיב מרכזי באסטרטגיות הגנת סייבר במדינות המפותחות. הדירקטיבה של האיחוד האירופי בתחום הגנת הסייבר, Network Information Security Directive, דורשת מהמדינות החברות להקים מרכז שיתוף מידע מדינתי, שיפעל מול כלל המשק והארגונים הפועלים בו. חקיקה זו נכנסה לתוקפה ביום 10.05.2018.

עוד מוצע לכלול בסעיף הסמכה של ראש הממשלה, בהסכמת שר המשפטים, להתקין תקנות שבהן ייקבעו עקרונות לאיסוף ועיבוד מידע שתכליתן להבטיח שככל שהפעולות הנוגעות למידע יכולות להביא לפגיעה בפרטיות או במידע רגיש אחר, יינקטו אמצעים למניעה או למזעור פגיעה זו, אם בנקיטת אמצעים מקדמיים (privacy by design) או באמצעות בקרות מפצות. כיום פועל המערך בהתאם למסמך עקרונות ה- CERT הלאומי אשר תואם עם היועץ המשפטי לממשלה. ביטוי נוסף לנושא זה גם בסעיף 38 "עיצוב לפרטיות, הגנה על מידע מוגן – עקרונות על", כמפורט להלן.

סעיפים 17-18 היכולת לאתר תקיפות סייבר ובפרט תקיפות מתקדמות והתפשטותן מבוססת על איתור פעילות חריגה או סממנים לפעילות חריגה במרחב הסייבר. לכן יש צורך באיסוף מידע טכנולוגי אשר ניתן יהיה לאתר באמצעותו תקיפות או תקשורות עם תקיפות. מסיבה זו קיים צורך להקים מערך גילוי וזיהוי שמבוסס על איסוף ועיבוד מידע בעל ערך אבטחתי בזמן אמת, במטרה לאפשר גילוי מוקדם של תקיפות סייבר והתמודדות עמן.

מערך הגילוי והזיהוי נועד להיות מערכת "על ארגונית" כזו. הוא לא נועד להחליף את מערכות ההגנה הארגוניות או את הצורך של הארגונים לנטר את הפעילות במחשביהם באופן שוטף. הנחת העבודה היא כי איתור מתקדם של תקיפות סייבר במרחב הישראלי מחייב יכולת איתור על ארגונית.

בין הגופים שיכלול מערך הגילוי והזיהוי מנויים משרדי הממשלה, גופים הנמנים בתוספת החמישית לחוק להסדרת הביטחון בגופים ציבוריים, וכן גופים ציבורים נוספים אשר שיתופם יתרום לאיתור תקיפות סייבר ולהגנה עליהם. הסעיף מאפשר הכללת בעלי רשיונות לפי חוק התקשורת, אך מתנה לגבי בעלי רישיונות שניתן לגביהם צו לפי סעיף 13 לאותו חוק, שחיבורם למערך הגילוי והזיהוי יעשה באישור הגורם המוסמך האחראי על אותו בעל רישיון. ארגונים נוספים שיתנו הסכמתם לכך, לפי בחירתם, יוכלו אף הם להיכלל במערך הגילוי והזיהוי. עוד כולל הסעיף אפשרות לכלול גוף שאינו מנוי בסעיף ושלא נתן הסכמתו, ככל שהוברר כי שיתופו של גוף זה יתרום תרומה ממשית לגילוי מוקדם של איומי סייבר וכי הוא מספק שירותים בהיקף משמעותי במרחב הסייבר הישראלי. מהלך זה מחייב הוראה מפורשת של ראש הממשלה ושר המשפטים.

לנוכח חשיבות השמירה על הפרטיות, לצד הוראות סעיף 38 הסעיפים כוללים הוראות בתחום "עיצוב לפרטיות", כלומר הוראות שמטרתן שילוב אמצעים טכנולוגיים ומנהליים שמטרתם צמצום סיכוני פרטיות, כגון צמצום איסוף המידע הנדרש לצורך איסוף מידע בעל ערך אבטחתי, צמצום החשיפה של מידע מוגן או ניתן לזיהוי במסגרת פעילות מערך הגילוי והזיהוי.

בנוסף המערך נדרש לפרסם מידע שמטרתו גילוי ושקיפות אודות השותפות במערך הגילוי והזיהוי ללקוחות ועובדים של הארגונים.

תכליתו המבצעית של מערך הגילוי והזיהוי מביאה לכך שעיצובו ופעילותו הטכנולוגיים אינם מכוונים לאיסוף מידע אודות יחידים, אלא אודות סממנים לתקיפות ממוחשבות, שמאפשרים זיהויים המוקדם והתמודדות עם התפשטותם.

העקרונות המשפטיים שתוארו לעיל נועדו להבטיח כי מאפיינים אלה יבואו לידי ביטוי בפעילותו של מערך הגילוי והזיהוי, וכן יפותחו בתקנות ובכללים לפי הסעיף. כך למשל, ניתן יהיה להסדיר גישה למידע שנאסף במערך הגילוי והזיהוי באופן שייחשף מידע מוגן או מידע שניתן לזיהוי רק בנסיבות שייקבעו בנהלי המערך שבהן אין אפשרות אחרת לאתר תקיפת סייבר או להתמודד עמה.

יובהר כי אין הכוונה להקים בהתאם להוראות אלה מערכת מעקב או ניטור על תקשורת או פעילות יחידים, או ניטור של סוד שיחס, אלא מערכת הגנה מפני תקיפות סייבר אשר חלק ממושא הגנתה מצוי בתחום התקשורת. איסוף מידע למטרות אחרות מאשר איתור תקיפות, כגון לצורך האזנת סתר לאדם מסוים הטעונה היתר לפי חוק האזנת סתר, אינה מוסדרת בהצעה, ולכן יחול עליה הדין הרלבנטי.

סעיף 19 סעיף זה הוא סעיף כללי שחל על כל הפעלת סמכות מהסמכויות המוצעות בפרק ג׳. הסעיף מבהיר כי תנאי מקדמי להפעלת הסמכויות על ידי המערך הוא קיומו של יסוד סביר להניח כי מתבצעת מתקפת סייבר שעלולה לגרום פגיעה לאינטרס חיוני והפעלת הסמכות נדרשת לאיתור התקיפה, התמודדות עמה או מניעתה. עוד ישקול בעל הסמכות, טרם הפעלתה, אם הפעלת הסמכות עלולה לגרום פגיעה בזכויות במידה העולה על הנדרש, ככל שפגיעה כזו מסתברת מהפעלת הסמכות. הסעיף מבהיר, כי בעל הסמכות מחויב לבחור בדרך הפוגענית פחות שעומדת לפניו לשם הטיפול במתקפת הסייבר, האפשרית בנסיבות הענין. בכך קובע הסעיף באופן מפורש את הדרישה להפעלה מידתית של הסמכויות בכל מקרה שבו נדרשת הפעלתן.

בהתאם לעקרונות הסעיף, נהלי העבודה של המערך יסדירו את מסגרת שיקול הדעת על מנת לאפשר התמודדות מהירה וקבלת החלטות מבצעית במידה שנדרש, תוך שמירה על מסגרת שיקול הדעת.

סעיף 19 (ה) נועד להבהיר, כי מקום שארגון מבקש מהמערך סיוע, ומתקיימות הוראות סעיף 35 לעניין אופן מתן הסכמה (לפי העניין), המערך יכול לסייע לו בדרך של הפעלת סמכויות כלפי הארגון גם לעניין תקיפות שאינן במדרג החומרה הגבוה. זאת על בסיס משימתו הכללית של מערך הסייבר לסייע לקידום הגנת הסייבר בישראל, ועל בסיס הניסיון שהצטבר בדבר הערך בפעילות זו. כיום מסייע מערך הסייבר באמצעות ה-CERT הלאומי לארגונים וליחידים הפונים אליו, גם בתקיפות שאינן בהכרח תקיפות ברמת החומרה הגבוהה ביותר, וזאת במסגרת המשאבים הקיימים והרצון לקדם את הגנת הסייבר בישראל.

סעיף 20 מוצע להסמיך עובד מוסמך של המערך לדרוש מארגון הנוגע בדבר מידע ומסמכים ובכלל זה עותק של חומרי מחשב הנדרשים לצורך מניעת תקיפת הסייבר, מיזעור נזקיה, או טיפול אחר בה. הפעלת סמכות זו, כפופה לקיומו של יסוד סביר להניח שמתרחשת תקיפת סייבר כפי שמובהר בסעיף 19.

סעיף 21 מוצע, על מנת לטייב את איתור תקיפת הסייבר וכן את ההתמודדות עמה, לאפשר לעובד מוסמך במערך להורות לארגון הנוגע בדבר, למנות איש קשר לשם קבלת הוראות והעברת מידע לפי הוראות הפרק.

סעיף 22 מוצע לאפשר לגורם אחראי במערך להיכנס או להורות לעובד מוסמך להיכנס למקום שיש יסוד להניח שנמצא בו מחשב או חומר מחשב המכיל מידע בעל ערך אבטחתי הנדרש לפעילות הגנת סייבר לפי חוק זה, ובלבד שלא ייכנס למקום המשמש למגורים אלא על פי צו מאת בית משפט השלום, ולאחר שהזדהה כעובד המערך. מאחר שמרחב הסייבר הרלבנטי בעת תקיפה בארגון, מורכב ממחשבים של הארגון המצויים לרב בחצריו, סמכות הכניסה נדרשת על מנת לאפשר לעובד המוסמך לבצע פעילות בחצרי הארגון. גם למקרה אחרון זה מוצע חריג בסעיף. ניתן להיכנס ללא צו גם למקום שהכניסה אליו מחייבת צו שופט, ככל שמתחייבת גישה מיידית למקום לנוכח הסכנה הממשית והמידית לשלום הציבור או בטחונו הנובעת מתקיפת הסייבר, והעדר קיומן של אפשרויות פעולה אחרות וזאת באישור ראש המערך.

סעיף 23 מוצע להסמיך עובד מוסמך לתפוס חפץ שיש לו יסוד סביר להניח כי הוא מכיל מידע בעל ערך אבטחתי, לשם ביצוע בדיקה מיידית הנדרשת לצורך איתור התקיפה, התמודדות עמה או מניעתה. לעניין זה מובהר, כי תפיסת חפץ כאמור תיעשה לאחר שהעובד המוסמך יתן למחזיק החפץ הזדמנות לטעון טענותיו. אם מתן זכות הטיעון טרם התפיסה עשויה להביא לפגיעה ביכולת לאתר את התקיפה או ביכולת להתמודד עמה או ביכולת למנוע אותה, והדבר יביא לסכנה ממשית ומיידית לשלום הציבור או בטחונו – תינתן למחזיק זכות טיעון מאוחרת לתפיסה. חפץ שנתפס לפי סעיף זה, יוחזר תוך חמישה עשר ימים למחזיק שנתפס ממנו. הסעיף מקנה סמכות לבית משפט שלום לדון בהחזקת החפץ שנתפס ולהורות על המשך ההחזקה שלו בידי המערך מעבר לחמישה עשר הימים הראשונים או על החזרתו לארגון ממנו נתפס, על פי בקשתו.

סמכות זו נדרשת על מנת לאפשר ביצוע בדיקות פורנזיות מעמיקות יותר בחומר מחשב, או תפיסת מחשב נגוע

לצורך הפסקת פעילות הפצה או הדבקה, וכן למצבים שבהם לא ניתן להעתיק את חומר המחשב בשל היותו משולב ברכיב פיזי. יובהר כי הסעיף עצמו אינו מסמיך ביצוע פעולה בחומר מחשב בחפץ. לצורך כך יידרש צו פעולה בחומר מחשב לפי סעיף 27 או הסכמה של הארגון לפי סעיף 35.

סעיף 24 סמכות נוספת שמוצע ליתן לעובד המוסמך היא הסמכות לדרוש הצגה או המצאה של חפץ המכיל מידע בעל ערך אבטחתי ובדיקתו המידית נדרשת לצורך איתור מתקפת הסייבר, התמודדות עמה או מניעתה. העובד המוסמך יציין בדרישתו את הזמן, המקום והאופן שבו יוצג החפץ המבוקש.

סעיף 25 הטיפול בתקיפת סייבר דורש לעתים מומחיות ספציפית. כך למשל, במקרים שבהם התקיפה היא במערכות מחשב המשמשות לצורך בקרה תעשייתית בתעשייה מסויימת, או במקרים אחרים שבהם התקיפה כוללת שימוש בכלים ייחודיים. לא תמיד הידע האמור נמצא בידי עובדי המערך ולעיתים נדרשת מומחיות של מומחים מהשוק הפרטי. בנסיבות אלה יש צורך בהסתייעות במומחים חיצוניים בתחום הגנת הסייבר, ולכן מוצע לקבוע כי עובד מוסמך במערך יהיה רשאי להסתייע במומחה חיצוני שהוא בעל ניסיון, ידע או אמצעים הנדרשים לטיפול בתקיפת סייבר. המומחה אינו צריך להיות עובד ציבור, אך העובד המוסמך יפקח על ביצוע הפעולות על ידו.

סעיף 26 מוצע כי לצורך איתור תקיפת סייבר והתמודדות עמה יוסמך עובד מוסמך במערך לתת הוראות לארגון, ובכלל זה הוראות בדבר ביצוע פעולות בחומר מחשב של הארגון, בידי הארגון או מי מטעמו. הוראות מסוג זה יינתנו רק שהן נדרשות לצורך איתור תקיפת סייבר, התמודדות עמה או מניעתה. סעיף זה הוא סעיף מרכזי ביכולת ניהול ההגנה מפני תקיפת הסייבר על ידי המערך.

בהוראות ניתן לכלול מגוון רחב של פעולות בחומר המחשב. רשימת הפעולות הנכללות במונח "פעולת חומר מחשב" שהעובד המוסמך רשאי להורות על ביצוען בידי הארגון מנויה בהגדרת "פעולה בחומר מחשב" בסעיף ההגדרות.

על מנת לייצר הבנה, שקיפות והגנה על הארגון בדבר הפעולות הנדרשות מובהר בסעיף שהעובד המוסמך יפרט בבקשה הן את הרקע העובדתי שהוביל למסקנה שנדרשות הפעולות הספציפיות המבוקשות והן את ההסבר המקצועי טכנולוגי ביחס להן. מאחר שהפעולות יבוצעו על ידי הארגון או נציגו עשויה להידרש מהם שמירה על סודיות. הדבר נדרש, בין היתר, כדי לא להביא לידיעת התוקף את העובדה שדבר התקיפה נחשף ומטופל, מה שעלול לסכל את השלמת הטיפול הכולל ומניעת הישנותו.

הפעילות לפי סעיף זה מבוצעת במערכות הארגון בידי עובד הארגון ומטעמו, וללא פעולה ישירה בחומר מחשב בידי עובד המערך. במידה שנדרשת פעילות בידי עובד המערך, נדרש לבקש צו לפי סעיף 27 או לקבל הסכמה לפי סעיף 35, אלא אם מדובר בפעולת הגנת סייבר דחופה לפי סעיף 36.

סעיפים 27-28 לעתים מתעורר צורך מקצועי בביצוע פעולות במחשב או חומר מחשב שבארגון על ידי עובד המערך עצמו ולא על ידי הארגון (או מי מטעמו) בהנחיית העובד המוסמך.

במקרים אלה עשויה גם להידרש הפעלה של כלים ייחודים שהפעלתן היא חלק מהמומחיות וההתמחות של המערך. מוצע כי פעילות זו תבוצע רק לאחר קבלת אישור מבית משפט השלום, אשר יהיה רשאי להתיר בצו לעובד מוסמך לבצע את הפעולות הנדרשות. הסעיף כולל הבניה של השיקולים שבית המשפט ישקול טרם מתן הצו שעיקרם איזון בין חומרת תקיפת הסייבר מחד גיסא, ופוטנציאל פגיעה בארגון או בפרטיות, מאידך גיסא. הדיון צריך להתקיים במעמד הארגון בו מבוצעת הפעולה, ככל הניתן.

סעיף 29 ברירת המחדל המוצעת בסעיף זה, היא דיון המתקיים במעמד שני הצדדים. לכלל זה יש חריג בהתקיים טעמים המצדיקים הגשת חומר חסוי. במקרה אחרון זה, מוצע לאפשר לעובד המוסמך להגיש את החומר החסוי לבית המשפט שייעתר לעיון בחומר זה מבלי להציגו למשיב (נציג הארגון) אם יסבור כי חשיפת החומר עלולה לסכל את הטיפול בתקיפת הסייבר ובפרט אם יגיע לידיעת התוקף. פעולות במחשב או בחומר המחשב יבוצעו בידיעת הארגון, ובנוכחות נציג מטעמו, למעט במקרים שבהם הדבר עשוי לסכל את ביצוע הפעולה.

מוצע להסמיך את ראש הממשלה ושר המשפטים לקבוע סדרי דין למימוש הוראות הפרק.

סעיף 30 על החלטת בית המשפט ניתן להגיש ערעור בתוך 30 יום מקבלת ההחלטה.

סעיף 31 ביצוע הצו ייעשה ככל הניתן בנוכחות נציג מטעם הארגון.

סעיפים 32-33 לצד הפעילות הריאקטיבית של איתור והתמודדות עם תקיפות סייבר, ופעולת מערך הגילוי והזיהוי, שאף היא אמורה לסייע בגילוי תקיפות כאמור, עולה לעתים צורך בחיפוש אקטיבי לשם איתור תקיפת סייבר. צורך זה הוא פועל יוצא של מאפייני פעילות בארגון או הקישוריות שלו לארגונים אחרים במשק. לשם כך, מוצע כי שופט בית משפט השלום יהיה רשאי, לפי בקשת גורם אחראי במערך, להתיר בצו ביצוע פעולה בחומר מחשב של ארגון לצורך ביצוע הפעולות כאמור.

סעיף 33 מאחר שהבקשה לביצוע פעילות כאמור נסמכת על ניתוח מודיעיני של אטרקטיביות הארגונים שעלולים לשמש כיעדים לתקיפת סייבר, הדיון בבקשה צריך להיות בדלתיים סגורות והפרוטוקול שלו חסוי.

סעיף 34 מאחר שחלק מהפעולות המנויות בפרק זה יכולות להתפרש כחדירה לחומר מחשב או כהאזנת סתר, לנוכח ההגדרות הטכניות בחוקים האמורים, מוצע להבהיר כי הן אינן נופלות למסגרת זו.

סעיף 35 הנחה בסיסית ועקרונית ביחס לפעולת המערך היא שיש לו ולארגון המותקף אינטרס משותף באיתור התקיפה, בזיהויה, בהכלתה, ובהתמודדות עמה תוך מזעור הנזקים. מסיבה זו מוצע לעגן את האפשרות לבצע את הפעולות המנויות בפרק הסמכויות בהסכמת הארגון שהפעולות המבוקשות מתייחסות למערכות המחשב או מערכות המידע שלו. מודגש בהקשר זה, כי על אף שקיימת עילה להפעלת הסמכות הרי ההנחה בדבר הפעולה הנדרשת, שמיועדת להבטיח את האינטרסים של הארגון ולהגן עליו מתקיפה, שונה ממצב שבו ההסכמה הניתנת היא לשם הפעלת סמכויות שמנוגדות לאינטרס של מי שהן מופעלות כלפיו (למשל, במישור הפלילי – חיפוש במקום). על אף זאת, מוצע ליידע את הארגון בדבר הסיבות שבגינן נדרש ביצוע הפעולה ואת זכותו לחזור בו מהסכמתו כדי להבטיח שקיפות מלאה של פעולות המערך ביחס לארגון.

על מנת להבטיח שההסכמה ניתנת בצורה שקופה וברורה, הסעיף המוצע כולל דרישות גילוי כלפי הארגון, על מנת לאפשר לו לקבל החלטה מושכלת ומודעת בנושא.

סעיף 36 מטרת הסעיף לאפשר מענה מהיר במקרים שבהם עולה חשש ממשי לתקיפת סייבר שעלולה לגרום לנזק משמעותי, ולצורך הטיפול בה נדרש עובד המערך או הפועל מטעמו לבצע פעולה בחומר מחשב ברשת הארגון, ואין שהות לפנות לבית המשפט לקבל צו. במקרים חריגים אלה, מוצע כי ראש המערך יהיה רשאי להורות על הפעלת הסמכות, אולם יידרש להודיע על כך ללא דיחוי ליועץ המשפטי לממשלה, וכן לפנות לבית המשפט, לעדכן אותו לגבי הפעילות, ולקבל את הנחיותיו באשר להמשך. עדכונו המיידי של היועץ המשפטי לממשלה מאפשר לבצע בקרה מיידית על אופן הפעלת הסמכות, והפנייה לבית המשפט תוך פרק זמן קצר מבטיחה כי הנושא יוחזר לנתיב הבסיסי המוצע בפרק.

סעיף 37 מטרתו של סעיף זה להסדיר את הממשקים עם רשויות אחרות בעלות סמכות, אשר ייתכן שנדרשות לסייע במניעת פגיעה באינטרסים חיוניים כתוצאה מתקיפת סייבר, בפעילות שאינה במרחב הסייבר. לצורך כך נדרש מנגנון תיאום אשר יאפשר קבלת סיוע ושיתוף פעולה.

סעיף 38 מטרתו של סעיף זה להטיל על ראש המערך או מי מטעמו, אחריות למימוש העקרונות המקובלים לעיצוב לפרטיות במסגרת מערכות והתהליכים שבהן נאסף או נשמר מידע מוגן, שהוא מידע שחוק הגנת הפרטיות חל עליו או מידע רגיש מסחרית. עקרונות אלה כוללים עיצוב טכנולוגי של איסוף מידע לא מזוהה ככל הניתן, וביצוע עיבודים על המידע באופן שהוא לא מזוהה, וכן שילוב בקרות טכנולוגיות שיאפשרו פיקוח על עמידה בהוראות החוק ובכללים לפיו. מאחר שמדובר בנושא טכנולוגי מתפתח, נדרש כי עקרונות נוספים ייקבעו בחקיקת משנה באופן שיאפשר התאמה טובה יותר למציאות הטכנולוגית והמבצעית. מוצע להסמיך את ראש הממשלה ושר המשפטים לקבוע תקנות נוספות על מנת לאפשר הסדרה מפורטת יותר.

סעיף 39 סעיף זה נועד להסדיר את ההגנה על סודיות מידע שנמסר לארגון או נציגו במסגרת טיפול בתקיפה או היערכות לה. בהתאם לסעיף 19(ב) המוצע, נדרש נציג המערך לתת גילוי ורקע לצורך הטיפול בתקיפה, שעשוי לכלול מידע רגיש בטחונית או מסיבות אחרות. על מנת לאפשר שיתוף הארגון במידע זה, כדי שיכלכל את צעדיו ויבין את ההקשר של הפעילות, נדרש למסור לו מידע. עם זאת, על מנת למנוע פגיעה בסודיות מידע, באמצעים או בשיטות או באינטרסים אחרים, נדרש למנוע את גילוי המידע. על מנת לאזן בין אינטרס זה לבין אינטרס ציבורי בגילוי

המידע האמור, מוצע כי בית המשפט יהא רשאי להתיר את הפרסום.

סעיף 40 מטרתו של סעיף זה להגביל את ההפצה של מידע שנאסף במערך במסגרת תפקידיו לנסיבות מצומצמות בלבד.

סעיף 41 על מנת לאפשר שיתוף פעולה בין הארגונים לבין מערך הסייבר מוצע לקבוע כי מידע שנמסר בהסכמה למערך במסגרת טיפול בתקיפה לפי הוראות פרק זה לא ישמש כראיה כנגד מוסרו, למעט עבירות שייקבעו בתוספת הראשונה לחוק. בנוסף מוצע להבהיר, כי על מידע שנמסר למערך בידי ארגון יחול סעיף 9(א) לחוק חופש המידע, התשנ"ח-1998, כלומר לא ניתן יהיה למוסרו.

פרק ד': אסדרה לאומית בתחום הגנת הסייבר

כללי ביום 15.2.2015 קיבלה הממשלה החלטה מס' 2443 שעניינה קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר. במסגרת זו החליטה הממשלה "לקדם אסדרה לאומית בהגנת הסייבר ולפעול להובלה ממשלתית בהגנת הסייבר, כחלק מיישום האסדרה הלאומית וכמהלך של דוגמה לציבור ולמשק". החלטת הממשלה קבעה, בין השאר, כי היא מאמצת את עקרונות תפיסת האסדרה הלאומית בהגנת הסייבר, ובהתאם לתפיסה זו נקבע, כי "אסדרת היערכות הארגונים במשק בתחום הגנת הסייבר תיעשה מתוך כוונה שלא להוסיף למשק עוד רגולטורים, אלא באמצעות העצמה של הרגולטורים הקיימים, וזאת באמצעות מגוון הכלים העומדים לרשותם וחיזוק כלים אלה ככל הנדרש, על מנת להעלות את רמת החוסן של המגזר האזרחי לאיומי סייבר, ובכלל זה באמצעות היערכות וכשירות".

עוד קובעת ההחלטה, כי יש "להטיל על המנכ"לים של משרדי הממשלה, שבמסגרתם מופעלות סמכויות רגולציה כלפי גופים או פעילויות החשופים לאיומי סייבר, לקדם את הטיפול בהיערכות לאיומי סייבר במסגרת המגזר שבו הם פועלים כדלקמן: [...] לפעול לקידום הגדרת המדיניות ודרישות האסדרה למימוש החלטה זו במסגרת המגזר עליהם אחראים."

דברי ההסבר של החלטת הממשלה מבהירים כי "הארגונים במשק משויכים בחלקם למגזרים (בית חולים לדוגמה משוייך למגזר הבריאות), ובחלקם אינם משוייכים באופן מובהק למגזר. על מנת ליישם הגנה הולמת בסייבר בכלל המגזר, נדרש לחזק את משרדי הממשלה ולשם כך יוקמו או יחוזקו (היכן שקיימות) יחידות להכוונה להגנת הסייבר במשרדים הממשלתיים, שיכווינו ויפקחו על מימוש הגנת הסייבר בגופים המשוייכים למגזרם. כדי שיחידות אלו יוכלו להסדיר באופן יעיל את הגנת הסייבר של הגופים המצויים בתחום אחריותם, נדרש לחזקם בהיבטי ידע וכח אדם מקצועי ולהגדיר באופן ברור את סמכויותיהם. על המשרדים לקיים תהליך סדור של מיפוי מושאי ההגנה, תכנון תכנית להגנה, מימוש ובקרה על התכנית, הפעלת מנגנוני פיקוח ותמרוץ פנים מגזריים וכן בנייה והפעלה של תהליכי שיתוף מידע פנימיים וחיצוניים. בהקשר זה, יוזכר כי למשרדי הממשלה סמכויות חוקיות כלפי הגופים שבתחום אחריותם בהיבט המקצועי. כדוגמה לכך, רגולטורים רשאים להתקין תקנות למגזר הרלוונטי וכן להפעיל, בחלק מהמקרים, מנגנוני רישוי לחברות. במסגרת זו, רגולטורים אלו יכולים להתנות רישוי חברות בעמידה ברגולציה בתחום הגנת הסייבר. יודגש כי היקף הפעילות בתחום הסייבר אינו אחיד בין המגזרים השונים. רמת האיום הנשקפת למגזר מסוים אינה בהכרח דומה למגזר אחר. כפועל יוצא, נדרש לבנות את יחידות הכוונת הגנת הסייבר במשרדים הממשלתיים בהתאמה להיקף פעילותן הנדרש בתחום הגנת הסייבר. בנוסף, על פעילויות או גורמים החשופים לאיומי סייבר, לעיתים יש יותר מגורם מקצועי אחד מפקח, ובעניין זה נדרש לקבוע את הגורם המתאים. מטרתו של פרק ד' המוצע היא לעגן בחקיקה את התפיסה שאימצה הממשלה בהחלטה מס' 2443, ולהניח את הבסיס החוקי-משפטי לאסדרה בתחום הגנת הסייבר ביחס לכלל המשק והמרחב האזרחי בישראל, הן של מערך הסייבר הלאומי והן של הרשויות המאסדרות הנוגעות בדבר, תוך כדי קביעת מנגנונים מפורטים המסדירים את מארג היחסים בינן לבין עצמן, ובינן ובין הארגונים הפועלים במרחב האזרחי. בנספח לתזכיר מפרסם המערך "מסמך הערכות השפעות רגולציה" לפרק זה בתזכיר, בהתאם להחלטת ממשלה 2118.

יצוין כי לצד הסדרה זו יש מסגרות ייחודיות להסדרת סייבר הקבועות בחוק להסדרת הביטחון בגופים ציבוריים,

המהווה דין ספציפי לעניין הגורמים המוסמכים בו בתחום הסייבר.

סעיף 42 מוצע לקבוע את מטרות הפרק במפורש בסעיף זה - להעלות את רמת העמידות והחוסן של המגזר האזרחי לאיומי סייבר, ובכלל זה באמצעות היערכות וכשירות; ולהסדיר את הנחיית המשק בתחום הגנת הסייבר, תוך קביעת מדיניות אחידה והתחשבות באינטרסים ציבוריים ומשקיים אחרים.

סעיף המטרות ינחה הן את המערך ואת הרשויות המאסדרות בפעילותן בתחום, והן את ראש הממשלה בעת קביעת תקנות לפי הפרק.

סעיף 43 מוצע כי בעת הפעלת סמכות לפי פרק זה, ובכלל זה קביעת תקנות, הוראות וצווים לפי חוק זה ובמילוי תפקידי מערך הסייבר הלאומי או רשות מאסדרת, יישקלו שיקולים שמטרתם לבדוק את מידתיות האסדרה. העקרונות המוצעים בסעיף זה, נועדו להבטיח כי האסדרה הישראלית בכל הנוגע להגנת הסייבר, תשיק לאסדרה במדינות המפותחות, באופן שיקל על זרימה של ידע, שירותים ומוצרים ממדינת ישראל לחוץ לארץ ולהיפך. כן מוצע כי כל אסדרה בנושא, ובכלל זאת סטייה מתקנים מקובלים בעולם, תיבחן לאור השפעתה האפשרית על הפעילות העסקית והכלכלית, על מנת להבטיח שתועלתה הציבורית תהיה גבוהה יותר מעלותה. כמו כן נדרש לבחון את הזיקה לתפיסות מקובלות בעולם על בסיס ההבנה כי מדובר בתחום גלובלי, להתאים את המדיניות לסיכונים וכן להתחשב בהשפעות משקיות.

עקרונות דומים עומדים בבסיס החלטת ממשלה מס' 2118 מיום 22.10.2014 שעניינה הפחתת הנטל הרגולטורי, ואשר עקרונותיה נועדו ליישום גם במסגרת ההסדרה לפי החוק. על מנת לאפשר ודאות גבוהה יותר במימוש עקרונות אלה במסגרת שיקול הדעת המנהלי מוצע לקבוע, כי ראש הממשלה רשאי לקבוע תקנות לעניין אופן בחינה כאמור.

סעיף 44 מערך הסייבר הלאומי הוא הגוף הממשלתי בעל המומחיות, כוח האדם, והידע בתחום, אשר אמון, בין היתר, על יישום מדיניות הממשלה והחלטותיה בכל הנוגע להגנת הסייבר. לפיכך מוצע כי המערך ינחה את הרשויות המאסדרות ביחס לאופן מימוש הוראות חוק זה בתחום הגנת הסייבר.

סעיף 45 מוצע כי המערך יפרסם הנחיות בתחום הגנת הסייבר, בהתאם לקבוע בפרק זה, לצורך קביעת תפיסה אחידה של הגנת הסייבר. המערך משמש גורם מרכזי אשר מתכלל את הידע בתחום הגנת הסייבר תוך שילוב תובנות ותפיסות מקובלות בתחום זה עם ידע ייחודי הקיים בידי המדינה. המערך מקיים ממשקים שוטפים עם קבוצות מקצועיות במגזרים שונים על מנת לוודא, כי ההנחיות מעודכנות ותואמות את מאפייני הארגונים והאתגרים שעמם הם מתמודדים. קיומו של גורם לאומי מרכזי הוא בעל חשיבות לצורך יצירת כלים אחידים.

סעיף 46 מוצע כי ראש מערך הסייבר הלאומי יקבע שיטה לקביעת רמת סיכון הסייבר לאינטרס ציבורי חיוני המבוססת על רמת חומרת סיכונים לאינטרסים ציבוריים חיוניים המוגדרים בחוק. המערך יעשה זאת על בסיס סוגי הנזק והסיכון להתממשותם בשל אירועי סייבר בארגון. במסגרת זו יובאו בחשבון בין השאר שיקולים שונים ביחס לארגונים, וביחס לכלל המשק. פעילות זו מבוססת על שילוב של איתור פעילויות ואינטרסים חשובים במשק הישראלי, ועל מידת החשיפה שלהם לאיומי סייבר.

מטרתה של השיטה היא למפות את המרחב האזרחי ולזהות היכן נדרשים מוכנות וחוסן להגנת סייבר. פעולת הארגונים וכן המדינה על מוסדותיה השונים (לרבות הרשויות המאסדרות) תונחה ותתועדף בהתאם לתוצאות המיפוי.

סעיף 47 הסעיף מגדיר מהי רשות מאסדרת לצורך ממשקי ההנחיה והעבודה שלה מול המערך בהקשר החוקי המוצע. המאפיינים הכלליים המוצעים בסעיף מתייחסים לרשות מנהלית המוגדרת בחוק כלשהו כבעלת סמכות להנחות, לפקח ולאכוף הוראות הנוגעות לארגונים שפועלים בתחומים שמנויים בתוספת השנייה. ההגדרה היא פונקציונלית לסוגי הפעילויות המרכזיות אשר יש להן השלכה לאסדרת אינטרסים ציבוריים חיוניים. תפיסה דומה עולה גם בחקיקה של האיחוד האירופי.

סעיף 48 מוצע כי רשות מאסדרת שאמונה על אסדרה של פעילות משקית אשר חשופה לאיומי סייבר תקבע את תרחישי הנזק בשל אירועי סייבר ומידת חומרתם בארגונים המפוקחים על ידה, בהתאם לשיטה ולהנחיות שקבע מערך הסייבר הלאומי בהתאם לסעיף 46 המוצע. כן מוצע כי רשות מאסדרת תסווג את הארגונים המפוקחים על ידה בהתאם לתרחישי הנזק, לשיטה ולהנחיות של המערך.

יובהר כי הנחת העבודה היא ששמירה על תפקודן התקין של מערכות הארגון ונכסי המידע שלו הם אינטרס של הנהלת הארגון ובעליו. בהתאם לכך, מעת שיש בידי הנהלות הארגונים כלים להיערך לאיומי סייבר, ניתן להניח כי ינקטו אמצעים לכך. לכן לא בהכרח נדרשת אסדרה מקום שאין תרחיש נזק אשר אין בו סיכון לאינטרס ציבורי חיוני או אינטרס מוסדר בהתאם לאסדרה מגזרית.

תכלית הסעיף המוצע גם לאפשר תיעדוף בכל הנוגע להסדרה של הגנת הסייבר - להתמקד תחילה בארגונים המפוקחים שעל פי סיווגם ותרחישי הנזק הנוגעים להם מצריכים הנחיה ופיקוח במידה רבה יותר מאשר ארגונים אחרים, ולהיערך להנחייה ולהכוונה של המגזר לפי סדרי העדיפויות שייקבעו בהתאם למידת החשיפה לסיכונים והיקף הנזק הפוטנציאלי, ולשיטה כאמור לעיל.

סעיפים 49 -50 מוצע כי רשות מאסדרת תבחן את הצורך בקביעת הוראות בתחום הגנת הסייבר לארגונים המפוקחים על ידה, בהתאם להוראות לפי פרק זה, ותקבע אותן בהסכמה של ראש מערך הסייבר הלאומי. ההוראות שתקבע רשות מאסדרת יהיו בהתאם לסמכויות שניתנו לה על פי דין. כן מוצע כי מערך הסייבר הלאומי ייתן הסכמתו לקביעת הוראות כאמור לעיל, בשל מומחיותו ויתרונו היחסי בתחום.
תכלית הסעיף להבטיח כי משרדי הממשלה והרשויות הרגולטוריות השונות, יפעילו את הסמכויות שיש בידם על מנת לקבוע הוראות הגנת סייבר עבור המגזרים שתחת אחריותם, בהתאם לעקרונותיה של החלטת הממשלה מס׳ 2443 מיום 15.2.2015.
סעיף 51 מוצע לקבוע כי רשות מאסדרת תוכל להורות לארגון מפוקח למנות ממונה הגנת סייבר, אם רמת הנזק בשל איומי הסייבר הנשקפת מפעילותו היא במדרג גבוה. במקרים אלה, היקף הנזק הפוטנציאלי מחייב מינוי של גורם מקצועי אשר יהיה אמון על הגנת הסייבר בארגון. מינויו של בעל תפקיד ייעודי משפר את הסיכוי כי הארגון ייערך כראוי לאירועי סייבר. מוצע כי הרשות המאסדרת, בהתייעצות עם מערך הסייבר הלאומי, רשאית לקבוע כי ממונה הגנת הסייבר יהיה בעל התאמה ביטחונית לתפקיד.
בנוסף מוצע כי ראש הממשלה יהיה רשאי לקבוע בתקנות פרטים נוספים לגבי תפקיד ממונה הגנת הסייבר בארגון המפוקח, כשירותו וחובותיו, כדי להגביר את האפקטיביות של דרישה זו.
סעיף 52 מוצע לקבוע במפורש סמכות לרשות מאסדרת לדרוש דיווח תקופתי מארגון על אופן העמידה בהוראות לפי פרק זה. דיווחים עיתיים של ארגונים מפוקחים, נדרשים על מנת שלרשות המאסדרת תהיה התמונה המלאה על יישום של ההוראות שנקבעו, ומידת המוכנות של המגזר שבאחריותה והארגונים המפוקחים שנכללים בו.
סעיפים 53, 55 מוצע לקבוע כי יוקמו יחידות הכוונה להגנת סייבר ברשויות המאסדרות, כפי שנדרש במגזר שעליו אמונה כל רשות מאסדרת. הטעם בהקמת יחידת הכוונה מגזרית, הוא הצורך לשלב בין ידע בתחום הגנת הסייבר לבין הידע של הרגולטור המגזרי, בהתאם לסיכונים והפעילות במגזר. זאת בהמשך לנספח ד׳ להחלטת הממשלה 2443.
עוד מוצע כי ראש הממשלה יקבע תקנות לעניין תפקידים והכשרה הנדרשת מעובדי יחידות הכוונה מגזריות הפועלות לפי חוק זה ברשות מאסדרת.
מוצע כי על אף האמור בחוק שירות המדינה (מינויים), התשי״ט-1959, ראש הממשלה יהיה רשאי, לאחר התייעצות עם שר האוצר ועם נציב שירות המדינה, לקבוע בתקנות או בכללים הוראות אחרות מאלה החלות בשירות המדינה לעניין ארגון וניהול כוח אדם הנדרש למילוי תפקידי יחידות ההכוונה המגזריות, והכל בכפוף להוראות חוק יסודות התקציב, התשמ״ה-1985, ולהוראות חוק התקציב השנתי.
עוד מוצע כי לא ימונה עובד או יועץ בתחום הגנת הסייבר ליחידת הכוונה מגזרית אלא בהסכמת המערך.

סעיפים 54, 56 מוצע כי רשות מאסדרת אשר מעניקה היתר או רישיון לפעילות, תהיה רשאית לקבוע כי תנאי לקבלת ההיתר או הרישיון שניתן לארגון מפוקח או תנאי לחידושו יהיה עמידה בדרישות ההוראות שנקבעו לפי סעיף 51 המוצע. הוראה זו נדרשת על מנת להבהיר כי הוראות בנושא הגנת סייבר עשויות להיות תנאי מהותי ברישיון או בהיתר שיש לקיימו כתנאי להמשך הפעילות המוסדרת מכוחו. יודגש כי השימוש בתנאים ברישיון הוא אחד מהכלים הרגולטוריים המצויים בידי המאסדרים, ומובן כי מקום שבו קיים בידי הרשות המאסדרת כלי אסדרתי אפקטיבי בהלימה לרמת הסיכון, שאינו תנאים ברישיון, ניתן יהיה להשתמש גם בו.

מוצע להבהיר כי מקום שבו הוסמך אדם כמפקח ברשות מאסדרת והוקנו לו סמכויות פיקוח ניתן יהיה לעשות בהן שימוש גם לצרכי קיום הוראות לפי הפרק.

כן מוצע לקבוע שמערך הסייבר הלאומי יהיה רשאי, בהתייעצות עם הרשות המאסדרת, לקבוע שארגון מפוקח יוכיח עמידה בדרישות ההוראות האמורות באמצעות חוות דעת של מומחה מתאים. עוד מוצע כי הרשות המאסדרת, בתיאום עם מערך הסייבר הלאומי, תקבע כללים לגבי חוות דעת מומחה כאמור.

סעיף 57 מוצע להסמיך את ראש הממשלה להורות בצו על פיקוח והנחייה ישירים בידי מערך הסייבר הלאומי של ארגונים מסוג שקבע בצו. הסעיף קובע מספר תנאים, שבהתקיימם ניתן יהיה לקבוע הנחיה ישירה של המערך על הארגון, המשקפים את הסיכון הגבוה לאינטרס הציבורי למול הצורך במענה.

תכליתו של הסעיף להבטיח כי לא יוותר מגזר פעילות או ענף משקי, החשוף לאיומי סייבר משמעותיים שאינו כפוף לרשות מאסדרת קיימת או אפקטיבית שיכולה להסדיר את פעילותו בכל הנוגע להגנת הסייבר באמצעות מתן הנחיות ופיקוח על יישומן. במקרה כזה, ועד שיוסדרו סמכויות הנחיה ופיקוח בידי רשות מאסדרת אחרת, תיוותר האחריות להנחיה ופיקוח של המגזר בידי מערך הסייבר הלאומי.

סעיף 58 לאחר קביעת ראש הממשלה כי מגזר מסוים יהיה כפוף להנחיה ישירה של המערך, יפעל המערך כלפי הארגונים המצויים באותו המגזר והוא יוסמך לפרסם הוראות שיחייבו את הארגונים במגזר ליישם אותן לשם הגנת הסייבר, בהתאם לסיווג שיקבלו.

סעיף 59 לשם פיקוח על ארגונים במגזר שקבע ראש הממשלה בצו לפי סעיף 57, מוצע לתת למערך סמכויות המנויות בסעיף זה ובכללן הסמכות לדרוש הזדהות של אדם, לדרוש מסירת ידיעות ומסמכים ולהיכנס למקום ככל שלא מדובר במקום המשמש למגורים.

סעיף 60 במצב שבו המערך מנחה הנחיה ישירה מגזר מסוים, מוצע לתת לעובד מוסמך סמכות להורות לארגון, שמצא כי לא יישם הוראות להגנת הסייבר שניתנו על ידי ראש המערך, לנקוט פעולות נדרשות לשם יישום ההוראות האמורות.

סעיף 61 קיים חשש שבמקרים מסוימים רשות מאסדרת אינה מצוידת בסמכויות המתאימות בדין שמאפשרות לה מתן הוראות בתחום הגנת הסייבר ופיקוח על ביצוען ביחס לארגונים שמצויים תחת פיקוחה. במקרה כזה, מוצע לאפשר הסמכה של רשות מאסדרת בסמכויות המנויות בסעיפים 58-60, שאותם הסעיפים מעניקים למערך לצורך הנחיה ישירה.

סעיף 62 מוצע לקבוע כי ראש המערך רשאי להורות על הנחיה ופיקוח ישירים זמניים של ארגון מסוים על ידי מערך הסייבר הלאומי. הנחיה זו בידי המערך תינתן לתקופת זמן מוגבלת והיא מותנית בכך שהארגון מקיים פעילות החשופה לאיומי סייבר ולא קיימת רשות מאסדרת בעלת סמכות ביחס לארגון האמור ולכן אין בהקשרו רשות מנהלית בעלת סמכויות שיכולה להנחותו בתחום הגנת הסייבר.

תכלית הסעיף היא להבטיח כי ארגון שיש לו פעילות משמעותית, אשר אין ביחס אליו רשות מנהלית שמוסמכת להסדיר את פעילותו בכל הנוגע להגנת הסייבר, במובן של מתן הנחיות ופיקוח על יישומן, יטופל בידי מערך הסייבר. במקרה זה, האחריות להנחיה ופיקוח תהיה נתונה למערך הסייבר הלאומי לתקופה מוגבלת. בתקופה זו יפעל המערך למתן ההנחיות הנדרשות ופיקוח על יישומן לשם העלאת המוכנות של הארגון.

סעיף 63 מוצע לקבוע כי בדירקטוריון של חברה מסוג שקבע ראש הממשלה בהתייעצות עם שר המשפטים, נדרש יהיה לקיים דיון שנתי לפחות באופן ההתמודדות של החברה עם איומי סייבר. מטרת הוראה זו לקדם את ניהול איומי הסייבר בתאגידים בדרך רכה יותר מאשר הנחייה ישירה באשר לאופן ההגנה. הנחת העבודה היא שבמידה שארגון חשוף לאיומי סייבר משמעותיים אשר עלולים לסכן את פעילותו או נכסיו, קיום דיון בדירקטוריון יניע אותו להיערך מבחינת אמצעי הגנת סייבר, ביטוחים או הקצאת משאבים אחרים הנדרשים להתמודדות עם תקיפות סייבר.

סעיף 64 סעיף זה עוסק בפעילות מותרת לצורך הגנת הסייבר. מטרת סעיף זה להבהיר את המצב המשפטי הקשור במתח שבין צרכי הגנת הסייבר המחייבים ניטור שוטף של רשתות הארגון, לבין החשש כי בניטור זה או בחלקו יש משום פגיעה אסורה בפרטיות עובדים או לקוחות. הסעיף משקף קודיפיקציה של הסדרים מקובלים בעולם, ומטרתו להקנות ודאות לארגונים לגבי הפעילות המותרת. בנוסף, ניתן אף לומר כי הגנה על פרטיות המידע מחייבת במידה רבה קיום פעילות ניטור והגנה על ידי ארגונים, כלומר מדובר בפעילות לגיטימית לצרכי עמידה בהוראות אבטחת המידע של דיני הפרטיות עצמם.[18] יודגש כי הסעיף מגביל את מטרת הפעילות המותרת לפעילות הגנת סייבר בלבד. הסעיף לא מסדיר מטרות נוספות לפעילות ניטור רשתות בארגון, אף אם הן לגיטימיות מסיבות אחרות.

סעיף 65 בהמשך לסעיף 64 מטרת הסעיף להבהיר כי שיתוף מידע בעל ערך אבטחתי בין ארגונים ועם מערך הסייבר אף הוא אינו פוגע בפרטיות.

הוראה מעין זו קיימת בחקיקת האיחוד האירופי General Data Protection Regulation, בסעיף 49 להוראות המבוא.

בנוסף בדומה להוראות סעיף 19 לחוק הגנת הפרטיות, התשמ"א-1981 מוצע להקנות ודאות לעובד המערך או מי מטעמו לעניין טיפול במחשבים או ברשתות. סעיף 19 האמור מהווה הכרה של המחוקק כי פעילויות מסוימות עלולות לפגוע בפרטיות, אולם בשל התועלת שעשויה להיות בהן לאינטרס בטחוני או ציבורי אחר, יש לאפשר לאיש הביטחון לבצע את תפקידו על אף החשש מפני פגיעה בפרטיות. הוראות אלה הולמות את תפקידיו של מערך הסייבר הלאומי. פעילות הטיפול בתקיפות סייבר היא מול מחשבים באופן קבוע. הדבר דומה לחשיפה הקבועה של מנהל רשת או טכנאי מחשבים למידע. עם זאת, בשונה מרשויות הביטחון, תכלית הפעילות של הגנת הסייבר היא איתור תקיפה ולא פגיעה באדם. יוצא מכך, שברוב רובם של המקרים כלל לא יעלה חשש לפגיעה בפרטיות. עם זאת, לנוכח החיכוך הקבוע והשוטף עם מערכות מידע, ייתכן מקרה שבו תהיה חשיפה למידע פרטי. במאזן ההסתברויות, לנוכח היותו של מערך הסייבר גוף בטחוני לאומי שתפקידו להגן על מרחב הסייבר, יש לאפשר למי שפועל מטעמו באותו מקרה נדיר מרחב ביטחון גבוה יותר.

סעיף 66 מטרת הסעיף להבהיר, בדומה להוראות סעיף 64 ו-65 כי שיתוף מידע למטרת הגנת הסייבר אינו מפר את דיני התחרות, כל עוד הוא עוסק במידע בעל ערך אבטחתי. עמדה דומה פורסמה בידי הממונה על הגבלים עסקיים בגילוי דעת מטעמו ופורסמה גם מטעם משרד המשפטים ורשות הסחר הפדרלית האמריקאית.[19]

סעיף 67 סעיף זה מסדיר את אופן תחולת החוק והפעלת סמכויות לפיו על גופים אשר הם בעלי עצמאות חוקתית מהרשות המבצעת, או שפעילות הגנת הסייבר שלהם אינה במסגרת המנדט של מערך הסייבר הלאומי בהתאם

---

[18] Andrew Cormack, Incident Response: Protecting Individual Rights Under the General Data Protection Regulation, SCRIPTed
A Journal of Law, Technology & Society, Volume 13, Issue 3, December 2016, https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/

[19] רשות ההגבלים העסקיים, גילוי דעת 3/17 שיתוף מידע לצורך התמודדות עם איומי סייבר, http://www.antitrust.gov.il/files/34745/%D7%92%D7%99%D7%9C%D7%95%D7%99%20%D7%93%D7%A2%D7%AA_3_17%20%D7%A1%D7%99%D7%99%D7%91%D7%A8%200717.pdf

להחלטות הממשלה. מטרת הסעיף לאפשר הפעלת סמכויות במקרים אלה, במידה שיהיה בכך צורך ובהתאם לגורם הבכיר המוסמך להחליט על כך.

סעיף 68 מרחב הסייבר מורכב ממחשבים ורשתות בארגונים. לכן על מנת לעמוד על מצב ההגנה הכולל בישראל, לצורכי גיבוש תמונת מצב, תיעדוף והכוונת מאמצים, נדרש ראש המערך לגבש תמונת מצב משקית. לצורך כך מוצע להסמיכו לבצע סקרים ואיסוף מידע שיאפשר לעמוד על רמת ההגנה הכוללת.

סעיף 69 מובהר למעלה מהצורך כי החוק אינו מונע קביעת הוראות ודרישות הסכמיות בתחום הרכש, ובכלל זה בגופים ציבוריים, והוא מאפשר למי שמתקשר עם ספק להסדיר את דרישות הגנת הסייבר, במסגרת מערכת היחסים המסחרית. זאת בפרט על רקע האחריות של הגופים המיוחדים להגנה על מערכותיהם, ואחריות הממונה על הבטחון במערכת הביטחון להגנה על מערכות במערכת הביטחון.

סעיף 70 יעד מרכזי של מערך הסייבר במסגרת תפקידיו הוא יצירת שיתופי פעולה בינלאומיים אופרטיביים שמטרתם חילופי מידע רלבנטי להגנה, וכן קידום מעמדה של ישראל כמובילה בתחום הסייבר בעולם. כבר כיום מקיים המערך רשת קשרי חוץ עם גורמים מקבילים אשר מהווה כלי עבודה משמעותי בהגנה על מרחב הסייבר המהווה מרחב גלובלי ללא גבולות פיזיים. לצורך כך מוצע להסמיך את ראש המערך, בהמשך להחלטות הממשלה בנושא, בסמכות להתקשר בהסכמים בתחום זה. מובהר כי הסכמים כאמור ייערכו בהתאם לכללים שייקבעו בידי ראש הממשלה ויאפשרו ביטוי לאינטרסים רלבנטיים ותיאום מדינתי במקרים המתאימים.

סעיף 71 לנוכח משימותיו וייעודו של שירות הביטחון הכללי, ייתכנו נסיבות אשר בהן הטיפול בתקיפת הסייבר מצויה במסגרת ייעודו, ומצריכה שימוש בסמכויות למול המרחב האזרחי המוצעות בחוק. בהתאם לכך מוצע בסעיף, להסמיך עובד מבין עובדי שירות הביטחון הכללי בסמכויות אלה לצורך טיפול באותה תקיפה, בנסיבות שנקבעו בסעיף. מוצע עם זאת כי הדיווח והפיקוח על הפעלת הסמכויות לפי סעיף זה לא יבוצע בידי הוועדה המפקחת אלא בידי היועץ המשפטי לממשלה, כפי שנקבע ביחס לשירות הביטחון הכללי מכוח חוקים שונים.

סעיף 72 מוצע לקבוע כי פעילות מערך הסייבר בתחום הגנת הסייבר אינה נתונה לגילוי, למעט כמוסדר בחוק או בתקנות שיקבעו ראש הממשלה ושר המשפטים, וזאת על רקע הצורך להגן על סודיות שיטות, אמצעים ומידע רלבנטי להגנת הסייבר. לעניין זה ראו גם הוראות סעיפים 9(א) ו – 14 לחוק חופש המידע.

סעיף 73 ראש הממשלה הוא השר האחראי על החוק ובהתאם לכך מוסמך להתקין תקנות לביצוע החוק.

סייבר ישראל
Cyber Israel

הערכת השפעות רגולציה

פרק האסדרה
בחוק הסייבר

יוני 2018

INCD@cyber.gov.il
*9344
מערך הסייבר הלאומי - משרד ראש הממשלה
National Cyber Directorate - Prime Minister Office

תוכן עניינים

תקציר מנהלים 1

חלק א' – הגדרת תכלית והצורך בהתערבות 4

1. כללי 4
2. זיהוי הבעיה וסיבותיה.. 8
3. סקירה השוואתית בינלאומית 14
4. סקירת ההסדר הממשלי הקיים בישראל בהגנה על ארגונים בסייבר 16
5. תכליות וסיכונים 18

חלק ב' – ניסוח חלופות 19

1. חלופה 0... 19
2. מודל של רגולציה משותפת.. 20
3. מודל מבוזר.. 20
4. מודל ריכוזי.. 20
5. מודל משולב... 20

חלק ג' – הערכת חלופות והשוואה 21

1. ניתוח חלופות 22
2. אמצעים נוספים שהוטמעו בחוק על מנת למזער עומס רגולטורי.......... 25
3. הערכת העומס הרגולטורי והתועלות הצפויים מהחלופה הנבחרת........ 26

חלק ד' – שיח עם בעלי עניין 31

10 יוני 2018

כ״ז בסיון תשע״ח

סימוכין: ב-מאא951

תקציר מנהלים

איומי הסייבר הולכים ומתעצמים עם צמיחתו של מרחב הסייבר, העלייה בתלות בו ובעומק החיבור בינו לבין המרחב הפיסי. איומים אלו עלולים להוביל לפגיעה בתוך המרחב (למשל במידע או בתפקוד), לפגיעה בעולם הפיסי (למשל פגיעה במערכות רפואיות או תשתיות אנרגיה), לפגיעה תפקודית משקית קשה, ואף לפגיעה בחיי אדם. תקיפות הסייבר הולכות והופכות מתוחכמות יותר, ותוצאותיהן קשות יותר ומורכבות יותר לטיפול.

התגברות האיומים על אינטרסים לאומיים, חברתיים וכלכלים כתוצאה מתקיפות סייבר, נובעת מהמשרעת הרחבה של תוקפים, בהן מדינות, ארגוני טרור, ארגוני פשיעה, ״האקטיביסטים״, ותוקפים מזדמנים. מאפייניו הייחודיים של מרחב הסייבר מאפשרים לתוקפים לגרום לפגיעה בנפש או ברכוש, פגיעה ברציפות תפקודית של תהליכים חיוניים, גניבת מידע, הדלפתו או שיבושו, ואף נזק תודעתי כתוצאה מתקיפת סייבר.

מרחב הסייבר הוא מרחב אזרחי ברובו, הוא מורכב ממחשבים, רכיבי תקשורת וטכנולוגיות אזרחיות, המופעלים ונשלטים ע״י ארגונים, ולא על ידי המדינה. מאחר שזירת ההגנה היא במערכות המידע והתקשורת של הארגונים האזרחיים, ובשל חשיבותו הרבה של מרחב הסייבר לחדשנות ולתנועה חופשית של מידע, נדרשת תפיסה חדשה לתפקיד המדינה. בראיה צופה פני עתיד – תלות גוברת של החברה המודרנית במרחב הסייבר לצד התפתחותו כמרחב לחימה של ממש, ניכר כי ההגנה על מרחב הסייבר, במיוחד בראי אחריות המדינה כריבון, אינה נגזרת של דיסציפלינה ביטחונית קיימת, כי אם דיסציפלינה ייחודית ועצמאית.

במדינות המערב מקודמת מדיניות הגנת סייבר לאומית. בשנת 2015 המליץ ה-OECD למדינות הארגון לגבש מדיניות הגנת סייבר הכוללת התמודדות עם הסיכונים למרחב הדיגיטלי[1]. בשנת 2016, נחקק באיחוד האירופי (בתוקף החל מ-10.5.2018[2]) חוק המחייב את חברות האיחוד

[1] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

לגבש מדיניות הגנת סייבר, לקבוע אסדרה לתשתיות קריטיות ולהקים מרכז טיפול לאומי באירועי סייבר.
בדו"ח לשנת 2018, קבע הפורום הכלכלי העולמי כי הסייבר הוא אחד מחמשת הסיכונים הגדולים בעולם[3] והמליץ להגביר את ההיערכות לאירועי סייבר.

לאור מגמה עולמית זו, ולאור אירועי הסייבר הרבים הפוקדים ארגונים בישראל ובעולם כולו, החליטה ממשלת ישראל על מדיניות כוללת להעלאת החוסן בארגונים ולצמצום סיכוני הסייבר של המשק, באמצעות הפעלת כלי מדיניות שונים כגון אסדרה, חקיקה, הנחיה ותמריצים.

תזכיר חוק הסייבר, אליו נסמך מסמך זה, נועד לממש את החלטות המדיניות שאישרה הממשלה בהחלטות 2444 ו-2443, ובמרכזן הקמה של גוף לאומי חדש וייעודי להגנת הסייבר, לצורך העלאת החוסן של ארגוני המשק ולצורך מניעה של אירועי סייבר, והתמודדות והכלה שלהם בזמן אמת. התזכיר מפרט את השיטה והאמצעים של האסדרה המדינתית בתחום זה.

מטרתו של מסמך זה היא לסקור את הערכת השפעות רגולציה לקראת פרסומו של תזכיר חוק הסייבר.

מסמך זה מציג את כשלי השוק ואת הצורך באסדרה ממשלתית בתחום הגנת הסייבר בראיה מדינתית, תוך ניתוח של הצעדים הנדרשים להעלאת רמת החוסן והמוכנות של המרחב הישראלי בתחום. המסמך סוקר מודלים שונים של התערבות מדינתית, ומציג את החלופות להתערבות רגולטורית לאור סקירה זו.

פרק הרגולציה בתזכיר חוק הסייבר, עוסק במכלול הפעילות הממוקדת במניעה והיערכות, על יסוד מנגנוני הנחיה ברמה הלאומית והמגזרית, אשר יאפשרו למדינה לחזק את החוסן המשקי. זאת, על פי תפיסת שלושת שכבות ההגנה[4] של מערך הסייבר הלאומי. תפיסת הרגולציה להגנת סייבר נועדה ליצור מסגרת מידתית להפעלת שיקול דעת רגולטורי, תוך שימוש בעקרונות תוכן ובעקרונות תהליכיים למימוש תפיסה זו. לצד זאת, ולנוכח אתגרי מרחב הסייבר שבו איומים חדשים ודרכי חיסון חדשות מופיעים כל העת, נדרשת מסגרת משפטית שתאפשר הפעלה גמישה של סמכות.

תפיסת הרגולציה בחוק מדגישה את הצורך לאזן בין אינטרסים ציבוריים רבים. מחד, אינטרסים ציבוריים שמרחב הסייבר מציב בפניהם סיכונים חדשים שאל מולם חייבת המדינה להיערך. מנגד, הרצון להימנע מסיכונים רגולטוריים הנובעים מהטלת נטל רגולטורי עודף על המשק ומפגיעה בחדשנות ובתמריצים חיוביים, בהקשר הסייבר ובכלל. יש לציין שמעבר להשפעות איום הסייבר על המשק האזרחי,

---

https://www.ncsc.gov.uk/guidance/introduction-nis-directive ליישום באנגליה ראו:

[3] The Global Risks Report 2018, World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2018

[4] מערך הסייבר הלאומי, האסטרטגיה הישראלית להגנת הסייבר, 2017

הוא מקושר באופן מובהק לביטחון לאומי. זהו רובד שיקולים נוסף בעל השפעות רוחב וקשרי גומלין שאינו ניתן לכימות והערכה במונחי כלכלה ומשק בלבד. על כן, הצורך ליצור מסגרת רגולטורית גמישה, בעלת יכולת להסתגל לנסיבות המשתנות במהירות, מקבל משנה תוקף.

בהחלטת ממשלה מס׳ 2118 בנושא הפחתת הנטל הרגולטורי, חויבה כל חקיקה ממשלתית המכילה רגולציה חדשה לקיים הערכת עלות רגולציה. תזכיר חוק הסייבר אינו מכיל רגולציה חדשה, אלא עוסק בסמכויות. מעבר לנדרש, נערכה הערכת עלות רגולציה, ונטל הרגולציה הוערך בסכום של 1.7 מיליארד ש״ח ל-5 שנים. שיטת החישוב מוצגת במסמך זה.

מסקירת כשלי השוק, לא מצאנו סיבה להאמין שהשוק יתקן את כשליו בעצמו. הכשלים הם מהותיים ולא נצפית מגמה ואף לא התחלה של מגמה לתיקון המצב ללא התערבות ממשלתית. אדרבא, הצפי של מומחי הסייבר בארץ ובעולם הוא שהפער יחריף. לפיכך, בסופו של תהליך ניתוח והיוועצות, הוחלט לקדם מודל רגולטורי משולב, המאזן בין ריכוזיות וביזוריות ומתאים את עוצמת המענה לרמות הסיכון השונות, באופן אשר שואב את המרב מהניסיון המקומי והבינלאומי בתחום וישיא את סיכויי קיום תכלית המדיניות.

עמדתנו הינה כי באופן כולל, בשקלול התועלת לארגונים עצמם בהגנה על נכסיהם ולמשק בכלל כתוצאה ממניעת נזקי רוחב, עליית המוניטין והעצמת האמון במרחב הסייבר הישראלי, אנו סבורים שהתועלת לאינטרס הציבורי תהיה רבה ומשמעותית לאין שיעור מהעלויות הכרוכות בחוק זה.

חלק א' – הגדרת תכלית והצורך בהתערבות

1. כללי

הסייבר הוא מרחב מלאכותי מעשה ידי אדם, המורכב מכלל רשתות המחשבים והתקשורת, מהמידע שבהן, ומהפעולות שמתבצעות בהן. ההתפתחות המהירה של הקישוריות בין מערכות מחשב, של יכולות העיבוד והאגירה ובעיקר של הממשקים מול הגורם האנושי בפרט והמרחב הפיסי בכלל, מעצימים את השפעותיו של הסייבר והופכים אותו לתופעה מרכזית בהתפתחות האנושית בעת הנוכחית.

את תפקודו התקין והבטוח של מרחב הסייבר מסכנת משרעת איומים ייחודית בהיקפה, אשר הולכים ומתעצמים עם צמיחתו של המרחב, העלייה בתלות בו ובעומק החיבור בינו לבין המרחב הפיסי. איומים אלו עלולים להוביל הן לפגיעה בתוך המרחב (למשל במידע או בתפקוד) והן לפגיעה היוצאת ממנו אל העולם הפיסי (למשל פגיעה במכשור רפואי, במתקני הטפלה, בפסי ייצור, בתחנות כוח ועוד). פגיעות אלה עשויות לגרום לפגיעה כלכלית חמורה ואף לפגיעות בגוף ובנפש. איומים אלו, הביאו את הפורום הכלכלי העולמי לקביעה כי אירוע סייבר מוגדר כאחד מחמשת הסיכונים הגדולים ביותר בעולם בעשור הקרוב[5].

מאחורי איומי הסייבר עומדים מגוון גורמים עוינים: מדינות וגורמים הנתמכים על ידי מדינות, ארגונים לא-מדינתיים זדוניים ובהם ארגוני טרור, קבוצות פשיעה, "האקטיביסטים" ויחידים. המניעים מאחורי התקפות הסייבר נעים מפגיעה בביטחון לאומי, ריגול, וטרור, דרך פשיעה, גניבת קנין רוחני, ריגול עסקי, ועד מחאה אזרחית ומטרות פרטיות.

במרחב הקינטי, התקבלה התפיסה שהאזרח הבודד וחברות פרטיות אינם כשירים או מוסמכים להתמודד בעצמם עם איומים חיצוניים משמעותיים כגון איומים ביטחוניים, אסונות טבע או משברי איכות סביבה. בהתאם לכך, המדינה אמונה על יצירת מענה הולם באמצעות תקינה ותקינה ובאמצעות הספקת שירותים ישירה לאזרח, כדוגמת צבא ומשטרה. בדומה לכך, במרחב הסייבר, במקרים בהם ארגונים במשק אינם מעוניינים או אינם מסוגלים להגן על עצמם אל מול איומי סייבר משמעותיים המשפיעים על מרחב הסייבר כולו. החשיפה למרחב גלובלי חדש בו פוגענים מרחבי הגלובוס נעים במהירות ומגיעים בקלות לארגונים בישראל ולמערכותיהם, הביאה לצורך במימוש תפקידה של המדינה כאחראית על הביטחון והתפקוד התקין במרחב חדש זה.

איומי הסייבר מתאפיינים גם בתכונות והתנהגות שונה מאיומים מדינתיים מסורתיים. בין המאפיינים הייחודיים, ניתן למנות:

[5] The Global Risks Report 2018, World Economic Forum: https://www.weforum.org/reports/the-global-risks-report-2018

- התפתחות והשתנות מהירה - עולם התוכן של הגנת הסייבר מתעדכן בקצב מהיר מאוד, הדורש מהמגן להתעדכן ולהיערך בהתאם. היכולת של ארגון לייצר תמונת מצב רחבה, לסקור את הנעשה במשק ובעולם ולקבל החלטות משמעותיות בפרקי זמן קצרים, מוגבלת עד בלתי אפשרית (ראו לדוגמה את ניהול המערכה ברמה המדינתית אל מול מתקפת WannaCry במאי 2017).
- גלובליות האיומים - בעוד שעל גבולות המדינה הפיזיים, קיימת הגנה מדינתית, הרי שבמרחב הסייבר, נדרש כל ארגון במשק להשיג לעצמו את ההגנה אל מול תוקפים מכל רחבי הגלובוס.
- אסימטריה בין המגן לתוקף - בעוד שעל המגן להצליח בהגנה היקפית מתמשכת, הרי שעל התוקף להצליח רק פעם אחת בנקודה אחת במערכת. בנוסף, בעוד שהתוקף פועל לא פעם "ללא גבולות משפטיים", הרי שהמגן נדרש לתת מענה במסגרת נורמטיבית ומשפטית מקובלת. שוני נוסף, נובע מהעובדה שהתוקף יכול להפעיל כלים התקפיים מתקדמים אשר עלותם זניחה יחסית (כגון במקרה של ניצול חולשות שהתפרסמו או כלי תקיפה שדלפו והינם נחלת הכלל) ומאידך, על המגן להצטייד בידע ובטכנולוגיות יקרות.
- תלות מובהקת בגורמים שאינם בשליטת הארגון – בעוד שבמרחב הפיזי המסורתי, הארגון מוגן בהתאם לתהליכי ניהול הסיכונים שלו, הרי שבמרחב הסייבר, ארגון מושפע ישירות ובאופן מובהק בתופעות חוצות מגזר וברמת ההגנה של שרשרת האספקה שלו. היכולת של איום סייבר להתפשט באופן מגפתי[6] בין גופים, לצד כמות המתקפות שמקורן בגורם חיצוני מחייבת הסתכלות מתכללת על רמת ההגנה המגזרית והמשקית במקביל לרמת הארגון הבודד.

המאפיינים הייחודיים של איומי הסייבר שהוזכרו לעיל, השתנות האיום והשפעותיו על הארגונים המאוימים, מדגישים את הצורך במענה גמיש, המאפשר למערך הסייבר או לרשות המאסדרת לפי העניין, להתאים את המענה הרגולטורי למחוללי הסיכון.

1.1 החלטות הממשלה 3611, 2443, 2444 ו-3270– המדיניות והתפיסה הלאומית להגנת הסייבר

בהחלטת ממשלה מספר 3611 בנושא "קידום היכולת הלאומית במרחב הקיברנטי" מיום 07.08.2011 (להלן – החלטה 3611), הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה) והוטל עליו, בין היתר, לגבש תפיסת הגנה לאומית במרחב הסייבר. בהחלטות הממשלה 2443 ("קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר") ו-2444 ("קידום ההיערכות הלאומית להגנת הסייבר") מיום ה-15.02.2015, אישרה הממשלה את התפיסה שגיבש המטה. בהחלטת ממשלה 3270 מיום 17.12.2017 החליטה הממשלה על איחוד מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר לכדי מערך הסייבר הלאומי, גוף אשר יישא באחריות לביצוע ההחלטות המתוארות מעלה.

---
[6] ראה כדוגמא את מתקפת הכופרה "wannacry" ששיתקה את מגזר הבריאות הבריטי ב-12.5.17.

החלטות הממשלה, עבודת המטה המקיפה שקדמה להן, והתפיסה שעומדת בבסיסן מהוות יחד את נקודת המוצא לתזכיר החוק.

המדיניות העומדת בבסיס החלטות הממשלה, מבקשת להתמודד עם מאפיין יסודי של ההגנה על תפקודו התקין של מרחב הסייבר, והוא שרובו המכריע מבוסס על תשתיות, מערכות וטכנולוגיות אזרחיות, המופעלות ע״י פרטים וארגונים אזרחיים. מכאן שמרבית האיומים במרחב מופנים כלפי המגזר האזרחי וברשותו מצוי גם רוב המידע אודות המתרחש במרחב. כפועל יוצא מכך, יש מגבלות על יכולתם של גופי הביטחון לעמוד כחיץ הרמטי בין הארגון לבין מי שתוקף אותו במרחב הסייבר.

לאור כל זאת ובהסתכלות שאינה עוצרת בבעיות השעה, אלא צופה פני עתיד – תלות גוברת של החברה המודרנית במרחב הסייבר לצד התפתחותו כמרחב לחימה של ממש – מסקנה מרכזית הנובעת מעבודת המטה, היא שההגנה על מרחב הסייבר, במיוחד בראי אחריות המדינה כריבון, אינה נגזרת של דיסציפלינה ביטחונית קיימת, כי אם דיסציפלינה ייחודית ועצמאית.

האסטרטגיה הלאומית לסייבר מחלקת את מאמצי ההגנה לשלוש שכבות:

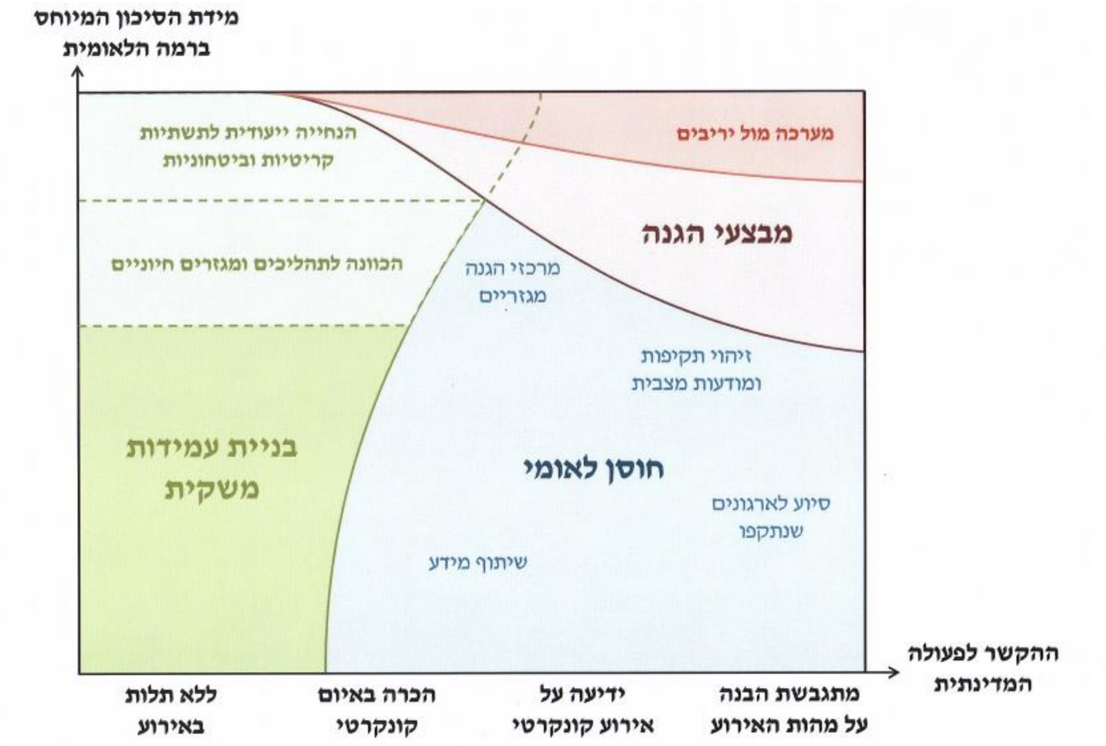
- <u>שכבת העמידות המשקית</u>- עמידות סייבר היא היכולת להתמיד בפעילות תחת שגרת איומי סייבר, באמצעות צמצום משטח התקיפה (Attack surface) באופן המקטין את פוטנציאל התממשותן של תקיפות.
- <u>שכבת החוסן המערכתי</u>- חוסן סייבר הינו היכולת להתמודד עם אירועי סייבר, לפני, במהלך ואחרי התממשותם, ולחזור במהרה לשגרה תוך צמצום הנזקים הנלווים.
- <u>שכבת ההגנה הלאומית</u> - ההגנה הלאומית הינה המאמצים המדינתיים אשר נועדו להתמודד באופן ממוקד עם איומי סייבר קונקרטיים המהווים סכנה משמעותית לאינטרסים לאומיים.

המענה הלאומי הנדרש הינו מענה אינטגרטיבי השונה משכבה לשכבה והכולל את הרכיבים הבאים להם נדרש החוק:

- עמידות משקית:
  - שיפור רמת הכשירות והמוכנות של הארגונים במשק ושל שוק הסייבר באמצעות פעילויות רגולטוריות, הכשרתיות והסברתיות;
- חוסן מערכתי:
  - איתור, גילוי וזיהוי של תקיפות באמצעות שיתוף מידע אודות הנעשה במערכות הארגונים וניתוחו, בשילוב עם מקורות נוספים ובכלל זה של גופי הביטחון, לטובת גילוי וזיהוי של איומי סייבר טרם התממשותם וגיבוש תמונת מצב לאומית;
  - פיתוח והטמעה של תהליכים ומנגנונים רוחביים לשיתוף מידע.

- התמודדות בזמן אמת עם אירועי סייבר, לרבות סיוע לארגון בהכלת האירוע, בהתאוששות ממנו ובתחקורו ;
- עבודה שוטפת עם גופים מקבילים בעולם ;

• הגנה לאומית :
- הפעלת יכולות ביטחוניות



ברמה המוסדית, המענה מתבטא בהקמה של גוף מרכזי לאומי ייעודי, מערך הסייבר הלאומי (להלן : המערך), שתפקידו לעסוק בנושאים אלה באופן שוטף. מרכיבי המענה נגזרים תפקידים שונים למדינה ולגופיה ובממשק ביניהם לבין הארגונים.

המשפט הינו מימד מרכזי בו פועלת המדינה למול המרחב האזרחי, ובהתאם לכך התזכיר המוצע נועד להסדיר ממשקים אלה.

1.2 פרק הרגולציה

דו״ח זה מתמקד בהערכת השפעות פרק הרגולציה של החוק.

כאמור לעיל, חלק אינטגרלי במענה הלאומי הנדרש מבוטא תחת סעיף העמידות : ״שיפור רמת

הכשירות והמוכנות של הארגונים במשק באמצעות פעילויות רגולטוריות, הכשרתיות והסברתיות". פרק הרגולציה ממסד את המערך כסמכות מקצועית לאומית בתחום הידע, השיטות והאמצעים של איומי מרחב הסייבר, דרכי ההתמודדות עמם, וכפועל יוצא, מדיניות ההכוונה של גופים אזרחיים במשק. הפרק מיישם הלכה למעשה את האבחנה שמבצע המערך בחלוקה של ארגוני המשק לקטגוריות סיכון שונות על פי תבחינים ומשקלים.

הפרק עוסק בהסדרת היחסים בין המערך לרשויות מאסדרות מגזריות משמעותיות לעניין הגנת סייבר, כמו גם בסמכויות המערך להנחות גופים במישרין ולהשלים את סמכותן של רשויות מאסדרות מגזריות בהינתן שישנם פערים.

פרק הרגולציה אינו עוסק בשאר הסעיפים שהוזכרו, בהתמודדות עם אירועים בזמן אמת ובהפעלת יכולות מבצעיות אחרות. אזורים אלה אינם סמכויות רגולטוריות אלא סמכויות אופרטיביות ומטופלות בפרק מתאים בחוק. סמכויות אלה מופעלות משעה שיש חשש קונקרטי לתקיפת סייבר, וההקשר של הפעלתן הוא מניעה, הכלה או צמצום של נזקים מתקיפות סייבר. בכך דומות סמכויות אלה לסמכויות ביטחוניות וסמכויות בתחום אכיפת החוק אשר אינן סמכויות "רגולטוריות".

יצוין עוד, כי ההגנה על תשתיות מחשוב קריטיות, מבוצעת בהתאם לחוק להסדרת הביטחון בגופים ציבוריים ותזכיר החוק המוצע איננו עוסק בהן.

2. זיהוי הבעיה וסיבותיה

2.1 אינטרסים ציבוריים בסיכון

אינטרס ציבורי הוא מושג המייצג צורות שונות של טובת הכלל בתחומים שונים (למשל: תחבורה יעילה, איכות הסביבה, רווחת הפרט, בריאות הציבור ועוד). על המדינה לאזן מתחים מובנים קיימים בין טובת הפרט לצרכי הכלל.

דוגמה מובהקת לכך במרחב הסייבר, באה לידי ביטוי בהגנה על חיי אדם ועל סמלי שלטון כפי שהיא משתקפת מהחוק להסדרת הביטחון בגופים ציבוריים (תשנ"ח-1998)[7]: המדינה מתערבת על פי חוק בהגנת תשתיות מחשוב קריטיות בחברות פרטיות, תחת ההנחה שהאינטרס הפרטי של הארגון לעניין זה אינו הולם לאינטרס הציבורי.

[7] http://main.knesset.gov.il/Activity/committees/ForeignAffairs/LegislationDocs/sec7-2.doc

לטובת יצירת מענה מידתי אל מול הסיכון שלשמו מתבצעת ההתערבות הממשלתית, הוגדרו מספר "תבחיני על". תבחינים אלו מהווים את הסרגל מולו נבחנת הפגיעה הפוטנציאלית לאינטרס הציבורי וממנו נגזרת צורת ומידת ההתערבות הממשלתית.

להלן עיקרי התבחינים:

- חיי אדם, בריאות ושלום הציבור - לדוגמא על ידי תקיפת בקר תעשייתי האחראי על אחזקת חומר נפיץ.
- רציפות תפקודית משקית - לדוגמא על ידי השבתת פס ייצור של מפעלי מזון משמעותיים בשעת חירום.
- יציבות פיננסית ושגשוג כלכלי - לדוגמא על ידי השבתת מערכות בנקאיות או אחרות הקשורות בשוק ההון.
- הזכות לפרטיות - לדוגמא על ידי גניבה או השחתה של פרטים אישיים של האוכלוסייה באמצעות פריצה למאגר מידע גדול. הגנת הסביבה - לדוגמא על ידי השבתת מערכות האחראיות על סינון פליטות או מזהמים אחרים במפעל גדול.
- יציבה ותודעה לאומית - פגיעות מהסוג שתוארו לעיל יכולות להצטבר לכדי פגיעת מאקרו. עם זאת, גם השחתת סמלי שלטון באמצעים מקוונים או תקיפה כנגד נותני שירותים מקוונים משמעותיים ללא הקשר ספציפי או גניבת פרטיהם של עובדי מדינה יכולים כולם להיחשב לפגיעה כזו.

2.2 הערכת וכימות הסיכון לאינטרס הציבורי (במצב הקיים)

בפתח הדברים נציין כי יש קושי מתודולוגי להעריך בצורה מדויקת את הסיכון לאינטרס הציבורי, וזאת לנוכח המציאות הטכנולוגית הדינאמית שבה משרעת האיומים מתפתחת, ולנוכח העובדה שאין עדיין מתודולוגיה יציבה להערכת נכסים וסיכונים ברמה המגזרית והמשקית. בסקירה שנערכה במטרה לבחון מודלים להערכת פוטנציאל הנזק כתוצאה מפגיעה במרחב הסייבר, נמצא כי ישנה שונות רבה בין המחקרים.

קשיים אלה מלווים גם בקשיי איסוף וקבלה של מידע הנובעים מהצורך בהסתמכות על מידע של ארגונים על הנעשה ברשתותיהם.

2.2.1. נטל רגולטורי הנובע מהיעדר אסדרה אחודה במשק

כיום, ארגונים במשק נדרשים לאמץ וליישם הנחיות בתחום הגנת הסייבר ממספר רגולטורים וגופי תקינה שונים, בהתאם לתחום פעילותם ולשווקים בהם הם פועלים. במציאות זו, עשויים ארגונים להשקיע משאבים רבים בהגנת סייבר, מבלי שהדבר ישפיע באופן מהותי על רמת ההגנה שלהם בפועל. לדוגמה, במידה וגוף מוסדי מעוניין להטמיע פתרונות ענן, יהיה עליו לעמוד בהנחיות של מספר רגולטורים וגופי תקינה (כגון הרשות להגנת הפרטיות, רשות שוק ההון, הרשות לניירות ערך, תקן ISO, דרישות PCI ועוד).

ריבוי התקנים הבינלאומיים והעצמאיים להגנת סייבר מוביל להשקעה עודפת בעמידה בתקנות

והנחיות הנוגעות לנהלי עבודה בארגונים (פיתוח מאובטח, הדרכת עובדים, החתמת ספקים וכו׳). היעדר תקן לאומי ובסיס ידע רחב, נגיש ומקובל, מוביל לבזבוז משאבים ארגוני המצטבר להוצאות עודפות ניכרות בכלל המשק.

2.2.2. הסייבר הינו מחולל חירום לאומי חדש ועוצמתי

לצד ההיבטים הביטחוניים, טומנים בחובם מצבי חירום השפעות כלכליות נרחבות ביותר. אחד התרחישים הקיצוניים ביותר של התקפת סייבר כנגד המשק האזרחי הוא תקיפה של תשתיות האנרגיה. מחקר של חברת הביטוח וניהול הסיכונים לויד׳ס (Lloyd's), העריך כי מתקפה כנגד אחת ממפעילות רשת החשמל האמריקנית תעלה למשק האמריקני 243 מיליארד $ בתרחיש הביניים וטריליון $ בתרחיש הקיצוני[8]. הערכות בסדר גודל דומה קיימות בהקשר של פגיעה בתשתיות תחבורה, פיננסים ותקשורת גדולות.

ההנחה היא שהתקפה מסוג כזה דורשת רמת תחכום גבוהה בשל המורכבות הטכנית של תקיפת בקרים תעשייתיים בשרשרת הייצור האנרגטית. על כן, מצד אחד ההסתברות להתרחשותה נמוכה יותר, ומצד שני הסיכוי שתבוצע על ידי שחקן מדינתי ו/או טרוריסטי עוין בצמוד לתרחיש חירום רחב יותר (כגון מלחמה הופכות את התרחיש למסוכן אף יותר במקרה הישראלי. כמו כן, יש לציין כי גם תקיפות רחבות היקף כנגד רשתות IT, בכלים בסיסיים יחסית, יכולה לגרום לשיבושים חמורים של רציפות תפקודית משקית. ניתן לראות בהתקפה שבוצעה כנגד מגזר הבריאות הבריטי במאי 2017[9] סנונית מבשרת רעות בהקשר זה.

מתקפות מסוג זה עדיין אינן שכיחות, אולם מתקפה מעין זו בוצעה כנגד רשת החשמל האוקראינית בשתי הזדמנויות שונות במהלך 2015[10]. ב-2014 הותקפה מערכת הייצור של מפעל גרמני לייצור פלדה ותפקודו נפגע. הסימנים מעידים כי מתקפות מסוג זה יהפכו שכיחות יותר ויותר.

ברור אם כן, כי לסיכון מימדים מובהקים של ביטחון הלאומי, שהרי פגיעה ברציפות תפקודית משקית בשעת חירום מהווה סיכון פוטנציאלי חמור לביטחון הלאומי, יותר מכל סוג אחר של סיכון. בבסיס החלטות הממשלה בשנת 2015, עומדת ההנחה שסיכונים אלה יכולים להתפרץ במרחב האזרחי הכללי, ולא רק ביחס לפעילויות שהוסדרו היסטורית כתשתיות קריטיות.

איום הסייבר מתאפיין ביכולת לתקוף בו זמנית ארגונים רבים בעלי מאפיינים דומים ולכן, לדוגמא,

---

[8] https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

[9] Ransomware Attack 2017, International Journal of Advanced Research in Computer Science: http://www.ijarcs.info/index.php/Ijarcs/article/download/4021/3642

[10] Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

תחנות כוח קטנות יוגדרו כארגון בסיווג סיכון גבוה למרות שכל אחת בפני עצמה איננה מסכנת סיכון קריטי את האינטרס הציבורי. כמו כן, ארגונים מסוימים יוגדרו בסיווג סיכון גבוה משום שהם מהווים צומת לשרשרות אספקה של תשתיות קריטיות, ופגיעה בהם עשויה להוביל לתרחישים הדומים לאלה שתוארו לעיל.

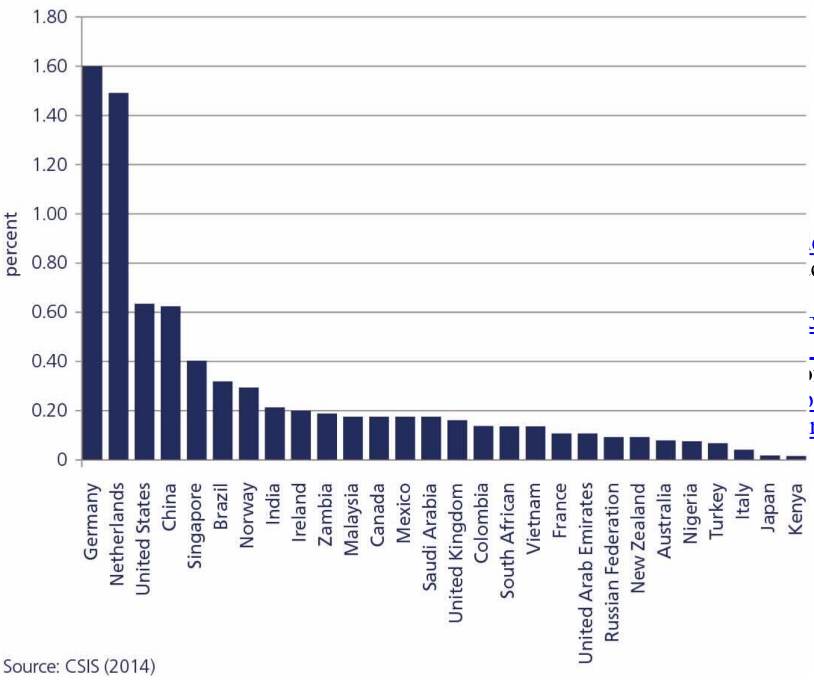
2.2.3. סייבר כאיום עולה על הכלכלה והחברה

מחקרים רבים העריכו את הנזק שבתקיפות "מסורתיות" כנגד רשת ה-IT. ההערכות לנזק ברמה הלאומית מגיעות עד 1.6% מהתמ"ג בשנה למדינות מערביות בטווח נזקים של בין חצי מיליון ל-20 מיליון יורו לארגון בשנה[11]. עם זאת, יש לזכור כי מחקרים אלה מתרכזים בעיקר בנזק הישיר לארגון ולא בנזק העקיף לאינטרסים הציבוריים.

לגבי נזק עקיף, ברור, כפי שכבר תואר לעיל שנזק לתשתיות משקיות עלול ליצור גלי הדף בעלי משמעויות קשות ביותר ברמת המאקרו. עם זאת, יש לשקלל גורם נוסף הרלוונטי בעיקר למרחב הסייבר. **__אינטראקציה דיגיטלית מקוונת__** היא אחד ממנועי הצמיחה החשובים של כלכלות מתקדמות[12]. היכולת של אזרחים לסחור באינטרנט, לגשת לשירותים תוך חשיפת נתונים אישיים ולעשות שימוש ביישומים מתקדמים תלויה ברמת האמון שלהם בביטחון הסייבר.

ככל שהמענה לאיום הסייבר ברמה המשקית חלש, נפגע האמון הכללי של כלל השחקנים, החל מהאזרח הבודד וכלה בקובע המדיניות הממשלתי והעסקי, ביתרונות הדיגיטיציה והשימוש במרחב הסייבר. רמות האמון בעולם המערבי נמוכות כבר היום[13], ליכולת להעצים תחושת ביטחון ואמון זו משמעויות כלכליות מרחיקות לכת[14].

Figure 9: The cost of cybercrime and cyber espionage expressed as percent of GDP



Source: CSIS (2014)

11 The cost of incidents affecting CIIs: ...ents-affecting-ciis/at_download/fullReport

12 ...ct of the Internet on economic growth and prosperity": ...ch/Our%20Insights/The%20great%20tran ..._of_Internet_on_economic_growth.ashx

13 ...meter 390 cyber security report 390/2012: ...licopinion/archives/ebs/ebs_390_en.pdf

14 ...rg/cyberrisks/risk-nexus-september-2015-overcome-by-cyber-risks.pdf

2.3.הגדרת הבעיה ומחוללי הבעיה

קיימות מספר בעיות המובילות לסיכון האמור לעיל אליהן מתייחס החוק. פרק הרגולציה מטפל באחת מהן. בעיית העל עמה יש להתמודד בשכבת העמידות היא רמת הגנת סייבר בלתי מספקת של ארגונים וחברות במשק. הגנה מספקת ואפקטיבית מתקיימת כאשר הארגון מבין את איומי הסייבר המופנים כלפיו ומספק מענה הולם באמצעות נהלים ומדיניות ארגונית, מערכות טכנולוגיות וכשירות בעלי תפקידים בארגון.

בהיעדר תקינה מחייבת, רשאי כל ארגון לקבוע את רמת ההגנה שלו בהתאם לניהול סיכונים המתייחס לשיקולים פרטיים בלבד. משכך, לא ניתן להבטיח שארגונים במשק יעשו את מירב המאמץ להשגת רמת הגנה נאותה, ובכך נפגע המאמץ להשגת עמידות מצרפית למשק כולו.

מכיוון ששיפור רמת העמידות הארגונית והשקעה נאותה של משאבים לצמצום פוטנציאל הפגיעה, צריכים להיות אינטרס בסיסי של ארגונים ופרטים במשק, טוב היה לו ניתן היה לסמוך על כוחות השוק שיביאו לתיקון הבעיה. אולם, מספר "כשלי שוק" מונעים זאת, וכל אחד מהם מהווה בעיית משנה בפני עצמה.

2.3.1. **<u>הגנת חסר כתוצאה מחוסר מודעות</u>** - ארגונים במשק אשר אינם משקיעים בהגנה בסייבר מאחר והם אינם מודעים לסיכונים השונים ולפוטנציאל הנזק. ארגונים אלו מתנהלים לעיתים תחת רמת הגנה נמוכה, מאחר והם אינם יודעים כי הם חשופים לאיומי סייבר רבים.

2.3.2. **<u>הגנת חסר כתוצאה מחוסר ידע</u>** – ארגונים המכירים באיומי הסייבר, אך אינם יודעים מה בכוחם לעשות בנדון. לא פעם, ארגונים אלו מנסים באופן לא מוסדר ותשתיתי להשקיע ולרכז מאמצים כתוצאה מאירוע סייבר שחוו או אירוע שאליו נחשפו. השקעה זו איננה נשענת על ניתוח סיכונים והבנת מפת האיומים, אלא מתוך מתן מענה נקודתי ("כיבוי שריפות").

2.3.3. **<u>הגנת חסר כתוצאה מחוסר יכולת</u>** – ארגונים אשר מבינים ורוצים להשקיע ולשפר את רמת ההגנה שלהם, אך אין להם הכלים ו/או המשאבים הנדרשים להגיע לרמת ההגנה הרצויה. לדוגמה, ארגון אשר משקיע בהגנה בסייבר על עצמו בתוך הארגון, אך הוא עדיין חשוף לאירוע סייבר כתוצאה מתלות בשרשרת האספקה שלו שעליה אין לו יכולת להשפיע.

2.3.4. **<u>הגנת חסר כתוצאה מאינטרס ארגוני שונה</u>** – כשל "סיכון מוסרי". ארגונים אשר בוחנים את רמת ההגנה שלהם בסייבר מתוך רצון לבצע אופטימיזציה מקומית, בהתעלם מהשפעות חיצוניות על בעלי עניין ועל המרחב הציבורי. לדוגמה, ארגון אשר קובע את רמת ההגנה בהתאם לניהול סיכונים המביא בחשבון אך ורק שיקולי עלות, ללא שיקולים של חשיפת לקוחות, שותפים וספקים לאיומי סייבר.

2.4. אוכלוסיית המטרה

הגנה על מרחב הסייבר, כוללת משרעת רחבה מאוד של גופים בעלי מאפיינים רבים ומגוונים, מתשתיות מדינתיות קריטיות (דוגמת רכבת ישראל, חברת החשמל, חברת מקורות ועוד) דרך גופים בעלי פוטנציאל נזק ציבורי נמוך יותר (דוגמת עיריות, מפעלים, חברות תחבורה ציבורית ועוד), וכלה בעסקים קטנים ובעלי משלח יד חופשי.

על מנת לספק מענה מידתי אל מול פוטנציאל נזק זה, נקבעו בעבודת מטה של המערך שלוש רמות שונות של פגיעה אפשרית באינטרס הציבורי (A,B,C). אל מול כל רמה כזו, מוגדרת מידת מעורבות ועומק רגולציה בהתאם לפוטנציאל הנזק.

- ארגונים ברמה A – ארגונים אשר פגיעה בהם מהווה סיכון חמור לאחד מן האינטרסים הציבוריים שתוארו. הליך סיווג ארגון כ-A כולל היוועצות עם הרשות המאסדרת האחראית על האינטרס הציבורי הרלוונטי (לדוגמא, משרד האנרגיה בעולם הרציפות התפקודית של מגזר האנרגיה) ושילוב של תובנות מתהליכים אופרטיביים של המערך: איסוף מודיעין, ניתוח דפוסי תקיפה, ניתוח איומים וכיו״ב. סיווג A כולל כמה מאות ארגונים.
- ארגונים ברמה B - ארגונים אשר פגיעה בהם מהווה סיכון מהותי לאחד מן האינטרסים הציבוריים שתוארו. התהליך המביא לסיווג ארגון כ-B קשור לניהול הסיכונים הפנימי של הרגולטור הרלוונטי ולקבוצת הייחוס השגרתית שלו. סיווג B כולל כמה אלפי ארגונים.
- ארגונים ברמה C – ארגונים אשר פגיעה בהם מהווה סיכון נמוך לאחד מן האינטרסים הציבוריים שתוארו. מדובר למעשה בכל ארגון במשק שלא עונה לסיווג A או B.

2.5. תיקוף קיומה של הבעיה

כחלק מפעילות מערך הסייבר הלאומי, מתקיים תהליך מתמיד של הבנת תמונת המצב של הגנת הסייבר במשק. בשנת 2016 ערך מטה הסייבר בשיתוף עם רשות החירום הלאומית והרשות להשקעות ולפיתוח התעשייה סקר בקרב 50 מפעלים חיוניים. מטרת הסקר הייתה לאבחן את מצב ההגנה, את פערי ההגנה ואת הסיבות לפערים, כחלק מהכנת תכנית לתמרוץ הגנת סייבר במפעלים אלה. הסקר מצא כי ב-62% מהארגונים אין מודעות כלל לנזק הכלכלי (הישיר) שעלול להיגרם לארגון, ובהתאמה, 62% לא ביצעו מעולם סקר סיכוני סייבר ואין להם מסמך מדיניות ארגוני שמסדיר את הטיפול באירוע. ב-44% מהארגונים אין בעל תפקיד ממונה לנושא הגנת סייבר, וכ-20% מהארגונים מאבחנים את הסיבה העיקרית לאי ביצוע פעולות בסיסיות בהקשר זה לחסך בידע, הכשרה או כ״א מתאים ו-35% לסדר העדיפויות של הנהלת החברה. ממצאים אלה מאשרים את ההערכה שקיים מחסור במידע ושחברות אינן לוקחות על עצמן את מלוא האחריות לנזקי התקפת סייבר.

סקר שנערך בשנת 2017 ע"י חברות Konfidas, Deloite, אוניברסיטת תל אביב ואיגוד האינטרנט הישראלי הצביע על פערי מודעות משמעותיים. על השאלה "מהם להערכתך המכשולים הגדולים ביותר ביישום האסטרטגיה או התכנית בתחום הגנת הסייבר של חברתך?" 33% השיבו שהמכשול הגדול ביותר הוא חוסר בחזון או בהבנה של השפעת תחום הגנת הסייבר על הפעילות של הארגון, 33% נוספים השיבו שהמכשול הוא מחסור בידע ובניסיון בתחום הגנת הסייבר, ממצא התומך את ההערכה שקיים מחסור במידע. 33% השיבו שהנושא אינו בסדר העדיפויות של ההנהלה, ו-37% השיבו שהבעיה נתפסת כבעיה של מנהל אבטחת המידע ולא של כלל המנהלים בארגון, ממצא התומך את ההערכה שקיימת החצנה שלילית של הבעיה (ניתנה אפשרות לבחור יותר מתשובה אחת).

משרד התחבורה מעריך כי הפער בהשקעה הכספית הנדרשת במגזר התחבורה הרחב (כולל הציבורי) מגיע לעשרות מיליוני ש"ח[15]. ההערכות לגבי הפערים במערכת הבריאות הרחבה דומות. במגזרים אחרים טרם התבצעה עבודת מטה מסודרת שתאפשר אמירה מקצועית ברורה. במהלך עבודתו של ה-CERT הלאומי ואגפי ההנחיה של המערך נוצרה היכרות עם רמת ההיערכות של עשרות ארגונים, בכולם נמצאו ליקויים קשים בכל הנוגע לרמת ההיערכות.

סקר הגנת סייבר במשק הבריטי שבוצע על ידי המשרד לדיגיטל, מדיה, תרבות וספורט בבריטניה סקר באופן נרחב ומעמיק את התפיסות והעמדות של ארגונים וחברות במשק באמצעות מדגם של 1008 משיבים. הסקר מצא שרק 18% מהמשיבים מודעים לסטנדרטים בהגנת סייבר לארגון, ורק ל-29% יש מדיניות ארגונית להגנת סייבר.

נתונים אלה מלמדים על פערים משמעותיים מאוד בידע ויישום של מתודולוגיות להגנת סייבר בארגון ומאשרות את ההערכות בעניין כשלי השוק הנובעים מפערים במודעות, בידע וביכולת. הנתונים מצביעים על כשל השוק של "החצנה שלילית" (סיכון מוסרי) כבעיה רוחבית המתקשרת לקבלת החלטות בארגונים שבהם קיימים מודעות, ידע ויכולת ברמה סבירה.

3. סקירה השוואתית בינלאומית

ככלל, ניתן להבחין בשלושה מודלים שונים של היערכות מדינתית להגנה על ארגונים בסייבר.[16]

המודל הראשון הוא **המודל המבוזר**. מודל זה מאופיין בכך שמדיניות ההגנה על ארגונים חיוניים מתבצעת ברמה הסקטוריאלית. לא קיים הסדר חקיקתי לאומי אחד, כל רשות מאסדרת או רשות ציבורית מוסמכת מקיימת הסדרים בתחומי סמכותה, בחלק מהמקרים תוך הפנייה או התאמה לתקנים מקובלים בתחום זה. במקרים מסוימים הסדרים חוקיים מטילים על ארגונים פרטיים את החובה לקיים הגנת סייבר נאותה ללא גורם מאסדר, מפקח או מבקר. דוגמאות מובהקות למודל זה מתקיימות **בשוודיה, קפריסין, אוסטריה, פינלנד ושוויץ**.

המודל השני הוא **המודל הריכוזי**. מודל ריכוזי מאופיין בכך שמוקמת סוכנות ממשלתית ייעודית למטרות הגנה בסייבר על ארגונים חיוניים,

---

[15] נייר עבודה פנימי שמסקנותיו הספציפיות לא מפורטות מטעמי סיווג.
[16] Stocktaking, Analysis and Recommendations on the Protection of CIIs, ENISA, 2016

המקבלת בכירות על פני הסוכנויות המגזריות. מאפיין נוסף הוא קיומו של הסדר חקיקתי מקיף וייעודי. הסוכנות הראשית אחראית במידה רבה לזיהוי הארגונים, להתוויית שיטות ההגנה, למתן הנחיות ולבקרה על עמידת הגופים בהם. לעיתים תפעל הסוכנות הראשית דרך סוכנויות משנה מגזריות. דוגמא די מובהקת למודל זה היא **צרפת**, מדינה נוספת לה מאפיינים דומים היא **צ'כיה**.

המודל השלישי, הוא **הרגולציה המשותפת**. במודל זה המדינה והמגזר הפרטי מקיימים מודל של שותפות אופקית בו החלטות מתקבלות במשותף, בד"כ בפורומים משותפים או מיזמי (PPP (Public Private Platform מסוגים שונים. במשטרי רגולציה כאלה מנוסחים לעיתים Best Practices וקודי ציות אחרים אך אילו לרוב אינם מגובים במנגנונים רגולטוריים מחייבים. הנטייה במשטרי רגולציה מסוג זה היא לעשות שימוש בכלי תמרוץ רותמי שוק מסוגים שונים. דוגמא מובהקת למודל זה ניתן למצוא **בהולנד**, נטייתן של רוב המדינות האנגלוסקסיות **בריטניה, ארה"ב, אוסטרליה וקנדה**, היא למודל הזה. עם זאת, חשוב לציין שבמגזרים ברמת הסיכון הגבוהה ביותר, כמו אנרגיה ופיננסים, בד"כ יתקיים אחד משני המודלים הראשונים שהוזכרו.

בגרמניה פועל מודל המשלב בין המודל השני לשלישי, תחת המורכבות של גרמניה כמדינה פדרלית, המבוסס על הטלת אחריות על גורם אחד בממשל הפדרלי, אשר התקנים אותם הוא מטמיע מבוססים על שיתוף פעולה עם ההתאחדויות הרלבנטיות של התעשיינים.

נזכיר כי ב-2016 פרסם האיחוד האירופי את דירקטיבת NIS[17] העוסקת במישרין בקידום ההגנה על ארגונים חיוניים באיחוד. מטרת הדירקטיבה ליצור מכנה משותף למדינות האיחוד בתחום האסדרה של ארגונים חיוניים, הקמה של CERT לאומי בכל אחת מהמדינות, ומינוי נקודת קשר לאומית לצורך טיפול באירועים חוצי גבולות. הדירקטיבה מחייבת מדינות להסדיר בחקיקה, בין היתר, תהליכים לזיהוי תשתיות קריטיות במגזרים ספציפיים, להגדיר מנגנוני ניהול סיכונים ובקרת אבטחה ולהחיל חובות דיווח. דירקטיבת NIS עוסקת גם במפעילים של תשתיות חיוניות וגם בספקי שירותים דיגיטליים (DSP) כמו שירותי ענן, שווקים מקוונים ואף מנועי חיפוש.

מהלך זה משלים מהלך משמעותי אחר בתחום רגולציה על שימוש בטכנולוגיית מידע, ה- GDPR- General Data Protection Regulation אשר מעדכנת בצורה מקיפה את הכללים החלים על עיבוד מידע אישי, כלומר רגולציית מאגרי מידע. הצפי הוא ש-NIS ו-GDPR יחדפו מדינות אירופיות נוספות למימוש של אחד משני המודלים הראשונים שהוזכרו.

ניתן למנות את המדינות הבאות שהחילו, או שנמצאות לקראת החלה קרובה של חקיקה הנוגעת להגנה על תשתיות קריטיות/חיוניות, בעלת קווים מקבילים מובהקים לפרק הרגולציה בישראל. נציין שוב שכל מדינות האיחוד האירופי צפויות לאמץ חקיקה דומה תחת דירקטיבת NIS.

- <u>ארה"ב</u>: נכון להיום, אין חקיקה פדראלית גורפת המקבילה לנושאים המנויים בדירקטיבת NIS. קיימים שלושה חוקים פדרליים: HIPAA, FISMA וה- Gramm Leach Bliley Act, אשר מסדירים את הצורך ברפי מינימום להגנה במגזרי הבריאות, הסוכנויות הפדראליות והפיננסים בהתאמה. על פי גישה משפטית מסוימת, לממשל האמריקני יש כבר היום סמכויות להסדיר הגנה בסייבר בכל מגזר התשתיות הקריטיות, אולם גישה זו לא נבחנה דה פקטו[18]. ברמת המדינות קיימת דיפרנציאציה גבוהה: כל מדינות ארה"ב חוקקו חובות דיווח לתקריות של דלף מידע פרטי, ורגולטורים של מדינות נוספות החילו הוראות נוספות בתחומים מגזריים ספציפיים, כמו המגזר הפיננסי.
- <u>בריטניה</u>: בשנת 2018 פרסמה הממשלה מדיניות לקראת החלת דירקטיבת NIS במדינה[19]. נראה שהדירקטיבה תחול על יותר מ-400 ארגונים במגזרי המיקוד של NIS. הרגולציה צפויה להיות ברמה שטחית יותר מרוב התקנים המקובלים.

---

[17] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[18] Do Agencies Already Have the Authority to Issue Critical Infrastructure Protection Regulations?: http://www.circleid.com/posts/20120820_agencies_authority_to_issue_critical_infrastructure_protection

[19] The Network and Information Systems Regulation 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf

- <u>צרפת</u>: בשנת 2013 קיבלה צרפת חקיקה אשר מטרתה להגדיר חובות דיווח, מנגנוני הנחיה וחובות הגנת מינימאליות על תשתיות קריטיות במדינה[20]. החוק אמור לחול על כ-200 ארגונים ב-12 מגזרים.
- <u>צ׳כיה</u>: בשנת 2017 הוגש תיקון לחוק הסייבר הצ׳כי[21] המחיל את מנגנוני NIS על מאות ארגונים נוספים לאחר שחובות אלו כבר חלו במסגרת החוק הקיים על מגזרי האנרגיה, הבנקאות, התקשורת, התחבורה והמים
- <u>גרמניה</u>: ב-2015 נחקק בגרמניה חוק[22] המסדיר את חובתם של ארגונים חיוניים לעמוד בחובות הגנה בסיסיות בסייבר. הצפי הוא לכ-2000 ארגונים מושפעים. החוק מסדיר גם חובת דיווח לרגולטור.
- <u>הולנד</u>: בשנת 2017 הוצא צו המציב קריטריונים לתשתיות קריטיות בסייבר במדינה ל-8 מגזרים שונים. בשלב ראשון מוטלת על הגופים חובת דיווח על אירועי סייבר.
- <u>סינגפור</u>: בשנת 2017 נחקק חוק[23] המזהה אחד עשר תהליכים קריטיים במדינה ומטיל חובות הגנה, דיווח והערכה עצמית על גופים פגיעים לסייבר לאור התהליכים הקריטיים שנקבעו.

4. <u>סקירת ההסדר הממשלי הקיים בישראל בהגנה על ארגונים בסייבר</u>

4.1. הסדרים רגולטוריים קיימים

הרגולציה הישראלית על רמת הגנת הסייבר של תשתיות קריטיות מוסדרת במסגרת ״החוק להסדרת הביטחון בגופים ציבוריים״ (תשנ״ח-1998). חוק זה הטיל על שירות הביטחון הכללי להיות המנחה של כמה עשרות תשתיות מחשוב קריטיות במדינת ישראל. הוספת ארגון לרשימת הארגונים מתבצעת לאחר בחינה של ועדת היגוי בראשות ראש מערך הסייבר הלאומי, ובאישור ועדת כנסת. החל משנת 2016 מערך הסייבר הלאומי הוא הגורם האחראי לפי החוק (למעט בעלי רישיון תקשורת המופיעים בתוספת הרביעית לחוק שנותרו באחריות שב״כ).

כמה רשויות ציבוריות ורשויות מאסדרות מגזריות פיתחו הוראות בתחום אבטחת מידע והגנת הסייבר בתחומי סמכותן. ניתן למנות את המפקח על הבנקים, רשות שוק ההון ומשרד האנרגיה כרשויות מאסדרות אשר ביצעו כבר צעדים קונקרטיים ופיתחו הוראות בתחום אבטחת מידע ייעודיות למגזר שלהן.

הוראות אלה נכתבו באופן שהמאסדר המגזרי ביצע מחקר השוואתי, איתר תקנים רלבנטיים בתחום הגנת הסייבר, ופיתח הוראות רגולציה ייעודיות עבור המגזר עליו הוא אחראי. כתוצאה מכך יש שונות במידת הפירוט ובתכנים של הוראות האסדרה, על אף שהן מבקשות להסדיר את אותו סיכון – סיכון הסייבר לארגון.

---

[20] The French CIIP Framework: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/
[21] 181/2014 Czech Cyber Security Act: http://senat.cz/xqw/xervlet/pssenat/htmlhled?action=doc&value=83936
[22] Critical infrastructure protection: https://www.bmi.bund.de/EN/topics/civil-protection/critical-infrastructure-protection/critical-infrastructure-protection-node.html
[23] Singapore Cybersecurity Act 2017: https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

לאחרונה נקבעו לפי חוק הגנת הפרטיות תקנות בתחום אבטחת המידע למחזיקים במאגרי מידע המכילים מידע מוגן פרטיות.

4.2.פערים בהסדר הרגולטורי הישראלי

ניתן לראות אם כן, שבהגנת הסייבר בישראל מתקיים מודל ריכוזי בתחום התשתיות הקריטיות. רגולציית הסייבר הינה שכבה נוספת החלה על גופים שהינם תשתיות קריטיות. בחלק קטן מהמגזרים המשקיים הרלוונטיים מתקיים מודל ביזורי ברמות שונות של עוצמה, אולם ברוב המגזרים אין כל הסדר משמעותי.

במסגרת עבודת המטה שהתבצעה לקראת החלטת הממשלה 2444 ולאחריה, מופו הפערים המונעים מרשויות המדינה להפעיל את סמכותה כלפי ארגונים בסיווג סיכון גבוה.

כאמור לעיל, המערך רואה את המגזרים האזרחיים הבאים כרלוונטיים: אנרגיה, מים וביוב, מזון, תקשורת, תחבורה, בריאות, פיננסים, מפעלים חיוניים כהגדרתם בחוק, גופים המחזיקים חומרים מסוכנים, המגזר הממשלתי והשלטון המקומי, מאגרי מידע, תשתיות ICT ותקשורת, גופים המצויים בשרשרת האספקה של תשתיות קריטיות ומגזר ההשכלה הגבוהה. במסגרת העבודה התקיימו התייעצויות עם כלל הרשויות המאסדרות הרלוונטיות.

המסקנות העיקריות:

א. במגזרים רבים קיימת רשות מאסדרת מובהקת העוסקת בהיבטים רבים הנוגעים לאינטרסים הציבוריים בהם החוק אמור לטפל (רציפות תפקודית, יציבות פיננסית וכיו״ב). עם זאת, לרשות המאסדרת חסרים כלים רגולטוריים ומקצועיים על מנת להכוון התנהגות של ארגונים בהגנת סייבר.
ב. כלפי ארגונים מסוימים אין כלל גורם מאסדר מובהק העוסק באינטרסים ציבוריים רלוונטיים.
ג. לרשויות מאסדרות רבות חסרים משאבי כוח אדם וידע, על מנת לבצע את התהליכים הנדרשים.

5. תכליות וסיכונים

5.1.תכליות

תכלית הפרק הרגולטורי בחוק היא הגנה על האינטרסים הציבוריים כמתואר בסעיף 2.1. מטרתו הראשונה של הפרק היא להקנות למדינה את ארגז הכלים הרגולטורי הנדרש, על מנת להכווין את התנהגותם של ארגונים בכל הנוגע להיערכותם ולכשירותם להגנת סייבר. מטרתו השנייה היא לסנכרן בין הסוכנויות הרגולטוריות השונות הן ברמת הביצוע והן ברמה המקצועית.

5.2.סיכונים רגולטוריים

קיימות שתי משפחות של סיכונים רגולטוריים:

5.2.1. נטל רגולטורי עודף

החוק מאפשר התערבות מדינתית בחופש הפעולה הארגוני באמצעות קביעת כללים לטיפול בסיכוני סייבר, וכן חיכוך בירוקרטי הנובע מאמצעים להטמעת הכללים כגון רישוי, פיקוח ואכיפה. אמצעים רגולטוריים אלה ישיתו נטל רגולטורי של עלויות על הארגונים לגביהם הם חלים.

על אף שאמצעים אלה להעלאת רמת החוסן הארגוני והמשקי מקובלים ונדרשים, יש סיכון כי לא יהיו יעילים דיים, וכן כי תופעות הלוואי שלהם, ברמה המשקית, יפגעו באופן לא מידתי בפריון של הארגונים ושל המשק בכלל.

5.2.2. סיכוני רגולציה מנחה

סיכוני רגולציה מנחה הם הסיכונים הפנימיים של הכלים הרגולטיביים המופעלים, ומוכרים כסיכונים גנריים הכרוכים ברגולציה ממשלתית כופה[24]:

- עידוד תרבות צ׳קליסט: יישום פרקטיקות הגנה ונהלים ארגוניים ללא הבנת מהות הפעולות והקשרי האיום באופן שעשוי להוביל לחוסר אפקטיביות.
- ״ציות יצירתי״: אוכלוסיית המטרה תמלא אחר הוראות הרגולטור במדויק, אף שהתוצאה לא תעלה בקנה אחד עם כוונת הרגולטור.
- פגיעה בחדשנות: הסתמכות על תקינה וציות כמענה לאיומי סייבר אינה מניעה ליצירת פתרונות טכנולוגיים חדשניים ויצירתיים, מכיוון שהיא מהווה אישור תקינות לפתרונות הקיימים ברגולציה.

[24] תורת הערכת השפעות רגולציה, אגף ממשל וחברה, משרד ראש הממשלה, 2013:
http://www.pmo.gov.il/policyplanning/Regulation/Documents/RIA.pdf

- העברת אחריות מהמשק למדינה: כאשר המדינה מפקחת ומאסדרת, עשויה להתקבע תודעה שנושא הרגולציה הינו באחריותה הבלעדית בעוד שמושאי הרגולציה הם האחראים בפועל.

חלק ב' – ניסוח חלופות

ככלל, החלופות התמקדו בבחינת המודלים הקיימים בישראל ובעולם, ובחינתם אל מול חלופת ה-0, המשך המצב הקיים על פי החלטת ממשלה 2443 המהווה את המדיניות הממשלתית העכשווית בנושא.

עיקרי החלטת ממשלה 2443:[25]

א. תפיסת האסדרה תקודם תוך שאיפה לא ליצור רגולטורים חדשים אלא להעצים קיימים. (1ב)
ב. מטה הסייבר ימפה את משרדי הממשלה האמונים על מגזרים רלוונטיים ויסווגם לפי רמת המשאבים הנדרשת להם. (נספח ד', 4א)
ג. משרדי ממשלה האמונים על רגולציה מגזרית רלוונטית, יקימו יחידות הכוונה מגזריות בהגנה בסייבר, הללו יפעלו בהנחיה מקצועית של מערך הסייבר. (1ה1)
ד. משרדי הממשלה יפעלו להגדרת מדיניות ודרישות אסדרה כלפי המגזר עליו הם אחראיים (1ה2). תתבצע עבודת מטה על מנת לקבוע האם נדרשים תיקוני חקיקה ספציפיים על מנת לעמוד במשימה המגזרית של כל משרד (3).
ה. החלטה מפרטת מנגנונים שונים לתקצוב ואיוש יחידות ההכוונה (נספח ד')
ו. להכין תזכיר חוק שיכיל את תיקוני החקיקה הנדרשים ליישום ההחלטה (1ז)

מאחר ומדובר בחקיקה מסמיכה ראשית, אשר תחתיה ייבנו הסדרים רגולטוריים רבים ומגוונים למימוש, על ידי מספר סוכנויות, ניתן לבחון חלופות רק ברמה האסטרטגית. דהיינו, אין יכולת לפרוט את שלל דילמות המדיניות כמו אמצעי האכיפה או הפיקוח הנדרשים, לחלופות שעלו בשעת גיבושם.

1. <u>חלופה 0</u>

המשך המצב הקיים על פי החלטות ממשלה 2443. בחלופה זו עשרות הארגונים המהווים את ליבת הסיכון, לגביהם חל החוק להסדרת הביטחון בגופים ציבוריים, ימשיכו להיות מונחים כרגיל על ידי מערך הסייבר הלאומי על פי החוק להסדרת הביטחון בגופים ציבוריים. לגבי שאר המשק, משאבים נוספים יוזרמו לרשויות מאסדרות על מנת לחזקן מקצועית וביצועית, כאשר המערך יהווה מנחה מקצועי עבורם. לא יתווספו סמכויות חוקיות נוספות לאף גורם.

---

[25] החלטת ממשלה 2443 - קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר: https://www.gov.il/he/departments/policies/2015_des2443

2. מודל של רגולציה משותפת

גם במסגרת מודל זה לא יתווספו סמכויות חדשות לאף גורם. במודל זה ישאף מערך הסייבר הלאומי למסד פורומים, שולחנות עגולים וקבוצות שיח עם גורמי ממשלה ומשק רלוונטיים על מנת לקדם תהליכים משותפים. ההבדל העיקרי בין חלופה זו לחלופה 0 למעט הניסיון למסד תהליכים משותפים הוא השקעה של משאבים ציבוריים בתכניות רתימת שוק מסוגים שונים, התעדה מרצון, פרסום והעלאת מודעות וכו׳.

3. מודל מבוזר

במסגרת מודל זה השאיפה תהיה להעצים את סמכויותיהן של רשויות מאסדרות, על מנת להביא אותן לעמידה בתכלית כפי שמוגדרת בחלק א׳ סעיף 4.1. מערך הסייבר הלאומי יהיה גורם מתכלל ומתאם, אשר מנחה מקצועית את הסוכנויות המגזריות אך מתערב פחות בשיקולי הביצוע שלהן בפועל.

4. מודל ריכוזי

במסגרת מודל זה המערך יהפוך לרגולטור סייבר חדש בעל סמכויות מקיפות להנחות ארגונים בסיווג סיכון גבוה בכלל המגזרים.

5. מודל משולב

המודל לפיו בנוי פרק הרגולציה המוצע הוא מודל המשלב בין הגישות, על פי מדרג של רמת הסיכון לאינטרס הציבורי שיש בפגיעה במשפחות שונות של גופים.

כלפי ארגונים בסיווג סיכון A שאינם תשתיות קריטיות יתקיים מודל ביניים. לרה״מ תהיה הסמכות להאציל סמכויות תוספתיות לרשות מאסדרת רלוונטית במידה וקיימת ובמידה שיש צורך. המערך יקיים בקרה מוגברת אודות ביצועי הרשויות המאסדרות. במידה ולא קיימת רשות מאסדרת מגזרית רלוונטית (עקב אי יכולת או מסיבה אחרת) המערך יפעל במישרין אל מול הארגונים בעצמו, אם באופן זמני ואם באופן קבוע. ההערכה היא כי קיימים <u>כמה מאות ארגונים</u> מסוג זה.

כלפי ארגונים בסיווג סיכון B יתקיים מודל מבוזר. לא יתווספו סמכויות חדשות והרשויות המאסדרות יפעלו בהנחיה מקצועית של המערך כמתואר בהחלטה 2443.

כלפי ארגונים בסיווג סיכון C, המערך יחיל מדיניות שלא תעשה שימוש בכללים כופים אלא בארגז של אסטרטגיות התערבות רכות המכוונות לכלל המשק (העלאת מודעות, הכשרות וכיו״ב).

כמו כן ובהמשך לכך, לא ייזנחו כלל המרכיבים של מודל הרגולציה המשותפת, ויתקיימו ערוצים מגוונים לקידום תהליכים יחד עם ציבור הארגונים, כמו גם מודלים לתמרוץ ותכניות וולונטריות. עם זאת, מרכיבים אלה יהוו מנופים משניים להגשמת תכליות המדיניות.

חלק ג' – הערכת חלופות והשוואה

	חלופה 0	**מודל ריכוזי**	**מודל מבוזר**	**רגולציה משותפת**	**מודל משולב**
תועלת ישירה (העלאת רמת החוסן המשקית)	נמוך	גבוה	בינוני	נמוך	גבוה
קצב השינוי	נמוך	בינוני	בינוני-נמוך	נמוך	גבוה
תועלת עקיפה	נמוך	גבוה	בינוני	בינוני	גבוה
הימנעות מנטל ועומס רגולטורי	גבוה	נמוך	בינוני	גבוה	בינוני

*<u>תועלת עקיפה</u>:

מלבד התועלת הראשית של העלאת רמת החוסן, על נגזרותיה, דהיינו, השבחת כלל האינטרסים הציבוריים שהוזכרו מסביבה ועד כלכלה, צפוי שהתערבות ממשלתית שתחייב הגדלת הביקושים למוצרי, שירותי וכ״א סייבר תתרום לחיזוק תעשיית הסייבר הישראלית ולמובילות הישראלית הכללית בתחום הסייבר. ברור כי תועלת זו הינה תוצר לוואי אשר אינו עומד בליבת המדיניות, אולם אין להתעלם ממנה.

1. ניתוח חלופות

1.1 חלופה 0

הערכתנו כי המצב הקיים איננו מספק בשל מס' טעמים:

1.1.1. אין סיבה להאמין שהשוק יתקן את כשליו בעצמו. הכשלים הם מהותיים ולא נצפית מגמה ואף לא התחלה של מגמה לתיקון המצב ללא התערבות ממשלתית. אדרבא, הצפי של מומחי הסייבר בארץ ובעולם הוא שהפער יחריף.

1.1.2. החלטה 2443 למעשה לא מוסיפה סמכויות רגולטוריות חדשות, לא למערך ולא לאף סוכנות סטטוטורית רלוונטית אחרת, ואין למערך כל סמכות כלפי ארגונים לא ממשלתיים. מצב זה מותיר פערים מהותיים ביכולתה של הממשלה להתערב ולתקן את המצב הקיים, כך שהמצב תלוי בחסדי כוחות השוק, אשר כאמור נמצא במצב של כשל. השימוש בכלים הקיימים ימנע את ביצועם של התהליכים הנדרשים בקצב הנדרש ויאפשר להגיע לתוצאות חלקיות בלבד.

1.1.3. גם אם רשויות סטטוטוריות יחליטו לפעול עצמאית ולקבע את הסמכויות הנדרשות להן בחוק, מהלך כזה יכול שיתבצע באופן איטי מדי, ללא סנכרון, שלא בסדר העדיפויות הנכון ולא על פי השקפתה של הרשות המקצועית המובילה בממשלה לעניין זה, היא מערך הסייבר.

1.1.4. יתר על כן, חפיפות וסתירות בין גבולות הגזרה של רשויות מאסדרות קיימות יהוו בעיה, לה לא ניתן לתת פתרון מאחר ולמערך אין סמכות בוררות והכרעה בנושא.

1.1.5. אותו הדבר אמור גם לגבי שימוש בסמכויות קיימות. למערך הסייבר, תחת החלטה 2443, אין את הכלים הנדרשים על מנת להכתיב נורמות מקצועיות ואת מדיניות החוסן הלאומית, על פני אג'נדות סותרות של גורמים אחרים בממשלה. הדבר יוביל להיעדר אחידות ולהגנה לא שלמה על האינטרס הציבורי.

למרות האמור לעיל, ברור שבהיבטי נטל רגולטורי, חלופה זו היא המסוכנת פחות מאחר והיא צפויה להוסיף מינימום הכרחי של רגולציה כופה חדשה, ולכן ממזערת את הסיכון לנזק במובן זה.

1.2 מודל של רגולציה משותפת

הערכתנו היא שמודל של רגולציה משותפת הינו נדבך חשוב אך לא מספק על מנת לעמוד בתכליות המדיניות. על טהרתו, הכלים שיתווספו למערך על פני הקיים יהיו כלים רכים בלבד, אשר לא סביר שיאפשרו השגת התכלית בקצב מהיר או באיכות גבוהה יותר משמעותית. הבעיה של "סיכון מוסרי" נותנת משנה תוקף להערכה זו מכיוון שגם אם תתקיים נכונות מצד המשק לשתף פעולה עם הנחיות המערך, הדבר כרוך בעלויות גבוהות לארגונים, ויוביל להעדפת סיכון להוצאה אפשרית על פני הוצאות הגנה ודאיות. צפוי שהשקעה נוספת של משאבים ממשלתיים בתמרוץ רך של המשק תניב פעילות בנפח גבוה יותר, ולכן ניתן לחלופה זו יתרון קל לעניין התועלת העקיפה על פני חלופה 0.

1.3 מודל מבוזר

לעניין התועלת הראשית, מודל זה מקבל ציון בינוני מכמה סיבות:

1.3.1. כאמור לעיל, לא ניתן לאתר רשות מאסדרת מגזרית רלוונטית לכל ארגון במפת הארגונים בסיווג גבוה של מערך הסייבר. אזורים שלמים יוותרו ללא מענה אסדרתי ויפגמו באפקטיביות הרגולציה.

1.3.2. גם אם ניתן ליצור מודל אשר יעמיק את סמכויות כל הרשויות המאסדרות באופן גנרי, בחלק מהמקרים נדרשת הרחבה אופקית. קרי, שרשות מאסדרת תכווין ארגונים במגזרה אשר אינם בסמכותה החוקית בתחומים אחרים. הרחבה מסוג זה היא עניין של "כל מקרה לגופו" ויקשה להתמודד עם נושא זה בחוק אחד.

1.3.3. בעיית החפיפות והסתירות בין רשויות מאסדרות לא נפתרת.

1.3.4. היכולת של המערך ליצור סטנדרט מקצועי אחיד, לקבוע סדרי עדיפויות ולהתערב באזורים בהם העשייה לא מתקדמת באופן או בקצב הנכונים, מוגבלת. הדינמיקה של מודל זה מעמידה את המערך בעמדה הקרובה יותר למוקד ידע מקצועי מאשר למנחה לאומי.

מאחר ותוספת הסמכויות הרגולטוריות היא בינונית, גם התועלת העקיפה והסיכון לעומס רגולטורי הצפוי מתיישרים בהתאם.

1.4 מודל ריכוזי

מודל זה פותר את רוב הבעיות שהוזכרו מעלה, מאחר והוא מעניק למערך סמכות ריכוזית ועוצמתית אותה הוא יכול להקרין על פני כל ארגון במשק. עם זאת, למודל הבעיות הבאות:

1.4.1. העומס הרגולטורי צפוי להיות גבוה יחסית לחלופות אחרות, קיימת תוספת משמעותית של סמכויות לגבי ארגונים רבים מאוד במשק והצפי הוא לתוספת משמעותית של רגולציה בהתאמה בשנים הקרובות ולעלייה משמעותית בסיכון לנטל רגולטורי עודף.

1.4.1. מאחר והמערך צובר לעצמו את כל הסמכות והאחריות, הרשויות המאסדרות הקיימות מאבדות תמריץ להוביל תהליכים משמעותיים והמערך נדרש להוביל בכל הגזרות. עקב כ"א ומשאבים מוגבלים יידרש למערך זמן ארוך יותר לטפל בכלל הארגונים לגביהם נדרש טיפול, וקצב השינוי צפוי להיות נמוך יותר.

1.5 מודל משולב

מודל זה הוא החלופה הנבחרת בשל הטעמים הבאים:

1.5.1. סמכויות חדשות יתווספו למדינה רק כלפי הארגונים בסיווג סיכון A, על פי קריטריונים סדורים. התחזית היא שכמה מאות ארגונים יוגדרו ככאלה.

1.5.2. ברירת המחדל החוקית תהיה להאציל את הסמכות לרשות מאסדרת קיימת. מאידך, המערך שומר אצלו סל כלים עוצמתי יותר ולכן יכול להתערב ביעילות ובמהירות במקרה ורשות מאסדרת איננה ממלאת את תפקידה.

1.5.3. כלפי רוב רובו של המשק, לא יתווספו סמכויות רגולטוריות חדשות, ולכן צפוי עומס רגולטורי מינימלי. זאת ועוד, כל הרשויות המאסדרות יפעלו בהסתמך על קריטריונים אחידים לפי תורת ההגנה בסייבר, כך שיימנע הסיכון מעומס רגולטורי הנובע מכפילויות באסדרה.

1.5.4. קצב השינוי יהיה גבוה עקב אי אובדן התמריץ של רשויות מאסדרות קיימות לעבוד עם המערך.

1.5.5. לא יהיו פערים בסמכות רגולטורית של המדינה כלפי ארגונים בהגנת סייבר באזורי סיכון מהותיים, רה״מ יוכל להאציל סל סמכויות כלפי כל הארגונים ברמת סיווג A גם אם אין רשות מאסדרת רלוונטית לטיפול בהם.

2. אמצעים נוספים שהוטמעו בחוק על מנת למזער עומס רגולטורי

2.1 תהליכים מובנים להערכת השפעות רגולציה

עקב תהליכי ההיוועצות עם בעלי העניין ועם התפתחות התהליך, הוטמעו מנגנונים בחוק אשר צפויים להפחית עוד יותר את העומס הרגולטורי הצפוי. החוק עתיד לחייב את מערך הסייבר או רשויות מאסדרות רלוונטיות, לפי העניין, להפעיל את סמכותם הרגולטורית בכפוף לעקרונות הבאים (מתוך תזכיר החוק, סעיף 43):

א. התאמת האסדרה לתקינה בינלאומית או תקינה מקובלת ונוהגת במדינות מפותחות בעלות שווקים משמעותיים.
ב. באסדרה מגזרית - התאמת האסדרה למאפייני המגזר ולמאפייני פעילותם של הארגונים השונים במגזר.
ג. קיום יחס הולם בין היקף ואופן האסדרה לסוגי הארגונים וסיכוני הסייבר להם הם חשופים.
ד. קביעת אסדרה תעשה לאחר בחינת מידע זמין על העלויות הישירות הנובעות ממנה והשפעתה על פעילות עסקית, תחרות הוגנת ורווחת צרכנים; ראש הממשלה רשאי לקבוע תקנות לעניין אופן ביצוע סעיף זה.

דהיינו, ראשית, החוק יחייב את רגולציית הסייבר להתבסס על תקינה בינלאומית כברירת מחדל ובכך למזער את הצורך של ארגונים לעמוד בתקינה כפולה ולהגדיל את הסיכוי לכך שדרישות הרגולציה יעלו בקנה אחד עם מדיניות מקבילה בעולם, בעלת ניסיון מוכח של הצלחה.

שנית, החוק יחייב את הרשות המאסדרת לנהל את סיכון הסייבר אל מול מאפייני המגזר, בין היתר מופיעה התייחסות ישירה לעומס הרגולטורי (בדמות עלויות, השפעה על פעילות עסקית וכיו״ב).

2.2 תורת הגנה מבוססת ניהול סיכונים (תוה״ג)

ביוני 2017 פרסם המערך את תורת ההגנה הארגונית אשר מהווה את הבסיס המקצועי לאורו יפותחו הנחיות רגולטוריות כלפי ארגונים בסיכון גבוה שאינם תשתיות קריטיות. תורה זו פותחה על פי מודל של ניהול סיכונים, המתאים את חליפת הדרישות לפי עוצמת הסיכון ומאפייני הארגון, תוך הסתמכות על תקינה בינלאומית קיימת. תורת ההגנה מקדישה התייחסות מיוחדת לארגונים קטנים ובינוניים בעלי תשתית מחשוב בסיסית, עבורם פותח תהליך מקוצר, רך ונפרד מהערוץ התורתי המרכזי. תורת ההגנה משאירה מרחב שיקול דעת משמעותי להנהלת הארגון בבואה לאמצה.

חשוב לציין כי תורת המערך תהווה בסיס מקצועי מחייב, וככלל, הוראות רגולטוריות חדשות בתחום הגנת הסייבר יבוקרו על ידי המערך לאורה.

אימוץ מסמך זה, כבסיס לשפה אחודה של הממשל אל מול המשק, מהווה בשורה למשק בהיבטי אחידות דרישות והצגת סך הדרישות מהמשק בצורה יעילה.

עבודה בנושא החלה מול מספר משרדי ממשלה, כך שהוראות ופרסומים שלהם יותאמו ויסונכרנו אל מול תורת ההגנה הארגונית בסייבר. דוגמאות לפעילות זו, ניתן למצוא במסמך שפרסם המשרד להגנת הסביבה בתחילת שנת 2018, במסמך המגובש בימים אלו על ידי משרד הבריאות, בתהליך שמובל מול מחב״א (מרכז החישוב הבין-אוניברסיטאי) ובמסמך הכרה הדדית שנכתב אל מול הרשות להגנת הפרטיות.

השנים 2018-2019 מוגדרות כשנות ההטמעה וההרחבה של תורת ההגנה. במסגרת זו, מערך הסייבר מסייע לארגונים להפחית את הנטל הכרוך באימוץ תורה זו, על ידי בניית עזרים וכלים תומכים, מיכון המתודה לתוך מערכת מידע אשר תהווה כלי לשימוש חופשי של המשק, התאמת המתודה לתקנים מקומיים ובינלאומיים, שילובה באקדמיה וקורסים מקצועיים ועוד.

תורת ההגנה הוצגה מאז פרסומה לראשונה ביוני 2017 לאלפי אנשים במשק באמצעות כנסים ייעודיים והשתלבות בכנסים קיימים, קמפיין דיגיטלי רשתות החברתיות וברדיו, הצגה לבעלי עניין כגון חברות הייעוץ, רגולטורים, איגודים מקצועיים ועוד.

במקביל, התבצעו סקרי סיכונים רבים כפיילוט מבוקר, לצד הרצת המתודה על ידי חברות שונות במשק.

3. **הערכת העומס הרגולטורי והתועלות הצפויים מהחלופה הנבחרת**

פרק הרגולציה הינו חקיקה מסמיכה, אשר נותנת כלים בידי הרשות המאסדרת ומשאירה מרחב שיקול דעת גדול בכל הנוגע להטלת דרישות ואמצעי פיקוח ואכיפה בפועל. עובדה זו מקשה מאוד על הערכה כמותית מדויקת של הסיכון לנטל רגולטורי על שלל מרכיביו.

בשורה התחתונה החוק עוסק בסמכויות ולא בדרישות עצמן, כך שקשה לבצע תרגום מהימן לעומס רגולטורי.

העומס הרגולטורי העיקרי ינבע מדרישות להצטיידות במערכות אבטחה חדשות, בצורך לשנות תהליכים ארגוניים, לבצע שינויים בתשתיות מחשוב של ארגונים, רכישת שירותי ייעוץ והגנה, העסקת כ״א מיומן וכיו״ב. הנטל האדמיניסטרטיבי הכרוך בעבודה מול הרשות המאסדרת צפוי לכלול מענה לדרישות

מידע של הרשות המאסדרת, השתתפות בהליכי פיקוח וביקורת ובמקרים מסוימים גם הגשה של אישורים רלוונטיים. עם זאת, החלק הזה צפוי להיות שולי יחסית בשקלול הכולל של העומס הרגולטורי.

בהתאם להחלטת ממשלה 2118, נקבע כי בעת הפעלת סמכות לפי חוק הסייבר, ובכלל זה קביעת תקנות, הוראות וצווים ובמילוי תפקידי מערך הסייבר הלאומי או רשות מאסדרת אחרת, יישקלו שיקולים שמטרתם לבדוק את מידתיות האסדרה. עקרונות אלה כוללים התאמה לאסדרה במדינות מפותחות, ובחינת ההשפעה על הפעילות העסקית והכלכלית במשק, על מנת להבטיח שתועלתה הציבורית תהיה גבוהה מעלותה.
על מנת לאפשר ודאות גבוהה יותר במימוש עקרונות אלה במסגרת שיקול הדעת המנהלי נקבע כי ראש הממשלה רשאי לקבוע תקנות לעניין אופן בחינת הסמכויות הרגולטוריות כאמור.

3.1. הערכת העומס הרגולטורי הנובע מפרק הרגולציה הישראלי

המתודולוגיה שבחרנו להשתמש בה לביצוע ההערכה מבוססת על תפוקות ולא על תשומות, כלומר, על מרכיבי העלות השונים אשר ינבעו מדרישות הגנת הסייבר החדשות שהחוק צפוי לאפשר לרגולטורים להחיל. ההערכה בוצעה באופן הבא:

3.1.1. נבחרה אוכלוסיית הארגונים הנכללת במגזרים המובילים, שאנו צופים שיכולו לגביהם הנחיות רגולטוריות בהתאם לתפיסת האסדרה (פירוט המגזרים חסוי מטעמי סיווג).
3.1.2. הללו פולחו לפי השייכות המגזרית ולפי גודלם על פי היקף מועסקים (קטן, בינוני או גדול).
3.1.3. התבצעה הערכת עלות ממוצעת שתידרש מארגון בכדי לעמוד בדרישות המחמירות ביותר של התוה"ג, בהתאם לגודלו.
3.1.4. לכל מגזר ניתן ציון ייחוס לרמת בשלותו הנוכחית להגנת סייבר ורמת ההגנה שתידרש ממנו בהתאם לרמת האיום שנשקפת לו וחומרת תרחישי הנזק.
3.1.5. הערכת העלות כוללת עלויות הצטיידות, כוח אדם והטמעת מערכות ותהליכי עבודה, כמו גם רפורמות ארגוניות.

בשורה התחתונה, ההערכה היא שהעלות התוספתית למשק, הנובעת מפרק זה היא כ-1.7 מיליארד ש"ח ל-5 השנים מיום תחולת החוק. (פירוט שיטת החישוב מכיל נתונים כמותיים של פוטנציאל נזק וארגונים, ולכן הינו מסווג).

מדובר בהערכה, אשר יש לשים עליה את הסייגים הבאים:

3.1.6. התחזית מתבססת על מספר הארגונים שאנו צופים שיכללו באסדרות הרגולטיביות בהתאם לתפיסת ההפעלה הנוכחית של המערך, ובהתאם לגרסה הנוכחית (1.0) של תורת ההגנה בסייבר לארגון.

3.1.7. התחזית היא ל-5 השנים הראשונות בלבד, תחת ההנחה שהחוק איננו פועל בסביבה סטרילית וידרוש תהליכי תכנון והתארגנות של המאסדרים והמוסדרים שעשויים להאט את קצב המימוש. קצב השינויים בעולם הסייבר גדול מכדי שניתן יהיה להעריך מעבר לכך.

3.1.8. יש לזכור כי הערכה זו טומנת בחובה עלויות, אשר את חלקן ארגונים היו בוחרים להשית על עצמם כחלק מהמשך העלייה ברמת האיום והמודעות המשקית אליו. כמו כן, חלק מהעלויות ינבעו מדרישות של רגולטורים קיימים, תחת סמכויותיהם הקיימות, גם ללא חוק זה, ובכלל זה, רגולציה עולמית מתפתחת המשפיעה על המשק הישראלי בדגש על ה-GDPR האירופאי.

3.1.9. הערכה מתייחסת בעיקר למישור ה-IT, המערך אינה צופה כי עולמות ה-OT וה-IoT יהיו במוקד פעילותה בשנים הראשונות לגבי אוכלוסיות היעד המדוברות בהקשר של פרק הרגולציה, אולם בהחלט ייתכן שבעתיד הדבר ישתנה.

3.1.10. הערכה עושה שימוש בממוצעים גסים בתחום אשר מתקיימת בו שונות גבוהה בין ארגונים בהתאם למאפיינים הייחודיים של כל ארגון. הרגישות של משתני החישוב גבוהה מאוד וכוללת מרכיב משמעותי מאוד של אי ודאות.

3.2. השוואה בינלאומית

בהסתמך על הניסיון העולמי, הערכת השפעות הרגולציה[26] שביצעה הנציבות האירופית לפני החלתה של דירקטיבת NIS קובעת כי בממוצע ארגונים שיושפעו מהדירקטיבה יגדילו את השקעתם בהגנת סייבר מעבר להשקעה במצב ללא רגולציה על פי החלוקה הבאה:

*הסכומים באלפי יורו.

	ממוצע לחברה	סה"כ למגזר
פיננסים	21-43	170-340
תחבורה	8-16	118-236
בריאות	4.5-9	67-143

בבריטניה בוצע הליך הערכת השפעות מקביל[27] שמסקנותיו המקבילות לפי סוג ארגון.

[26] European Commission: Commission Staff Working Document, Summary Of The Impact Assessment: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0167&from=EN

[27] Network and Information Security Directive, Impact Assessment (IA): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf

*הסכומים באלפי לישי"ט.

	ארגון קטן	ארגון גדול
אנרגיה	40-90	780-1560
פיננסים	41-83	720-1440
תחבורה	3-8	130-250
בריאות	1.5-3	23-47

יש לציין שהמתודולוגיה העומדת בבסיס ההערכות הנ"ל בעלת מגבלה משמעותית, שכן היא מתבססת על מדידת תשומות בלבד, ברמת המאקרו, תוך הסתמכות על מדדי יחוס אשר המתודה העומדת בבסיסם לא ברורה דיה. דהיינו, הערכת ההשקעה המגזרית כיום בהגנת סייבר והשוואת ההשקעה לארגונים הנחשבים "מובילים" בחוסנם בסייבר על פי מדדים בלתי תלויים. השוואה זו נותנת מענה חלקי ביותר. כמו כן, דירקטיבת NIS איננה זהה לתורת ההגנה הישראלית, הסביבה החוקית הנוכחית בין מדינות האיחוד לישראל ודאי שאינה זהה וגם משרעת האיומים שונה. על כן, קשה להסיק מסקנות חדות בנוגע להשוואות מסוג זה.

אין כמובן הסכמה על המתודולוגיה להערכת הנזק הכספי השגרתי לארגונים מאיומי סייבר ומובן שכל הערכה בסוגיה זו מסובכת אף יותר מהערכת עלות הרגולציה עצמה. הארגון האירופי ENISA במחקרו מאוגוסט 2016 ערך "רשימת מצאי" של מחקרים בתחום זה. אם נשתמש באומדן הנמוך ביותר המצוי במחקרים אליו מפנה הדו"ח, המניח כי הנזק הממוצע לארגון בסייבר הוא 425 אלף יורו בשנה, ונחיל על נתון זה אחוז השינוי ברמת ההגנה העולה מהמתודולוגיה שלנו ואף ננכה את הארגונים הקטנים מהחישוב, נגיע לחיסכון תיאורטי של 100-450 מליון ש"ח לארגונים עצמם, כלומר לפני ששקללנו את התועלת לאינטרסים הציבוריים המנויים בחלק הראשון של מסמך זה.

3.2. הערכת התועלות

את הערכת העלות יש להעמיד מול שלושה סוגים של תועלות:

3.2.1. מניעת נזק לאינטרסים ציבוריים נוספים

לא ניתן להעריך כמותית באופן מושכל סעיף זה. אולם בהמשך לסעיף 2 בחלק א׳, ברור כי אם ימנע אירוע מרכזי אחד של הפרעה לרציפות התפקודית המשקית, אם בתחבורה, בפיננסים, בבריאות או באנרגיה, הרי שהתועלת למשק תכסה את העלות המוערכת, וודאי אם הדבר יתרחש בשעת משבר או מצב חירום מדינתי. כמו כן, יש לזכור את התועלות הצפויות ממניעת נזקים לפרטיות, לבריאות הציבור, לסביבה, לתודעה, לצמיחה וכו׳.

3.2.2. שוק הסייבר

בישראל קיים שוק סייבר מפותח למדי, בכלל זה מוצרי הגנת סייבר, שירותים ואנשי מקצוע. עקב כך צפוי כי חלק ניכר מהעלויות יתועל חזרה למשק הישראלי ויסייע לחיזוק תעשייה זו, בפרט עלויות כ״א ואינטגרציה אשר מהוות חלק ארי מהעלויות.

3.2.3. הגדלת אמון במרחב הדיגיטאלי

הגדלת האמון במרחב הדיגיטאלי יכולה לשמש זרז בפני עצמה לצמיחה משקית. מדובר בחישוב מורכב ברמה הכלכלית ולכן לא נציע נתון כמותי, אולם רכיב תועלת זה הינו משמעותי למדי.

חלק ד׳ – שיח עם בעלי עניין

א. במהלך שנת 2014 בעת ניסוח החלטת ממשלה 2443 נפגשו אנשי המערך עם כלל משרדי הממשלה על מנת להבין את תפקידם כרגולטורים ולהתייעץ עמם לגבי מדיניות פרק הרגולציה. התייעצות מקיפה ומעמיקה יותר בוצעה עם משרדים שזוהו כרלוונטיים יותר לרגולציית הגנת הסייבר.

ב. במקביל לאותו תהליך נפגשו אנשי המערך עם ארגונים במשק מכל משפחות הארגונים בקבוצת הייחוס של המטה (A,B,C). לרוב, נערכו הפגישות עם אנשי המקצוע בתחום הסייבר והחירום ולעיתים עם מנהלים בעמדות שונות בארגון.

ג. כחלק מהתהליך, נפגשו אנשי המערך גם עם מומחים בתחום הסייבר, מחברות ייעוץ, חברות למוצרי ושירותי סייבר, חברות לשירותי IT ואנשי מערכת הביטחון.

ד. בסך הכל השתתפו בהליך ההיוועצות לא פחות מ-10 משרדי ממשלה ורשויות סטטוטוריות, 8 חברות ייעוץ, כ-20 חברות פרטיות במשק וגופי ההתעדה המובילים בישראל.

ה. לאחר החלטת הממשלה 2443, בוצע תהליך בדיקה נוסף אל מול משרדי הממשלה, בכדי לקבוע את גודל יחידת האכוונה הנדרשת בכל משרד. גם סבב זה כלל סיורים בארגוני הקצה של המשרדים.

ו. החל מסוף שנת 2015 מפתח מערך הסייבר את תורת ההגנה בסייבר לארגון, המהווה בסיס להנחייתו המקצועית של המערך כלפי ארגונים וכלפי רגולטורים.

ז. כחלק מפיתוח התוה״ג, התקיים שיח ממושך עם קבוצות עניין שונות, בכלל זה חברות ייעוץ, תעשיית הסייבר הרחבה ומנהלי אבטחת מידע והגנת סייבר ארגוניים במגזר הפרטי והממשלתי. שיח זה כלל הפצת טיוטות להתייחסות למגוון ארגונים בתעשיית הסייבר, המגזר הציבורי והתעשייה.

ח. בסוף שנת 2016 טיוטת החוק נמסרה לרגולטורים המובילים והתקיים עמם סבב היוועצות נוסף.

ט. תהליך ההיוועצות הינו תהליך רציף ומתמשך אשר מהווה חלק מיישום המדיניות בפועל ואין לו תאריך סיום של ממש. ב-27.5.2018 התקיימה פגישת היוועצות מרכזית עם התאחדות התעשיינים כגוף היציג של ארגונים רבים האמורים להיכלל במתווה הרגולציה.