טיוטת הצעת חוק מטעם הממשלה:

הצעת חוק סמכויות לשם חיזוק הגנת הסייבר (הוראת שעה), התשפ"א-2021

1. מטרתו של חוק זה לקבוע סמכויות לצורך הגנה על תפקודו התקין והבטוח של מרחב הסייבר ובכלל זה לשם התמודדות עם תקיפות סייבר שיש בהן כדי ליצור סיכון לפגיעה באינטרס ציבורי חיוני.

הגדרות

2. בחוק זה -

"אינטרס ציבורי חיוני" – כל אחד מאלה:

(1) שלום הציבור;

(2) חיי אדם;

(3) כלכלת המדינה;

(4) הגנה על הסביבה;

(5) בריאות הציבור או בטיחותו;

(6) הגנה מפני אירוע אבטחה חמור במאגר שחלה עליו רמת האבטחה הגבוהה; לעניין זה, "אירוע אבטחה חמור" ו-"מאגרים שחלה עליהם רמת האבטחה הגבוהה" – כהגדרתם בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017[1];

(7) תפקודם התקין של תשתיות, מערכות או שירותים חיוניים;

"ארגון" – מוסד כהגדרתו בסעיף 35 לפקודת הראיות;

"ארגון שמקיים פעילות חיונית" – ארגון שתקיפת סייבר נגדו תגרום לפגיעה בדירוג גבוה במדרג שנקבע בתקנות לפי סעיף 13, או בהתאם למדרג זמני לפי סעיף 14, ומתקיים לגביו אחד מאלה:

(1) הוא מקיים פעילות בעלת מאפיינים ציבוריים הנוגעת לכלל הציבור או לחלק משמעותי ממנו, אשר נדרשת לצורך קיום אספקה של מצרך חיוני או שירות חיוני לציבור, בשגרה או בחירום, או לצורך מניעת פגיעה חמורה בענף החשוב למשק המדינה;

[1] ק"ת התשע"ז, עמ' 1022.

(2) הוא מספק שירותים בתחום מערכות המחשב או בתחום התקשורת הנדרשים לצורך המשך פעילותו התקינה של ארגון שמתקיים לגביו האמור בפסקה (1) ושבאמצעות תקיפת סייבר נגדו ניתן לפגוע בפעילותו החיונית של הארגון;

"בית משפט" – בית משפט לעניינים מינהליים כמשמעותו בחוק בתי משפט לענינים מינהליים, התש"ס-2000[2];

"גוף ביטחוני" – אחד מאלה:

(1) צבא הגנה לישראל;

(2) שירות הביטחון הכללי;

(3) משטרת ישראל;

(4) המוסד למודיעין ולתפקידים מיוחדים;

(5) משרד הביטחון ובכלל זה הממונה על הביטחון במערכת הביטחון;

"גורם אחראי" – כמשמעותו בסעיף 7;

"הגנת סייבר" – הגנה על מחשב, על חומר מחשב השמור בו או על תקשורת הנתונים אליו וממנו מפני תקיפת סייבר, ובכלל זה פעולות ל היערכות לה איתורה, מניעתה או טיפול בה וצמצום הנזקים הנגרמים ממנה, במהלכה או לאחריה;

"חומר מחשב", "מחשב", "שפה קריאת מחשב" ו-"תוכנה" – כהגדרתם בחוק המחשבים, התשנ"ה-1995[3];

"חוק להסדרת הביטחון" – חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998[4];

"מאסדר" - הגורם המנוי בטור א' לתוספת, המוסמך להסדיר פעילות בתחום מתחומי המשק המנוי בטור ב' שלצדו, לפי כל דין כמפורט בטור ג' שלצדו.

"מידע בעל ערך הגנתי" – מידע טכני שיש בו כדי לסייע להגנת הסייבר, ובכלל זה מידע כמפורט להלן:

---

[3] ס"ח התשנ"ה, עמ' 366.
[4] ס"ח התשנ"ח, עמ' 348.

(1) מידע על שיטות לביצוע תקיפת סייבר;

(2) מידע על חולשות ודרכי הטיפול בהן;

(3) מאפיינים טכנולוגיים של תקיפת סייבר, ובכלל זה כתובת המחשב שהותקף או שממנו בוצעה התקיפה;

(4) נתונים בשפה קריאת מחשב המעידים על תבנית תקיפת סייבר;

"המערך" או "מערך הסייבר הלאומי" – מערך הסייבר הלאומי כהגדרתו בחוק להסדרת הביטחון;

"עובד מוסמך" – כמשמעותו בסעיף 8;

"עובד השירות" – עובד בכיר בשירות הביטחון הכללי שמינה ראש שירות הביטחון הכללי לעניין סעיפים 5 ו-6;

"פגיעות" – נקודת תורפה במחשב או בחומר מחשב אשר אפשר לנצל לביצוע תקיפת סייבר נגד מחשב או חומר מחשב;

"פעולה להגנת סייבר" – פעולה הנעשית לשם הגנת סייבר, שהיא אחת מאלה:

(1) מתן הוראות למחשב בשפה קריאת מחשב;

(2) בחינה של חומר מחשב או תקשורת נתונים ובכלל זה סריקה ממוכנת שלהם לצורך איתור מידע בעל ערך הגנתי;

(3) העתקה של חומר מחשב או תקשורת נתונים לצורך ביצוע הפעולה המנויה בפסקה (2);

(4) דיווח על איתור מידע בעל ערך הגנתי למערך הסייבר הלאומי;

(5) התקנת מחשב או התקנת תוכנה במחשב לשם ביצוע פעולה מהפעולות המנויות בפסקאות (1) עד (4);

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

"תבנית תקיפת סייבר" – סדרת פעולות המבוצעת במחשב או בחומר מחשב במסגרת תקיפת סייבר או הכנות לתקיפה כאמור;

"תקיפת סייבר" – פעולה המבוצעת בחומר מחשב שנועדה לפגוע במחשב, בחומר מחשב המאוחסן בו או בתקשורת הנתונים מהמחשב או אליו או גישה לחומר מחשב או לתקשורת נתונים בלא הרשאה;

[5] דיני מדינת ישראל, נוסח חדש 18, עמ' 421.

"תקיפת סייבר חמורה" – תקיפת סייבר שמתקיים לגביה אחד מאלה:

(1) קיימת הסתברות גבוהה שהיא תגרום לפגיעה ממשית באינטרס ציבורי חיוני; לעניין זה יראו פגיעה ממשית באינטרס ציבורי חיוני כפגיעה בדירוג גבוה בהתאם למדרג לפי סעיף 13 או 14;

(2) יש יסוד סביר להניח שהיא תגרום לפגיעה ממשית באינטרס ציבורי חיוני לנוכח חומרת הסכנה להתפשטותה למחשבים אחרים ולפגיעה בהם או במידע השמור בהם באופן היוצר נזק מצרפי בענף משקי או במשק כולו; לעניין זה יראו פגיעה ממשית באינטרס ציבורי חיוני כפגיעה בדירוג גבוה בהתאם למדרג לפי סעיף 13 או 14;

(3) היא אותרה בארגון שמקיים פעילות חיונית או שיש יסוד סביר להניח שהיא מכוונת כלפי ארגון כאמור;

(4) יש יסוד סביר להניח שהיא נועדה לפגוע בביטחון הלאומי;

"תקשורת נתונים" – מעבר של חומר מחשב ממחשב אחד למחשב אחר באמצעות התקשרות או התחברות של מחשב עם מחשב אחר.

צו לביצוע פעולות להגנת סייבר

3. (א) בית המשפט רשאי, בצו, לבקשת גורם אחראי (להלן – צו), להתיר לעובד מוסמך לבצע, במחשב או בחומר מחשב של ארגון, פעולות להגנת סייבר שפורטו בבקשה (בסעיף זה – הפעולות המבוקשות), ורשאי הוא ליתן לארגון כל הוראה אחרת בנוגע לביצוען של פעולות כאמור.

(ב) בית המשפט ייתן צו כאמור בסעיף קטן (א) אם שוכנע, לאחר ששקל את השיקולים האמורים בסעיף קטן (ד), כי הפעולות המבוקשות נדרשות לצורך מניעת פגיעה באינטרס ציבורי חיוני בשל תקיפת סייבר חמורה, או התמודדות עם פגיעות קריטית, וכי גורם אחראי הציג בפני נציג מוסמך של הארגון את הטעם המקצועי לביצוע הפעולות ואופן ביצוען, ונתן לו הזדמנות להתמודד עם תקיפת הסייבר החמורה, או עם הפגיעות הקריטית, לפי העניין, זמן סביר בנסיבות הענין לפני הגשת הבקשה לבית המשפט.

(ג) לא יפנה גורם אחראי לארגון או לבית המשפט לפי סעיף זה אם הוא ארגון המצוי בפיקוח מאסדר המנוי בטור א' לתוספת הראשונה, המוסמך להסדיר פעילות בתחום מתחומי המשק המנוי בטור ב' לתוספת הראשונה לפי כל דין המנוי בטור ג' לתוספת הראשונה, אלא לאחר הסכמה עם המאסדר או השר לפי העניין, בדרך שתתואם בין הצדדים ובלבד שעמדת המאסדר תימסר תוך זמן סביר בנסיבות העניין;

(ד) בבואו לתת צו כאמור בסעיף קטן (א), ישקול בית המשפט, בין השאר, את אלה:

(1) מאפייני הארגון השפעת הפעולות המבוקשות על פעילותו של הארגון;

(2) התאמת הפעולה המבוקשת לצרכי הגנת הסייבר במידה שאינה עולה על הנדרש;

(3) האפשרות שהפעולה המבוקשת תבוצע בידי אדם בעל ידע ומומחיות מטעם הארגון;

(4) עמדת המאסדר הנוגע בדבר אם תחום הפעילות של הארגון מופיע בתוספת, ככל שהוצגה לגורם האחראי;

(5) מידת הסיכון לאינטרס ציבורי חיוני כתוצאה מתקיפת סייבר נגד הארגון;

(ה) בית המשפט רשאי, בצו כאמור בסעיף קטן (א), להתיר לעובד מוסמך להיכנס למקום, אם שוכנע כי הדבר נדרש לצורך ביצוע פעולה מהפעולות המבוקשות.

(ו) צו לפי סעיף זה יעמוד בתוקפו למשך התקופה שתיקבע בו ושלא תעלה על 90 ימים; בית המשפט רשאי, לבקשת גורם אחראי, להאריך את תוקף הצו בתקופות נוספות שלא יעלו על 90 ימים כל אחת.

(ז) שר המשפטים רשאי לקבוע בתקנות סדרי דין לעניין הליכים לפי סעיף זה.

(ח) בסעיף זה -

"בית משפט" – בית משפט לעניינים מינהליים כמשמעותו בחוק בתי משפט לעניינים מינהליים, התש"ס-2000[6];

"פגיעות קריטית" – פגיעות במחשב או בחומר מחשב של הארגון, שיש לגורם אחראי יסוד סביר להניח שנוצר בשלה סיכון לתקיפת סייבר חמורה או לתקיפת סייבר בהיקף נרחב שאינה תקיפת סייבר חמורה, ושהארגון אינו נוקט בפעולות הנדרשות לטיפול בה; בקביעת הסיכון כאמור יובאו בחשבון אחד או יותר מאלה:

(1) המאפיינים הטכנולוגיים של הפגיעות;

---

[6] ס"ח התש"ס, עמ' 190.

(2) קיומם של שיטות או אמצעים המאפשרים לנצל את הפגיעות לביצוע תקיפת סייבר;

(3) שכיחותה של הפגיעות;

הגנה על פרטיות וסודות מסחריים

4. (א) בביצוע פעולות לפי חוק זה לא יאסוף המערך מידע כהגדרתו בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981[7] (להלן – חוק הגנת הפרטיות), או ידיעה על ענייניו הפרטיים של אדם כמשמעותה בחוק האמור אף שאינה בגדר מידע כאמור וכן סוד מסחרי (בסעיף זה – מידע מוגן) אלא אם כן המידע האמור הוא מידע בעל ערך הגנתי כמפורט בפסקאות (3) ו-(4) להגדרה "מידע בעל ערך הגנתי" שבסעיף 1 או שמתקיים אחד מאלה:

(1) איסוף המידע מותר לפי דין;

(2) בית המשפט אישר את איסוף המידע מנימוקים מיוחדים שיירשמו; לעניין מידע מוגן בית המשפט ייתן אישור כאמור אם שוכנע, לאחר ששקל את מידת הפגיעה הנובעת מכך בפרטיותו של אדם וכי איסוף המידע נדרש לצורך הגנה על אינטרס ציבורי חיוני.

(ב) לא יעשה אדם שימוש במידע מוגן שהתקבל או שנאסף לפי חוק זה אלא לצורך הגנת סייבר, או אם אישר זאת בית המשפט מהנימוקים ובהתאם לשיקולים כאמור בסעיף קטן (א)(2), בשינויים המחויבים.

(ג) לא יעביר אדם מידע מוגן שהתקבל או שנאסף לפי חוק זה אלא לגוף ציבורי כאמור בפסקה (1) להגדרה "גוף ציבורי" שבסעיף 23 לחוק הגנת הפרטיות, ולצורך הגנת סייבר; ואולם, המערך רשאי להעביר מידע מוגן גם לארגון שאינו גוף ציבורי כאמור, אם המידע האמור הוא מידע בעל ערך הגנתי כמפורט בפסקאות (3) ו-(4) להגדרה "מידע בעל ערך הגנתי" שבסעיף 1, והעברת המידע לארגון כאמור נדרשת לצורך הגנת סייבר, ובמידה שנדרשת.

(ד) מידע מוגן שהתקבל או שנאסף לפי חוק זה יימחק עם תום הצורך בו.

(ה) אין בהוראות סעיף זה כדי למנוע העברה, במקרה מסוים, של מידע שהתקבל או שנאסף לפי חוק זה לגוף ביטחוני בכפוף לכל דין.

[7] ס"ח התשמ"א, עמ' 128.

קבלת מידע מספק גישה לאינטרנט או מעובד השירות

5. (א) נודע לגורם אחראי כי קיימת פגיעות קריטית במחשב או בחומר מחשב של מנוי של ספק גישה לאינטרנט כהגדרתו בסעיף 4ט(א) לחוק התקשורת (בזק ושידורים), התשמ"ב-1982[8] (בסעיף זה – ספק גישה לאינטרנט), או שמתרחשת או עומדת להתרחש תקיפת סייבר נגד מנוי כאמור, רשאי הוא לדרוש מספק הגישה לאינטרנט או מעובד השירות מידע על אודות שמו, פרטי זהותו, מענו, מספר הטלפון וכתובת הדואר האלקטרוני שלו, המצויים ברשות הספק.

(ב) ספק גישה לאינטרנט או עובד השירות שקיבל דרישה למידע כאמור בסעיף קטן (א) לגבי מנוי שהוא ארגון, יעביר את המידע לגורם האחראי בהקדם האפשרי ולא יאוחר מ-72 שעות מקבלת הדרישה.

(ג) מידע שהועבר לגורם אחראי לפי סעיף זה ישמש לצורך יצירת קשר עם המנוי והפעלת סמכות לפי חוק זה, בלבד.

(ד) על אף האמור בסעיף קטן (א), גורם אחראי לא יפנה לספק גישה לאינטרנט בדרישה למידע כאמור באותו סעיף קטן, אלא לאחר שראש הממשלה או מי שהוא הסמיך לעניין זה התיר זאת בכתב, באופן כללי או לעניין מסוים, ואם ההיתר ניתן בתנאים – בהתאם לתנאי ההיתר; פנה גורם אחראי לראש הממשלה או למי שהוא הסמיך כאמור בבקשה לקבלת היתר כאמור בסעיף קטן זה, ידווח על כך לראש שירות הביטחון הכללי.

(ה) אין בהוראות סעיף קטן (ד) כדי לגרוע מחובתו של ספק גישה לאינטרנט להעביר, לפי הוראות סעיף קטן (ב), מידע כאמור בסעיף קטן (א), לגורם אחראי שדרש ממנו את המידע כאמור באותו סעיף קטן.

סמכויות עובד השירות

6. (א) הסמכויות הנתונות לגורם אחראי לפי סעיף 3 יהיו נתונות גם לעובד השירות, אם הפעלתן נדרשת לשם מילוי תפקידי השירות הקבועים בסעיף 7(ב)(1) לחוק שירות הביטחון הכללי, התשס"ב-2002 (להלן – חוק שירות הביטחון הכללי).

(ב) עובד השירות לא יפעיל סמכות כאמור בסעיף קטן (א) אלא אם כן התיר זאת ראש השירות, לאחר ששוכנע כי הפעלת הסמכות נדרשת לצורך איתורה של תקיפת סייבר חמורה נגד ארגון, היערכות לה, מניעתה או טיפול בה.

(ג) ראש השירות ידווח לראש הממשלה או למי שהוא הסמיך לעניין זה על היתרים שניתנו לפי סעיף קטן (ב); העתק מהדיווח יימסר לראש המערך.

מינוי גורם אחראי

7. ראש המערך ימנה עובד בכיר מעובדי המערך לגורם אחראי שיהיו נתונות לו הסמכויות לפי סעיפים 3 ו-5 (בחוק זה – גורם אחראי).

---

[8] ס"ח התשמ"ב, עמ' 218.

מינוי עובד מוסמך

8. (א) ראש המערך ימנה עובד מעובדי המערך לעובד מוסמך שיהיו נתונות לו הסמכויות לפי סעיף 3 (בחוק זה – עובד מוסמך).

(ב) לעובד מוסמך ימונה רק מי שמתקיימים לגביו כל אלה:

(1) הוא לא הורשע בעבירה שמפאת מהותה, חומרתה או נסיבותיה אין הוא ראוי, לדעת ראש המערך, להיות עובד מוסמך;

(2) הוא קיבל הכשרה מתאימה בתחום הסמכויות שיהיו נתונות לו לפי חוק זה, כפי שהורה ראש המערך;

(3) הוא עומד בתנאי כשירות נוספים כפי שקבע ראש הממשלה.

(ג) עובד מוסמך לא יעשה שימוש בסמכויות הנתונות לו לפי חוק זה אלא בעת מילוי תפקידו ובהתקיים שני אלה:

(1) הוא נושא באופן גלוי תג המזהה אותו ואת תפקידו;

(2) יש בידו תעודה החתומה בידי ראש המערך, המעידה על תפקידו ועל סמכויותיו של עובד מוסמך, שאותה יציג על פי דרישה.

שמירת דינים

9. (א) אין בהוראות חוק זה כדי לגרוע מסמכות הנתונה למערך הסייבר הלאומי לפי כל דין אחר ומסמכותו לבצע כל תפקיד שהטילה עליו הממשלה, ובכלל זה בתחום הגנת הסייבר.

(ב) אין בהוראות חוק זה כדי לפגוע בייעוד שירות הביטחון הכללי כאמור בסעיף 7 לחוק שירות הביטחון הכללי, או בתפקידים או בסמכויות הנתונים לגופים הביטחוניים לפי דין, ובכלל זה בתחום הגנת הסייבר.

הסדרים חוזיים בתחום הגנת הסייבר

10. אין בהוראות חוק זה כדי למנוע הסדרה של פעולות שעניינן הגנת סייבר באמצעות הסכם, ובכלל זה במסגרת הסכם בין גוף ביטחוני לבין ספק שלו.

סייג להפעלת סמכות

11. (א) סמכויות המערך לפי חוק זה לא יופעלו כלפי כל אלה:

(1) גוף ביטחוני;

(2) גוף המנוי בתוספת הרביעית או החמישית לחוק להסדרת הביטחון;

(3) גוף הנמנה על מפעלי מערכת הביטחון כמשמעותם בסעיף 20 לחוק להסדרת הביטחון;

(4) משרדי הממשלה, הכנסת, מערכת בתי המשפט, משרד מבקר המדינה, לשכת נשיא המדינה וועדת הבחירות המרכזית לכנסת.

(5) ארגון שהוא ספק של גוף ביטחוני, שאינו מנוי בפסקה (3), ושמתקיימים לגביו כל אלה:

(א) הוא התקשר עם הגוף הביטחוני בהסכם כאמור בסעיף 10;

(ב) פגיעה בו באמצעות תקיפת סייבר עלולה לפגוע בביטחון המדינה;

(ג) אגף הממונה על הביטחון במערכת הביטחון ומערך הסייבר הלאומי הסכימו על כך שמתן הנחיות מקצועיות לעניין הגנת סייבר לאותו ארגון או ביצוע פעולות להגנת הסייבר כלפיו ייעשו על פי הסכם כאמור בסעיף 10; התעוררה מחלוקת לעניין פסקת משנה זו, יכריע בדבר ראש המטה לביטחון לאומי.

ביצוע, תקנות ושינוי התוספת

12. (א) ראש הממשלה ממונה על ביצוע הוראות חוק זה והוא רשאי להתקין תקנות לביצועו.

(ב) ראש הממשלה רשאי, בצו, לאחר התייעצות עם השר הממונה על תחום הפעילות הנוגע לעניין, לשנות את התוספת, ובכלל זה להוסיף כל תחום מתחומי המשק, שהפעילות בו מוסדרת לפי דין, ושתקיפת סייבר נגד ארגון הפועל בו עלולה לפגוע באינטרס חיוני.

מדרג

13. (א) ראש הממשלה יקבע בתקנות מדרג לפגיעה באינטרס ציבורי חיוני, שלפיו ידורגו הארגונים במשק בהתאם לחומרת הפגיעה האפשרית באינטרס ציבורי חיוני כתוצאה מתקיפת סייבר נגדם, ולחשיפתם לתקיפה כאמור, לאחר ששקל את עמדת המאסדר הנוגע לעניין, ובשים לב לאלה:

(1) רמת השירות ומאפייני השירות הנדרשים מארגון או מסוגי ארגונים בשגרה ובחירום;

(2) שיעור המשתמשים, באופן ישיר או עקיף, בשירותי הארגון מקרב הציבור;

(3) השפעה של תקיפת סייבר בארגון על גורמי ייצור, משאבים, שירותים, תהליכים, שירותי מיחשוב, תקשורת ומוצרים החיונים לקיום האוכלוסיה, לכלכלת המדינה ולפעילות הגורמים המיוחדים בשגרה ובחירום;

(4) היקף המידע המצוי בידי הארגון, טיבו ורגישותו;

מדרג זמני 14. עד להתקנת תקנות כאמור בסעיף 13 יפעל המערך בהתאם למדרג שיקבע ראש המערך על פי התבחינים האמורים בסעיף 13.

תוקף 15. חוק זה יעמוד בתוקפו שנתיים מיום פרסומו.

תוספת

טור א' – מאסדר	טור ב' - תחום פעילות משק	טור ג' – הדין
שר התחבורה והבטיחות בדרכים	תחבורה	פקודת התעבורה והתקנות מכוחו תקנות התעבורה חוק רשות הספנות והנמלים, התשס"ד-2004 חוק הספנות (ימאים), התשל"ג – 1973 והתקנות מכוחו חוק ספנות חופית(היתר לכלי שיט זר), התשס"ו – 2005 והתקנות מכוחו חוק הטייס, התשע"א-2011 והתקנות מכוחו חוק שירותי הובלה תשנ"ז-1997 והתקנות מכוחו חוק רישוי שירותים ומקצועות בענף הרכב, התשע"ו – 2016 והתקנות מכוחו

דברי הסבר

כללי

טיוטת החוק נועדה להקנות למערך הסייבר הלאומי סמכויות לפנות לבית המשפט במקרה של סיכון משמעותי להגנת הסייבר. כיום פועל מערך הסייבר הלאומי מכוח החוק להסדרת הביטחון בגופים ציבורים, התשנ"ח-1998, כלפי הגופי המנויים בתוספת החמישית לחוק בלבד, ואילו מול יתר הגופים במשק פועל המערך בהתאם להחלטות הממשלה בתחום הסייבר, בהסכמה בלבד. זאת, בהתאם להחלטות הממשלה והדין הכללי בהתאם למסגרת משפטית שתואמה עם היועץ המשפטי לממשלה ב"עקרונות ה-CERT הלאומי".[9] מסגרת משפטית זו, של פעולה בהסכמה, מהווה ברירת המחדל של פעולת מערך הסייבר הלאומי מול המשק. בנוסף, בהתאם למדיניות הממשלה בהחלטותיה, מערך

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

הסייבר הלאומי אינו מחליף את המאסדרים במגזרי המשק השונים, כי אם מהווה גוף שתפקידו לנהל את מאמצעי ההגנה המבצעיים במרחב הסייבר האזרחי בשיתוף ולצד גופי הביטחון והמאסדרים.
החוק המוצע אינו מהווה מסגרת משפטית שלמה להסדרת היבטי הגנת הסייבר בישראל, אלא נועד לתת למערך הסייבר כלי משפטי מיידי להגנה מפני תקיפת סייבר, כמוגדר בו.
על כן במקביל לקידום החוק המוצע ממשיך מערך הסייבר הלאומי בקידום מסגרת משפטית שלמה כמקובל במדינות העולם.
בהקשר זה יצוין כי מרחב הסייבר הלאומי נתון כל העת לאיומים על תפקודו התקין. בשנה האחרונה, עקב התפרצות משבר הקורונה, רמת הסיכון עלתה במידה ניכרת, בין השאר בשל עלייה חדה בהיקף העבודה מרחוק במגזר הציבורי והפרטי, הרחבת הפעילות בזירה הדיגיטלית ותהליכי דיגיטציה מואצים של שירותים ציבוריים ופרטיים.
לנוכח האמור, במסגרת החוק מוצע להסמיך את המערך לפנות בבקשה למתן צו שיפוטי שיאפשר ביצוע פעולות נדרשות להגנה, ובכלל זה להסמיך את המערך לבצע בעצמו פעולות הגנת סייבר אם ארגון מסרב לשתף פעולה. על מנת להבהיר כי אין באמור כדי לייתר את תפקידם ואחריותם של המאסדרים לפי דין הפועלים כבר כיום בתחום הגנת הסייבר מובהר בנוסח כי פנייה לבית המשפט תיעשה רק בהסכמה של המאסדרים הרלבנטים בתחומי המשק השונים, כמפורט בתוספת לחוק.
לנוכח פוטנציאל הסיכון הרחב בתחום הגנת הסייבר, ועל מנת להגביר את הוודאות לגבי הגופים המקיימים פעילות חיונית, מוצע לקבוע בחוק הגדרה המבהירה מהי פעילות חיונית, ולצדה להסמיך את ראש הממשלה, לאחר התייעצות עם המאסדר הנוגע בדבר, לקבוע "מדרג" פגיעה באינטרס הציבורי החיוני, לצורך הפעלת החוק רק במקרים שבהם הסיכון הוא חמור. לצד זאת מוצע לקבוע כי עד לתקנות כאמור יעביר המאסדר את התבחינים האמורים. במקרים שבהם לא יועברו תבחינים, מוצע הסמיך את ראש מערך הסייבר הלאומי לקבוע תבחינים זמניים, עד להשלמת חקיקת משנה כאמור.

בנוסף, ועל מנת לאתר סיכונים להגנת הסייבר הלאומית ולסייע לארגונים נתקפים או לארגונים החשופים לתקיפות סייבר הנובעות מחולשות מוכרות הנגישות מרשת האינטרנט, מוצע לאפשר למערך הסייבר לקבל פרטי קשר של ארגונים (בלבד) הקשורים לכתובת IP שבהן מבוצעת התקיפה או נמצאה חולשה המאפשרת ניצול. בהתאם לדין הקיים, שירות הביטחון הכללי מקבל מידע זה מספקיות התקשורת, כחלק מביצוע תפקידיו בתחום הסייבר והגנת הסייבר. על כן לצורך יעילות הפעילות מול גופי התקשורת מוצע כי ברירת המחדל היא כי המערך יקבל מידע זה משירות הביטחון הכללי, המקבל מידע זה בהתאם לייעודו.

על מנת להתמודד עם המצב המשפטי הקיים, ולענות על הצורך המיידי של מערך הסייבר הלאומי בעת הזו, החוק מוצע כהוראת שעה, ואין בו כדי ליתן מענה שלם לצרכי הגנת מרחב הסייבר הישראלי.

דברי הסבר מפורטים

מערך הסייבר הלאומי הוקם מכוח שורה של החלטות שקיבלה הממשלה וכחלק ממדיניותה בתחום הגנת הסייבר. כך, בהחלטת ממשלה מספר 3611 מיום ה' בתמוז התשע"א (7 ביולי 2011) בעניין "קידום היכולת הלאומית במרחב הקיברנטי", הוחלט על הקמת המטה הקיברנטי הלאומי (להלן – המטה) והוטל עליו, בין השאר, לגבש תפיסת הגנה לאומית למרחב הסייבר. בהחלטת ממשלה מספר 2443 בעניין "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" ובהחלטת ממשלה מספר 2444 בדבר "קידום ההיערכות הלאומית להגנת הסייבר" (להלן – החלטה 2444), שתיהן מיום כ"ו בשבט התשע"ה (15 בפברואר 2015), אישרה הממשלה את התפיסה שגיבש המטה.

עוד יצוין כי ביום כ"ט בכסלו התשע"ח (17 בדצמבר 2017) החליטה הממשלה, בהחלטה מספר 3270, כי המטה והרשות הלאומית להגנת הסייבר שהוקמה בהחלטה 2444 יאוחדו לגוף אחד – מערך הסייבר הלאומי (להלן – המערך).

בשנת 2016, במסגרת הוראת שעה בחוק להסדרת הביטחון בגופים ציבורים, התשנ"ח-1998 (להלן – חוק להסדרת הביטחון), נקבע כי המערך יפעיל סמכויות מכוח אותו חוק כלפי הגופים המנויים בתוספת החמישית לחוק האמור (ראו: חוק להסדרת הביטחון בגופים ציבוריים(הוראת שעה), התשע"ו-2016 (ס"ח התשע"ו, עמ' 1219)). מול שאר הגופים במשק פועל המערך בהסכמה בלבד, זאת בהתאם להחלטות הממשלה בתחום הסייבר והדין הכללי ובהתאם למסגרת משפטית שתואמה עם היועץ המשפטי לממשלה במסמך "עקרונות ה-CERT הלאומי" (ראו בקישור: https://www.gov.il/he/Departments/Policies/principles).

בשנת 2018, הפכה הוראת השעה האמורה בחוק להסדרת הביטחון להוראה של קבע.

בשנת 2018, הפיץ משרד ראש הממשלה את תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח-2018 (להלן – התזכיר), במטרה להשלים את קידום המדיניות שנקבעה בהחלטות הממשלה הנזכרות ולהסדיר מסגרת משפטית מקיפה לפעילות המערך לצורך הגנת מרחב הסייבר. ואולם, לנוכח תקופות הבחירות לכנסת ה-20, לכנסת ה-21 ולכנסת ה-22, החל מחודש נובמבר 2018 עד חודש מרס 2020, ולאחר מכן לנוכח התמודדות המדינה עם המשבר שנגרם בשל ההתפרצות וההתפשטות של נגיף הקורונה החדש, לא הושלמו הליכי החקיקה של התזכיר.

בשנה האחרונה, גם עקב משבר הקורונה, רמת הסיכון במרחב הסייבר עלתה במידה ניכרת, בין השאר בשל עלייה חדה בהיקף העבודה מרחוק במגזר הציבורי והפרטי, הרחבת הפעילות בזירה הדיגיטלית ותהליכי דיגיטציה מואצים של שירותים ציבוריים ופרטיים.

החוק מוצע במטרה להתמודד עם המצב המשפטי הקיים, שבו אין למערך הסייבר הלאומי כלי משפטי שמאפשר לו לחייב ארגון המהווה יעד לתקיפת סייבר לבצע פעולות הגנה הנדרשות למניעת סיכונים לאינטרסים ציבורים חיוניים. בשונה מההסדר שהוצע בתזכיר, ההסדר המוצע בחוק זה אינו עוסק באסדרה ובמערכות היחסים שבין המערך למשרדי הממשלה המפעילים סמכויות אסדרה. היבטים אלה של פעילות המערך מוסדרים כיום בהחלטות הממשלה ובהסדרים בין משרדי הממשלה הרלבנטיים לבין מערך הסייבר הלאומי, בהתאם להקשר.

החוק המוצע אין בו כדי ליתן מענה שלם לצרכי הגנת מרחב הסייבר הישראלי, ועל כן מוצע לקבוע את ההסדר המוצע בו כהוראת שעה למשך שנתיים, שבמהלכן יושלם מהלך החקיקה השלם הנדרש למימוש

החלטות הממשלה הנזכרות לעיל ולמתן מענה שלם כאמור.

סעיף 1

בסעיף 1 להחלטה 2444, קבעה הממשלה כי "ההגנה על תפקודו התקין והבטוח של מרחב הסייבר מהווה יעד ביטחוני לאומי חיוני של המדינה ואינטרס ממלכתי חיוני לביטחונה הלאומי". קביעה זו נכונה ביתר שאת כיום לנוכח התרחבות השימוש והתלות בטכנולוגיות מידע ותקשורת לפעילות כלכלית וחברתית. נוסף על כך, בעת משבר הקורונה התרחשה "טרנספורמציה דיגיטלית" מואצת, שבמסגרתה שירותים חיוניים ופעילות עסקית עברו להתבסס על פעילות באמצעים מקוונים במרחב הסייבר. תפקודו התקין של מרחב הסייבר מהווה בסיס לפעילות המבוטאת במסגרת "אינטרסים ציבורים חיוניים".

סעיף 2

מוצעות הגדרות למונחים שונים המשמשים בחוק המוצע. מונחים אלה נוגעים בעיקר לשני תחומי תוכן: הגנת הסייבר וההגנה על אינטרסים ציבורים חיוניים.

מונחים בתחום ההגנה על אינטרסים ציבוריים חיוניים

להגדרה "אינטרס ציבורי חיוני" – הגדרה זו נועדה למנות את הערכים שההגנה עליהם מפני תקיפות במרחב הסייבר מנחה את פעילות מערך הסייבר הלאומי, ובמילים אחרות, שפעילות המערך מכוונת להגנתם. כך, למשל, האפשרות לפגיעה ממשית באינטרס ציבורי חיוני היא אחד היסודות שבשלהם תקיפת סייבר נחשבת לתקיפת סייבר חמורה ומקימה סמכות למערך להפעיל סמכויות כלפי הארגון המותקף.

אם כן, האינטרסים הציבוריים החיוניים המנויים בהגדרה המוצעת הם נקודת מוצא להפעלת סמכויות המערך כמוצע בחוק, אולם הפעלת הסמכות בפועל מחייבת קיום תנאים נוספים המוגדרים בהוראות המהותיות. מכאן שהמונח "אינטרס ציבורי חיוני" צריך להיבחן בתוך הקשר ובהתאם לאינטרס הספציפי הנדון. בפרט נדרש להתייחס למדרג לפי סעיף 14 או 15 המוצעים.

להגדרה "ארגון המקיים פעילות חיונית" – מונח זה נועד להבהיר את סמכותו של המערך בכל הנוגע למתן הנחיות מקצועיות לביצוע פעולות להגנת סייבר לפי סעיף 2 לחוק המוצע, לגופים שמבצעים פעילות חיונית ושתקיפת סייבר נגדם עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני. ההגדרה ממוקדת במאפייני הפעילות כגון החשיבות של הפעילות לכלל הציבור או לחלק משמעותי ממנו, חשיבותה לקיום אספקה סדירה של מוצרים או שירותים חיוניים, או מניעת פגיעה בענף חשוב למשק המדינה. תנאים אלה יש לפרש לפי הקשר ובנסיבות העניין, בשים לב לחשיבות השירות.

כמו כן מוצע לקבוע כי ארגונים שמספקים שירותי מחשוב ותקשורת לארגונים המקיימים פעילות חיוניתזאת על רקע התובנה המצטברת כי תשתיות מחשוב ותקשורת מהוות כר פורה לתקיפות סייבר משום שהן מאפשרות לתוקף נגישות לארגונים רבים באמצעות תקיפה מוצלחת אחת. תקיפות אלה הפכו נפוצות מאוד והן ידועות כ"תקיפה באמצעות שרשרת האספקה".

מוצע לקבוע כי ההגדרה תתבסס על מדרג חומרה שייקבע בתקנות (ראו דברי הסבר לסעיף 14), או באופן זמני בהתאם להגדרה של המאסדר הרלבנטי או ראש המערך אם אין מאסדר.

מונחים בתחום הגנת הסייבר

להגדרה "הגנת סייבר" – מוצע להגדיר את המונח "הגנת סייבר" באופן רחב במטרה להקיף את האמצעים הטכנולוגיים המהווים יעד לתקיפה, ובהם מחשב, חומר המחשב (מידע או תוכנה) ותקשורת הנתונים ממנו ואליו.

בהתאם לכך, הגדרה זו נועדה לכלול את כל פעולות ההגנה הנדרשות כדי למנוע תקיפה אפשרית או קונקרטית, לפני ביצועה, וכן פעולות שיש לבצע לשם התמודדות עם התקיפה, במהלכה ולאחריה. תחום "הגנת הסייבר" כולל את תחום הידע המקצועי הידוע כ-"אבטחת מידע", שהתפתח במקביל להתפתחות תחום טכנולוגיית מידע והשימוש בה. בעולם אבטחת המידע, הערך המוגן המרכזי היה שמירת המידע מפני דלף או שיבוש. בעידן הגנת הסייבר, פוטנציאל הנזק התרחב מאוד, שכן ניתן באמצעות תקיפת סייבר גם לשבש פעילויות ולגרום לנזק. הקישוריות הרבה המאפיינת את עידן הסייבר 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. זאת, כדי לאפשר איתור חשד לתקיפת סייבר מוקדם ככל האפשר, זיהוי התקיפה, הכלתה במידת הצורך וקביעת דרכי התמודדות עמה, ולאפשר להנהלת הארגון תמונת מצב רציפה על אודות תפקוד המערכות הנדרשות לפעילות הארגון.

להגדרה "מידע בעל ערך הגנתי" – בדומה להגדרה המוצעת למונח "הגנת סייבר", גם ההגדרה המוצעת למונח "מידע בעל ערך הגנתי" נועדה לאפיין את סוגי המידע המקצועי והטכנולוגי המשמש את אנשי הגנת הסייבר לצורך פעילות הגנת הסייבר, כגון איתור תקיפות סייבר, דרכי התמודדות איתן ופעולות לצמצום הנזק הנגרם מהן. כך למשל, מידע בעל ערך הגנתי כולל על פי המוצע מאפיינים טכנולוגיים שיש בהם כדי להצביע על חשש לתקיפת סייבר, על השיטה או האמצעי לביצועה, על המחשב שממנו התבצעה התקיפה או המחשב המותקף, כתובות פרוטוקול תקשורת (כגון IP – Internet Protocol Adress) וכתובות דואר אלקטרוני שנוגעות לתקיפת סייבר, שמות מתחם (Domain Name) ומען משאבים אחיד (URL) שנוגעים לתקיפת סייבר ; מידע על פגיעות ; ונתונים בשפה ממוחשבת המעידים על מזהים של תבנית תקיפת סייבר כהגדרתה המוצעת.

להגדרה "פגיעות" – מונח זה מוכר בשפה המקצועית כ-Vulnerability, אך ההגדרה המוצעת למונח בחוק זה רחבה יותר וכוללת גם פגיעויות המהוות נקודות תורפה הנובעות למשל מאופן השימוש במחשב אשר ניתן לנצלן כדי לבצע תקיפת סייבר.

ההגדרה המוצעת מתייחסת הן לפגיעות באמצעי עצמו, למשל פגיעות במחשב, בחומר מחשב (ובכלל זה תוכנה) או בפרוטוקול תקשורת, והן לפגיעות שנובעת מהתצורה של מערכת המחשבים או מהנהלים הנוגעים להפעלתה.

ככלל, פגיעות מאפשרת לגורם זדוני להשתמש במחשב, בחומר מחשב או בתקשורת נתונים בניגוד לאופן שבו הם תוכננו לפעול או בניגוד לאופן הפעולה התקין שלהם, ולבצע בהם שימוש לרעה, הכולל גם ביצוע תקיפת סייבר, או פעולות הכנה לתקיפה כאמור. הדבר יכול לנבוע מ-"באג" בתוכנה, או מתקלות אחרות בתחום הגדרת המערכת, תכנונה והבקרה עליה. מעת שמתגלה פגיעות, מתחיל מרוץ בין המתגוננים לתוקפים. המתגוננים נדרשים להתמודד עם הפגיעות, בין בדרך של התקנת עדכון אבטחה, צמצום הסיכונים האפשריים ממנה בדרך של הגנה על הרכיב שבו התגלתה הפגיעות או הגנה מפניו, או באמצעים אחרים.

בהקשר של תקיפת סייבר כנגד ארגון, פגיעות מהווה פעמים רבות אמצעי להתקנת "ראש גשר" ברשת הארגונית. באמצעות ראש הגשר, עשוי התוקף להתקין ברשת הארגון תוכנות זדוניות המאפשרות לו שליטה והפעלה מרחוק.

בדרך כלל תוקף המנצל פגיעות כדי לחדור לארגון, משתמש בה כדי להתקין כלי תקיפה או אמצעי תקיפה נוספים ברשת הארגונית, בטכניקות שונות, ולצד זאת יוצר ערוץ גישה נוסף שכבר אינו תלוי בפגיעות. כך, אם תוקף יצר לעצמו תווך כניסה לארגון, תיקון הפגיעות בשלב זה כבר לא יהיה מספק מכיוון שהתוקף נמצא בתוך הארגון ואפשרויות הפעולה שלו ברשת הארגונית רחבות יותר.

ההגדרה המוצעת מבוססת על תובנות מקובלות בתחום הגנת הסייבר. מסמך מקובל בתחום זה הוא מסמך ה-CVSS (Common Vulnerability Scoring System) (ראו: FIRST , CVSS Common Vulnerability Scoring System version 3.1 User Guide Revision 1, https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf), אשר מנוהל בידי ארגון FIRST (Forum of Incident Response Teams) – ארגון שלא למטרת רווח המאגד ארגוני הגנת סייבר פרטיים וממשלתיים. מטרת מסמך זה לתת כלי לדירוג מאפייני הפגיעויות בתוכנה וחומרתן. בהתאם למסמך זה יש שלושה סוגי מדדים: Base – מדד הבוחן את מאפייניה הפנימיים הקבועים של הפגיעות, Temporal – מדד המשקף את רמת הפגיעות בזמן נתון, ו–Environmental – מדד העוסק במאפייני הפגיעות ביחס להקשר ארגוני או מגזרי מסוים. מובן כי שימוש במדד Environmental תלוי בקיומו של מידע אודות הארגון או המגזר הרלבנטי (ראו עוד בדברי ההסבר להגדרה "פגיעות קריטית" להלן בדברי ההסבר לסעיף 2 להצעת החוק).

לצד זאת, בקהילת האינטרנט, ארגון OWASP (Open Web Application Security Project) מקטלג סוגי תקיפות המנצלות פגיעויות שרלבנטיות לאתרי אינטרנט לפי מאפייניהן (ראו: OWASP, Vulnerabilities, What is a vulnerability?, https://owasp.org/www-community/vulnerabilities/). מאפיינים אלה מהווים פרמטר מקובל לתיאור ולדירוג פגיעויות מבחינת רמת סיכון וכפועל יוצא מבחינת חומרה.

להגדרה "פעולה להגנת סייבר" – מונח זה נועד לתאר את הפעולות במחשב או בחומר מחשב שמבצע איש הגנת הסייבר ("מגן הסייבר") כדי לאתר תקיפת סייבר ולהתמודד עמה. פעולות אלה הן חלק מהאמצעים המקובלים שמפעיל מי שעוסק בהגנת סייבר. בהתאם לתפיסה המקצועית של הגנת הסייבר, פעולות ההגנה נגזרות משיטות העבודה של התוקפים. על רקע זה מגדיר החוק המוצע את הפעולות להגנת סייבר. בתפיסת הגנה מתקדמת, פעולות אלה נגזרות מהבנה של דפוסי פעילות התוקף.

על רקע זה, בעת התרחשותה של תקיפת סייבר או כאשר קיים חשש לתקיפה כאמור, נדרש מגן הסייבר להבין אם אכן התבצעה תקיפה, ואם כן, מה חומרתה, וכן הוא נדרש לצמצם את השפעתה. במסגרת זו, נדרש המגן לאתר את המחשבים שנתקפו ברשת הארגונית ואת האופן שבו התבצעה החדירה לרשת, להבין אילו פעולות התוקף מסוגל לבצע בעקבות התקיפה, למנוע מהתוקף את היכולת לבצע פעולות ברשת או להכיל את הנזק, להסיר את כלי התקיפה ולמנוע את הישנותה.

על כן מוצע כי המונח "פעולה להגנת סייבר" יכלול את כל מגוון הפעולות הנדרשות לצורך איתור תקיפת סייבר וטיפול בה, ובכלל זה מתן הוראות למחשב בשפה קריאת מחשב כדי לאתר או להתמודד עם תקיפות (כולל הסרת תוכנות זדוניות), סריקה, הקלטה, העתקה ובחינה של חומר מחשב ותקשורת נתונים, וביצוע פעולות לגילוי מוקדם.

הפעולות שמוצע לכלול כאמור בהגדרה "פעולה להגנת סייבר" הן פעולות מקובלות בקרב אנשי הגנת סייבר העוסקים בטיפול בתקיפות. הכללתן במונח האמור נועדה להבהיר שמערך הסייבר הלאומי מוסמך לבקש מבית המשפט צו להורות על ביצוע פעולות מעין אלה במסגרת טיפול בתקיפת סייבר. על פי המוצע

בחוק, פעולות אלה אמורות להתבצע בידי הארגון בהתאם להנחיות מקצועיות שיקבל מהמערך.

להגדרה "תבנית תקיפת סייבר" – המונח "תבנית תקיפת סייבר" נועד לכוון את אופן הפעלת הסמכות של מערך הסייבר הלאומי, בכל הנוגע לאיסוף ועיבוד מידע בזיקה למטרת המערך – ביצוע פעולות להגנת סייבר, הכוללת איתור תקיפות סייבר.

ההגדרה המוצעת מבוססת על תפיסות מקובלות בקרב קהילת אנשי הסייבר, ובין השאר על מאגר הידע ושיטת המיון של של ארגון MITRE המכונה MITRE ATT&CK (ראו: MITRE Att&ck, https://attack.mitre.org/) המבקשת לארגן את המידע הקיים על אודות דרכי ביצוע של תקיפות בהתאם לשלבים השונים, כמפורט להלן. מאגר הידע נועד בין השאר ליצור שפה משותפת בין העוסקים בתחום הגנת הסייבר, לאפיין את ההתנהגות של תוקפים שונים, לסייע בשיפור מערכות הגנת הסייבר ולסייע באיתור מהיר של תקיפות סייבר.

בהתאם לתפיסת הגנה מתקדמת, כמפורט במאגר הידע MITRE, השלבים המרכזיים בתקיפת סייבר הם כדלקמן: איסוף מקדים על מערכות היעד לקראת תקיפת סייבר; הכנת כלי תקיפת סייבר המתאים למערכות; הגעה אל היעד; השגת גישה ראשונית לרשת הנתקפת; ניצול פגיעות ברשת הנתקפת; הוצאה לפועל של תקיפת סייבר; שהייה ברשת; העלאת הרשאות; התחמקות מכלי הגנה; השגת נגישות להרשאות; חשיפת מבנה רשת והכרת המערכות ברשת; תנועה רוחבית ברשת; איסוף מידע; שליטה ובקרה; הזלגת מידע; והשפעה. זיהוי דפוס התקיפה של תוקף, מאפשר איתור תקיפה והערכה טובה יותר של הצעדים והאמצעים שהתוקף צפוי להפעיל ברשת הארגונית, ולשפר את ההתמודדות בארגון הנתקף ואת רמת ההיערכות בארגונים אחרים שעלולים להיתקף באותו אופן.

להגדרה "תקיפת סייבר" – לנוכח ריבוי הטכניקות הקיימות כיום לביצוע תקיפות סייבר מוצע כי הגדרה זו תכלול את מגוון הפעולות שמטרתן היא פגיעה בפעילות של מחשב או השפעה עליה. פעילות זו אסורה בהתאם לדינים אחרים האוסרים על האזנת סתר לתקשורת נתונים, פגיעה בתקשורת נתונים או השפעה עליה; פגיעה בסודיות מידע, מהימנותו ונגישותו; הפרעה לחיבור של מחשב לרשת תקשורת או מניעת חיבור כאמור; וחדירה אסורה לחומר מחשב שלא כדין כמשמעותה בסעיף 4 לחוק המחשבים, התשנ"ה-1995.

להגדרה "תקיפת סייבר חמורה" – על פי המוצע, תקיפת סייבר חמורה היא תקיפת סייבר שתוחלת הנזק שלה גבוהה באופן יחסי לתקיפות סייבר אחרות. חוק המוצע כולל תבחין הפעלת סמכות מחמיר של "פגיעה ממשית באינטרס ציבור חיוני".

המונח כולל ארבע חלופות, כמפורט להלן. הראשונה – תקיפת סייבר שיש הסתברות גבוהה שתגרום לנזק ממשי לאינטרס ציבורי חיוני. במסגרת הבחינה של חלופה זו יש לבחון את מכלול המאפיינים של התקיפה, ובכלל זה רמת התחכום של התקיפה, העדרם של אמצעים טכנולוגיים זמינים לטיפול בתקיפה ולצמצום הנזקים ממנה, משך הזמן שנדרש להיערכות להגנה מפני התקיפה או משך הזמן שנדרש לטיפול בתקיפה וקיומו של סיכון ממשי לאינטרס ציבורי חיוני.

החלופה השנייה היא תקיפת סייבר אשר יש יסוד סביר להניח כי היא מסכנת אינטרס ציבורי חיוני בכך שהיא עלולה להתפשט למחשבים רבים אחרים.

לצורך הגברת הוודאות מוצע בסעיפים 13 ו – 14 לאפשר קביעת תבחינים מפורטים יותר למהי פגיעה ממשית באינטרס ציבורי חיוני.

החלופה השלישית כוללת תקיפת סייבר שמכוונת כלפי ארגון חיוני, והחלופה הרביעית – תקיפה שיש

יסוד סביר להניח שנועדה לפגוע בביטחון הלאומי.

סעיפים 3, 7, 8

בסעיף 7להצעת החוק מוצע להסמיך את ראש מערך הסייבר הלאומי למנות עובד בכיר מבין עובדי המערך שיהיה אחראי על קבלת החלטות וביצוע פעולות לצורך הגנת הסייבר כמפורט בסעיף 3 לחוק המוצע (להלן – גורם אחראי). הביטוי "עובד בכיר" מכוון לכך שנדרש למנות לתפקיד זה עובד שמוגדר כבכיר לפי הכללים המקובלים בשירות המדינה.

בסעיף 3 להצעת החוק מוצע להסמיך את הגורם האחראי לפנות לבית המשפט בידי בא כוח היועץ המשפטי לממשלה במידה שפנייה מוקדמת לארגון שמקיים פעילות חיונית לבצע פעולות הנדרשות לטובת הגנת הסייבר בארגון אם קיימת במחשבי הארגון פגיעות שעולה כדי פגיעות קריטית אשר עלולה לסכן אינטרס ציבורי, או תקיפת סייבר חמורה והארגון אינו נוקט בפעולות הנדרשות לטיפול בפגיעות.

בדומה להגדרה המוצעת למונח "פגיעות", גם ההגדרה המוצעת למונח "פגיעות קריטית" מבוססת על תובנות מקובלות בקהילה המקצועית לגבי מדידת החומרה של פגיעויות בהתאם למדדים מקובלים בהקשרים הרלבנטיים לפעילות הגנת סייבר. בהתאם לכך, המונח פגיעות קריטית מתייחס לשילוב בין פגיעות לבין מאפייני סיכון נוספים, שיחד מגדילים את ההסתברות לניצול הפגיעות ואת עוצמת הנזק הפוטנציאלי לארגון.

על פי המוצע, ובהתאם לתפיסות מקובלות בקהילה המקצועית, מאפיינים אלה מתחלקים לשלושה סוגים: המאפיינים הטכנולוגיים של הפגיעות; קיומם של שיטות ואמצעים לנצל את הפגיעות לתקיפת סייבר או למנוע ניצול שלה לתקיפה כאמור; ושכיחותה של הפגיעות.

במסגרת בחינת המאפיינים הטכנולוגיים של הפגיעות יש להביא בחשבון את אלה: היכולת של התוקף לעשות שימוש בפגיעות; המורכבות של התקיפה הנדרשת כדי לנצל את הפגיעות, ובכלל זה מאפייני מערכת המחשב החשופה לפגיעות ותלות (או היעדר תלות) בפעולות מצד מושא התקיפה; רמת ההרשאה הנדרשת, היקף השליטה או ההרשאות הנדרשות במחשבי הארגון כדי לנצל את הפגיעות, הצורך באיסוף מידע מקדים כדי לבצע את התקיפה, חלון ההזדמנויות שבו ניתן לנצל את הפגיעות והמיומנות הנדרשת לניצולה; הצורך להתגבר על מנגנוני הזדהות, לרבות מספר המנגנונים ורמת ההגנה שלהם; ומידת ההשפעה של ניצול הפגיעות על פגיעה במידע.

במסגרת הבחינה של שיטות ואמצעים לניצול פגיעות או למניעתה, ניתן לבחון שיקולים כגון: רמת הבשלות של הכלים והשיטות לניצול הפגיעות והאפשרות להשתמש בהם למנעד רחב של מצבים; ניצול הפגיעות בעבר – בארץ או בחוץ לארץ; מידע לגבי האפשרות של ניצול הפגיעות או לגבי זהות התוקף שניצל או שמעוניין לנצל את הפגיעות; הימצאות של עדכון אבטחה לטיפול בפגיעות, לרבות מידת האפקטיביות של העדכון או הצורך באמצעים אחרים לצמצום הסיכון; ומהימנות המידע הקיים לגבי הפגיעות.

פעולות שיש לבצע לטובת הגנת סייבר ושיש להן קשר לצמצום הסיכון מהפגיעות, ובמרכזן התקנת עדכוני אבטחה למערכות הארגון או הוראות אחרות לסגירת הפגיעות, וכן אמצעים נוספים שיצמצמו את הסיכון לפי העניין, כגון הגבלת גישה למחשבים חיוניים בארגון, הגבלת גישה חיצונית למחשבי הארגון (למשל סגירת כניסות (Port) מסוימות), החלפת סיסמאות, סריקה של תקשורת נתונים לצורך ניטור של חשש לניצול הפגיעות או של פעולות הנובעות מניצולה או פעולות להגנת התקשורת הארגונית.

על פעולות אלה להיות קשורות במישרין לאיתור הפגיעות הקריטית או להתמודדות עמה וסגירתה,

ולמניעת האפשרות לניצולה.

מוצע להסמיך גורם אחראי לפנות לבית המשפט בבקשה למתן צו שיאפשר לעובד מוסמך מטעם המערך לבצע בעצמו פעולות בחומר מחשב, במערכות הממוחשבות של הארגון או לתת הוראות אחרות הנדרשות למניעת תקיפת סייבר או להתמודדות עם תקיפה כאמור.

לצורך כך מוצע, בסעיף 8 להצעת החוק, להסמיך את ראש המערך למנות עובד בעל הכשרה מתאימה לתפקיד של "עובד מוסמך". בשונה מגורם אחראי, עובד מוסמך יכול לבצע פעולות בחומר מחשב בעצמו. בהתאם, מוצע לקבוע דרישות סף לתפקיד, וכן לקבוע כללים להתנהלות של עובד מוסמך מול ארגונים ונושאי משרה בעת מילוי תפקידו.

סעיף 3 להצעת החוק מהווה ציר מרכזי בהסדר המעוגן בה, משום שהוא מאפשר למערך הסייבר הלאומי לנקוט במקרים המתאימים בצעדים משפטיים לצורך הגנת הסייבר, באמצעות החלטה של בית המשפט המנהלי.

על פי המוצע, יוכל בית המשפט, בצו, לתת את ההוראות המיידיות המתאימות לנקיטת פעולות להגנת סייבר. כך למשל, יוכל בית המשפט להורות לארגון למסור לעובד המוסמך ידיעות ומסמכים שנדרשים לשם הגנת הסייבר. מאחר שהפעלת הסמכויות לפי הצו לא נועדה לצרכי חקירה פלילית או רגולציה, מוצע כי בית המשפט שיהיה מוסמך לעניין זה יהיה בית המשפט לעניינים מינהליים.

על פי המוצע, בקשה לצו כאמור תוגש לבית המשפט רק אם מתקיים אחד התנאים המנויים בסעיף קטן (ב) כנוסחו המוצע. בקשה כאמור עשויה לכלול את טווח האמצעים הנדרשים במישרין להשגת תכלית הפעלת הסמכות, ובין השאר קבלת מידע נדרש, העברת עותקים של חומרי מחשב, וכל הוראה אחרת שימצא לנכון בנוגע לביצוע פעולות להגנת סייבר במחשבי הארגון.

בהתאם למוצע, יבחן בית המשפט במסגרת זאת כמה שיקולים, ובהם התאמת הפעולה המבוקשת לתקיפה הקונקרטית שבקשר אליה מתבקש הצו, והשפעת פעולות הגנת הסייבר על פעילות הארגון.

כמו כן, תיבחן האפשרות של הארגון או מי מטעמו לבצע את הפעולה באמצעות אדם בעל ידע ומומחיות מטעם הארגון, בלא צורך בביצוע הפעולה בידי עובד מוסמך מטעם המערך. עם זאת, במקרים שבהם קיים מידע רגיש מבחינה ביטחונית או ידע ייחודי הקשור להתמודדות עם התקיפה, עשויה להידרש מעורבות ישירה של המערך בביצוע פעולות ההגנה הנדרשות.

בהתאם לסעיף קטן (ג), משעה שמופעלת הסמכות לפי הוראת השעה, וגורם אחראי סבור כי ארגון נדרש לבצע פעולות הגנת סייבר, עליו לקבל את הסכמת הרשות המאסדרת הרלבנטית, בהתאם לרשימה שתיקבע בתוספת, לפעולה זו. מנגנון הסכמה זה נועד לאפשר תיאום ושיתוף בעל הסמכות הרלבנטי העוסק באסדרה של הארגון בשגרה. סל כלי הפעולה של מערך הסייבר עוסק במיקוד אופרטיבי במיגור התקיפה בהתאם לתפקידיו וייעודו, כמפורט לעיל, אולם מעורבות המאסדר נדרשת כחלק מאחריות המאסדר הכוללת על האינטרס החיוני.

על פי המוצע בית המשפט יקבל את הבקשה רק אם שוכנע כי הפעולות להגנת סייבר שהגורם האחראי מבקש לבצע אכן נדרשות לצורך מניעת פגיעה באינטרס ציבורי חיוני אשר קשורה לתקיפת סייבר, ובכלל זה לצורך התמודדות עם פגיעות שעלולה לאפשר תקיפה כאמור.

הסדר זה נועד לאפשר למערך הסייבר הלאומי למלא את ייעודו ולטפל בתקיפות סייבר חמורות או במקרים של פגיעות קריטית, גם אם הארגון המותקף או שבו התגלתה הפגיעות מסרב לכך, ביצוע פעולות

להגנת סייבר כאמור. על כן, בית המשפט יקבל את הבקשה לצו רק אם שוכנע שנסיבות אלה מתקיימות. בדיון לפני בית המשפט יוכל הארגון הנוגע בדבר להציג לבית המשפט את עמדתו בעניין התקיימות הנסיבות המתוארות ואת החלופות שהובאה בחשבון עמדתו של הארגון הנוגע בדבר.

בסעיף קטן (ד) מוצע להסמיך את בית המשפט, בצו שהוא נותן, לאפשר לעובד מוסמך להיכנס למקום, זאת כפעולת עזר הנדרשת לצורך ביצוע הצו.

כאמור, בקשות של גורם אחראי למתן צו לפי סעיף זה תוגשנה לבית המשפט לעניינים מינהליים. בהתאם, יחולו על בקשות אלה סדרי הדין שחלים בבית המשפט לעניינים מינהליים, לרבות דיון על יסוד תצהירים וכן סייגים למסירת מידע או מסמכים, כמו גם אפשרות לעריכת דיון בדלתיים סגורות או במעמד צד אחד, שבמסגרתו רשאי בית המשפט לקבל מידע והסברים מנציג היועץ המשפטי לממשלה או מגורם אחראי, אף בהיעדר יתר בעלי הדין.

כמו כן, מוצע להסמיך את שר המשפטים לקבוע בתקנות סדרי דין לעניין הליכים לפי סעיף זה, ככל שהדבר יידרש.

סעיף 4 ככלל, המערך אינו אוסף מידע מוגן פרטיות לצורך ביצוע תפקידו, אלא מידע טכני שיש בו כדי לסייע להגנת סייבר, ואשר מוצע להגדיר בסעיף 1 להצעת החוק כ"מידע בעל ערך הגנתי". עם זאת, לעתים עלול להגיע לידי המערך מידע מוגן כאמור כ"תופעת לוואי" של ביצוע פעולות להגנת סייבר. ודוק, פעולות הגנה רבות דורשות לבצע סריקה ממוחשבת, שבסופה מופק פלט הכולל מידע בעל ערך הגנתי, ובכלל זה מידע על אודות קיומה של תקיפה או סממנים לקיומה.

בהתאם למוצע בהוראת שעה זו, ובמטרה לצמצם כמה שיותר את החשש לפגיעה בפרטיות, מוצע שמידע מוגן פרטיות ייאסף בידי המערך בנסיבות מצומצמות המנויות בסעיף, ושנחלקות לשלושה סוגי מקרים: מקרים שבהם פוטנציאל הפגיעה בפרטיותו של אדם מזוהה הוא נמוך מאוד למול התועלת להגנת הסייבר, מקרים שבהם הפעילות מותרת לפי דין אחר המסדיר את ההגנה על הפרטיות, ומקרים שבהם יתקבל לכך אישור שיפוטי בנסיבות שבהן אין דרך אחרת לבצע את פעילות הגנת הסייבר.

הסוג הראשון של האיסוף שיהיה מותר למערך לבצע מהווה הסדר ייחודי המבוסס על בחינה של פוטנציאל הסיכון לפרטיות כתוצאה מאופן העיבוד וההפקה של מידע בעל ערך הגנתי ואיזונו ללמול פוטנציאל הסיכון לפרטיות כתוצאה מתקיפת סייבר. במסגרת זו, מוצע לקבוע כי המערך רשאי לאסוף מידע בעל ערך הגנתי. מידע כאמור עשוי להיות בין השאר מידע מהסוגים האלה: מידע לגבי המאפיינים הטכנולוגיים של תקיפת סייבר, ובכלל זה המחשב שממנו התבצעה התקיפה או המחשב הנתקף, כתובות פרוטוקול תקשורת (IP) וכתובות דואר אלקטרוני שנוגעות לתקיפת סייבר, שמות מתחם (Domain Name) ומען משאבים אחיד (URL) שנוגעים לתקיפת סייבר; ומידע לגבי "תבנית תקיפת סייבר", כלומר מידע שנוגע לשלבים השונים ב"מעגל החיים" של תקיפת סייבר. ההסדר המוצע בעניין זה נועד להבהיר את אופן תחולת דיני הפרטיות בנסיבות האמורות בו, ולהקנות למערך סמכות לאסוף את המידע האמור.

הסוג השני של איסוף מידע מוגן שיהיה מותר למערך לבצע הוא איסוף שמותר על פי דין אחר, והסוג השלישי הוא איסוף מידע באישור בית משפט. סוג זה של איסוף מידע מוגן יתאפשר רק אם בית המשפט ישתכנע כי הדבר נדרש כדי להגן על אינטרס ציבורי חיוני.

עוד מוצע להבהיר כי המידע הפרטי שייאסף לפי החוק המוצע ישמש רק לצרכי הגנת הסייבר.

כמו כן, מוצעים תנאים להעברת מידע מוגן שייאסף לפי החוק, בהתאם לגוף המקבל את המידע

ובהתאם לסוג המידע.

על מנת לצמצם את הסיכונים לפרטיות מוצע, בסעיף קטן (ד), להורות על מחיקת מידע כשאינו נדרש עוד.

מוצע להחיל הסדר זה גם על מידע שהינו סוד מסחרי.

כן מוצע להבהיר, בסעיף קטן (ה), כי הסדר זה אינו מונע מהגופים הביטחוניים ומשטרת ישראל לקבל מידע במסגרת סמכויותיהם, מקום שהדבר נדרש ורלבנטי, ובהתאם לכללים בדין הנוגע לעניין.

סעיף 5 תקשורת האינטרנט מבוססת על שימוש בכתובות IP המאפשרות למחשבים לזהות אחד את השני ברשת האינטרנט. כתובת ה-IP אינה כוללת מידע על אודות זהות הארגון שהוא בעל המחשב. בהתאם לכך, כאשר קיים בידי המערך מידע על אודות כתובות IP שהמחשבים או הרשתות הקשורים אליהן חשופים לתקיפה בשל פגיעויות, אך אין ברשותו פרטי קשר של הארגון, הוא אינו יכול להתריע בפני הארגון או לפעול להגנה עליו. מידע זה על אודות קיומן של פגיעויות מתקבל משימוש בכלים ובמאגרים מסחריים, שחלקם יכולים לשמש אף תוקפים, וממקורות נוספים. איתור המידע נעשה ללא שימוש בכלים המבצעים חדירה אסורה לחומר מחשב שלא כדין כמשמעותה בסעיף 4 לחוק המחשבים, התשנ"ה-1995.

לכן, מוצע להסמיך גורם אחראי לפנות לספק גישה לאינטרנט ולדרוש ממנו מידע מזהה (שם, פרטי זהות ומען) לגבי ארגון, שהוא לקוח של הספק, ופרטים לשם יצירת קשר עמו (מספר טלפון וכתובת דואר אלקטרוני).

קבלת מידע לפי סעיף זה מוגבלת לנסיבות שבהן הגורם האחראי, על בסיס המידע שמצוי בידיו, סבור כי מתרחשת או עומדת להתרחש תקיפת סייבר נגד הלקוח או כי קיימת אצלו פגיעות קריטית. המידע על אודות זהות הלקוח ופרטי הקשר עמו נועד לאפשר למערך לפנות לארגון ולהמליץ לו על סוג הפעולות הנדרשות, או במקרים העונים על התבחינים שנקבעו בחוק המוצע (ראו סעיפים 2 ו-3 להצעת החוק), להורות לו לנקוט פעולות לצמצום הפגיעות או לטיפול בתקיפה, לפי העניין. פעולה זו של המערך מבטאת את תפקידו כמוקד לאומי להגנת הסייבר, האוסף מידע בעל ערך הגנתי שיש בו כדי לתרום לשיפור החוסן של מרחב הסייבר.

בשל החשיבות שיש לטיפול מהיר בתקיפה או בפגיעות הקריטית בנסיבות מסוימות, מוצע לקבוע כי העברת המידע מספק הגישה לאינטרנט לידי המערך תתבצע ככלל בתוך 72 שעות. עוד מובהר כי אין להעביר למערך פרטי קשר או פרטים אחרים על אודות לקוח שהוא יחיד. כלומר, ההסדר המוצע בסעיף זה מאפשר אך ורק העברת מידע כמפורט לעיל על אודות מנוי שהוא ארגון.

בהתאם לדין הקיים, שירות הביטחון הכללי מקבל את המידע המתואר לעיל מספקיות התקשורת, כחלק מביצוע תפקידיו בתחום הסייבר והגנת הסייבר. על כן, ולצורך ייעול הפעילות מול ספקיות התקשורת, הרי שככלל, המערך יקבל מידע זה משירות הביטחון הכללי (באמצעות עובד השירות – עובד בכיר בשירות הביטחון הכללי שראש השירות מינה לכך), אשר כאמור מקבל מידע זה בהתאם לייעודו של השירות. ככל שיהיה צורך בקבלת המידע בידי המערך ישירות מספקיות התקשורת, בהתאם להסדר המוצע בסעיף זה, יהיה עליו לקבל היתר לכך באופן כללי או לעניין מסוים מאת ראש הממשלה, שרשאי לקבוע תנאים למתן ההיתר, וידווח על הפנייה לראש שירות הביטחון הכללי.

עוד מוצע להבהיר כי ההסדר המינהלי הקיים בין שירות הביטחון הכללי לבין מערך הסייבר הלאומי לגבי קבלת מידע כאמור, אינו מקנה עילה לספק תקשורת לסרב לפנייה של גורם אחראי בדרישה למידע

לפי סעיף זה, ככל שהתקבלה.

סעיף 6 שירות הביטחון הכללי מופקד במסגרת תפקידו ובכפוף לייעודו לפי חוק שירות הביטחון הכללי, התשס"ב-2002 (להלן – חוק שירות הביטחון הכללי), גם על פעולות בתחום הגנת הסייבר. בהתאם לכך, מוצע לקבוע שעובד השירות יוכל במקרים מסוימים ועל פי היתר מאת ראש השירות להפעיל סמכויות לפי סעיפים 3 ו-4 לחוק המוצע, בתנאים הקבועים בהם, וזאת אם הדבר נדרש לשם מילוי תפקידי השירות לפי סעיף 7(ב)(1) לחוק האמור.

סעיף 9 הסעיף בא להבהיר שאין בחוק הנוכחי כדי למנוע או להגביל פעילויות שמבצע המערך או אחד מהגופים הביטחוניים כהגדרתם המוצעת בסעיף 2 להצעת החוק, לפי דין אחר. על פי המוצע, וכמקובל בהקשרים דומים בחקיקה, כולל המונח "גוף ביטחוני", לצד צבא הגנה לישראל, שירות הביטחון הכללי, המוסד למודיעין ולתפקידים מיוחדים ומשרד הביטחון ויחידות הסמך שלו, לרבות הממונה על הביטחון במערכת הביטחון, גם את משטרת ישראל (ראו למשל סעיף 19 לחוק הגנת הפרטיות).

כאמור בחלק הכללי של דברי ההסבר, המערך פועל כיום כלפי הגופים המנויים בתוספת החמישית לחוק להסדרת הביטחון מכוח אותו חוק, וכלפי שאר הגופים במשק – בהתאם לתפקידים שהטילה עליו הממשלה לפי חוק-יסוד: הממשלה, ובכפוף למסגרת שנקבעה בהחלטות הממשלה בתחום הסייבר ולעקרונות ה-CERT הלאומי, אשר נקבעו כאמור בתיאום עם היועץ המשפטי לממשלה. מסגרת פעולה זו מבוססת על עבודה בהסכמה מדעת מול ארגוני המשק תוך יישום עקרונות של אחריותיות, ובכלל זה התייחסות מיוחדת לאיסוף ולעיבוד של מידע מוגן ואופן השימוש בו.

מאחר שהחוק המוצע מסדיר פעולות של המערך כלפי ארגונים, אשר מבוצעות בלא הסכמה של הארגונים הנוגעים בדבר, מוצע להבהיר כי אין בהסדר המוצע בו כדי לשנות את יכולתו של המערך להמשיך לפעול בהסכמה כלפי ארגונים מכוח החלטות הממשלה והמסגרת המשפטית שחלה עליו כמתואר לעיל כניסתו של החוק המוצע לתוקף.

באשר לגופים הביטחוניים, הרי שאלה פועלים כיום בהתאם לסמכויותיהם וייעודם הביטחוני גם בתחום הגנת הסייבר, ואין הכוונה בחוק זה לגרוע מסמכויותיהם או לשנות את אופן פעולתם בתחום זה.

המערך מתמקד בקידום ההגנה על גופי המשק, בשיתוף מידע בעל ערך הגנתי ובטיפול בתקיפות סייבר חמורות המסכנות פעילות חיונית. בינו לבין הגופים הביטחוניים מופעלים הסדרי תיאום ומנגנוני תיאום שוטפים, מנגנונים של העברת מידע רלבנטי להגנת הסייבר, והסדרה שמטרתה אחדות הפעולה. הסדרים אלה נדרשים לעדכון ולשינוי מעת לעת, בהתאם למתאר האיומים המתפתח והמשתנה, וכמענה לדינאמיות הרבה בתחום זה, ומוצע על כן להותיר מצב דברים זה על כנו.

סעיף 10 ארגון הרוכש שירותים שיש בהם חשיפה לסיכוני סייבר, נדרש להסדיר את הטיפול בסיכוני הסייבר במסגרת הסכם הרכש. היבט זה של הגנת הסייבר ידוע כהגנה מפני סיכוני "שרשרת האספקה". הגנה זו מבטאת את הצורך להתמודד עם תקיפות שמנצלות פגיעויות אצל ספקים, כאמצעי כניסה לארגון.

כך, ארגונים שעשויים להיות מוגנים מאוד במערכותיהם שלהם, עלולים להיחשף לסיכונים הנובעים מפעילות מחשוב או קישוריות של ספקים שלהם. במשק כלכלי מתקדם שבו יש חשיבות למיקור חוץ לגופים כלכליים בעלי יתרון יחסי, נדרש אם כן לאפשר מיקור חוץ, ולצד זאת, לנהל את הסיכונים הנגרמים בשל כך מהיבט הסייבר.

סעיף זה לחוק המוצע בא להבהיר כי ההסדר המוצע בחוק לא נועד להתערב בהוראות הסכמיות-

חוזיות, שגופים כוללים בהסכמים שלהם, ובפרט לעניין ספקי הגופים הביטחוניים ובהם ספקים של משרד הביטחון.

מערכת הביטחון מסדירה את הדרישות מספקים הקשורים להגנה על אינטרסים ביטחוניים כחלק ממכלול הסכמי הרכש, ובכלל זה גם בהיבטי סייבר. הסעיף מבהיר כי החוק לא נועד לפגוע בהוראות חוזיות אלה, להתערב בהן או להשפיע עליהן. הוראות אלה מעוצבות באופן ספציפי בהתאם למאפיינים המקצועיים הכלכליים והמשפטיים של ההתקשרות, ובכך מבטאות מסגרת ספציפית לטיפול בסיכוני הסייבר.

סעיף 11 מוצע כי הסמכויות שמוצע להקנות בחוק זה לגורם אחראי או לעובד מוסמך של המערך, לא יופעלו כלפי הגופים הביטחוניים, שבהתאם להחלטות הממשלה בתחום הסייבר, אחראים על הגנת הסייבר של עצמם.

כמו כן, הסמכויות כאמור לא יופעלו כלפי הגופים המנויים בפרט (3) בתוספת הראשונה לחוק להסדרת הביטחון – גופים אשר מונחים על ידי הממונה על הביטחון במערכת הביטחון מכוח סעיף 18 לאותו חוק. לנוכח מאפייני הפעילות של גופים אלה ולנוכח החלטות הממשלה בתחום הסייבר, גופים אלה מצויים באחריותו המלאה של הממונה על הביטחון במערכת הביטחון, כולל בהיבטי סייבר, ומוצע כי החוק לא יחול עליהם.

עוד מוצע לקבוע כי החוק המוצע לא יחול של משרדי הממשלה, משום שאין מקום להליכים משפטיים בבית המשפט של מערך הסייבר הלאומי נגד משרדי הממשלה. בנוסף, פעילות משרדי הממשלה בתחום הגנת הסייבר הינה באחריות היחידה להגנה בסייבר ברשות התקשוב הממשלתית.

בהמשך לכך, מוצע כי החוק לא יחול על הכנסת, מערכת בתי המשפט, משרד מבקר המדינה, לשכת נשיא המדינה וועדת הבחירות המרכזית, משום שאין מקום להליך משפטי נגד גופים אלה בידי מערך הסייבר הלאומי.

לעניין פסקה (5) לצד גופים אלה, קיימים ספקים של מערכת הביטחון המספקים רכיבים או שירותים בעלי רגישות ביטחונית החשופים לתקיפות סייבר שעלולות לגרום לפגיעה בביטחון המדינה, ושאינם כלולים בצו שר הביטחון שניתן לפי פרט (3) בתוספת הראשונה לחוק להסדרת הביטחון. זאת בין השאר משום שמדובר בספקים שמשתנים מעת לעת, המבצעים גם פעילות שאינה עבור משרד הביטחון בלבד.

לאחר בחינה של אופן הטיפול בהגנת הסייבר בגופים מעורבים אלה, נקבעו בין המערך לבין הממונה על הביטחון במערכת הביטחון עקרונות לטיפול בהיבטי הגנת הסייבר בגופים אלה. בהתאם לכך, מוצע כי הסמכויות שבחוק המוצע לא יופעלו כלפי גופים אשר נקבע לגביהם, בהסדרה שבין המערך לבין הממונה על הביטחון במערכת הביטחון, כי ניתן להסדיר את הסיכונים לביטחון המדינה בשל תקיפת סייבר נגדם בדרך שבה הם מטופלים כיום, קרי באמצעות הוראות חוזיות הכלולות במסגרת הוראות הרכש של משרד הביטחון. בהתאם לכך, הממונה על הביטחון במערכת הביטחון יהיה אחראי להנחות לבצע, או לבצע בעצמו, פעולות הגנה נדרשות לפי העניין, וזאת מכוח אותם חוזים. בהתאם לכך, במקרים אלה החוק לא יחול, והסמכות תהא נתונה לממונה על הביטחון במערכת הביטחון, בלבד.

סעיף 12 מוצע כי השר הממונה על ביצוע החוק יהיה ראש הממשלה והוא יהיה רשאי להתקין תקנות לביצועו וכן לתקן את התוספת הקובעת את רשימת המאסדרים האחראים על תחומים לעניין הסכמה לפי

סעיף 3.

סעיף 13 מוצע כי ראש הממשלה יוכל לקבוע בתקנות מדרג לפגיעה באינטרס ציבורי חיוני, על מנת לכוון את הפעלת הסמכות לפגיעה ממשית באינטרס חיוני. קביעת המדרג תיעשה לאחר קבלת המאסדר או השר הנוגע בדבר. הסעיף המוצע כולל שיקולים כמותיים ואיכותיים שמטרתם הכוונת שיקול הדעת לגבי הזיקה בין הפעילות לפגיעה ממשית באינטרס ציבורי חיוני.

סעיף 14 החוק המוצע כולל תבחין הפעלת סמכות מחמיר של "פגיעה ממשית באינטרס ציבור חיוני". על הגורם האחראי יהיה להראות רף זה לבית המשפט, בעת הפעלת הסמכות. עם זאת, ועל מנת להגביר את הוודאות ותיאום בין הגורמים השונים, ועד להתקנת תקנות כאמור בסעיף 13, ובהמשך לפעילות מערך הסייבר הלאומי בהתאם להחלטות הממשלה, מוצע כי ראש המערך יקבע מדרג זמני.