

תזכיר חוק

א. שם החוק המוצע

חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023

ב. מטרת החוק המוצע, הצורך בו, עיקרי הוראותיו והשפעתו על הדין הקיים

במסגרת הלחימה המתמשכת מתחוללת עליה בהיקף ובעוצמת מתקפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת בחוסנה של מדינת ישראל באמצעות פגיעה בכלכלה ובתפקודו התקין של המשק. תקיפות סייבר עלולות להוביל לפגיעה בתוך במרחב הסייבר (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.

חברות המספקות שירותים דיגיטליים ושירותי האחסון, כהגדרתם בחוק המוצע, מתאפיינות בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה וגופים ציבוריים, בהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שנגרם מתקיפה כנגד חברות אלו עלול להתפשט ולהשפיע על חברות רבות במשק. בנוסף לזאת, למרות רגישותן וחיבתן המשקית של חברות אלו, אין כיום גורם ממשלתי האמון על הסדרת פעילותן ככל שהדבר נוגע להגנת הסייבר. ככל שחברות כאמור מחזיקות או מעבדות מידע אישי, הרי שקיימת הסדרה של פעילות זו על-ידי הרשות להגנת הפרטיות. בנסיבות אלו, ספקי שירותי האחסון והשירותים הדיגיטליים, מהווים יעד מועדף לתקיפות סייבר. בתקופת הלחימה, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה רחבה בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים.

בהתאם, ביום 27.11.23 אישרה הממשלה פרסום את תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023 שהצעת החוק באה להחליפו.

מוצע כי בהתקיים חשש ממשי לתקיפת סייבר חמורה כנגד ספק שירותי אחסון או שירותים דיגיטליים, קרי – תקיפת סייבר אשר מנהל מוסמך במערך הסייבר, בשירות הביטחון הכללי או במלמ"ב, מצא כי בשל חשש ממשי להיותה בעלת השפעה מהותית שאינה מוגבלת לספק הנתקף ולנוכח מאפייניה, וכן בשל התרחשותה בתקופת הפעולות הצבאיות המשמעותיות יש חשש ממשי שתפגע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, יהיה רשאי עובד מוסמך באחד מבין שלושת הגופים האמורים להודיע לספק על קיומו של חשש כאמור.

בהמשך לכך, ככל שהספק הנתקף לא יפעל באופן הולם ובתוך פרק זמן סביר לטיפול בתקיפת הסייבר החמורה

ולא יגיש תצהיר על עמידתו בתקן כמפורט להלן, יהיה רשאי עובד מוסמך בכל אחד מהגופים האמורים, לפי העניין, לתת לספק הנתקף הוראות לביצוע פעולה לצורך איתור התקיפה, מניעתה או בלימתה וזאת מתוך מטרה להגן על האינטרס הציבורי ולהפחית את מידת הנזק שעלולה להיגרם מתקיפות סייבר חמורות.

ג. להלן נוסח תזכיר החוק המוצע ודברי הסבר

תזכיר חוק מטעם משרד ראש הממשלה:

תזכיר חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה - חרבות ברזל), התשפ"ד-2023

הגדרות

1.

"ידיעה או מסמך" – לרבות העתק חומר מחשב;

"חומר מחשב" ו-"מחשב" – כהגדרתם בחוק המחשבים;

"חוק המחשבים" – חוק המחשבים, התשנ"ה-1995¹;

"חוק להסדרת הביטחון" – החוק להסדרת הביטחון בגופים ציבוריים,
התשנ"ח-1998²;

"מלמ"ב" – הממונה על הביטחון במערכת הביטחון כמשמעותו בסעיף 21 לחוק
להסדרת הביטחון;

"מנהל מוסמך" – אחד מאלה או ממלא מקומו, לפי העניין:

(1) ראש מחלקה בחטיבת איומי סייבר בשב"כ;

(2) ראש מרכז תגובה (IR) במערך הסייבר;

(3) ראש היחידה הטכנולוגית במלמ"ב;

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

"ספק" – אחד מאלה:

(1) מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, ומתקיים
חיבור פיזי או לוגי, קבוע או עתי, או העברת מידע תדירה ממחשבי הספק
למחשבי מקבל שירותיו;

(2) מי שעיסוקו באספקת שירותי תחזוקה, ניהול או בקרה של שירותי
האחסון או שירותים דיגיטליים;

"עובד מוסמך" – כל אחד מאלה:

(1) עובד השירות כהגדרתו בחוק שירות הביטחון הכללי, התשס"ב-2002³
שהוסמך בכתב לעניין חוק זה בידי ראש חטיבת איומי סייבר בשב"כ או מנהל
בשב"כ בדרגת ראש מחלקה הממלא את מקומו;

¹ ס"ח התשנ"ה, עמ' 366.

² ס"ח התשנ"ח, עמ' 348.

³ ס"ח התשס"ב, עמ' 179.

(2) עובד מערך הסייבר שהוסמך בכתב לעניין חוק זה בידי ראש חטיבת ההגנה במערך הסייבר;

(3) עובד מלמ"ב שהוסמך בכתב לעניין חוק זה בידי ראש היחידה הטכנולוגית במלמ"ב, לעניין ספק של הגופים המנויים בפרטים 2 ו-3 לתוספת הראשונה לחוק להסדרת הביטחון;

"פעולה להגנת סייבר בחומר מחשב" – מתן הוראות למחשב לצורך הגנת סייבר, ובכלל זה סריקה, עיבוד, הסרה של חומר מחשב הנוגע לתקיפת סייבר, התקנת סוג תוכנה שפעולתה מוגבלת לרשת הספק בלבד, חסימה או ניתוק של מחשב, או יצירת עותק של חומר המחשב;

"הפעולות הצבאיות המשמעותיות" – הפעולות הצבאיות המשמעותיות שעליהן החליטה ועדת השרים לענייני ביטחון לאומי לפי סעיף 40 לחוק-יסוד: הממשלה והודיעה לגביהן לוועדת החוץ והביטחון של הכנסת ביום כ"ג בתשרי התשפ"ד (8 באוקטובר 2023);

"צה"ל" – צבא הגנה לישראל;

"שב"כ" – שירות הביטחון הכללי;

"שירותי אחסון" – שירותי אחסון של מידע שנמסר לשם העלאתו לרשת האינטרנט, שירותי עיבוד ואחסון נתונים ושירותים לאספקת מידע, תשתית לאחסון או עיבוד נתונים;

"שירותים דיגיטליים" – אחד מאלה:

(1) שירותי תכנה לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח;

(2) שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תכנה וטכנולוגיות תקשורת;

(3) שירותי עיבוד, הזנת או שחזור נתונים, התקנה והגדרת תצורה של מחשבים, התקנת תכנה או שירותי הגנת סייבר;

(4) אספקה או התקנה של מחשבים או של ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי;

"תקיפת סייבר" – פעולה או חשש ממשי לפעולה, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב השמור בו לרבות -

(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 לחומר מחשב כהגדרתה בסעיף 4 לחוק המחשבים ;
- (5) האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט-1979⁴ ;
- (6) גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הוצאתו שלא כדין של מידע על-ידי גורם כאמור ;
- (7) הפרעה או מניעה של חיבור של מחשב לרשת תקשורת ;

"תקיפת סייבר חמורה" – תקיפת סייבר שמנהל מוסמך מצא כי בשל חשש ממשי להיותה בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף ולנוכח מאפייניה, לרבות מתאר התקיפה או זהות התוקף, וכן בשל התרחשותה במהלך תקופת הפעולות הצבאיות המשמעותיות, יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, ובכלל זה תקיפת סייבר שראש חטיבת הגנה בסייבר בצה"ל מצא כי יש בה לפגוע ברציפות התפקוד המבצעי של צה"ל.

2. התמודדות עם תקיפת סייבר חמורה

התעורר חשש ממשי לתקיפת סייבר חמורה כנגד ספק והודיע עובד מוסמך לספק על קיומו של חשש כאמור, לאחר שהזדהה בפניו, יחולו הוראות אלה :

(1) העובד המוסמך יפרט בפני הספק את התשתית העובדתית והמקצועית לקיומו של חשש כאמור, ככל שאין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים ;

(2) העובד המוסמך ייתן לספק הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה או בלימתה בפרק זמן סביר שאין בו כדי לפגוע בטיפול בתקיפת הסייבר החמורה, והכל בהתחשב במאפייני תקיפת הסייבר ;

⁴ ס"ח התשל"ט, עמ' 118.

(3) הספק יעדכן את העובד המוסמך בדבר הפעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה או ימסור לעובד המוסמך תצהיר בנוסח שבתוספת בדבר אספקת שירותי אחסון או שירותים דיגיטליים ללקוחותיו תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations, והכל תוך פרק זמן סביר כאמור בפסקה (2);

(4) לא מסר הספק תצהיר כאמור בפסקה (3) ומצא העובד המוסמך כי הספק הנתקף לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה של תקיפת הסייבר החמורה כאמור בפסקה (2), רשאי העובד המוסמך, ככל שהדבר חיוני לצורך איתור התקיפה, מניעתה או בלימתה, לאחר שהודיע לספק על כוונתו ונתן לו הזדמנות להשמיע את טענותיו, לתת לספק הוראות, בכתב או בעל פה, ובכלל זה הוראות הנוגעות לחומר מחשב שיהיו רק פעולות להגנת סייבר בחומר מחשב, או הוראות למסירת ידיעה או מסמך לידי העובד המוסמך;

(5) במתן הוראות לפי פסקה (4), ישקול העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות, על פעילות הספק ועל צד שלישי, לרבות על העלות הכלכלית המוערכת של יישום ההוראה ועל הרציפות התפקודית של הספק; העובד המוסמך יורה לנקוט אמצעי שפגיעתו פחותה לצורך איתור התקיפה, מניעתה או בלימתה; העובד המוסמך יפרט את המועד האחרון לביצוע ההוראה;

(6) נתקבלה הוראה מעובד מוסמך לפי פסקה (4), יפעל הספק בהתאם לה ועד המועד האחרון שנקבע לביצועה כאמור בפסקה (5), וידווח על אופן ביצועה לעובד המוסמך עד למועד האמור.

עובד מוסמך יתעד בכתב את ההוראות שנתן לספק לפי סעיף 2 וימסור לו נוסח כתוב של ההוראות שאינו מכיל מידע מסווג בתוך פרק זמן סביר ממתן ההוראה; לעניין זה, "מידע מסווג" – מידע שסיווגו הביטחוני נקבע בידי מערך הסייבר, שב"כ, צה"ל או מלמ"ב, לפי העניין, כסיווג ברמת 'שמור' ומעלה.

(א) אדם שקיבל מידע שהתקבל מספק לפי חוק זה ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לצורך איתור תקיפת סייבר חמורה, מניעתה או בלימתה.

תיעוד

.3

סודיות

.4

- (ב) מידע שהתקבל מספק במסגרת פעולה לפי חוק זה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, למעט מידע שקבע מנהל מוסמך שהוא חיוני לזיהוי מאפייני תקיפת הסייבר; מידע שנקבע לגביו כאמור יישמר בהיקף המזערי הנדרש.
- (ג) בחוק זה "מידע" – למעט מידע על התוקף, התקיפה, מאפייני התקיפה או אמצעי הטיפול בה.
5. אופן הפעלת סמכויות
- הפעלת סמכויות כלפי ספק לפי סעיף 2 לעניין תקיפה מסוימת יינתנו בידי עובד מוסמך מקרב גוף אחד בלבד.
6. דיווח
- (א) מערך הסייבר, השב"כ ומלמ"ב ידווחו אחת לשבועיים ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת בדבר המקרים שבהם ניתנו הוראות לספק בהתאם לפסקה 2(4), הנימוק למתן ההוראות וסוגן.
- (ב) דיווח לפי חוק זה יהיה חסוי ופרסומו אסור.
7. תיקון חוק בית משפט לעניינים מינהליים
- בתקופת תוקפו של חוק זה, בחוק בתי משפט לעניינים מינהליים, התש"ס-2000⁵, בתוספת הראשונה, בפסקה 65, במקום "החלטה לפי תקנות שעת חירום (חרבות ברזל)(התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023" יבוא:
- "(65) החלטה של רשות לפי חוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה- חרבות ברזל), התשפ"ד-2023".
8. שמירת דינים
- (א) הוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן.
- (ב) בלי לגרוע מהאמור בסעיף קטן (א), הוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת הממשלה או הסכם, ואולם בכל מקרה של סתירה יגברו הוראות חוק זה.
9. תוקף
- חוק זה יעמוד בתוקף בתקופה שממועד תחילתו ועד חודש לאחר מועד פקיעתה של הכרזה על מצב מיוחד בעורף שתחילה ביום 7 באוקטובר 2023.
10. ביטול תקנות שעת חירום והוראות מעבר
- (א) תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, בטלות.

⁵ ס"ח התש"ס, עמ' 190.

(ב) הוראות שניתנו ופעולות שבוצעו לפי תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023, לפני תחילתו של חוק זה, יראו אותן כאילו נעשו לפי חוק זה והוראותיו יחולו עליהן.

תוספת

(סעיף 2(3))

תצהיר ספק על עמידה בתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations

אני _____, נושא ת.ז. _____, נציג חברת _____, לאחר שהוזהרתי כי עליי לומר את האמת וכי אהיה צפוי/ה לעונשים הקבועים בחוק באם לא אעשה כן, מצהיר/ה בזה בכתב כדלהלן:

1. חברת _____ (להלן – החברה) מספקת ללקוחותיה שירותי אחסון או שירותים דיגיטליים, כהגדרתם בחוק התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל), תשפ"ד-2023, תוך יישום הנחיות אבטחה בהתאם לתקן NIST 800-53 Security and Privacy Controls for Information Systems and Organizations בגרסתו העדכנית ותוך ניהול הסיכונים הרלוונטיים.
2. הגורם הנושא בתפקיד _____ ששמו/ה _____ ת.ז. _____ הוא הגורם המוסמך מטעם החברה לעניין זה.
3. הגורם המוסמך מטעם החברה, כאמור בסעיף 2, יעדכן עובד מוסמך ככל שיחול שינוי בנוגע לאמור בתצהיר זה תוך 7 ימים.

אני מצהיר/ה כי השם דלעיל הוא שמי, והחתימה דלמטה היא חתימתי, וכי תוכן תצהירי זה אמת.

תאריך

חתימה

אישור

אני, _____, עו"ד מרחוב _____ בעיר _____ מאשר/ת בזה כי ביום _____ הופיעה בפניי מר/גב' _____ המוכר/ת לי באופן אישי / שהזדהה/תה בפניי באמצעות תעודת זהות מס' _____, ולאחר שהזהרתיו/ה כי עליו/ה לומר את האמת וכי י/תהיה צפוי/ה לעונשים הקבועים בחוק באם לא י/תעשה כן, אישר/ה את ההצהרה דלעיל וחתם/מה עליה בפניי.

_____ חותמת

_____ חתימה

דברי הסבר

כללי

ביום 7 באוקטובר 2023 פתחו ארגוני טרור במתקפה רצחנית כנגד כוחות הביטחון ואזרחי מדינת ישראל. מתקפה זו גבתה את חייהם של מאות אזרחים ושיבשה את מערך החיים בחזית ובעורף. בעקבות מתקפה זו הכריז שר הבטחון, ביום 7 באוקטובר 2023, על מצב מיוחד בעורף, כהגדרתו בחוק ההתגוננות האזרחית, התשי"א-1951, וועדת השרים לענייני בטחון לאומי החליטה על נקיטת פעולות צבאיות משמעותיות, בהתאם לסעיף 40 לחוק-יסוד: הממשלה, בשל המלחמה שנכפתה על מדינת ישראל ("חרבות ברזל").

במסגרת הלחימה המתמשכת מתחוללת עליה בהיקף ובעוצמת מתקפות הסייבר כנגד גופים אזרחיים במשק הישראלי. מטרת תקיפות סייבר אלו היא לפגוע, כחלק מהמתקפה המשולבת המכוונת בחוסנה של מדינת ישראל באמצעות פגיעה בכלכלה ובתפקודו התקין של המשק. תקיפות סייבר עלולות להוביל לפגיעה בתוך במרחב הסייבר (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.

חברות המספקות שירותים דיגיטליים ושירותי האחסון, כהגדרתם בחוק המוצע, מתאפיינות בחיבוריות גבוהה לגופים רבים במשק הישראלי, לרבות משרדי ממשלה וגופים ציבוריים, בהם גם גופים ביטחוניים, תשתיות מדינה קריטיות וארגונים חיוניים לתפקודו של המשק, ועוד. בשל חיבוריות זו, הנזק שנגרם מתקיפה כנגד חברות אלו עלול להתפשט ולהשפיע על חברות רבות במשק.

בנוסף לזאת, למרות רגישותן וחשיבותן המשקית של חברות אלו, אין כיום גורם ממשלתי האמון על הסדרת פעילותן ככל שהדבר נוגע להגנת הסייבר. ככל שחברות כאמור מחזיקות או מעבדות מידע אישי, הרי שקיימת הסדרה של פעילות זו על-ידי הרשות להגנת הפרטיות.

בנסיבות אלו, ספקי שירותי האחסון והשירותים דיגיטליים, מהווים יעד מועדף לתקיפות סייבר. בתקופת הלחימה, תקיפות סייבר חמורות כנגד ספקים אלה עלולות להביא לפגיעה רחבה בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים.

בהתאם, מוצע כי בהתקיים חשש ממשי לתקיפת סייבר חמורה כנגד ספק שירותי אחסון או שירותים דיגיטליים, קרי – תקיפת סייבר אשר מנהל מוסמך במערך הסייבר הלאומי, בשירות הביטחון הכללי או במלמ"ב, מצא כי בשל חשש ממשי להיותה בעלת השפעה מהותית שאינה מוגבלת לספק הנתקף ולנוכח מאפייניה, וכן בשל התרחשותה בתקופת הפעולות הצבאיות המשמעותיות יש חשש ממשי שתפגע בביטחון המדינה, בביטחון הציבור או בקיום האספקה והשירותים החיוניים, יהיה רשאי עובד מוסמך באחד מבין שלושת הגופים האמורים להודיע לספק על קיומו של חשש כאמור.

בהמשך לכך, ככל שהספק הנתקף לא יפעל באופן הולם ובתוך פרק זמן סביר לטיפול בתקיפת הסייבר החמורה או יגיש תצהיר על עמידתו בתקן כמפורט להלן, יהיה רשאי עובד מוסמך בכל אחד מהגופים האמורים, לפי העניין, לתת לספק הנתקף הוראות לביצוע פעולה לצורך איתור התקיפה, מניעתה או בלימתה.

בנוסף, בכדי להבטיח כי ניתנו רק ההוראות החיוניות להתמודדות עם תקיפת הסייבר החמורה וזאת כאשר פגיעתן בנסיבות העניין היא הפחותה ביותר, מוצע לקבוע את השיקולים שנדרש עובד מוסמך לשקול טרם מתן הוראות לספק. וכמו כן מוצע לקבוע הוראות לעניין שמירת מידע, העברתו ומחיקתו.

נקודת המוצא היא שמרבית הספקים יטפלו באופן הולם בתקיפת הסייבר החמורה, בוודאי בעת מלחמה, וככל שיבקשו אף יינתן להם סיוע והכוונה על ידי הגופים. ברם, החקיקה נועדה לאפשר בזמן החירום הלאומי גם מתן הוראות לספקי שירותים דיגיטליים או שירותי אחסון אשר לא יפעלו כך.

מוצע להסדיר את סמכויות מערך הסייבר הלאומי, שירות הביטחון הכללי או הממונה על הביטחון במשרד הביטחון, לתת הוראות כאמור במסגרת הוראת שעה, שתפקע חודש לאחר פקיעתה של ההכרזה על מצב מיוחד בעורף.

סעיף 1 בסעיף זה מוצע לקבוע הגדרות למונחים בהם נעשה שימוש בחוק המוצע.

מוצע להגדיר "שירותי אחסון" כשירותי אחסון של מידע שנמסר לשם העלאתו לאינטרנט, שירותי עיבוד ואחסון נתונים ושירותים לאספקת מידע, תשתית לאחסון או עיבוד נתונים.

עוד מוצע להגדיר "שירותים דיגיטליים" כאחד מהבאים:

- א. שירותי תכנה לרבות כתיבה, התאמה, שינוי, בדיקה, תמיכה, מחקר ופיתוח;
- ב. שירותי ניהול או הפעלה של מערכות מחשבים המשלבות חומרה, תכנה וטכנולוגיות תקשורת;
- ג. שירותי עיבוד, הזנת או שחזור נתונים, התקנה והגדרת תצורה של מחשבים, התקנת תכנה או שירותי הגנת סייבר;
- ד. אספקת או התקנת מחשבים או ציוד בקרה, המהווים חלק ממכונות וציוד תעשייתי.

החוק המוצע נועד לחול על מי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים, בעיקר בשל היותם

חלק משרשרת האספקה של גופים רבים במשק הישראלי, כאשר החיבוריות הגבוהה של ספקים אלו עלולה להיות מנוצלת על ידי תוקפים לגרימת נזק רחב היקף. על כן, מוצע להגדיר "ספק", לגביו יחול החוק, כמי שעיסוקו באספקת שירותי אחסון או שירותים דיגיטליים וכן מתאפיין בחיבוריות גבוהה כאמור, כלומר אחד מהבאים:

א. ספק שירותי אחסון או שירותים דיגיטליים שמתקיים חיבור פיזי או לוגי, קבוע או עתי בין מחשבו למחשבי מקבלי שירותיו או שמתקיימת העברת מידע תדירה ממחשבו למחשבי מקבלי שירותיו; ב. מי שמספק שירותי תחזוקה, ניהול או בקרה של שירותי אחסון או של שירותים דיגיטליים.

עוד מוצע להגדיר את המונח "עובד מוסמך" אשר יהיה מוסמך ליתן הוראות לפי חוק זה אשר יהיה, לפי העניין, עובד מערך הסייבר הלאומי שהוסמך לכך בכתב על ידי ראש חטיבת ההגנה במערך הסייבר הלאומי; עובד השירות שהוסמך בכתב על ידי ראש חטיבת איומי סייבר שבש"כ או על ידי מנהל בדרגת ראש מחלקה הממלא את מקומו; או עובד מלמ"ב שהוסמך בכתב על ידי ראש היחידה הטכנולוגית במלמ"ב. סמכויות עובד מוסמך במלמ"ב יחולו רק ביחס לספק של הגופים המנויים בפרט 2 ובפרט 3 לתוספת הראשונה לחוק להסדרת הביטחון.

כמפורט לעיל, בהתקיים התנאים לכך, העובד המוסמך יהיה רשאי להורות לספק, בין היתר, לבצע "פעולה להגנת סייבר בחומר מחשב" שתכליתה הגנת סייבר, אשר מוצע להגדיר כדלקמן:

- א. ביצוע סריקה על ידי הספק במחשבו;
- ב. ביצוע פעולות עיבוד על ידי הספק;
- ג. הסרה של חומר מחשב ממחשבי הספק על ידו ובלבד שהוא נוגע לתקיפת הסייבר;
- ד. התקנת סוג תוכנה שפעולתה מוגבלת לרשת הספק בלבד. יובהר, שבהתאם להנחיית היועצת המשפטית לממשלה מספר 1.2500 מיום 10 באוקטובר 2019 שכותרתה "כללים מנחים לגיבוש הסדרים דיגיטליים", לפיה "הסדר דיגיטלי לא יעדיף ככל הניתן אמצעי טכנולוגי אחד על פני אמצעי טכנולוגי אחר, אם שניהם מגשימים את השימושים והמטרות של אותו ההסדר", מוצע לקבוע שהעובד המוסמך יהיה רשאי להורות על התקנת סוג תוכנה ולא על התקנת תוכנה מסוימת, מקום בו יש יותר מתוכנה אחת המגשימה את אותם השימושים והמטרות. זאת ועוד, מתן הוראה מחייבת על ידי עובד מוסמך לפי חוק זה להתקנת תוכנה, תהיה לסוג תכנה שפעולתה מוגבלת לרשת הספק בלבד.
- ה. חסימה או ניתוק של מחשב על ידי הספק יצירת עותק של חומר מחשב על ידי הספק

מוצע להגדיר "תקיפת סייבר" כפעילות או חשש ממשי לפעילות, שנועדה לפגוע שלא כדין בשימוש במחשב או בחומר מחשב, לרבות:

- א. שיבוש פעולתו התקינה של מחשב או הפרעה לשימוש בו;
- ב. מחיקת חומר מחשב, שינויו, שיבושו או הפרעה לשימוש בו;
- ג. אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם;
- ד. חדירה לחומר מחשב כהגדרתה בסעיף 4 לחוק המחשבים;
- ה. האזנת סתר לתקשורת בין מחשבים כמשמעותה בחוק האזנת סתר, התשל"ט–1979;
- ו. גישה של גורם שאינו מורשה למידע השמור במחשב, ובכלל זה בדרך של פגיעה בתהליך הזדהות, או הוצאתו שלא כדין של מידע על-ידי גורם כאמור;
- ז. הפרעה או מניעה של חיבור של מחשב לרשת תקשורת;

כאמור לעיל, הצעת חוק זו מוצעת על רקע צורך מבצעי שהתעורר בתקופת הפעולות הצבאיות המשמעותיות ובכדי למנוע פגיעה בביטחון המדינה, ביטחון הציבור או בקיום האספקה והשירותים החיוניים. על כן מוצע לקבוע, שבכדי שעובד מוסמך יהיה רשאי לתת הוראות לפי חוק זה, לא די בהתקיימותה של תקיפת סייבר, אלא שצריך להתקיים חשש ממשי לתקיפת סייבר חמורה. מוצע להגדיר "תקיפת סייבר חמורה" כתקיפת סייבר שמנהל מוסמך לעניין זה מצא, לרבות על בסיס אינדיקציה מודיעינית או מידע שהספק בחר להעביר לו, שמתקיימים לגביה התנאים הבאים:

א. תקיפת סייבר שקיים חשש ממשי להיותה בעלת השפעה משמעותית שאינה מוגבלת לספק הנתקף, כלומר תקיפה שעלולות להיות לה השלכות על גופים נוספים או על הציבור. תקיפה תוגדר כבעלת השפעה משמעותית כאמור, בין היתר, אם היא עלולה להתפשט במהירות למחשבים רבים או בשל השפעתה האפשרית על עובדי, ספקי או לקוחות הספק (ובכלל זאת, פעילות גופים חיוניים או תשתיות מדינה קריטיות).

ב. התקיפה היא חמורה לנוכח מאפייניה, ובכלל זאת תקיפה המתאפיינת במתאר תקיפה ייחודי, מורכב טכנולוגית או חדש, או בשל זהות התוקף.

ג. תקיפת הסייבר מתרחשת במהלך תקופת הפעולות הצבאיות המשמעותיות ובשל כך יש חשש ממשי שיש בה כדי לפגוע בביטחון המדינה, ביטחון הציבור או בקיום האספקה והשירותים החיוניים, לרבות תקיפת סייבר שרח"ט הגנה בסייבר בצה"ל מצא כי יש בה לפגוע ברציפות התפקוד המבצעי של צה"ל.

כמו כן, מוצע לקבוע שמידע שיתקבל לפי חוק זה יימחק בסמוך לאחר סיום הטיפול בתקיפת הסייבר החמורה, למעט מידע על התוקף, התקיפה, מאפייני התקיפה, או אמצעי הטיפול בה או מידע אחר שקבע מנהל מוסמך שהוא חיוני לזיהוי מאפייני תקיפת הסייבר; מידע כאמור יישמר בהיקף המזערי הנדרש. לצורך כך, מוצע לקבוע המנהל המוסמך במס"ל יהיה ראש מרכז תגובה (IR), המנהל המוסמך במלמ"ב יהיה ראש היחידה הטכנולוגית במלמ"ב והמנהל המוסמך בשב"כ יהיה ראש מחלקה בחטיבה לאיומי סייבר בשב"כ.

סעיף 2

מוצע לקבוע שאם התעורר חשש ממשי לתקיפת סייבר חמורה יהיה עובד מוסמך רשאי, לאחר שהזדהה בפני הספק, להודיע לו על קיומו של חשש כאמור. בהודעה יפורטו בפני הספק התשתית העובדתית והמקצועית לקיומו של חשש כאמור, ככל שאין בכך כדי לחשוף מקורות מידע, שיטות או אמצעים.

במסגרת האמור, מוצע, כי לאחר מתן ההודעה לספק על קיומו של חשש לתקיפת סייבר חמורה כאמור, תינתן לו הזדמנות לפעול באופן הולם לצורך איתור התקיפה, מניעתה, לרבות מבעוד מועד או מניעת הישנותה, או בלימתה לאחר שהחלה, והכל בתוך פרק זמן סביר שאין בו כדי לפגוע בטיפול בתקיפת הסייבר החמורה. בהמשך לכך, הספק יידרש, לעדכן את העובד המוסמך בדבר פעולות שביצע לצורך איתור התקיפה, מניעתה או בלימתה, וזאת מבלי שתחול עליו חובה לגלות במסגרת העדכון סוד מסחרי. לחלופין, באפשרות הספק למסור תצהיר, כמפורט בתוספת, בדבר יישום הנחיות אבטחה בהתאם לתקן הבינלאומי NIST 800-53 Security and Privacy Controls for Information Systems and Organizations. מדובר בתקן בין-לאומי מקצועי הנותן מענה לתקיפות בעלות רמת מורכבות ועוצמה גבוהה אשר שחקני תקיפה מתקדמים, עתירי משאבים ונחשבים (APT), עשויים לעשות בהן שימוש ובכלל האמור כולל הוראות שיש בהן כדי להביא לצמצום משמעותי של התקיפה מהספק הנתקף למקבלי השירות. התקן כולל הוראות שיש בהן כדי להביא לצמצום משמעותי של

התקיפה מהספק הנתקף למקבלי שירותיו, הוא התקן מכיל, בין היתר, בקרות ברזולוציה מפורטת, וכולל, בין השאר, הוראות לעניין ניטור עצמי רציף של חברות, עמידה ברמת הגנה בסייבר והתמודדות עם אירועים. מדובר בתקינה מוכרת ונגישה, וניתן למצוא מידע אודותיה באתר מכון התקנים האמריקאי. על מנת להנגיש את המידע ביתר קלות, תתווסף הפנייה לתקן זה באתר מכון התקנים האמריקאי באתר מערך הסייבר הלאומי. יודגש, כי לא יינתנו הוראות מכוח חוק זה לספק אשר מסר תצהיר כאמור ובמקרה כזה הספק גם לא יהיה מחויב למסור עדכון על אופן הטיפול בתקיפת הסייבר החמורה שלגביה התריעו בפניו.

בהתאם למוצע, אם לא הגיש הספק תצהיר בדבר אבטחה בהתאם לתקן כאמור ואם מצא העובד המוסמך כי הספק הנתקף לא פעל באופן הולם לאיתור התקיפה, מניעתה או בלימתה, יהיה רשאי העובד המוסמך להודיע לספק על כוונתו לתת לו הוראות, ולספק תינתן הזדמנות להשמיע את טענותיו לעניין הכוונה לתת לו הוראות מחייבות. החוק המוצע אינו מבקש לצמצם את האפשרות של מס"ל, שב"כ או מלמ"ב לפעול לסייע לספקים בהסכמתם בכל דרך אחרת שאינה מפורטת בחוק, אלא רק לקבוע תנאים למתן הוראות מחייבות.

לאחר שמיעת הספק, אם לא השתכנע העובד המוסמך אחרת, יהיה רשאי לתת לספק הוראות, בכתב או בעל פה, ככל שהדבר חיוני לצורך איתור התקיפה, מניעתה או בלימתה. במסגרת סמכותו לפי סעיף זה, מוצע שהעובד המוסמך יהיה רשאי לתת לספק הוראות, ובכלל זה הוראות הנוגעות לחומר מחשב שיהיו רק פעולות להגנת סייבר בחומר מחשב, או הוראות למסירת ידיעה או מסמך, לרבות עותק חומר מחשב, לידי העובד המוסמך;

מוצע להתוות את שיקול הדעת של העובד המוסמך ולקבוע שבמתן הוראות ישקול העובד המוסמך את השפעתן האפשרית על הזכות לפרטיות של כל מי שמידע אודותיו מצוי בידי הספק, בכלל זה מידע על לקוחות ועובדים, ועל פעילות הספק, ובכלל זה על הערכת העלות הכלכלית של יישום ההוראה ועל הרציפות התפקודית של הספק. כמו כן, מוצע להדגיש את חובת העובד המוסמך לפעול במידתיות ולקבוע שהוא יורה לנקוט באמצעי שפגיעתו פחותה לצורך איתור התקיפה, בלימתה או מניעתה. במסגרת חובה זו, העובד המוסמך ימנע מפעולות לזיהוי האנשים שאודותיהם המידע שיקבל מהספק, ככל שהדבר אינו חיוני לצורך איתור התקיפה, מניעתה או בלימתה. יובהר בהקשר זה שבמרבית המקרים, המידע המתקבל הוא מידע טכנולוגי שאינו מכיל מידע אישי.

בנוסף, מוצע בפסקה (5) לקבוע שבעת מתן ההוראה לפי פסקה (4) העובד המוסמך יפרט את המועד האחרון לביצועה. עד למועד זה הספק יפעל בהתאם להוראה שקיבל וידווח על אופן ביצועה לעובד המוסמך.

סעיף 3 מוצע לקבוע עוד שהעובד המוסמך יתעד בכתב את ההוראות שניתנו על ידו לספק וימסור לספק נוסח כתוב של ההוראות שאינו מכיל מידע מסווג בתוך פרק זמן סביר ממתן ההוראה. המסמך המפרט את ההוראות שניתנו יוכל לשמש את הספק לכל צורך שימצא לנכון.

סעיף 4 על מנת להגן על הזכות לפרטיות ולקניין של הספקים ולקוחותיהם, מוצע לקבוע שכל שאדם קיבל מידע שהתקבל מספק לפי חוק זה, הוא ישמור אותו בסוד, לא יגלה אותו לאחר ולא יעשה בו כל שימוש, אלא לצורך איתור תקיפת סייבר חמורה, מניעתה או בלימתה. חובה זו לא תחול ביחס למידע על תוקף, תקיפה (לרבות זהות הנתקף), מאפייני תקיפה או אמצעי טיפול בה. החרגה זו נועדה לאפשר, במקרים הנדרשים, שימוש

או פרסום לציבור של מידע, טכנולוגי בעיקרו, למניעת תקיפות דומות נוספות.

כמו כן, מוצע לקבוע שככל שיתקבל מידע במסגרת פעולה לפי חוק זה באחד הגופים, המידע ימחק בסמוך לאחר סיום הטיפול בתקיפת סייבר חמורה. מוצע להחריג מחובת מחיקת המידע האמורה מידע הנוגע לתוקף, לתקיפה, למאפייני התקיפה או לאמצעי הטיפול בה, וזאת בכדי לאפשר שימוש במידע זה להגנת מרחב הסייבר הישראלי. יובהר בהקשר זה, כפי שצוין גם לעיל, שבמרבית המקרים, המידע המתקבל הוא מידע טכנולוגי שאינו מכיל מידע אישי או סודות מסחריים. כמו כן, מוצע לקבוע שלמנהל מוסמך בכל אחד מהגופים תהיה סמכות לקבוע שיש לשמור מידע אחר אם מצא שהוא חיוני לזיהוי מאפייני תקיפת סייבר. עוד מוצע להתוות את שיקול הדעת של העובד המוסמך והמנהל המוסמך ולקבוע שמידע ישמר בהיקף המזערי הנדרש.

סעיף 5 מוצע לקבוע כי הוראות לספק לעניין תקיפה מסוימת יינתנו על-ידי עובד מוסמך מקרב גוף אחד בלבד, על מנת למנוע מצב שבו ספק נדרש לעמוד בקשר, לתת דין וחשבון או למלא אחר הוראות מצד גורמים ממשלתיים שונים, ביחס לאותו עניין.

סעיף 6 לשם קיום פיקוח ובקרה שוטפים על פעולותיהם של מס"ל, שב"כ ומלמ"ב לפי חוק זה, מוצע לקבוע חובת דיווח אחת לשבועיים ליועצת המשפטית לממשלה ולוועדת החוץ והביטחון של הכנסת בדבר המקרים בהם ניתנו הוראות לספק לפי פסקה (4)2, הנימוק למתן ההוראות וסוגן. לנוכח מהות המידע ואופיו הרגיש, מוצע לקבוע שדיווחים כאמור יהיו חסויים ופרסומם אסור.

סעיף 7 בכדי לאפשר ביקורת שיפוטית ונגישות לערכאות ביחס להוראות שייתן עובד מוסמך לספק, מוצע להסמיך את בית המשפט לענינים מינהליים לדון בעתירות בעניין החלטות לפי חוק זה.

סעיף 8 למען הסר ספק, מוצע לקבוע בסעיף שמירת דינים שהוראות חוק זה באות להוסיף על הוראות כל דין אחר ולא לגרוע מהן. עוד מוצע להבהיר, שהוראות חוק זה באות להוסיף על כל הוראה בעניין הנוגע להגנת סייבר, לפי החלטת ממשלה או הסכם, ואולם בכל מקרה של סתירה יגברו הוראות חוק זה.

סעיף 9 חוק זה נועד לאפשר התמודדות עם העלייה בהיקף ועוצמת מתקפות הסייבר אגב הלחימה המתמשכת בגינה הוכרו מצב מיוחד בעורף. בהתאם, מוצע לקבוע שחוק זה יעמוד בתוקף בתקופה שממועד תחילתו ועד חודש לאחר מועד פקיעתה של הכרזה על מצב מיוחד בעורף. לאור החשש מהמשך המתקפה במימד הסייבר גם לאחר סיום המצב המיוחד בעורף, מוצע לקבוע חודש נוסף לתוקף החוק. החשש הוא שככל שתוקפים מתקדמים יבססו תשתית לתקיפת סייבר חמורה הם יבחרו להוציאה לפועל גם סמוך לאחר סיום הלחימה, כפי ראינו בסבבי לחימה קודמים במימד הלחימה הקינטי.

סעיף 10 הוראות חוק זה נועדו להחליף את הוראות תקנות שעת חירום (חרבות ברזל) (התמודדות עם תקיפות סייבר חמורות במגזר השירותים הדיגיטליים ושירותי האחסון), התשפ"ד-2023. לפיכך, מוצע לקבוע כי עם תחילתו של החוק המוצע, הן יבוטלו. לצד ביטול תקנות שעת החירום, וכדי לאפשר ביצוע פעולות שאושרו מכוח תקנות אלה ולהחיל את הוראות החוק המוצע על ההוראות שניתנו והפעולות שבוצעו לפני תחילתו של חוק זה, מוצע לקבוע כי יראו הוראות שניתנו ופעולות שבוצעו כאילו נעשו לפי חוק זה והוראותיו יחולו עליהן.

