הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי

גבי סיבוני

מבוא

התפתחותן של מערכות המחשוב והתקשורת בעשורים האחרונים השפיעה על הביטחון הלאומי של מדינות, ובכללן של מדינת ישראל. מערכות אלו ותפוצתן הגלובלית גרמו למדינות להיות חשופות לפגיעה במרחב הקיברנטי שלהן על ידי גורמים שונים ומגוונים, בהם מדינות עוינות, ארגוני טרור, גורמים פליליים ואף פרטים הפועלים מתוך אתגר אישי או מתוך מניעים אנרכיסטיים. רוב המערכות בחברה מפותחת תלויות בתשתיות מחשוב ומידע, והתלות בטכנולוגיות אלו גורמת לכך שפגיעה במחשבים ובתהליכי זרימת מידע עלולה לשבש, לשתק ולעיתים אף לגרום לפגיעות פיזיות של ממש במערכים חיוניים. כך, למשל, ניתן לשבש מערכות ניהול, שליטה ובקרה באמצעות שינויים בתוכנת המחשב, ללא צורך בתקיפה פיזית שלהן. ניתן להעריך כי פני העימותים בעתיד ישתנו ללא הכר ויתבססו במידה רבה על לוחמה קיברנטית.

עוצמתה של מדינה נמדדת על ידי שילוב בין העוצמה הכלכלית, החברתית והמדעית שלה ובין העוצמה הצבאית. תפקידה של העוצמה הצבאית הוא להגן על האזרחים והטריטוריה כדי שאלה יוכלו לשמר ולפתח את העוצמה הכלכלית. פגיעותו של המרחב הקיברנטי לתקיפות באמצעות מערכות תקשורת ומחשבים, מביאה לשינוי דרמטי במשוואה זו. לראשונה ניתן לפגוע אנושות בעוצמה הכלכלית של מדינות על ידי שיתוק מערכים כלכליים ואזרחיים שלהן, ללא הפעלת כוח אש ותמרון כוחות. יכולות המדינות לפעול במרחב הקיברנטי, הן לצרכי הגנה והן לצרכי מתקפה, יתפסו בעתיד, קרוב לוודאי, מקום משמעותי לצד היכולות הצבאיות הקלאסיות.

אל"מ (מיל.) ד"ר גבי סיבוני הוא ראש תכנית המחקר צבא ואסטרטגיה והתכנית לחקר לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית

בצד קִדמה, רווחיות ורווחה שאפיינו מדינות רבות בעשורים האחרונים, נחשפו בשנים האחרונות אותן מדינות, ובכלל זה גורמי הייצור ואספקת השירותים הלאומיים בהן, לאיומים חדשים, שטרם ניתנה הדעת כיצד ראוי להתמודד עימם. עד לפני שנים לא רבות התעשייה (הפרטית והציבורית) הייתה מוגנת על ידי המדינה. כך, למשל, תחנת כוח ליצור חשמל, בין אם הייתה בבעלות פרטית ובין אם הייתה בבעלות ציבורית, הייתה חשופה לפגיעה פיזית שלא בגין תאונה רק באם המדינה הייתה נקלעת למלחמה פיזית של ממש. תפקידה של המדינה היה להבטיח את ההגנה על התשתיות, המוסדות הכלכליים, מפעלי תעשייה ועוד. מוסדות ציבוריים היו מוגנים על ידי המדינה מעצם קיומם במרחב הטריטוריאלי הנתון למרותה ושליטתה.

מדיניות ההפרטה שצברה תאוצה בעשורים האחרונים הפקידה בידיים פרטיות חלקים נרחבים ממפעלי התשתית שבאופן מסורתי היו בידי הריבון: תקשורת, תחבורה, חשמל, אנרגיה, תעשיות כבדות ועוד. לצידן של התעשיות המסורתיות עלו וצמחו תעשיות חדשות בתחומי הטכנולוגיה העילית, המהוות מרכיב נכבד בתל"ג של מדינות רבות.

בשל ההבנה האוניברסלית כי "המגן על הכל אינו מגן על כלום",[1] פיתחו מדינות שונות דרכים להגן בעיקר על התשתיות והמערכות הקריטיות לתפקודן. במדינת ישראל הוקמה בשנת 2002 הרשות הממלכתית לאבטחת מידע, ה"מופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה".[2] בהקשר זה הוקמה ועדת היגוי במועצה לביטחון לאומי, שתפקידה לבחון את סיכוני אבטחת המידע, ונקבע כי הכללים שתקבע יחולו על כמה גופים ומוסדות שמערכות המידע שלהם הוגדרו כקריטיות, בהם חברת החשמל, בנקים, משרדי ממשלה וכדומה. הוועדה גם הוסמכה להחליט על הוספת גופים לרשימה זו מעת לעת.[3]

הגופים בשירות הציבורי הנדרשים להגנה מפני התקפה קיברנטית נמצאים זה מכבר תחת הנחיית הרשות לאבטחת מידע. עם זאת, התפתחויות במבנה הכלכלה הישראלית הביאו לכניסה של גורמים, תהליכים, נכסים ופרויקטים חדשים, שפגיעה בהם היא בעלת פוטנציאל נזק משמעותי ברמה הלאומית. מצב זה חושף ומגדיל באופן קבוע את מגוון התורפות והמטרות לתוקפים במרחב הקיברנטי. לאור זאת, קיימת חשיבות רבה ליכולת לזהות ולבחון את הגורמים הנוספים שפעילותם מחייבת הנחיה של הרשות לאבטחת מידע.

לא תמיד ניתן לכַמֵת נזק אפשרי זה רק להיבטים הכספיים שלו או להשפעתו על התל"ג. נזקים משמעותיים יכולים להיגרם גם לנכסים וערכים בעלי חשיבות

לאומית. כך, לדוגמה, בארצות הברית תוכניות ההגנה מופעלות גם על אתרי מורשת וזיכרון.[4]

מאמר זה מבקש להציע גישה שתאפשר לקיים תהליך שיטתי, תוך שימוש בכלים סטטוטוריים קיימים, בעזרתו ניתן יהיה לזהות גופים נוספים (בעיקר מהסקטור הפרטי) שפגיעה בהם עלולה להשפיע על הביטחון הלאומי, ולחייבם להפעיל מנגנוני הגנה מתאימים על הנכסים והתשתיות הקריטיות שלהם.

על מה להגן?

במסמך של המשרד האמריקאי לביטחון פנים סוקר פטריק בֶּגְס[5] כיצד רואים הגורמים המוסמכים בארצות הברית את מערך התשתיות והמשאבים הקריטיים להגנה ואת הממשק של אלה עם מערך התשתיות הקיברנטיות והפיזיות.

מיפוי התשתיות הקריטיות להגנה בארצות הברית כולל את התחומים הבאים: מים, אנרגיה, תקשורת, תחבורה, תעשייה כימית, חקלאות ותעשיית מזון, מערכות מידע, בנקאות ושירותים פיננסיים ומסחריים, שירותי בריאות, ולבסוף נכסים בעלי חשיבות לזיכרון הלאומי האמריקאי (אנדרטאות, אתרי מורשת וכדומה). תחומים אלה נשענים על שני מרכיבי תשתית בסיסיים: הראשון נוגע למרכיבי התשתית הפיזית דוגמת תחנות כוח, סכרים, נמלי ים ואוויר, כבישים, מסילות ברזל, תשתיות הולכה למיניהן,[6] בתי חולים, מפעלים ועוד. המרכיב השני נוגע לתשתיות הקיברנטיות, בהן: מערכות תוכנה, חומרה, שרתי אינטרנט, מערכות שליטה ובקרה ושירותי מידע.

כדי לאפשר את הבסיס המתאים לגיבוש תוכניות הגנה, מפעיל המשרד האמריקאי לביטחון פנים מתודולוגיה בשם "סקירת עמידות קיברנטית"[7] של גופים ותשתיות קריטיות השייכים לסקטורים שתוארו לעיל. גישה זו מאפשרת לגבש תמונת מצב לגבי מספר היבטים, בהם: הגדרת נכסים קריטיים להגנה, ניהול התקשורת, מרכיבי המשכיות השירות, ניהול טכנולוגי, היקף התלות במרכיבים חיצוניים, ניהול אירועים ותאונות, יכולת הערכת מצב, איתור וניהול תורפות ועוד. כתוצאה מסקירה זו, יכולים מקבלי ההחלטות לקבל תמונת מצב ולגבש תוכנית פעולה לשיפור העמידות הקיברנטית של הארגון.

משאותר הארגון או הגוף שעליו יש להפעיל את המתודולוגיה, התהליך הינו שיטתי וסדור. הבעיה היא שאנו חסרים עדיין את הדרך בה ניתן לאתר את הגופים והארגונים שיידרשו לתהליך זה.

המצב בישראל דומה למדי. הרשות לאבטחת מידע מביאה מעת לעת לאישור ועדת ההיגוי במטה לביטחון לאומי (המועצה לביטחון לאומי לשעבר) רשימה של גופים נוספים שיידרשו להעמיק את הגנתם ולעמוד בהנחיות האבטחה של

הרשות, אולם אין בנמצא תהליך סטטוטורי שיטתי ומחייב שיאפשר איתורם של גופים כאלה.

העובדה כי תחום או סקטור המהווה תשתית קריטית מורכב ממספר רב של גופים ומערכות (מאות ולעיתים אלפים), גורמת לכך שאין משמעות להגנה על הסקטור ככזה. הביטוי בפועל של ההגנה נוגע לפעולות הנעשות על ידי ארגונים, חברות, מתקנים ותהליכים ספציפיים השייכים לאותו סקטור. השאלה הנשאלת היא כיצד ניתן לאתר את הגופים האלה, במיוחד כאשר כמעט לכל חברה עסקית או משרד ממשלתי ממשק עם הסקטורים המוגדרים במסגרת התשתיות הקריטיות להגנה. לדוגמה: הגנה על תשתיות אספקת המים ואיכותם בישראל אינה נוגעת רק לתהליכים בחברת "מקורות", כי אם גם לעשרות ספקי מים אחרים, אגודות, תאגידי מים, מתקני התפלה והולכה, מתקני טיפול בשפכים, מתקני טיפול והולכת קולחים ועוד. חלק גדול של מתקנים אלה מופעל על ידי יזמים פרטיים, שההפעלה של מנגנוני הגנה אינה בראש מעייניהם. המצב הזה חל גם על תחומים רבים נוספים.

זאת ועוד, במקרים רבים יש להגן גם על מערכות משיקות וקשורות לגורמים המוּנְחים. להלן דוגמה הממחישה היבט זה: מפעל תעשייתי שנקבע כי הוא מהווה מרכיב חיוני פועל תחת ההנחיה של הרשות לאבטחת מידע. לעיתים מפעל זה תלוי בפעולתו ביצרנים אחרים ("יצרני לוויין" קטנים יותר) המספקים תשומות (לעיתים קריטיות) לתהליך הייצור של המפעל המוגן. במקרים רבים נמצא כי חלק מ"גורמי לוויין" אלה אינם נכללים בקבוצת התשתיות הקריטיות להגנה, ולכן אינם מפעילים תהליכי הגנת מידע מסַפקים. כך, יתכן כי פגיעה קיברנטית בגורמים אלה עלולה לגרום לנזקים משמעותיים במפעל המוגן.

השימוש בטכנולוגיות מידע בישראל הוא נרחב מאוד, הן בסקטורים הציבוריים והן בסקטורים הפרטיים. ישראל מספקת, אפוא, כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי. לכן, איתור גופים נוספים, שפעילותם מחייבת הנחייה של הרשות לאבטחת מידע, הינו מטלה חיונית לצורך בניית מערכת הגנה אופטימאלית. סקרים הנערכים מעת לעת ומידע המועבר ממשרדי הממשלה השונים חיוניים בתהליך זה אולם אינם מספקים. יש ליצור תהליך מובנה שיאפשר שיפור משמעותי, בעיקר בכל הקשור למיזמים מסוימים בסקטור הפרטי החשופים לפגיעה קיברנטית, אשר השפעתה עלולה להיות רחבה ואף להגיע לרמה הלאומית.

התהליך המוצע: שימוש בכלים סטטוטוריים קיימים

עיקרי ההצעה לשיפור המצב שתואר לעיל נוגעים להכנסת תחום ההגנה הקיברנטית כמרכיב מובנה בתהליך הסטטוטורי הקיים, וזאת הן בשלבי ההקמה של מיזם (אישורו בוועדות התכנון השונות) והן בתהליך התפעול שלו (חוק רישוי עסקים). מוצע, כי במסגרת תהליכי התכנון במדינה יידרש כל מיזם המוגש

לאישור בוועדות התכנון להגיש תסקיר עמידות קיברנטית. תסקיר זה יהווה הכלי הסטטוטורי העיקרי לצורך איתור ובחינת חשיפתו של המיזם לאפשרות של התקפות קיברנטיות ולגיבוש תהליכי הגנה נגד חשיפות אלו. התסקיר גם יספק לרשות לאבטחת מידע כלי לאיתור וניהול מערך התשתיות הקריטיות להגנה במדינה. לצד זאת, תוכל הרשות הרלוונטית הממונה על רישוי המיזם – רישוי המחייב חידוש עיתי – לבדוק את העמידה המתמשכת של הגוף הנבחן בהוראות ההגנה הקיברנטית.

כדי להסביר הצעה זו יש להרחיבה ולפרטה. הקמה של כל מיזם במדינת ישראל, ובכלל זה מיזמי תשתיות לאומיות, מחייבת עמידה בתהליכי התכנון הסטטוטורי הנוהג בישראל. כך, מיזמים הכרוכים בבניית מתקנים ומבנים מחויבים לקבל את אישורן של ועדות התכנון השונות בהתאם לעניין: מקומיות, מחוזיות וארצית. הבדיקה של מסמכי התכנון המוגשים לאישור הגורם התכנוני בישראל הינה כלי הבקרה המרכזי של הרשויות על מיזמים אלה. במסגרת המסמכים המוגשים לבחינת ועדות התכנון כיום, ניתן למצוא מסמכים הנוגעים לכיבוי אש, להיבטים של בריאות הציבור, להיבטים סביבתיים, לטיפול בחומרים מסוכנים, להגנת העורף ועוד. מסמכים אלה מגדירים את הצעדים אותם ינקוט היזם כדי לעמוד בדרישות המתחייבות בכל תחום. אלה עוברים לבקרת גורמי הרגולציה המוסמכים, המפעילים מומחים שתפקידם להביא לכך שבסופו של התהליך יוכל המיזם להיות מוקם והאינטרס והביטחון הציבורי בתחומים השונים נשמרים.

במדינת ישראל נדונים מדי שנה עשרות מיזמים, שפגיעה בהם עלולה לפגוע בביטחון הלאומי. לדוגמה: מתקני תשתית, מתקני טיפול במים ובשפכים, מערכות הולכה, פרויקטים תחבורתיים, מתקני אנרגיה ותקשורת. לצד אלה נדונים הרחבות והקמות של מפעלי תעשייה ועוד מגוון רחב מאוד של פרויקטים שונים. פגיעה קיברנטית בפרויקטים ובמיזמים אלה, או בחלקם, עלולה לגרום נזק לכלכלת המדינה לא רק בצורה ישירה, כגון היעדר יכולת לספק שירות חיוני, אלא גם בצורה של פגיעה מסחרית ביכולת של חברות ישראליות שהותקפו לספק את מוצריהן למשך זמן נתון.

אחת הדוגמאות שיש בהן כדי לבאר את התהליך המוצע הינה הדרישה להגיש תסקיר השפעה על הסביבה. מטרתו של התסקיר הינה לאתר ולבחון את המִפגעים הסביבתיים העלולים להיגרם כתוצאה מהקמת המיזם ואת הדרכים למזער פגיעה זו לרמה נסבלת. הגשתו של התסקיר מעוגנת בתקנות התכנון והבנייה (משנת 1982, ובגרסתן הסופית משנת 2003). מקורו של התסקיר הינו בהתעוררות המודעות הציבורית בארצות הברית לנושאים הסביבתיים, אשר הביאה בשנת 1970 לחקיקת חוק המחייב הכנה של תסקירי השפעה על הסביבה כחלק מהתהליך התכנוני שם.

לצד המרכיב התכנוני למיזמים חדשים ניתן, כאמור, לעשות שימוש גם בתהליך רישוי העסקים המחייב חידוש עיתי, כדי לוודא שפעלת המיזם לאורך שנים עומדת בקריטריונים מתחייבים בתחומים שונים, כולל בתחום האבטחה מפני התקפה קיברנטית. שופט בית המשפט העליון לשעבר, מישאל חשין, קבע באחד מפסקי דינו: "מטרתו של החוק [לרישוי עסקים] היא לשמור ולהגן על ערכים שונים הנתפסים בחברתנו כערכים חשובים... כך הוא הערך של שלום הציבור, כך הוא הערך של שמירה על בריאות הציבור ובטיחותו, כך הוא הערך של שמירה על איכות הסביבה ואיכות החיים... להגנה על מטרות [ה]חברה..."[8] מדברי השופט חשין ניתן להסיק כי הכלים אותם מספק חוק רישוי עסקים ניתנים לשימוש גם לצורך הגנה קיברנטית וכי זו עולה בקנה אחד עם מטרותיו. בכך הם מאפשרים כלי בקרה חוקי נוסף בידי הרשות לאבטחת מידע, שבאמצעותו היא תוכל לוודא כי גם מיזמים קיימים יעמדו בקריטריונים מתחייבים, ובמקרים מסוימים אף לדרוש מבעלי עסקים פרטיים להגיש תסקיר עמידות קיברנטית ולחייבם למלא אחר הנחיות הביטחון.

כאמור לעיל, מיזמים בתהליך הקמה, ובמקרים מסוימים כאלה שכבר הוקמו, יידרשו על פי ההצעה להגיש תסקיר עמידות קיברנטית לבחינת הרשות לאבטחת מידע, כדי שזו תוכל לוודא שהוראות הגנה חיוניות מתקיימות. ניתן להציע כמה קווים מנחים לתוכנו של תסקיר זה, כמו גם לגורמים שיוסמכו לערוך אותו ולהגישו, וכן לגורמים שיוסמכו לבדוק אותו. מבחינה סטטוטורית, תחולת התסקיר צריכה להיות גורפת ועליה לחול על כל הבקשות, אלא אם ניתן לכך פטור מהגורם המוסמך. אולם מבחינה מעשית, תידרש הרשות לאבטחת מידע לקבוע אמות מידה שיגדירו את המיזמים והפרויקטים שלגביהם תתקיים חובת הגשת התסקיר. אמות מידה אלו יוכלו להתייחס למספר מרכיבים, כמו גודלו של המיזם, הסקטור אליו הוא משתייך (לדוגמה, מיזם הפועל בסקטור האנרגיה, גז טבעי וכדומה), הממשקים של מיזם זה עם גורמים הנמצאים כבר תחת הנחיית הרשות לאבטחת מידע, והיבטים שונים הנוגעים לתחולת הנזק של תקיפה קיברנטית על הגוף.

משהוחלט כי על גוף להגיש תסקיר עמידות קיברנטית, יופעל התהליך לאור אבני הדרך הבאות:

א. **הנחיות לתסקיר** – הרשות לאבטחת מידע תהיה אחראית להכין הנחיות לביצוע התסקיר. על הנחיות אלו להיות מותאמות למיזם או לגוף הקונקרטי. מוצע כי ההנחיות יכללו כמה מרכיבים, בהם: מיפוי פוטנציאל הנזק כתוצאה מתקיפה קיברנטית; מיפוי תורפות המיזם או התוכנית; הוראות שיאפשרו מזעור החשיפה והנזק.

ב. **הכנת התסקיר** – התסקירים יוכנו באחריותו ובמימונו של היזם. לצורך הכנה זו ייעשה שימוש ביועצים שייבחרו מתוך קבוצת יועצים ייעודיים שיוכשרו

ויוסמכו על ידי הרשות לאבטחת מידע. יועצים אלה יפעלו לאור ההנחיות להכנת התסקיר.

ג. **בדיקת התסקיר** – בדיקת התסקיר תבוצע באחריות הרשות לאבטחת מידע. גם כאן תוכל הרשות לעשות שימוש ביועצים חיצוניים שיוכשרו ויוסמכו לבדיקה של תסקירים. עלות הבדיקה תוכל להיות מוּחלת על היזם. בתהליך זה ייתכנו מספר מעגלי הערות ותשובות בין גורמי הרשות לאבטחת מידע ובין הנבדק.

ד. **אישור התסקיר** – בחינה ואישור התסקיר ייעשו על ידי הגורמים המוסמכים ברשות לאבטחת מידע, שגם תקבע את המשך הנחיית הגוף שמסר את התסקיר. אישור זה גם יוכל להתייחס להיבטים הנוגעים להתניות לרישוי העסק, כמו גם להוראות שיש להחיל על תוכניות היזם.

כאמור, השימוש בחוק רישוי עסקים מהווה פלטפורמה מתאימה ליישום הוראות והנחיות בתחום ההגנה מפני מתקפה קיברנטית. עם זאת, בשל מגבלות החלות על כל הקשור לביטחון וזליגה של מידע, נדרש יהיה להגדיר תהליך זה כתהליך ממודר, שאינו פתוח לציבור הרחב אלא רק לגורמים מוסמכים.

סיכום

האיומים על חברות אזרחיות גדלים והולכים, לא רק בשל היכולות לתקוף אותן על ידי מתחרים עסקיים אלא גם בשל החשיפה שלהן לתקיפות של גורמים עוינים. גורמים אלה מזהים את פוטנציאל הנזק לתשתית הכלכלית של המדינה, הגלום בפגיעה בחברות אלו.

מדינות נוטות להגן בעיקר על גופים להם זיקה ישירה לביטחון הלאומי. עם גופים אלה ניתן היה למנות עד לא מכבר בעיקר את משרדי הממשל, גופי מודיעין וביטחון, חברות העוסקות בייצור ביטחוני רגיש ומסווג, תשתיות קריטיות קלאסיות דוגמת חשמל, מים, תחבורה וכדומה. ההיגיון שהגדיר מי זכאי להיכנס לרשימה זו נגזר מהתפיסה האסטרטגית הקלאסית – רשימת התשתיות הלאומיות המוּעדות לפורענות במקרה של מלחמה, שפגיעה בהן עלולה לגרום לפגיעה ישירה בכושר הלחימה והעמידה של המדינה. כיום ברור שפגיעה בחברות אזרחיות, דוגמת חברת התרופות "טבע", חברות לייצור מזון כמו "תנובה" ו"שטראוס", חברות כבלים, טלוויזיה ואינטרנט, חברות ביטוח ועוד, וכן אתרי זיכרון ומורשת, עלולה לגרום לנזקים לא מבוטלים למדינה ולפגוע במרקם החיים של אזרחיה.

הקמת הרשות לאבטחת מידע וועדת ההיגוי במועצה (מטה) לביטחון לאומי הייתה צעד ראשון בכיוון המתאים. עתה, עם התגברות ההבנה שהמרחב הקיברנטי הופך לנגד עינינו למרחב לחימה של ממש, יש לשפר את העמידות של מדינת ישראל וכלכלתה מול תקיפות מסוג זה. הכנסה של תחום ההגנה מפני מתקפה קיברנטית לתוך התהליכים הסטטוטוריים במדינת ישראל תוכל לאפשר בקרה

קבועה ושיטתית על חסינותה של מערכת ההגנה הקיברנטית של ישראל ושיפור מתמשך של אמצעי ההתגוננות.

הערות

1 אמירה זו מיוחסת בדרך כלל לפרידריך הגדול.
2 אתר האינטרנט של הרשות הממלכתית לאבטחת מידע:
http://www.shabak.gov.il/about/units/reem/pages/default.aspx
3 גל מור, "אושרה תכנית לאבטחת מידע בממשלה", ynet, 11 בדצמבר 2002.
http://www.ynet.co.il/articles/1,7340,L-2310234,00.html
4 Patrick Beggs, *Securing the Nation's Critical Cyber Infrastructure*, U.S. Department of Homeland Security, February 25, 2010.
5 שם. פטריק בגס הינו ראש תחום הערכת ביטחון קיברנטי בחטיבה לביטחון קיברנטי במשרד לביטחון פנים של ארצות הברית.
6 המונח תשתיות הולכה משמש כדי לתאר תשתיות המוליכות מים, שפכים, קולחים, גז, נפט, חשמל, סיבי תקשורת וכדומה.
7 Cyber Resiliency Review (CRR).
8 השופט חשין, רשות ערעור פלילי (רע"פ) 4270/03, מדינת ישראל נגד תנובה.