מהו סייבר?

חלק ב: אתגרי האסדרה של הגנת הסייבר

דומה שאין צורך להסביר היום את עוצמת הנזקים של מתקפות סייבר. החל בפגיעה במערכות מחשוב של בתי חולים ועצירת טיפולים מצילי חיים, עובר במניעת הזרמת דלק לתחנות דלק וכשלים במערכות החשמל והמים, וכלה בדלף של מידע רגיש ואינטימי או חסימת גישה למערכות מחשב בעסקים קטנים. התגברות מתקפות הסייבר נובעת מכשלי שוק היוצרים הגנת סייבר חסרה. כשלים אלה מצדיקים התערבות של המדינה לשם אסדרת ההגנה על מרחב הסייבר.

רחל ארידור הרשקוביץ
תהילה שוורץ אלטשולר

מחקר מדיניות 173

המכון הישראלי לדמוקרטיה

המכון הישראלי
לדמוקרטיה

מהו סייבר?

חלק ב
אתגרי האסדרה של הגנת הסייבר

מחקר מדיניות 173

רחל ארידור הרשקוביץ | תהילה שוורץ אלטשולר

ינואר 2023

What Is Cyber Security? Part Two: The Challenges of Regulating Cyber Protection
Rachel Aridor Hershkovitz | Tehilla Shwartz Altshuler

עריכת הטקסט: חמוטל לרנר
עיצוב הסדרה והעטיפה: סטודיו Alfabees
ביצוע גרפי: רונית גלעד, ירושלים
הדפסה: גרפוס פרינט, ירושלים

מסת"ב: 978-965-519-411-1

אין לשכפל, להעתיק, לצלם, להקליט, לתרגם, לאחסן במאגר ידע, לשדר או לקלוט בכל דרך או אמצעי אלקטרוני, אופטי או מכני או אחר – כל חלק שהוא מהחומר בספר זה. שימוש מסחרי מכל סוג שהוא בחומר הכלול בספר זה אסור בהחלט אלא ברשות מפורשת בכתב מהמו"ל.

© כל הזכויות שמורות למכון הישראלי לדמוקרטיה (ע"ר) 2023
נדפס בישראל, תשפ"ג/2023

המכון הישראלי לדמוקרטיה
רח' פינסקר 4, ת"ד 4702, ירושלים 9104602
טל': 02-5300888
אתר האינטרנט: www.idi.org.il

להזמנת ספרים:
החנות המקוונת: www.idi.org.il/books
דוא"ל: orders@idi.org.il
טל': 02-5300800

כל פרסומי המכון ניתנים להורדה חינם, במלואם או בחלקם, מאתר האינטרנט.

המכון הישראלי לדמוקרטיה

המכון הישראלי לדמוקרטיה הוא מוסד עצמאי א־מפלגתי, מחקרי ויישומי, הפועל בזירה הציבורית הישראלית בתחומי הממשל, הכלכלה והחברה. יעדיו הם חיזוק התשתית הערכית והמוסדית של ישראל כמדינה יהודית ודמוקרטית, שיפור התפקוד של מבני הממשל והמשק, גיבוש דרכים להתמודדות עם אתגרי הביטחון מתוך שמירה על הערכים הדמוקרטיים וטיפוח שותפות ומכנה משותף אזרחי בחברה הישראלית רבת הפנים.

לצורך מימוש יעדים אלו חוקרי המכון שוקדים על מחקרים המניחים תשתית רעיונית ומעשית לדמוקרטיה הישראלית. בעקבותיהם מגובשות המלצות מעשיות לשיפור התפקוד של המשטר במדינת ישראל ולטיפוח חזון ארוך טווח של תרבות דמוקרטית נכונה לחברה הישראלית ולמגוון הזהויות שבה. המכון שם לו למטרה לקדם בישראל שיח ציבורי מבוסס ידע בנושאים שעל סדר היום הלאומי, ליזום רפורמות מבניות, פוליטיות וכלכליות ולשמש גוף מייעץ למקבלי ההחלטות ולציבור הרחב.

המכון הישראלי לדמוקרטיה הוא זוכה פרס ישראל לשנת תשס"ט על מפעל חיים – תרומה מיוחדת לחברה ולמדינה.

הדברים המובאים במחקר מדיניות זה אינם משקפים בהכרח את עמדת המכון הישראלי לדמוקרטיה.

תוכן העניינים

תקציר 7

מבוא 11

פרק 1. אתגרים באסדרת ההגנה על מרחב הסייבר 14

א. המדינה רבת הכובעים 14

ב. אתגרים טכנולוגיים והצורך באוריינות דיגיטלית 17

ג. הצורך בעבודה בין־תחומית וביצירת אסדרה חוצת מגזרים אך מותאמת למאפייניו הייחודיים של כל מגזר 19

פרק 2. אסדרת ההגנה על מרחב הסייבר – משפט משווה 22

א. ארצות הברית 23

ב. אוסטרליה 54

ג. האיחוד האירופי: אנגליה, דנמרק, צרפת 67

ד. ישראל 113

ה. סיכום המודלים הרגולטוריים להגנת מרחב הסייבר – משפט משווה 145

פרק 3. המודל הרגולטורי להגנת מרחב הסייבר בישראל – הערות והארות 160

א. ריבוי הכובעים של מערך הסייבר 160

ב. היעדר סעיף מטרות ברור 161

ג. רגולציית־על לצד רגולציה על רגולטורים: הצורך בהידוק, שיפור ואִזרוח של המודל 162

ד. הרחבת מעגל המטרות של הגנת סייבר: שימוש נרחב ברגולציית הציווי והשליטה הריכוזית וסכנת הפוליטיזציה 165

ה. סמכויות רחבות ומעורפלות 169

ו. מנגנוני פיקוח והגנה על הזכות לפרטיות בפעולות מערך הסייבר 181

ז. פטורים רחבים או לא ברורים בתזכיר חוק הסייבר 186

ח. חלוקת הסמכויות בין מערך הסייבר לרשויות ביטחון אחרות 188
ט. כשירות ראש המערך ועובדיו 192

פרק 4. סיכום והמלצות מדיניות 193

Abstract iii

תקציר

המאפיינים הייחודיים של מרחב הסייבר, ובעיקר ה"היפר־קישוריות" ומהירות העברת המידע, משפיעים הן על אופן השימוש במרחב והן על הסכנות הטמונות בו. הם גם אלה שיוצרים כשלי שוק המובילים לתמריצים נמוכים להשקעה בפיתוח של מוצרים ושירותים מאובטחים במרחב הסייבר. השילוב בין הנזקים העצומים העשויים להיגרם ממתקפות סייבר ובין היעדר תמריצים מספקים להשקעה בהגנת מרחב הסייבר יוצר כשל שוק שמצדיק התערבות ממשלתית לשם אסדרת המרחב הזה.

ואולם, על ההתערבות הממשלתית לאסדרת הגנת הסייבר להתמודד עם כמה אתגרים. חלקם הם אתגרים טכנולוגיים הקשורים בא־סימטריה בין התוקף למגן, ובהיעדר היכולת להעריך את מידת האפקטיביות של פעולות להגנת מרחב הסייבר ואת הרצף הנכון שלהן. אתגרים אחרים נובעים מהמורכבות של עולם הגנת הסייבר, המחייבת שילוב של מומחים מתחומים אחרים, כגון כלכלה, פסיכולוגיה, משפטים וסוציולוגיה, לצד מומחי טכנולוגיה. כמו כן, מתווה הגנת סייבר צריך להיות חוצה מגזרים, משום שהסכנות במרחב הסייבר אינן ייחודיות

למגזר מסוים או לתעשייה מסוימת, וההתמודדות עימן מחייבת מדיניות כוללנית מצד הרגולטור לצד הבנת המאפיינים הייחודיים לכל מגזר. נוסף על כך, הגנת הסייבר מחייבת אוריינות דיגיטלית בקרב המשתמשים במרחב הסייבר וקובעי המדיניות כדי שיוכלו לקבל החלטות שקולות ומאוזנות. לצד אתגרים אלו ניצב אתגר מרכזי המכונה "המדינה רבת הכובעים". למדינה כובעים רבים, ולפעמים סותרים, במרחב הסייבר: המדינה היא הבעלים של תשתיות קריטיות; האחראית לביטחון הלאומי ואמורה להגן על התשתית הקריטית עצמה; פועלת כרגולטור עבור גופי המגזר הפרטי המחזיקים בתשתיות במרחב הסייבר ואחראים להגנתו; שחקנית הלוקחת חלק בשיתופי פעולה ציבוריים ופרטיים להגנת מרחב הסייבר; נציגה במישור הבינלאומי ופועלת עם ומול מדינות אחרות במטרה להגן על מרחב הסייבר, שהגבולות הגיאוגרפיים בו מטושטשים; יצרנית ומפיצה של ידע ומידע בנוגע להגנת מרחב הסייבר; ולבסוף, המדינה יכולה לשמש גם כתוקפת במרחב הסייבר היוצרת בעצמה איומים.

מדינות המערב ובכללן ישראל עוסקות זה מספר שנים בניסיונות לאסדרת ההגנה על מרחב הסייבר. המשותף לניסיונות האסדרה השונים הוא ההבנה שהחיוניות של מרחב הסייבר לכלכלת המדינה ולחיי היום־יום בה, לצד החולשות הקיימות בו, מציבות סכנות רבות בפני המגזר הציבורי, המגזר הפרטי והציבור בכללותו. הבנה זו הובילה גם לאימוץ התפיסה העומדת בבסיס אסדרה אפקטיבית של הגנת סייבר, שלפיה האחריות צריכה להיות מוטלת על כלל השחקנים והאסדרה של מרחב הסייבר אינה צריכה לחול על תשתיות קריטיות בלבד או להתמקד רק במגזר הציבורי; אולם היקף האחריות, סוג האסדרה המתאימה והכלי הרגולטורי הנבחר ייגזרו מרמת הסיכון הנשקף לאינטרס הציבורי ממתקפת סייבר מוצלחת על כל שחקן, בדומה לעקרון האחריות ה"משותפת אך שונה" המקובל במשפט הבינלאומי בהקשר של שמירה על איכות הסביבה ומזעור הנזקים משינויי האקלים.

במחקר זה נסקרה מדיניות הגנת הסייבר במדינות שונות: ארצות הברית, אוסטרליה ואנגליה, האיחוד האירופי ומדינות החברות באיחוד – דנמרק וצרפת, וכן ישראל. המדינות השונות עושות שימוש במגוון כלים רגולטוריים המיועדים להגן על מרחב הסייבר במדינה: רגולציית ציווי ושליטה ריכוזית, רגולציית ציווי ושליטה רכה וביזורית, רגולציה שיתופית ורגולציה עצמית. מידת האחריות של כל אחד מהשחקנים במרחב הסייבר, וכנגזרת ממנה הכלי הרגולטורי שבו ייעשה

שימוש לאסדרת הגנת הסייבר, נקבעים לפי הערכת הסיכון הנשקף לאינטרסים לאומיים חשובים מתקיפת סייבר על ארגון מסוים או על ארגונים ממגזר מסוים. לפיכך, ההגדרה של אינטרסים לאומיים חשובים אלו היא המפתח להבנת היקפה של התערבות המדינה בשוק לשם הגנת מרחב הסייבר. קיים מתאם בין רמת הסיכון לבין מידת ההתערבות של המדינה בשוק החופשי, כפי שבאה לידי ביטוי בכלי הרגולטורי שבו נעשה שימוש: ככל שהסיכון גדול יותר המדינה נוטה להשתמש בכלי רגולטורי "מתערב" יותר. הנגזרת הברורה ביותר מהערכת הסיכון לאינטרסים לאומיים חשובים היא ההבחנה המקובלת בכל המדינות בין ארגונים המשתייכים למגזרי תשתיות קריטיות ובין אלו שאינם מפעילים או בעלים של תשתיות קריטיות, ולכן הרגולציה של הגנת הסייבר במגזרי תשתיות קריטיות שונה מהרגולציה במגזרים אחרים.

ההגדרה של אינטרסים לאומיים חשובים בישראל שונה מהגדרתם במדינות האחרות שנסקרו במחקר זה. שׁוֹנוּת זו משפיעה על הכלים הרגולטוריים שבהם נעשה שימוש כלפי ארגונים ממגזרים שונים, ובאה לידי ביטוי בעיקר בהיקף של רגולציית ציווי ושליטה ריכוזית או רכה וביזורית.

ביוני 2018 פורסם תזכיר חוק הסייבר, המבוסס על התפיסה שהאסדרה של הגנת הסייבר תיעשה על ידי רגולטורים מגזריים באמצעות שילוב כלים רגולטוריים של ציווי ושליטה ריכוזית וביזורית, בפיקוח מערך הסייבר. תזכיר חוק הסייבר הוא צעד חיובי ונכון לאור הצורך לעגן בחוק את אופן פעולתו וסמכויותיו של מערך הסייבר הלאומי, הפועל להגנת מרחב הסייבר מכוח החלטות ממשלה זה כמה שנים. אולם, לדעתנו, התזכיר איננו משקף את ההסתכלות הרחבה המתבקשת נוכח אתגרי היצירה והמימוש של אסדרת ההגנה על מרחב הסייבר. אסדרת הגנת הסייבר המוצעת בתזכיר אינה מבוססת על שיתוף פעולה אמיתי ועמוק עם המגזר הפרטי והאקדמיה, שהינו כורח המציאות נוכח מאפייניו של מרחב הסייבר. ההגדרה של אינטרסים לאומיים חשובים תחת המונח "אינטרס חיוני" רחבה, ואינה מבחינה בין אינטרס חיוני לבין יעד הגנה שתִּפקודו התקין חיוני לשם הגנה על אינטרס לאומי חשוב. משום כך, היקפה של הרגולציה המדינתית ושל התערבות הממשלה בשוק החופשי אינו ברור כלל ועלול להיות רחב ביותר.

לפיכך אנו ממליצות:

(**1**) להוסיף לחוק המוצע בתזכיר חוק הסייבר סעיף מטרה אשר יתחום את מרחב הפרשנות האפשרי של סמכויות מערך הסייבר על פי החוק.

(**2**) לשנות את מודל ה"רגולציה על רגולטורים" ולמצב את מערך הסייבר כרגולטור היחיד הקובע את התקינה וההנחיה הנדרשות להגנת הסייבר; הכלי הרגולטורי שבו ייעשה שימוש ייקבע לפי המאפיינים הספציפיים של כל מגזר ספציפי ולפי רמת הסיכון הנשקפת לאינטרס הציבורי מתקיפת סייבר נגד ארגון במגזר זה.

(**3**) להבטיח שסמכויות הפיקוח והאכיפה יינתנו בידי רגולטורים מגזריים שדפוסי פעולתם אינם של ארגון ביטחוני, ואלו יפעלו בהתאם לכללי המשפט המינהלי הרגיל ובכלל זה מתוך חובת שקיפות שלטונית.

(**4**) לאזרח את מערך הסייבר או לכל הפחות להחיל עליו עקרונות מתחום המשפט הציבורי, ולא רק את הנורמות המשפטיות המקובלות בארגוני הביטחון החשאיים.

(**5**) להעדיף ככל האפשר שקביעת התקינה להגנת הסייבר תיעשה תוך שיתוף התעשייה, האקדמיה והציבור כדי להתאימה למאפייני כל מגזר.

(**6**) לצמצם את סמכויותיו של מערך הסייבר, בין השאר באמצעות שינוי הגדרת המונחים "אינטרס חיוני" ו"מידע בעל ערך אבטחתי" והגדרת המונח "עיבוד מידע"; קביעת אמות מידה ברורות לאפקטיביות הנדרשת מרשות מאסדרת בכל הקשור להגנת הסייבר; צמצום סמכות הניטור; ביטול הסמכות השיורית הנתונה למערך; קביעת תנאי הכשירות לבעלי תפקידים במערך והבהרת מגוון הסמכויות הנתונות לכל אחד; הגבלת הסמכות לקבלת מידע מספק גישה לאינטרנט או מעובד השב"כ לפי תזכיר הוראת השעה; עיבוי מנגנוני הפיקוח על מערך הסייבר; והגבלת הפטור מאחריות אזרחית ופלילית המוענק לו.

(**7**) לקבוע בחוק חלוקת סמכויות ברורה בין מערך הסייבר לרשויות ביטחון אחרות, ובעיקר השב"כ.

מבוא

תכונותיו הייחודיות של מרחב הסייבר מקנות למשתמשים בו יתרונות רבים כמעט בכל תחום חיים בחברה של ימינו, אולם ככל שהשימוש במרחב הסייבר הופך לחלק אינטגרלי משגרת היום־יום של כולנו, כך גוברים גם הסיכונים. מתקפות הסייבר שאירעו בשנים האחרונות מלמדות ששימוש זדוני במרחב הסייבר יכול לגרום לנזקים בעלי השלכות חמורות, לפגיעה כלכלית קשה ואף לנזקי גוף ולאבדות בנפש.

כך, למשל, מתקפת הסייבר NotPetya משנת 2017 שיתקה את מערכות המחשב של חברת השילוח הבינלאומית מרסק (Maersk). עיכוב סחורות בלב ים גרם לעיכוב בביצוע פרויקטים אחרים, כמו בנייה ותיקון מוצרי חשמל. מתקפת הסייבר WannaCry, גם היא משנת 2017, הביאה להשבתת פעולתם של בתי חולים בבריטניה ולדחיית טיפולים רפואיים חשובים.[1]

במרץ 2020 פתחה ממשלת רוסיה במתקפת סייבר רחבת היקף, שיש אף טוענים שהובילה ל"פרל הרבור של מערכות המידע בארצות הברית".[2] התקיפה התגלתה על ידי רשויות הגנת הסייבר האמריקניות רק כעבור 9 חודשים לערך מתחילתה, והתאפשרה באמצעות חדירה לתוכנת אוריון (Orion) של חברת סולארווינדס (SolarWinds). תוכנת אוריון משמשת לניטור מערכות ורשתות מידע בארגון והוטמעה ברשויות ממשלתיות רבות בארצות הברית, כמו גם בחברות טכנולוגיה מובילות. החדירה אליה נתנה לתוקפים גישה למידע רב ורגיש שאוחסן במערכות המידע של משרדי ממשלה – בין השאר משרד ההגנה האמריקני, מזכירות המדינה ומשרד האוצר – ויש החוששים שפגעה פגיעה חמורה בביטחון הלאומי של ארצות הברית.[3]

1 Jon Ungoed-Thomas, Robbin Henry & Dipesh Gadher, *Cyber-Attack Guides Promoted on YouTube*, The Sunday Times (May 14, 2017); Danny Palmer, *WannaCry Ransomware Crisis, One Year On: Are We Ready for the Next Global Cyber Attack?*, ZDNet (May 11, 2018); Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017*, The Guardian (Sep. 30, 2017)

2 Steven J. Vaughan-Nichols, *SolarWinds: The More We Learn, The Worse It Looks*, ZDNet (Jan. 4, 2021)

3 David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. Times (Jan. 3, 2021)

עוד בשנת 2020, בזמן שמדינות העולם הסתגרו בניסיון להתמודד עם מגפת הקורונה הקטלנית, חברות תרופות המפתחות חיסונים לנגיף הקורונה ותרופות למחלה שהוא גורם נחשפו למתקפות סייבר לא מעטות המכוונות להעתקת הקניין הרוחני ותוצאות המחקר והפיתוח החדשניות.[4] במאי 2021 גרמה תקיפת כופר למטרות רווח כלכלי על חברת דלק אמריקנית שיבושים ניכרים באספקת הדלק בארצות הברית.[5] ובישראל, באפריל 2020 נבלמה תקיפת סייבר איראנית על תשתיות המים והביוב במדינה.[6] לקראת סוף שנת 2020 הותקפו מערכות המחשוב של חברת הביטוח הישראלית שירביט, והתוקפים הצליחו לשים ידם על כמויות גדולות של מידע אישי של אלפי מבוטחים, ביניהם עובדי מדינה בתפקידים רגישים.[7] לצד הסכנה שמידע כאמור יאפשר גנבת זהות והתחזות בהיקפים גדולים, למתקפה בסגנון זה עשויות להיות השלכות חמורות העלולות להתגלות רק כעבור זמן רב – למשל ניסיונות סחיטה של מי שמידע אישי רגיש עליהם הגיע לידיים לא מורשות. באוקטובר 2021 הביאה מתקפת כופר על מערכות ניהול הטיפולים של בית החולים הלל יפה לדחיית טיפולים אלקטיביים, להפניית חולים לבתי חולים אחרים ולמעבר לעבודה ידנית במשך מספר שעות. גם כעבור כמה ימים התקשה בית החולים להשיב את מערכות המחשוב לעבודה סדירה.[8]

4 Tara Seals, *Nation-State Attacker Actively Target COVID-19 Vaccine-Makers*, Threat Post (Nov. 13, 2020); Robert McMillan, *Covid-19 Vaccine Makers Face Russian, North Korean Cyberattacks, Microsoft Says*, Wall St. J. (Nov. 13, 2020); Alfred Ng, *Russian and North Korean Hackers Are Targeting COVID-19 Vaccine Researchers*, Cnet (Nov. 13, 2020)

5 Patrick Gray, *Is It Really the Wild West in Cybercrime? Why We Need to Re-examine Our Approach to Ransomware*, TechRepublic (May 27, 2021)

6 ליאור גוטמן "מתקפת הסייבר על תשתיות המים חושפת כאוס בסמכויות החירום" **כלכליסט** (24.5.2020); אחיה ראב"ד "חשד למתקפת סייבר חריגה על שורת מתקני מים בישראל" **ynet** (26.4.2020); "ארגון סורי ערך מתקפת סייבר נגד מערכת המים" **ynet** (25.5.2013).

7 אמיתי זיו "מתקפת הסייבר על שירביט – מי עומד מאחוריה ולמה זה מדאיג" **The Marker** (4.12.2020).

8 נבו טרבלסי "'תקלה קריטית': אירוע סייבר בביה"ח הלל יפה" **גלובס** (13.10.2021); אודי עציון "ראש מערך הסייבר: 'זקוקים לעוד סמכויות'" **ynet** (19.10.2021).

כפי שסקרנו בחלק א של המחקר "מהו סייבר",[9] המאפיינים הייחודיים של מרחב הסייבר, ובעיקר ה"היפר־קישוריות" ומהירות העברת המידע, משפיעים הן על אופן השימוש במרחב והן על הסכנות הטמונות בו. כמו כן, מאפיינים אלה יוצרים כשלי שוק המובילים לתמריצים נמוכים להשקעה בפיתוח של מוצרים ושירותים מאובטחים במרחב הסייבר.

השילוב בין הנזקים העצומים שמתקפות סייבר עלולות לגרום והיעדר תמריצים מספקים להשקעה בהגנת מרחב הסייבר מצדיק את הצורך בהתערבות ממשלתית לאסדרת ההגנה על מרחב זה. עם זאת, אסדרת ההגנה על מרחב הסייבר מעוררת אתגרים וקשיים מסוימים, ובראשם החשש מפגיעה בפרטיות. בפרק הראשון של מסמך זה נסקור את האתגרים והקשיים הכרוכים באסדרת ההגנה על מרחב הסייבר. בהמשך נציג סקירה השוואתית של מערכי אסדרה במדינות דמוקרטיות אחרות (ארצות הברית, אוסטרליה ואנגליה, לצד האיחוד האירופי ומדינות החברות באיחוד – דנמרק וצרפת), ונציג את מאמצי האסדרה במדינת ישראל. הפרק האחרון יציג את ההצעה לאסדרה כוללת של מערך הגנת הסייבר בישראל באמצעות תזכיר חוק הסייבר, ואת הביקורת שלנו עליה.

ענבל מנדלר סייעה לנו בכתיבת הגרסה הראשונה של המסמך ועל כך מסורה לה תודתנו. אנו מודות להוצאה לאור של המכון הישראלי לדמוקרטיה ולעורכת חמוטל לרנר על העבודה המסורה. תודה לעו"ד עמית אשכנזי, לעו"ד עמיר כהנא, לד"ר נדיב מרדכי ולפרופ' יובל שני על הערותיהם המפרות.

9 רחל ארידור הרשקוביץ, תהילה שוורץ אלטשולר ועידו סיוון סביליה **מהו סייבר? חלק א: על מרחב הסייבר, תקיפות סייבר והגנת סייבר** (מחקר מדיניות 171, המכון הישראלי לדמוקרטיה 2021) (להלן: **מהו סייבר א**).

פרק 1

אתגרים באסדרת ההגנה על מרחב הסייבר

אסדרת ההגנה על מרחב הסייבר כרוכה בארבעה אתגרים עיקריים. **ראשית**, ריבוי הכובעים של המדינה הבאה לאסדר, שעשוי ליצור ניגודי עניינים; **שנית**, האתגר הטכנולוגי והצורך באוריינות דיגיטלית לשם הבנת אפשרויות האסדרה; **שלישית**, הצורך ביצירת מסגרת רגולטורית שהיא חוצת מגזרים אך מותאמת למאפייניו הייחודיים של כל מגזר; **ורביעית** – הדומיננטיות המוחלטת של תפיסותיהם המהותיות והמוסדיות של גופי הביטחון באסדרת ההגנה על מרחב הסייבר, שרובו ככולו מרחב אזרחי.

א. המדינה רבת הכובעים

כפי שיפורט להלן, למדינה עשויים להיות כמה תפקידים הקשורים להגנת מרחב הסייבר, אולם לעיתים קיימת סתירה ביניהם:[10]

(**1**) **בעלים.** המדינה מחזיקה בבעלותה תשתיות קריטיות, לרבות מאגרי מידע אישי ורגיש על אזרחיה, העלולות להימצא בסכנה.

(**2**) **אחראית לביטחון הלאומי.** המדינה היא האחראית לביטחון הלאומי, ובהקשר זה היא פועלת להגדלת הביטחון ולמזעור האיומים. כלומר המדינה אחראית לפתרון המצוקה שבה היא עצמה מצויה בכובעה כבעלים של התשתית הנמצאת בסכנה.

(**3**) **מחוקקת ורגולטורית.** המדינה, כאמור, אחראית לביטחון הלאומי, אך מרבית התשתיות במרחב הסייבר מצויות בידיים פרטיות. משום כך, המדינה אינה יכולה

10 להרחבה בנוגע לתפקידיה הסותרים של המדינה ראו Myriam Dunn Cavelty & Florian J. Egloff, *The Politics of Cybersecurity: Balancing Different Roles of the State*, 15(1) St Antony's Int'l Rev. 37, 49–50 (2019)

להבטיח את הגנת מרחב הסייבר רק באמצעות הפעולות שהיא עצמה נוקטת, אלא חייבת לפעול כרגולטורית לשם אכיפת רמה מסוימת של הגנת סייבר בקרב גופים פרטיים, הנושאים אף הם באחריות להגנת מרחב הסייבר. כמו כן, עליה להביא לפתרונם של כשלי השוק, דוגמת החצנות שליליות ותמריצים נמוכים להשקעה בפיתוח מוצרים ושירותים שרמת הגנת הסייבר שלהם נאותה.[11]

(**4**) **שחקנית בשוק הגנת הסייבר.** המדינה היא שחקנית ששותפה להגנת מרחב הסייבר במסגרת שיתופי פעולה ציבוריים־פרטיים, בעיקר בכל הקשור לשיתוף במידע הדרוש להגנת תשתיות קריטיות במרחב הסייבר.

(**5**) **נציגת הציבור בזירה הבינלאומית.** מתקפות סייבר ואיומי סייבר הם תופעה חוצת גבולות, ולכן כדי למלא כמיטב יכולתה את תפקידה כאחראית להגנת מרחב הסייבר על המדינה לפעול במישור הבינלאומי לשם הנעת תהליכים שמטרתם הגנת מרחב הסייבר באופן התואם את צרכיה.

(**6**) **יצרנית ומפיצה של ידע.** המדינה מייצרת ומפיצה ידע ומידע בנוגע להגנת מרחב הסייבר. מידת האמינות המיוחסת למידע שמופץ על ידי המדינה תלויה ברמת אמון הציבור בשלטון.

(**7**) **מקור האיום.** במקרים מסוימים המדינה עצמה מאיימת על הביטחון במרחב הסייבר, כלומר המדינה היא הגורמת למצוקה שממנה היא עצמה מאוימת ושעימה היא עצמה צריכה להתמודד במסגרת תפקידיה האחרים. אנו מכירים כיום שני אופני פעולה שיוצרים איום מסוג זה:[12]

(א) המדינה יכולה לנקוט פעולות סייבר התקפי נגד מוסדות ציבוריים וחברות פרטיות במדינות אחרות. דוגמאות מהשנים האחרונות הן מתקפת הסייבר האיראנית בשנת 2012 ששיתקה את מערכות חברת הנפט ארמקו הסעודית (Saudi Aramco); תקיפת הסייבר הרוסית שהובילה לקריסת מערכת החשמל

11 לדיון בכשלי השוק המובילים להשקעה נמוכה בהגנת מרחב הסייבר ראו **מהו סייבר א**, **לעיל** ה"ש 9, בעמ' 27–30.

12 Michel van Eten, *Patching Security Governance: An Empirical View of Emergent Governance Mechanisms for Cybersecurity*, 19 Digital Policy, Regulation and Governance 429, 430 (2017)

באוקראינה בערב חג המולד בשנת 2015; מתקפת הסייבר ששיבשה את הפעילות בכל תחנות הדלק באיראן באוקטובר 2021, ולטענת ראש ההגנה האזרחית באיראן מקורה בישראל ובארצות הברית; ומתקפת הסייבר האיראנית באוקטובר 2021 שכוונה נגד חברת שרתי אינטרנט והובילה לפגיעה באתרי אינטרנט ישראליים רבים, לרבות אתר ההיכרויות "אטרף", המשמש בעיקר חברים בקהילת הלהט"ב.[13]

(ב) המדינה יכולה לעקוב באופן חודרני אחר תעבורת האינטרנט. לדוגמה, ב־2013 חשף אדוארד סנודן כי הסוכנות האמריקנית לביטחון לאומי (NSA) השתמשה בתוכנת PRISM כדי לאסוף מידע ישירות ממאגרי מידע של חברות אינטרנט מרכזיות.[14]

תפקידיה השונים של המדינה מדגישים את המתחים האפשריים בנוגע לאסדרת ההגנה על מרחב הסייבר. ראשית, בתחום הכלכלי, על המדינה לזכות באמון בעלי העסקים ולהוכיח שעל אף ניגוד העניינים שבו היא מצויה לעיתים עקב ריבוי התפקידים שלה, התערבותה בשוק ובהתנהלותם של בעלי העסקים היא מידתית ביחס לסיכון לתקיפת סייבר ולנזק האפשרי ממתקפה זו לאינטרסים לאומיים או ציבוריים חשובים. תפקידיה של המדינה כאמונה על אסדרת ההגנה על מרחב הסייבר, מחד גיסא, וכאמונה על שמירת זכויות הציבור (משתמשים וצרכנים), מאידך גיסא, מוביל למתח נוסף בין המדינה לאזרחיה, המחייב שאסדרת ההגנה על מרחב הסייבר תאזן כראוי בין הצורך בהגנה על מרחב הסייבר לבין שמירה על זכויות אדם במרחב הדיגיטלי, ובעיקר הזכות לפרטיות והזכות לחופש ביטוי.

כמו כן, אסדרת ההגנה על מרחב הסייבר נדרשת להתמודד עם המתח שבין התעשייה לאזרחים, ולייצר איזון ראוי בין ביטחון לחדשנות טכנולוגית ולשגשוג כלכלי. מצד אחד, על המדינה להגן על זכותו לפרטיות של כל משתמש, ומצד

13 ראו גם סוכנויות הידיעות "איראן: יסבורים שישראל וארה"ב עומדות מאחורי מתקפת הסייבר על תחנות הדלק'" **ynet** (31.10.2021); אמיתי זיו "ההאקרים שתקפו את סייבר־סרב החלו להדליף מידע רגיש מאתר ההיכרויות אטרף" **TheMarker** (30.10.2021) (להלן: זיו "ההאקרים").

14 ראו למשל Steven Levy, *How the NSA Almost Killed the Internet*, Wired (Jan. 7, 2014)

אחר עליה להבטיח שהרגולציה אינה פוגמת ביכולתה של התעשייה במדינה להתחרות בזירה הבינלאומית ולשמור על חדשנותה.[15]

ב. אתגרים טכנולוגיים והצורך באוריינות דיגיטלית

הטכנולוגיות החדשות המיושמות במרחב הסייבר מתפתחות במהירות ויוצרות סביבה דינמית הרצופה בסיכונים ובחוסר ודאות. מאפיינים אלה מקשים על קובעי המדיניות להבין את מגוון הכשלים שעל האסדרה לתקן, לתעדף ביניהם ולקבוע את המדיניות הציבורית המתאימה לאסדרת ההגנה על מרחב הסייבר.[16]

אחד הקשיים המרכזיים הוא הערכת מידת ההגנה האפקטיבית הנדרשת. קושי זה נובע לא רק מהיעדר אוריינות טכנולוגית מצד קובעי המדיניות, או מהיעדר הבנה מעמיקה של תחום הגנת מרחב הסייבר ושל הצורך להישמר מפני מתקפות סייבר באמצעות יצירת ביקוש למוצרים שרמת האבטחה שלהם גבוה יותר מאחרים, אלא גם ממאפייני הטכנולוגיה – ובעיקר מהא־סימטריה המובנית בין מאמצי ההגנה ומאמצי ההתקפה. בעוד התוקף נדרש לאתר חולשה אחת לשם ביצועה של תקיפת סייבר מוצלחת, המבקשים להגן על מרחב הסייבר והמערכות שבו נדרשים לאתר מספר לא ידוע של חולשות ולמנוע את ניצולן.[17]

אתגר נוסף הכרוך בגיבוש מתווה לאסדרת ההגנה על מרחב הסייבר הוא הקושי לקבוע מראש מהן הפעולות או מהו סדר הפעולות שיש לנקוט כדי להגן על

15 Cavelty & Egloff, **לעיל** ה"ש 10, בעמ' 50–52.

16 Jonathan Lewallen, *Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity*, 15 Regulation & Governance 1035 (2020)

17 Cormec Herely, *Unfalsifiability of Security Claims*, 113 PNAS 6415 (2016)

מרחב הסייבר באופן אופטימלי, וכך להבין אילו גופים יש לאסדר ומהי רמת האסדרה שיש להטיל על כל אחד מהם. זאת בעיקר בשל הדינמיות שבפיתוח נוזקות ומימושן, לצד חוסר היכולת של המבקש להתגונן מפני מתקפות סייבר לוודא אמפירית שפעולותיו או שנקיטת סדר פעולות קבוע ומוגדר מראש אכן ימנעו מתקפות סייבר ולא ייחשבו בדיעבד כבזבוז משאבים. במובן זה ניסיונות לגבש מתווה לאסדרת ההגנה על מרחב הסייבר נדמים למרוץ חימוש בלתי נגמר.[18] קושי זה מאפיין ניסיונות אסדרה של כל טכנולוגיה, והאמרה המוכרת בהקשר זה היא "המשפט רודף אחרי הטכנולוגיה". כמו כן, לשם גיבוש מתווה אסדרה מתאים ודינמי להגנת מרחב הסייבר המדינה נדרשת לקבל מידע רב שאין בידה – מידע המצוי בידי חברות פרטיות על פרצות אבטחה, ניסיונות תקיפה שחוו, כישלונן של אסטרטגיות הגנה מסוימות והצלחתן של אחרות. בהיעדר אסדרה הכופה על החברות הפרטיות לעשות כן, הן אינן ששות על פי רוב לשתף מידע זה בפתיחות עם המדינה או עם כל אחד אחר. במקרים רבים חברות פרטיות מעדיפות להסתיר או להמעיט במידע על מתקפות סייבר שעימן התמודדו, כדי למזער את הנזק התדמיתי והכלכלי העלול להיגרם להן מרגע היוודע דבר המתקפה. כך, למשל, בשנת 2010 דיווחה חברת גוגל כי הייתה נתונה לתקיפת סייבר. 34 חברות נוספות מתחומי תעשייה שונים ומגוונים, כולן מבין 500 החברות המדורגות ראשונות על ידי כתב העת פורצ'ן (Fortune 500), הותקפו גם הן, אך נמנעו מלדווח על התקיפה.[19]

עם זאת, הנוהג להסתיר את קיומן של מתקפות סייבר עשוי לעבור מן העולם בשנים הקרובות כיוון שיותר ויותר מדינות וגופים מחייבים בחקיקה דיווח על

18 Bruce Schneier, *Security in the Real World: How to Evaluate Security*, Schneier on Security (June 15, 1999)

19 Tucker Bailey, Andrea Del Miglio & Wolf Richter, *The Rising Strategic Risks of Cyberattacks* 4-5, McKinsey Quarterly (May 2014); Brian Cashell et al., The Economic Impact of Cyber-Attacks (CRS Report for Congress 2004); Jart Armin et al., *2020 Cybercrime Economic Costs: No Measure No Solution*, *in* 2015 10th International Conference on Availability, reliability and Security 701, 701-702 (2015); Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime 18 (2014); Oxford Economics, Cyber-attacks: Effects on UK Companies 10 (A Report for CPNI 2014)

מתקפות כאלה. לדוגמה, בתקנות החדשות להגנת פרטיות במידע של האיחוד האירופי, שנכנסו לתוקפן במאי 2018, נקבעה חובת דיווח על תקיפות סייבר;[20] חובת דיווח נקבעה גם בתיקון לחוק הגנת הפרטיות האוסטרלי,[21] בתקנות אבטחת מידע בישראל[22] ובחוק הדיווח על מתקפות סייבר במגזר התשתיות הקריטיות בארצות הברית.[23]

ג. הצורך בעבודה בין־תחומית וביצירת אסדרה חוצת מגזרים אך מותאמת למאפייניו הייחודיים של כל מגזר

אתגר נוסף העומד בפני גיבוש מתווה לאסדרת ההגנה על מרחב הסייבר נעוץ בעובדה שהגנת הסייבר מחייבת שילוב גורמים מתחומים שונים, כגון כלכלה, פסיכולוגיה, משפטים וסוציולוגיה, ואינה מתמצה בנקיטת אמצעים ומאמצים טכנולוגיים בלבד.[24] התפיסה שלפיה הגנת סייבר היא עניין טכנולוגי גרידא מתעלמת ממורכבות התחום ומהצורך לגבש מענה מקיף הנותן את הדעת

20 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 33, 34, 2016, O.J. (L 119/1) (להלן: GDPR).

21 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) §26WE

22 סעיף 11(ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

23 Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, Division Y, 136 Stat. 1038 (2022) (להלן: חוק הדיווח על מתקפות סייבר בתשתיות קריטיות).

24 Michael Daniel, *Why Is Cybersecurity So Hard?*, Harv. Bus. Rev. (May 22, 2017)

להיבטים נוספים, ומובילה פעמים רבות לאסדרה מצומצמת וחלקית שאינה מביאה לשיפור אמיתי בהגנה על מרחב הסייבר.[25]

ראשית, יש לתת את הדעת לכך שהגנת הסייבר תלויה במידה רבה בגורם האנושי. סקרנות אנושית, אדישות, בורות ושחצנות הן כולן תכונות אנושיות אשר יכולות לפגוע בהגנת הסייבר בארגון, גם אם ננקטו בו האמצעים הטכנולוגיים המתקדמים ביותר להגנת הסייבר. משום כך, הגנת סייבר מחייבת שילוב ואיזון בין השקעה באמצעים טכנולוגיים לבין השקעה בהכשרת כוח האדם, ואסדרת ההגנה על מרחב הסייבר מחייבת הבנה של הגורם האנושי, כלומר התחשבות בשיקולים פסיכולוגיים, כלכליים וסוציולוגיים.[26]

זאת ועוד, הגנת סייבר דורשת אוריינות דיגיטלית מצד משתמשים וערנות לגבי החשיבות של שמירה על הפרטיות שלהם. שני אלה אינם בנמצא תדיר. רכישת אוריינות דיגיטלית אורכת זמן, וכדי להשיגה נדרשת הסברה אינטנסיבית שתגיע אל הציבור ותהיה מובנת לו. מעבר לאוריינות הדיגיטלית, הערנות לחשיבות של שמירה על הפרטיות דורשת גם התגברות על "פרדוקס הפרטיות": אף שמשתמשים מודעים לסכנות אפשריות של מתקפות סייבר שעשויות להתרחש ולפגוע בפרטיותם, ומצהירים כי הם מעוניינים לשמור על פרטיותם ולהתגונן מפני עיבוד מידע אישי עליהם למטרות שאינן רצויות, עדיין מעטים הם המשתמשים הנוקטים את הפעולות הנדרשות כדי למנוע פגיעה כזאת.[27] לפיכך, אסדרה מיטבית של הגנת סייבר צריכה לכלול גם התייחסות לחינוך הצרכנים לפרטיות ולאוריינות דיגיטלית, ולהתבסס על התבוננות רחבה ורב־תחומית הנותנת את הדעת לגורם האנושי ולמאפייניו ואינה מתמקדת רק באסדרה טכנולוגית גרידא.

כמו כן, הסכנות במרחב הסייבר הן חוצות מגזרים ואינן ייחודיות למגזר מסוים או לתעשייה מסוימת. למשל, תקיפת סייבר יכולה להוביל לשיתוק מערכת

25 שם.

26 Dante Disparte & Chris Furlow, *The Best Cybersecurity Investment You Can Make Is Better Training*, Harv. Bus. Rev. (May 16, 2017)

27 Tomas Chamorro Premuzic & Nathalie Nahai, *Why We're So Hypocritical About Online Privacy*, Harv. Bus. Rev. (May 1, 2017)

החשמל, לשיבוש אספקת המים או לפגיעה בבנקים ובשירותי הרפואה. לפיכך, ההתמודדות עם הסכנות שבמרחב הסייבר באמצעות אסדרה מחייבת ראייה כוללנית מצד הרגולטור לצד הבנת המאפיינים הייחודיים לכל מגזר. לדוגמה, ההגנה על המערכות הממוחשבות השולטות בתשתיות המים במדינה אינה זהה לזו הנדרשת במגזר הפיננסי, האוסף, מעבד ומאחסן כמויות עצומות של מידע אישי רגיש. בכל אחד מהמגזרים מטרותיהן של מתקפות סייבר הן שונות וכך גם השלכותיהן על אינטרסים לאומיים חשובים.[28]

28 Lewallen, **לעיל** ה"ש 16.

פרק 2

אסדרת ההגנה על מרחב הסייבר - משפט משווה

מרבית מדינות המערב אימצו לאורך השנים מסגרת לאסדרת ההגנה על מרחב הסייבר, כפי שמעידים הליכי חקיקה, מסמכי מדיניות והחלטות ממשלה בכל אחת מהן. בפרק זה נסקור בקצרה את האסדרה העדכנית של הגנת מרחב הסייבר כפי שמשתקפת ממסמכי מדיניות שונים שפורסמו עד למחצית הראשונה של שנת 2022 בארצות הברית, אוסטרליה, האיחוד האירופי, אנגליה, דנמרק, צרפת וישראל, במטרה לספק מבט משווה לנעשה במדינות שונות בעולם.

הסקירה בוחנת גם את מיקומה של כל מדינה במדד הגנת הסייבר העולמי (Global Cybersecurity Index) לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי (International Telecommunication Union) של האו"ם, ובמדד הגנת מרחב הסייבר של חברת המחקר הבריטית Comparitech.

מדד הגנת הסייבר העולמי משקף את רמת המחויבות של המדינה להגנת סייבר ומבוסס על תשובות שהמדינה מספקת ל־82 שאלות בחמש קטגוריות:

(**1**) אמצעים משפטיים: חוקים ותקנות העוסקים בפשיעת סייבר, הגנת סייבר, אבטחת מידע והגנה על הזכות לפרטיות;

(**2**) אמצעיים טכניים: מידת ההטמעה של יכולות טכניות באמצעות רשויות לאומיות ומגזריות במדינה. הכוונה היא בעיקר לקיומו של CERT (Computer Incident Response Team) ברמה הלאומית והמגזרית;

(**3**) אמצעים ארגוניים: קיומה של אסטרטגיה לאומית עדכנית להגנת סייבר, הכוללת גם הגנה על תשתיות קריטיות והבטחת המשך פעולתן גם במקרה של תקיפת סייבר;

(**4**) היכולת לפתח אמצעי הגנת סייבר ויכולת הגנת הסייבר: קיומם של קמפיינים להעלאת מודעות, הכשרה וחינוך בתחום הגנת הסייבר ומתן תמריצים לפיתוח הגנת סייבר, והתמקדות באסדרת הגנת מרחב הסייבר גם בקרב ארגונים קטנים ובינוניים (SMEs);

(**5**) אמצעי שיתוף פעולה: שיתופי פעולה קיימים בין רשויות ברמה הלאומית והמגזרית, בין גופי ממשל לארגונים מהמגזר הפרטי ובין מדינות למטרת הגנת סייבר.[29]

מדד הגנת מרחב הסייבר של חברת המחקר הבריטית Comparitech מתמקד בהגנת הסייבר ברמת המשתמש הבודד. במסגרת מדד זה נבדקים, למשל, שיעור מכשירי הטלפון הסלולריים הנגועים בנוזקה, שיעור המשתמשים שמכשירי הטלפון הסלולריים שלהם הותקפו באמצעות סוס טרויאני המתמקד באפליקציות בנקאות, שיעור המשתמשים שמכשירי הטלפון הסלולריים שלהם הותקפו בנוזקות כופרה, שיעור המשתמשים שהותקפו בנוזקות המתחזות לתוכנות בנקאות (לא במכשירי הטלפון הסלולריים), ושיעור המחשבים הנגועים בנוזקה מבוססת אינטרנט אחת לפחות.[30]

א. ארצות הברית

ארצות הברית מדורגת במקום הראשון במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם.[31] עם זאת, במדד הגנת מרחב הסייבר של Comparitech זכתה ארצות הברית ב־31 מתוך 75 נקודות. כלומר מבחינת משתמש הקצה מרחב הסייבר בארצות הברית אינו בטוח לחלוטין.[32]

האסדרה של הגנת מרחב הסייבר ברמה הפדרלית במדינה משלבת כמה סוגי רגולציה: רגולציה עצמית, רגולציית ציווי ושליטה, רגולציית ציווי ושליטה רכה וביזורית ורגולציה שיתופית. סוג הרגולציה נקבע בהתאם למאפייני הגוף או המגזר המאוסדר ועל בסיס הערכה וניהול של מכלול הסיכונים הנשקפים

29 Global Cybersecurity Index 2020 (ITU Publications 2021)

30 Paul Bischoff, *Which Countries Have the Worst (and Best) Cybersecurity?*, Comparitech (Sep. 21, 2021)

31 Global Cybersecurity Index 2020, **לעיל** ה"ש 29.

32 Bischoff, **לעיל** ה"ש 30.

לביטחון הלאומי, לביטחון הציבור ולכלכלת ארצות הברית בשל מתקפת סייבר נגד הגוף או המגזר המאוסדר.[33] העיקרון המנחה בקביעת סוג הרגולציה והחלתה הוא עקרון ה"אחריות המשותפת אך שונה" (common but differentiated responsibilities), שלפיו כל השחקנים במרחב הסייבר נושאים באחריות משותפת להגנתו, אבל המחויבות של כל אחד מהם שונה ונקבעת לפי הערכת הסיכון הנשקף מתקיפת סייבר נגדו.[34]

השילוב של כלים רגולטוריים שונים בהתאם לעקרון האחריות המשותפת אך שונה במתווה של אסדרת ההגנה על מרחב הסייבר בא לידי ביטוי גם בהחלטה הנשיאותית של ממשל ביידן ממאי 2021. בהחלטה זו, המבטאת בעיני רבים את הנחישות של ממשל ביידן לחזק את הגנת הסייבר על תשתיות קריטיות במדינה,[35] קורא הנשיא ביידן לשיפור הגנת הסייבר ולשיפור חקירת אירועי סייבר בידי הממשל הפדרלי, כמו גם להחמרת הענישה של האחראים למתקפות סייבר או להגנת סייבר קלוקלת. כן מדגיש הנשיא ביידן את הצורך בשיתוף פעולה מצד המגזר הפרטי: על המגזר הפרטי להבטיח שהמוצרים והשירותים שהוא מוכר תוכננו מראש ומתופעלים באופן בטוח, וכן לשתף פעולה עם הממשל הפדרלי כדי לשפר את הגנת מרחב הסייבר.[36] עוד מצביעה ההחלטה

33 Executive Order No. 13800, Strengthening The Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Red. 22391 (May 11, 2017) (להלן: החלטה נשיאותית 13800).

34 עקרון האחריות המשותפת אך שונה מבוסס על עקרון השוויון (equity) בחוק הבינלאומי ומקובל בתחום ההגנה על איכות הסביבה. כך למשל אמנת המסגרת לשינוי האקלים של האו"ם משנת 1992 ואמנת קיוטו משנת 1997 אימצו עיקרון זה, וחילקו את המשימות להפחתת הפגיעה באיכות הסביבה בהתאם למידת האחריות של כל אחת מהמדינות החתומות לפגיעה שהתרחשה לאורך ההיסטוריה באיכות הסביבה. ראו החלטה נשיאותית 13800, **לעיל** ה"ש 33, בעמ' 17, 34; Estefanía Jiménez, The Principle of Common but Differentiated Responsibilities and Respective Capabilities (CBDR&RC) and the Compliance Branch of the Paris Agreement 2-4 (Organization of American States 2016); Office of the President, National Cyber Strategy of the United States of America 17, 34 (2018)

35 Kevin Collier, *Biden's Cybersecurity Policies Praised Despite Persistence of Ransomware*, NBC News (Jan. 20, 2022)

36 באזהרה שפרסם הנשיא ביידן במרץ 2022 מפני תקיפות סייבר שמקורן ברוסיה,

על שיקול אפשרי בבחינת מידת ההגנה שעל חברה פרטית לנקוט, בקבעה שהאמון שהציבור והממשל נותנים בתשתיות הדיגיטליות נגזר במישרין ממידת השקיפות והאמינות של התשתית עצמה ומההשלכות של הפרת אמון זה. כלומר חברה פרטית המבקשת לרכוש ולהבטיח את אמון הציבור והממשל חייבת לנהוג בשקיפות ולהטמיע הגנת סייבר במידה מספקת.[37]

במסגרת תפיסת ניהול הסיכונים ועקרון האחריות המשותפת אך שונה מקובלת ההבחנה בין מגזרי תשתיות קריטיות למגזרים אזרחיים שאינם תשתיות קריטיות. תשתית קריטית מוגדרת כמערכות ונכסים, פיזיים או וירטואליים, החיוניים לארצות הברית במידה כזאת שלהריסתם או לפגיעה בתפקודם תהיה השפעה הרסנית על ביטחון המדינה, כלכלתה, בריאות הציבור או ביטחון הציבור.[38] כיום נכללים 16 מגזרים בהגדרה זו: מגזר התעשיות הכימיות, מגזר המתקנים המסחריים, מגזר התקשורת, מגזר המפעלים החיוניים, מגזר הסכרים, מגזר התעשיות הביטחוניות, מגזר שירותי החירום, מגזר האנרגיה, מגזר השירותים הפיננסיים, מגזר החקלאות והמזון, מגזר המתקנים הממשלתיים, מגזר שירותי הבריאות ובריאות הציבור, מגזר טכנולוגיות המידע, מגזר הכורים הגרעיניים, החומרים והפסולת, מגזר מערכות התחבורה ומגזר מערכות המים והשפכים.[39]

הוא חזר והדגיש את הצורך בשיתוף פעולה מצד המגזר הפרטי בהיבט של הגברת שיתוף המידע הרלוונטי עם רשויות הממשל, ואת אחריות המגזר הפרטי לחיזוק הגנת הסייבר בקרב תשתיות קריטיות בהתאם לקווים המנחים שפותחו בשיתוף בין המגזר הציבורי למגזר הפרטי; Statement on Cybersecurity, 2022 Daily Comp. Pres. Doc. 190 (Mar. 21, 2022). ראו גם *Shields Up*, Cybersecurity & Infrastructure Security Agency

37 Executive Order No. 14028, Improving the Nation's Cybersecurity, §1, 86 Fed. Reg. 26633 (May 12, 2021) (להלן: החלטה נשיאותית 14028).

38 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56 §1016, 2001 U.S.C.C.A.N. (115 Stat.) 272; Executive Order No. 13636, Improving Critical Infrastructure Cybersecurity §6, 78 Fed. Reg. 11737 (Feb. 12, 2013) (להלן: החלטה נשיאותית 13636); Directive on Critical Infrastructure Security and Resilience (PPD-21), 1 Pub. Papers 106 (Feb. 12, 2013) (להלן: דירקטיבה נשיאותית 21).

39 President's Commission on Critical Infrastructure Protection, Cyberspace

המחלקה לביטחון המולדת (Department of Homeland Security, DHS) אחראית לבדיקה עיתית של רשימת מגזרי התשתיות הקריטיות ועדכונה בהתאם לצורך.[40]

הסוכנות להגנת סייבר ולאבטחת תשתיות (Cybersecurity and Infrastructure Security Agency, CISA), יחידה ב־DHS, אחראית לבניית היכולת הלאומית להגנה מפני מתקפות סייבר, ומוסמכת להוביל תוכניות להגנה על מרחב הסייבר ועל תשתיות קריטיות ולמיגור פשיעת סייבר.[41]

1. רגולציית ציווי ושליטה

בעת חירום, כאשר מתרחשת תקיפת סייבר משמעותית[42] העלולה לאיים על הביטחון הלאומי או על היציבות הכלכלית, תוחל על פי רוב רגולציה מסוג ציווי ושליטה על המגזרים המותקפים בהנחיית קבוצת תיאום מאוחדת לענייני סייבר, ה־Cyber Unified Coordination Group (להלן: UCG). קבוצה זו תורכב מנציגי הממשל הפדרלי בלבד, מתוך הנחה שעל פי רוב תקיפת סייבר משמעותית תערב במידה זו או אחרת מדינה זרה.[43]

נוסף על כך, במרץ 2022 נחקק חוק הדיווח על מתקפות סייבר בתשתיות קריטיות (The Cyber Incident Reporting for Critical Infrastructure

Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2009)

40 ראו דירקטיבה נשיאותית 21, **לעיל** ה"ש 38.

41 U.S. Dep't of Homeland Sec., U.S. Department of Homeland Security Cybersecurity Strategy 6 (2018); Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168

42 תקיפת סייבר משמעותית מוגדרת ככזו העלולה לגרום לנזק משמעותי מוחשי לאינטרס של הביטחון הלאומי, יחסי החוץ או הכלכלה של ארצות הברית, או לפגיעה משמעותית מוחשית באמון הציבור, בזכויות יסוד, בבריאות הציבור או בביטחונו. ראו Directive on United States Cyber Incident Coordination (PPD-41) §(II)(B), 2 Pub. Papers 1028 (July 26, 2016) (להלן: דירקטיבה נשיאותית 41).

43 **שם**, בסעיף (V)(B)(b).

Act).[44] החוק מטיל על בעלים ומפעילים של תשתיות קריטיות שתי חובות דיווח:

(**1**) חובה לדווח ל־CISA על מתקפות סייבר משמעותיות בתוך 72 שעות מהרגע שהגוף המאוסדר מאמין באופן סביר ("reasonably believe") שמתקפת הסייבר פרצה.[45] הדיווח על מתקפת הסייבר אינו חד־פעמי. לאחר הדיווח הראשוני, על הגוף המאוסדר לשוב ולדווח ל־CISA כל אימת שמתגלה מידע חדש או שונה מהמידע שדווח עליו קודם לכן. כמו כן עליו לדווח על סיום הטיפול במתקפת הסייבר.[46]

(**2**) חובה לדווח על תשלום כופר במקרה של מתקפת כופרה בתוך 24 שעות מהתשלום.[47]

חובות הדיווח ייכנסו לתוקפן לאחר שמנהל ה־CISA יפרסם בתקנות הגדרה ברורה של סוגי הגופים מקרב מגזרי התשתיות הקריטיות הכפופים לחובות אלו, של סוגי מתקפות הסייבר המשמעותיות שיש לדווח עליהן ושל תוכן הדיווח הדרוש. בהגדרת הגופים המאוסדרים על מנהל ה־CISA להתחשב בשיקולים המנויים בחוק, ובהם ההשפעה שעשויה להיות למתקפת סייבר אפשרית על הגוף המאוסדר, על הביטחון הלאומי, על הביטחון הכלכלי ועל בריאות הציבור, השלכות בטיחות אחרות, הסבירות שהגוף המאוסדר יותקף ורמת ההפרעה שמתקפת הסייבר עלולה לגרום לתפקוד האמין של תשתית קריטית.[48]

עם זאת, החוק קובע חריג שלפיו חובות הדיווח מכוחו לא יחולו על גופים מאוסדרים בהתקיים התנאים שלהלן:

44 חוק הדיווח על מתקפות סייבר בתשתיות קריטיות, **לעיל** ה"ש 23.

45 **שם**, בסעיף (4)2240.

46 **שם**, בסעיף (3)(a)2242.

47 **שם**, בסעיף (A)(2)(a)2242.

48 **שם**, בסעיף (1)(c)2242. על CISA להציג טיוטת תקנות בתוך שנתיים מחקיקת החוק, ואת הנוסח הסופי של התקנות בתוך שלוש שנים וחצי מחקיקתו. בניסוח התקנות עליה להתייעץ עם גופי ממשל כגון משרד המשפטים. ראו **שם**, בסעיף (b)2242.

(**1**) הגוף המאוסדר כפוף לחובות דיווח לרשויות פדרליות אחרות, ובלבד שחובות אלו זהות במהותן ובתזמון שלהן לאלו הקבועות בחוק הדיווח על מתקפות סייבר בתשתיות קריטיות;

(**2**) לרשות הפדרלית שהגוף המאוסדר חייב בדיווח אליה יש הסכם לשיתוף מידע עם CISA.[49]

גוף מאוסדר שאינו עומד בדרישות הדיווח חשוף לאפשרות ש־CISA תחקור אותו כדי להשיג מידע, תפנה בדרישה לקבלת מידע או תוציא נגדו צו למסירת מידע. אם גוף מאוסדר לא יציית לדרישת שיתוף המידע בצו יועברו הטיפול והאכיפה בעניינו למשרד המשפטים, והגוף המאוסדר עשוי שלא ליהנות מההגנות המוקנות בחוק לגופים המדווחים.[50] הגנות אלו נועדו להקטין את החשש של גוף פרטי משיתוף מידע עם רשויות הממשל, והן כוללות את הסעיפים שלהלן:

(**1**) פטור מאחריות: CISA, רשויות פדרליות אחרות וכן רשויות מדינתיות לא יוכלו להשתמש במידע שדווח להן לפי החוק כדי לאסדר או לאכוף פעולות על הגוף המאוסדר שציית לחובת הדיווח.[51]

(**2**) המידע הנכלל בדיווח נחשב מידע מסחרי, כלכלי וקנייני של הגוף המאוסדר שדיווח, אם האחרון ציין זאת.

(**3**) חוק חופש המידע או חוקים אחרים המחייבים חשיפת מידע אינם חלים על המידע המדווח.

(**4**) הדיווח אינו נחשב כוויתור הגוף המאוסדר מוסר הדיווח על זכות או הגנה המוענקת לו לפי חוק.[52]

(**5**) המידע המדווח ושאר החומרים ששימשו להפקתו אינם יכולים לשמש כראיה, להיות כפופים לחובת גילוי מסמכים בהליך משפטי או לשמש בהליך

49 **שם**, בסעיף 2242(a)(5).

50 **שם**, בסעיף 2244(a), (c), (d).

51 **שם**, בסעיף 2245(a)(5)(a).

52 **שם**, בסעיף 2245(b).

משפטי פדרלי או מדינתי כלשהו הננקט על ידי הממשלה כדי לאכוף צו נגד הגוף המאוסדר שמסר את הדיווח.[53]

גופים מאוסדרים רשאים לספק ל־CISA מידע רב יותר מהקבוע בחוק. לצד חובת הדיווח מעניק החוק ל־CISA סמכויות הקשורות לשיתוף מידע עם רשויות פדרליות ומדינתיות, עם התעשייה ועם הציבור בכללותו. על CISA לאסוף ולנתח את המידע הנלמד מדיווחי הגופים המאוסדרים ולשתף אותו עם רשויות פדרליות אחרות, עם הקונגרס, עם חברות אחרות ועם הציבור, כדי לגבש תמונת מצב עדכנית בנוגע לאיומי הסייבר הנשקפים למרחב הסייבר בארצות הברית. כאשר CISA משתפת את המידע עם גופים שאינם פדרליים או עם הציבור הכללי עליה להתמימו קודם לפרסום המידע. רשויות פדרליות מוסמכות לעשות שימוש במידע שנמסר להם על ידי CISA אך ורק למטרות שנקבעו בחוק: הגנת סייבר, זיהוי חולשות, תגובה לאיומים לפגיעה בחיי אדם או לפגיעה כלכלית משמעותית, מניעה של איומים כאלה או מזעור שלהם, וכן תגובה לאיום משמעותי על קטינים או לעבירה העולה מהמידע המדווח, או מניעה של איום או עבירה כאלה.[54]

2. רגולציית ציווי ושליטה רכה וביזורית

בשלושה מהמגזרים המוגדרים תשתיות קריטיות – מגזר שירותי הבריאות ובריאות הציבור, מגזר השירותים הפיננסיים ומגזר טכנולוגיות המידע בכל הנוגע למערכות המידע של הממשל הפדרלי – מקובלת רגולציית ציווי ושליטה רכה וביזורית באמצעות שלושה חוקים פדרליים מרכזיים.[55] בכל אחד מהחוקים

53 **שם**, בסעיף 2245(c)(3).

54 **שם**, בסעיף 2245(a)(1).

55 Financial Service Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338, המכונה גם Gramm-Leach-Bliley Act (GLBA), החל על המערכת הפיננסית; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (HIPAA), החל על מערכת הבריאות; Federal Information Security Management Act of 2002, 44 U.S.C. §3541 (FISMA), החל על רשויות ממשל.

מוטלת חובה לאמץ וליישם מנגנונים טכנולוגיים, מינהליים ופיזיים להבטחת הסודיות, השלמות והזמינות של מידע אישי במערכות של המגזר נשוא החוק.[56]

במגזר שירותי הבריאות ובריאות הציבור נחקק בשנת 1996 ה־Health Insurance Portability and Accountability Act (HIPAA),[57] שמכוחו התקין משרד הבריאות, הרגולטור האחראי על שירותי הבריאות, תקנות פרטיות הקובעות סטנדרטים לאומיים להגנה על מידע רפואי אלקטרוני (electronic Protected Health Information, ePHI),[58] ותקנות אבטחה המעגנות מסגרת גמישה לאמצעיים מינהליים, טכניים ופיזיים הנדרשים לאבטחת מידע רפואי אלקטרוני. מטרת התקנות היא להבטיח את פרטיות נושאי המידע מבלי לפגוע בשגשוגה של חדשנות טכנולוגית לשם שיפור האפקטיביות של השירותים הרפואיים.[59]

תקנות הפרטיות ותקנות האבטחה הללו חלות רק על ארגונים רפואיים שה־HIPAA חל עליהם, המעבירים או מחזיקים מידע רפואי אלקטרוני כחלק מעסקה שתקנות הפרטיות או אבטחת המידע חלות עליה.[60]

בתקנות האבטחה באה לידי ביטוי גישת רגולציית הציווי והשליטה הרכה, המקנה מידה מסוימת של שיקול דעת לגוף המאוסדר: עליו לבחור את אמצעי האבטחה המתאים לו מבין מכלול האמצעים המנויים בתקנות. בחירת אמצעי האבטחה

56 הבטחת הסודיות, השלמות והזמינות של המידע מוכרת כ"משולש ה־CIA": Confidentiality, Integrity, Availability.

57 **לעיל** ה"ש 55.

58 HIPAA Privacy Rules, 45 C.F.R. Part 160, and Subparts A and E of Part 164. ePHI מוגדר כמידע רפואי מזוהה על אדם המוחזק או מועבר בפורמט אלקטרוני, למעט מידע רפואי מזוהה במאגרי מערכת החינוך, במאגרי מעסיק או על אדם שנפטר לפני למעלה מ־50 שנה; **שם**, בסעיף 160.103.

59 HIPAA Security Rules, 45 C.F.R. Part 160 and Subparts A and C of Part 164

60 הגופים שעליהם חלות הוראות ה־HIPAA הם ספקי שירותי בריאות, לרבות רופאים, פסיכולוגים, רופאי שיניים, אחיות בית, רוקחים; ספקי תוכניות בריאות, כולל חברות ביטוח רפואי, תוכניות בריאות של חברות ותוכניות בריאות ממשלתיות; ומסלקות לשירותי בריאות. ראו הגדרת "covered entity", 45 CFR §160.103.

המתאים חייבת להיעשות לאחר שהגוף המאוסדר העריך את הסיכונים והביא בחשבון את מכלול השיקולים הקבועים בתקנות האבטחה: גודל הגוף, מורכבותו ויכולותיו, התשתית הטכנית שלו, עלות אמצעי האבטחה, סבירות הסיכון למידע רפואי אלקטרוני והשלכותיו האפשריות.[61] את הערכת הסיכונים יש לבצע באופן עיתי וליישם אמצעי אבטחה בהתאם.[62]

בשנים האחרונות נמתחת ביקורת לא מעטה על תקנות הפרטיות והאבטחה של HIPAA בנימוק שהן מצומצמות מדי, מעניקות תחושת ביטחון כוזבת ואינן נותנות מענה למתקפות סייבר המשביתות את פעולת שירותי הרפואה אף מבלי לסכן באופן ממשי מידע רפואי אלקטרוני.[63] נטען שתקנות הפרטיות והאבטחה של HIPAA אינן מעודדות נותני שירותים רפואיים לבצע הערכת סיכונים גם בכל החלטה אסטרטגית תוך התחשבות בסיכונים חיצוניים למערכת השירותים הרפואיים, כגון פשיעת סייבר. כמו כן, במסגרת ניהול הסיכונים לפי ה־HIPAA לא נשקלים כלל סיכוני סייבר הנלווים לרכישה והפעלה של ציוד רפואי מבוסס בינה מלאכותית המחובר כל העת לרשת האינטרנט.[64]

במגזר הפיננסי, הנחשב אף הוא תשתית קריטית, החברות המעניקות שירותים פיננסיים[65] כפופות לרגולציית ציווי ושליטה רכה במסגרת כללי האבטחה

61 **שם**, בסעיף 164.306(b)(2).

62 **שם**, בסעיפים 164.306(b)(2)(iv), 164.306(e), 164.308(a)(1)(ii)(D), 164.308(a)(8).

63 ראו למשל Jonathan Litchman, *The False Promise of HIPAA for Healthcare Cybersecurity*, Health IT Security (March 8, 2016). כך, למשל, בפברואר 2016 הותקף בית חולים בארצות הברית בתקיפת כופר אשר הצפינה מידע רפואי על מטופלים ומנעה את הגישה אליו עד לתשלום הכופר. צוות בית החולים לא היה מסוגל לספק טיפול רפואי לבאים בשעריו במשך כמה שעות עד לתשלום הכופר. ראו Robert S. Kaplan & Anette Mikes, *Managing Risks: A New Framework*, Harv. Bus. Rev. (June 2012)

64 Elizabeth Snell, *The Changing Roles of Healthcare Cybersecurity Leadership*, Health IT Security (Nov. 9, 2015)

65 התקנות קובעות שגוף פיננסי הוא כל עסק, ללא קשר לגודלו, שמעורב באופן משמעותי במתן שירותים ומוצרים פיננסיים, לרבות פירעון שיקים, הלוואות, משכנתאות, הלוואות שלא במסגרת בנק וייעוץ מס. ראו 16 C.F.R. Part 313.3(k).

והפרטיות (ה־Safeguards Rule משנת 2003 וה־Privacy Rules משנת 2000)[66] שקבע הרגולטור האחראי על המגזר הפיננסי – סוכנות הסחר הפדרלית (Federal Trade Commission, FTC), בהתאם להסמכתה בחוק Gramm-Leach-Bliley.[67] על פי כללים אלו על כל חברת שירותים פיננסיים לפתח תוכנית לאבטחת המידע של לקוחותיה ולפרט אותה בכתב. התוכנית חייבת להיות מותאמת לגודל החברה, מורכבותה, אופי עסקיה והיקפם ורגישות המידע האישי של הלקוחות. אותם הכללים גם מחייבים את חברת השירותים הפיננסיים לכלול בתוכנית האבטחה את הנושאים שלהלן: מינוי עובד לתפקיד מנהל תוכנית האבטחה; זיהוי והערכה של הסיכונים הנשקפים למידע של הלקוחות בכל תחום פעילות של החברה והערכת היעילות של אמצעי האבטחה הננקטים למזעור הסיכונים; תכנון ויישום של תוכנית אבטחה וניטור שגרתי שלה כדי לבדוק את כשירותה; בחירת ספקי שירות המסוגלים לעמוד בדרישות האבטחה וחיוב חוזי שלהם לנקוט את אמצעי האבטחה הנדרשים, תוך פיקוח של החברה על ספקי השירות כדי להבטיח את ההגנה על המידע של הלקוחות; וכן הערכה של תוכנית האבטחה והתאמתה לנסיבות משתנות, לרבות לתוצאות בדיקות האבטחה העיתיות שהחברה מחויבת לבצע לפי כללי האבטחה של ה־FTC. כללי האבטחה מאפשרים לחברה מהמגזר הפיננסי להטמיע אמצעי אבטחה כראות עיניה ובהתאם לשיקול דעתה, ובלבד שהם עומדים בדרישות המסגרת שקובעת ה־FTC.[68] בכך באה לידי ביטוי רגולציית הציווי והשליטה הרכה.

במגזר טכנולוגיות המידע ביחס למערכות המידע של הממשל הפדרלי, ספקים של תשתיות מידע ושירותי מידע דיגיטליים המתקשרים בחוזה עם רשויות

66 במרץ 2019 פרסמה ה־FTC הצעה לתיקון כללי האבטחה והפרטיות בניסיון להבהיר במדויק מהן דרישות תוכנית האבטחה שעל כל חברה במגזר הפיננסי ליישם. התיקון מפרט דרישות נוספות, כמו הצפנת מידע על לקוחות, הטמעת הרשאות גישה במטרה למנוע גישה ושימוש לא מורשה במידע על לקוחות, והגשת דוחות תקופתיים למועצת המנהלים של החברה כדי להגביר את הפיקוח על הציות לדרישות הכללים. נוסף על כך, בתיקון מוצע להרחיב את תחולת התקנות גם לחברות המעניקות שירותים פיננסיים נלווים, אף אם אין זה עיסוקן העיקרי. ראו Philip N. Yannella & Gina M. Pickerrell, *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules*, Cyber Adviser Blog (March 8, 2019)

67 The Gramm-Leach-Bliley Act (GLBA), **לעיל** ה"ש 55.

68 16 C.F.R. Part 314

פדרליות למתן מוצרים ושירותים טכנולוגיים מחויבים בחוזה לשמור כל מידע הקשור לאיומי סייבר ומתקפות סייבר על התשתיות או המוצרים שהם מספקים לרשויות הפדרליות, ולשתף את הרשויות במידע הרלוונטי.[69] חברות המספקות לממשל תוכנות שהממשל הפדרלי מגדיר כקריטיות[70] מחויבות בחוזה עימן לעמוד בכללים לאבטחה והגנה של תוכנות מחשב קריטיות שגיבש המכון הלאומי לסטנדרטים וטכנולוגיה (National Institute of Standards and Technology, NIST).[71] כן מחויבות הרשויות הפדרליות לפעול לפי "מודל אמון אפס" (Zero Trust Architecture) שבמסגרתו, בין השאר, הן ישתמשו אך ורק במכשירים המאושרים על ידי הממשל ובתוכנות קריטיות העומדות בסטנדרט הגנת הסייבר הנדרש.[72]

בעת חקיקת חוק שיתוף המידע 2015 (Cybersecurity Information Sharing Act of 2015)[73] נעשה ניסיון להרחיב את רגולציית הציווי והשליטה הרכה למגזרים נוספים של תשתיות קריטיות. הוצע להטיל על כל רשות פדרלית

69 החלטה נשיאותית 14028, **לעיל** ה"ש 37, בסעיף 2.

70 תוכנה קריטית הוגדרה על ידי המכון הלאומי לסטנדרטים וטכנולוגיה (NIST) כתוכנה שתלויה או שהייתה תלויה לצורך פעולתה ברכיב אחד או יותר בעל אחד מהמאפיינים האלה: (1) הרשאת מנהל או הרשאה מוגברת; (2) הרשאת גישה לרשת או למשאבי מחשוב; (3) שליטה על הגישה למידע או לטכנולוגיה אופרטיבית; (4) התוכנה ממלאת פונקציה קריטית של אמון או פועלת מחוץ לגבולות האמון השגרתיים עם הרשאת גישה מיוחדת. "פונקציה קריטית של אמון" מוגדרת כפונקציות אבטחה כגון שליטה על רשת, אבטחת נקודת הקצה והגנה על רשת. הגדרת "תוכנה קריטית" כוללת, בין השאר, מערכות הפעלה, דפדפני אינטרנט, כלים לניטור רשת, תוכנות גיבוי, תוכנות אחזור וכלים לאִחסון מרחוק. ראו NIST, Definition of Critical Software Under Executive Order (EO) 14028 (2021)

71 הכללים חלים הן על תוכנות קריטיות והן על הפלטפורמות שעליהן פועלות תוכנות אלו. ראו *Security Measures for "EO – Critical Software" Use Under Executive Order (EO) 14028*, NIST (July 9, 2021)

72 החלטה נשיאותית 14028, **לעיל** ה"ש 37, בסעיף 4; Off. of Mgmt. & Budget, Exec. Off. of the President, Memorandum for the Heads of Executive Departments and Agencies on Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09, Jan. 26, 2022)

73 The Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§1501-1533 (להלן: חוק שיתוף המידע 2015).

הרלוונטית למגזר מסוים של תשתיות קריטיות לקבוע מדיניות שמטרתה למזער את הסיכון שמתקפת סייבר על חברה ממגזר זה תוביל לפגיעה חמורה בביטחון הלאומי, בבריאות הציבור וביציבות הכלכלית. עוד הוצע לקבוע שהמדיניות תכלול פירוט של כל חולשות האבטחה המוכרות וכן המלצה לקונגרס בנוגע לחיוב חברות פרטיות מהמגזר הרלוונטי לדווח לרשות הפדרלית הרלוונטית על התרחשותה של תקיפת סייבר. הוראות אלו לא נכללו בסופו של דבר בחוק נוכח התנגדות עזה מצד בעלים ומפעילים של תשתיות קריטיות.[74] אלו סברו שהגברת הרגולציה מסוג ציווי ושליטה, רכה ושאינה רכה, על המגזר הפרטי תגדיל את הנטל הבירוקרטי עליהם ועלולה גם לחשוף אותם לאחריות משפטית.[75]

עם זאת, החלטה נשיאותית 13636,[76] דירקטיבה נשיאותית 21,[77] החלטה נשיאותית 13800[78] ובמידה מסוימת גם החלטה נשיאותית 14028[79] מחייבות את הסוכנויות הפדרליות המפקחות על חברות ממגזרי תשתיות קריטיות להטיל רגולציית ציווי ושליטה רכה ביזורית באמצעות פיתוח כללים לניהול סיכונים ולהגנת סייבר. בהתאם התוו מחלקות החקלאות, ההגנה, האנרגיה, ביטחון המולדת, התחבורה והאוצר המלצות ודרישות להגנת סייבר, כל אחת כלפי מגזר התשתית הקריטית שעליו היא מפקחת. לדוגמה, הרשות האמריקנית לניירות ערך (U.S. Securities and Exchange Commission) מנטרת את מערכות ניהול סיכוני הסייבר של חברות שבפיקוחה ודורשת מהן לדווח לציבור במקרים של תקיפת סייבר בהתאם לקווים מנחים שפרסמה בנושא.[80]

74 David Bender, *Congress Passes the Cybersecurity Act of 2015*, Inside Privacy (Dec. 18, 2015)

75 Letter from the American Bankers Association (ABA) et. al, Opposing Section 407 of S. 754, the Cybersecurity Information Sharing Act (CISA) (Nov. 12, 2015)

76 החלטה נשיאותית 13636, **לעיל** ה"ש 38.

77 דירקטיבה נשיאותית 21, **לעיל** ה"ש 38.

78 החלטה נשיאותית 13800, **לעיל** ה"ש 33.

79 החלטה נשיאותית 14028, **לעיל** ה"ש 37.

80 Keren Livneh & Jacob Reed, *USA*, *in* The Intetnational Legal Guide to Cybersecurity 2019 (2nd ed. 2018)

בהחלטה נשיאותית 14028 ממאי 2021 השיק ממשל ביידן יוזמה לשיפור הגנת הסייבר בתשתיות קריטיות באמצעות פעולה משותפת של הממשל הפדרלי וחברות פרטיות. במסגרת יוזמה זו יאומצו טכנולוגיות ומערכות המספקות שקיפות בנוגע לאיומי סייבר, אינדיקטורים לאיומי סייבר, גילוי אירועי סייבר ואזהרות מפני אירועי סייבר. היוזמה הוחלה בתחילה רק בתחום החשמל וביולי 2021 הורחבה גם לתחום הגז.[81] כך, במגזר החשמל הוטלה רגולציית הגנת סייבר מנדטורית המבוססת על מבחן התוצאה – כלומר הרגולציה קובעת מהי תוצאת הגנת הסייבר הדרושה והגופים המאוסדרים נדרשים להפעיל שיקול דעת ולהחליט אילו אמצעים יש להטמיע כדי להשיג את התוצאה המבוקשת.[82]

כמו כן, מינהלת ביטחון התחבורה במחלקה לביטחון המולדת (The Department of Homeland Security's Transportation Security Administration, TSA) הטילה ביולי 2021 על מפעילים ובעלים של צינורות המובילים נוזלים מסוכנים וגז טבעי דרישות מנדטוריות להגנת סייבר, לרבות החובה לדווח על אירועי סייבר, למנות רכז הגנת סייבר, לבצע סקירה של פרקטיקות הגנת הסייבר הנהוגות אצלם, לאמץ אמצעי הגנה מתאימים נגד מתקפות כופר, לפתח וליישם תוכנית להחלמה מאירוע סייבר ולבצע בחינה שנתית של מתווה הגנת הסייבר בארגון.[83]

עם זאת, כשנה לאחר מכן נמצא שהניסיון להטיל על מגזר זה דרישות הגנת סייבר מנדטוריות נתקל בקשיים רבים ולעת עתה נכשל. מפעילים ובעלים של צינורות המובילים נוזלים מסוכנים וגז טבעי טענו שדרישות הגנת הסייבר שהוטלו עליהם רחבות מדי, מותאמות לתעשיית המידע או התעופה ולא למגזר

81 Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, 2021 Daily Comp. Pres. Doc. 622 (July 28, 2021) (להלן: מזכר נשיאותי 2021).

82 Mandatory Reliability Standards for Critical Infrastructure Protection, 18 C.F.R. Part 39

83 *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators*, Homeland Security (May 27, 2021); U.S. Depratment of Homeland Security Transportation Security Administration, Security Directive Pipeline 2021-02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing (July 19, 2021)

העברת גז ונוזלים מסוכנים, אינן מקנות להם די שיקול דעת באימוץ האמצעים המתאימים להשגת מטרות הרגולציה, ואימוצן ככתבן וכלשונן עלול בסופו של דבר דווקא לסכן את פעולתה התקינה של התעשייה. יתרה מכך, נטען שכישלון רגולציה זו מעיד על הקושי של הממשל להטיל חובות רגולטוריות להגנת סייבר על כלל מגזרי התשתיות הקריטיות המאוסדרים על ידי רשויות פדרליות, כיוון שאלה אינן מכירות את פעולות המגזר שהן מאסדרות ועלולות להטיל רגולציית ציווי ושליטה שאינה רכה ואינה מביאה בחשבון את הצרכים והיכולות של כל מגזר ומגזר. הממשל מצידו הסביר שהלקח נלמד וכי עתה נציגי מינהלת ביטחון התחבורה במחלקה לביטחון המולדת מקיימים שיח עם גורמים בתעשייה לגבי הטענות בנוגע להתאמת דרישות הגנת הסייבר המנדטוריות למאפייניה של התעשייה, וכדי לבחון את אימוצם של כלים רגולטוריים גמישים יותר המותירים מקום לשיקול דעת של הגופים המאוסדרים בנוגע לאמצעים ליישום דרישות הגנת הסייבר הרגולטוריות.[84]

בקביעת הדרישות להגנת הסייבר, הרגולטורים המגזריים עשויים להיעזר במסגרת להגנת הסייבר שפרסם NIST.[85] באופן זה משמשת תוכנית NIST ככלי לרגולציית ציווי ושליטה רכה. מדובר בתוכנית מסגרת להגנת סייבר המורכבת משלושה חלקים: ליבה (Core), דרגות הטמעה (Implementation Tiers) ומְתארים (Profiles).

הליבה כוללת חמש פעולות, בחלוקה לקטגוריות, ששילובן חיוני לקיומה של הגנת סייבר אפקטיבית:

(**1**) **זיהוי** – מסייע לארגון להבין כיצד לנהל את סיכוני הסייבר הנשקפים למערכות, לנכסים, למידע וליכולות שלו;

(**2**) **הגנה** – מסייעת לארגון לפתח נקודות שליטה ואמצעים הנחוצים להגנה מפני איומי סייבר ולגילוים;

84 Eric Geller, *TSA Has Screwed This Up: Pipline Cyber Rules Hitting Major Hurdles*, Politico (Mar. 17, 2022)

85 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (version 1.1, 2018) (להלן: תוכנית NIST). הגרסה הראשונה של התוכנית פורסמה בשנת 2014.

(**3**) **גילוי** – מגוון הצעדים שעל ארגון לשקול את נקיטתם כדי לספק הגנה ואזהרות בזמן אמת על אירועי סייבר;

(**4**) **תגובה** – מסייעת לארגון לפתח מדיניות מתאימה להתגוננות מפני תקיפת סייבר בעת התרחשותה;

(**5**) **החלמה** – פיתוח תוכנית מתמשכת שתאפשר לארגון לשמור על חוסן ולחזור לשגרה לאחר תקיפת סייבר.

כל אחת מחמש פעולות ה"ליבה" מחולקת לקטגוריות הקשורות לצרכים פרוגרמטיים ולפעילויות ספציפיות, מתוך הכרה בכך שאי־אפשר ליישם מדיניות הגנת סייבר זהה בכל הארגונים הפועלים במגזרי התשתיות הקריטיות. הקטגוריות מחולקות לתת־קטגוריות המספקות הפניות לסטנדרטים, הנחיות או פרקטיקות ספציפיות שהטמעתן מאפשרת השגת התוצאה הרצויה בכל תת־קטגוריה. בדרך זו מספקת תוכנית NIST לכל ארגון אוסף של פרקטיקות מובילות בתעשייה להגנת סייבר, שעל הארגון לשקול את נקיטתן בהתאם למאפייניו ולסכנות האורבות לו.[86]

דרגות ההטמעה בתוכנית NIST מסייעות לארגון לבחור את דרגת החומרה של אמצעי האבטחה הנחוצים לו כחלק ממדיניות הגנת הסייבר שלו בהתאם לנסיבות והקשרים ספציפיים. דרגות ההטמעה מתארות את הקשר בין מאפייניו הייחודיים של כל ארגון (מטרותיו, דרגת הסיכון הרצויה לו ומשאביו) לחמש פעולות הליבה בתוכנית NIST. בדרך כלל ארגון עושה שימוש בדרגות ההטמעה כדי לזהות ולתעדף את האפשרויות לשיפור הגנת הסייבר שלו.[87]

מתארים הם האופטימיזציה של פעולות הליבה של תוכנית NIST למאפייניו הייחודיים של כל ארגון. בחלק זה הארגון מפרט את היישום של הסטנדרטים והקווים המנחים המתוארים בליבה על ידו בהתאם למאפייניו ולהערכת הסיכון שלו.[88]

86 **שם**; Andrea Arias, *The NIST Cybersecurity Fraemwork and the FTC*, FTC (Aug. 31, 2016)

87 תוכנית NIST, **לעיל** ה"ש 85.

88 לתיאור המרכיבים של תוכנית NIST ראו *An Introduction to the Components of the Framework*, NIST (Feb. 6, 2018)

באוגוסט 2021 הכריז ממשלביידן על הרחבת תוכנית NIST למגזרים נוספים לבד ממגזרי התשתיות הקריטיות, ועל חיוב NIST לפעול בשיתוף הציבור והתעשייה כדי לפתח קווים מנחים להגנת סייבר בתעשיות ספציפיות, לאו דווקא ממגזרי התשתיות הקריטיות.[89] במסגרת זו פעל NIST לגיבוש קווים מנחים להגנת סייבר בשרשראות אספקה טכנולוגיות (technology supply chains). הכוונה למכלול הגורמים המעורבים באספקה של שירות או מוצר, החל משלב חומרי הגלם או התכנון של השירות ועד למוצר הסופי או לשירות הניתן למשתמש הקצה. למשל, השרתים של Microsoft Exchange הם אחד הגורמים המעורבים באספקה של שירותים או מוצרים טכנולוגיים רבים, שכן הם משמשים ארגונים ברחבי העולם לניהול תיבות הדואר האלקטרוני ויומן הפגישות שלהם. מתקפת סייבר מוצלחת על שרתים אלו במהלך שנת 2021 אפשרה לתוקפים, שזוהו כפועלים מטעם ממשלת סין, לחדור לרשתות מערכות המידע של ארגון שעשה שימוש בשרת Microsoft Exchange ולאסוף מידע אישי ומידע המוגן בקניין רוחני.[90] כמה מהחברות שהתחייבו לקחת חלק בפיתוח מסגרת הגנה זו הן מייקרוסופט, גוגל, IBM, Traverlers ו־Coalition.[91] במהלך שנת 2022 פרסם NIST את התוצרים של שיתופי פעולה אלו – קווים מנחים להגנת סייבר בשרשראות אספקה בתוכנה,[92] וכן קווים מנחים להגנת סייבר במכשירי האינטרנט של הדברים (IoT).[93]

NIST נבחר לגוף שיגבש סטנדרטים וכללים מנחים להגנת סייבר בתשתיות קריטיות כיוון שזוהי סוכנות פדרלית לא רגולטורית הפועלת כמקור בלתי

89 החלטה נשיאותית 14028, **לעיל** ה"ש 37.

90 Charlle Osborne, *Everything You Need to Know about the Microsoft Exchange Server Hack*, ZDNet (April 19, 2021)

91 Press Release, The White House, Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bloster the Nation's Cybersecurity (Aug. 25, 2021)

92 NIST, Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (2022) (להלן: NIST, Software Supply Chain).

93 Michael Fagan et al., IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirement (NIST Special Publication 800-213, 2021)

משוחד למידע ופרקטיקות מדעיות, לרבות בתחום הגנת הסייבר, ובעלת ניסיון מוכח בהתמודדות עם נושאים הקשורים בתשתיות קריטיות ובעבודה בשיתוף פעולה בין המגזר הציבורי, האקדמיה והמגזר האזרחי הפרטי.[94] בהתאם לחוק שעל בסיסו הוקם NIST,[95] NIST אחראי לעדכון ולפיתוח של תוכנית NIST באופן שוטף.

3. רגולציה שיתופית על בסיס התנדבותי

סוג נוסף של רגולציה הנהוג בתחום הגנת הסייבר בארצות הברית הוא רגולציה שיתופית על בסיס התנדבותי.[96] ההצדקה המקובלת לרגולציה מסוג זה היא שמרבית מרחב הסייבר מצוי בידיים פרטיות,[97] ובנסיבות אלה שיתוף פעולה בין המגזר הציבורי למגזר הפרטי יביא לניצול יעיל של היכולות והמומחיות של כל אחד מהם. במסגרת שיתוף הפעולה המדינה מספקת לגופים פרטיים מידע מודיעיני על איומים פוטנציאליים ומקצה משאבים ציבוריים לשם הגנה מפני תקיפת סייבר, תגובה עליה והחלמה ממנה. המדינה יכולה גם לסייע לגופים פרטיים להבין טוב יותר את הסיכונים הצפויים להם, ועל בסיס המידע שיתקבל מהממשל חברה פרטית יכולה להחליט בעצמה כיצד עליה לנהל ביעילות את הסיכונים האלה. מנגד, חברות מהמגזר הפרטי, בייחוד מפעילים או בעלים של תשתיות קריטיות, הפועלות כדי להטמיע הגנת סייבר יעילה מסייעות למדינה

94 לתיאור תהליך גיבושה של תוכנית NIST באופן המצביע על היותה רגולציה שיתופית ראו *History and Creation of the Fraemwork*, NIST (Feb. 8, 2018); וכן הדיון בסעיף א.I.3. בפרק 2 **להלן**.

95 National Institute of Standards and Technology Act, 17 U.S.C. §272(c)

96 את ניצני הרגולציה השיתופית נהוג לייחס להמלצותיה של ועדה שמינה בשנת 1996 הנשיא דאז קלינטון, בדבר הצורך ליצור שיתופי פעולה בין הממשל הפדרלי לבעלים ולמפעילים של תשתיות קריטיות במגזר הפרטי כדי להגן עליהן מפני מתקפות סייבר. ראו President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (October 1997).

97 Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection §1-2, 63 Fed. Reg. 41804 (May 22, 1998) (להלן: דירקטיבה נשיאותית 63); National Infrastructure Advisory Council, Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations 3-7 (2008) (להלן: דוח ה־NIAC).

במילוי משימתה לשמור על הסדר והביטחון הציבורי והלאומי. כך, באמצעות רגולציה שיתופית המגזר הפרטי והציבורי יכולים להביא ליישום הגנת סייבר יעילה יותר לכלל המדינה.[98] אם כן, רגולציה שיתופית גם מאפשרת שיתוף פעולה בין בעלי עניין שונים, וזהו גורם חיוני לניהול יעיל של הסכנות הצפויות לתשתיות קריטיות במרחב הסייבר.[99]

ההחלטות הנשיאותיות שפורסמו לאורך השנים מייחסות חשיבות רבה לאופי הוולונטרי של הרגולציה השיתופית, ומגדירות זאת כתנאי לפיתוח יחסי אמון בין המגזר הפרטי למגזר הציבורי החיוניים להצלחת שיתוף הפעולה. כדי לעודד חברות מהמגזר הפרטי לקחת חלק ברגולציה השיתופית, הממשל הפדרלי מעניק תמריצים בצורת מידע חיוני ותמריצים כלכליים.[100]

רגולציה שיתופית נועדה להשיג כמה מטרות:

I. גיבוש סטנדרטים ותוכנית פעולה להגנת סייבר במגזרי התשתיות הקריטיות

שימוש ברגולציה שיתופית להשגת מטרה זו בא לידי ביטוי בתוכנית NIST ובקווים המנחים ש־NIST ממשיך לפרסם לאורך השנים.[101] בהחלטה נשיאותית 13636 נקבע כי על NIST, יחידה במחלקת המסחר האמריקנית, לגבש בשיתוף

98 ראו דוח ה־NIAC, **לעיל** ה"ש 97; U.S. Dep't of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (2013) (להלן: NIPP 2013).

99 ראו NIPP 2013, **לעיל** ה"ש 98; Executive Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing §§1, 2(d), 80 Fed. Reg. 9347 (Feb. 13, 2015) (להלן: החלטה נשיאותית 13691).

100 ראו דירקטיבה נשיאותית 63, **לעיל** ה"ש 97, בסעיפים 1–4; דוח ה־NIAC, **לעיל** ה"ש 97, בעמ' 3–7; NIPP 2013, **לעיל** ה"ש 98, בעמ' 3, 7, 10, 13; Stephen Goldsmith & William D. Eggers, Governing by Network: The New Shape of the Public Sector (2004); Boris Martor & Sébastien Thouvenot, *Partnership Agreements or the Revival of Public-Private Partnerships "à la française,"* 2 Int'l Bus. L.J. 111, 133 (2004); Rachel Nyswander Thomas, Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models 5, 38 (Center for Strategic & International Studies 2013).

101 ראו תוכנית NIST, **לעיל** ה"ש 85.

פעולה עם בעלי עניין מהממשל הפדרלי וממגזרי התשתיות הקריטיות האזרחיים מסגרת התנדבותית המבוססת על סטנדרטים, קווים מנחים ופרקטיקות נהוגות קיימות, לשם הערכה, ניהול והפחתה של סיכוני הסייבר לתשתיות קריטיות.[102] החלטה נשיאותית 14028 ממשיכה ברוח זו וקובעת כי על NIST לפתח קווים מנחים בשיתוף עם המגזר הפרטי, האקדמיה וגורמים אחרים בתחומים שונים, כמו למשל הערכת האבטחה של תוכנות מסחריות.[103]

תוכנית NIST, כמו גם הקווים המנחים ש־NIST מפרסם מעת לעת,[104] גובשו במסגרת רגולציה שיתופית על בסיס התנדבותי, אולם תוכנית NIST עצמה, כמו גם הקווים המנחים כאמור, יכולים לשמש ככלי לרגולציית ציווי ושליטה רכה כאשר הם מוטמעים כדרישות הגנת סייבר על ידי רגולטור מגזרי, כפי שנעשה במגזר התשתיות הקריטיות,[105] או ככלי לרגולציה עצמית מבוססת תמריצים – כאשר היא אינה נדרשת במפורש על ידי רגולטור מגזרי אך ארגונים עשויים להישען על הטמעתה כהוכחה לנקיטת אמצעי הגנת סייבר סבירים.[106]

II. שיתוף במידע על איומי סייבר, מתקפות סייבר ודרכים להתגונן מפניהן בין כלל השחקנים במרחב הסייבר, מהמגזר הפרטי ומהמגזר הציבורי

המסגרות לשיתוף מידע הוגבלו תחילה לשחקנים מהמגזר הציבורי ולמפעילים ובעלים של תשתיות קריטיות מהמגזר הפרטי,[107] אך בשנת 2015 הורחבו לכלל השחקנים במרחב הסייבר.[108]

102 החלטה נשיאותית 13636, **לעיל** ה"ש 38, בסעיף 6.

103 החלטה נשיאותית 14028, **לעיל** ה"ש 37, בסעיף 4.

104 ראו, למשל, NIST, Software Supply Chain, **לעיל** ה"ש 92.

105 ראו דיון בסעיף א.2 בפרק 2 **לעיל**.

106 ראו דיון בסעיף א.4 בפרק 2 **להלן**.

107 ההוראה להקים מסגרות לשיתוף מידע אלו, המכונות Information Sharing and Analysis Centers (ISACs), נתקבלה בשנת 1998. ראו דירקטיבה נשיאותית 63, **לעיל** ה"ש 97, בסעיפים 1–2.

108 בהחלטה נשיאותית 13691, **לעיל** ה"ש 99, נקבע כי יש להקים מנגנוני שיתוף

שיתוף המידע נועד להגביר את ערנות השחקנים מהמגזר הציבורי ומהמגזר הפרטי לסכנות הטמונות במרחב הסייבר ולדרכי ההתגוננות מפניהן, וכן לשמש פלטפורמה להחלפת דעות ורעיונות בנוגע לפעולות המועילות ביותר למניעת מתקפות סייבר, להתגוננות מפניהן ולהתמודדות עימן. הנחת המוצא היא שהתוויית מדיניות יעילה להגנת סייבר מחייבת מידע מלא על הסכנות הטמונות במרחב הסייבר ודרכי ההתמודדות עימן, והאיסוף של מידע חיוני זה מתאפשר רק באמצעות מסגרות לשיתוף מידע.[109]

המודל המרכזי לרגולציה שיתופית למטרת שיתוף מידע במגזרי תשתיות קריטיות הוא ה־Sector Partnership Model.[110] המודל מורכב משלושה גופים המוקמים בכל מגזר תשתית קריטית:

(**1**) **מועצת התיאום המגזרית** (Sector Coordinating Council, SCC). מורכבת אך ורק מנציגים מהמגזר הפרטי של בעלים ומפעילים של תשתיות קריטיות, ספקי השירות ושותפי המסחר שלהם. המועצה משמשת פלטפורמה לשיתוף במידע על סיכוני סייבר והגנת סייבר בשגרה ובעת תקיפת סייבר.[111]

(**2**) **הסוכנות המגזרית הספציפית** (Sector-Specific Agency, SSA). מורכבת רק מנציגי הממשל הפדרלי הרלוונטיים למגזר התשתיות הקריטיות המסוים. תפקידה לאפשר שיתוף במידע בין הרשויות הפדרליות הרלוונטיות, תעדוף מאמצי ההגנה, ניהול פעולות התגובה לתקיפת סייבר וקידום שיתוף הפעולה בין

מידע שאינם מכוונים לתשתיות קריטיות בלבד, המכונים Information Sharing and Analysis Organizations (ISAOs).

109 NIPP 2013, **לעיל** ה"ש 98; החלטה נשיאותית 13691, **לעיל** ה"ש 99; החלטה נשיאותית 13636, **לעיל** ה"ש 38, בסעיף 1; Press Release, The White House, Securing Cyberspace – President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015); Homeland Security Presidential Directive/HSPD-7 – Critical Infrastructure Identification, Prioritization, and Protection §25, 2 Pub. Papers 1739 (Dec. 17, 2003).

110 דוח ה־NIAC, **לעיל** ה"ש 97; גם האסטרטגיה הלאומית למרחב הסייבר מספטמבר 2018 ממשיכה לתמוך במודל זה לאסדרה של הגנת הסייבר. ראו Office of the President, **לעיל** ה"ש 34, בעמ' 8.

111 NIPP 2013, **לעיל** ה"ש 98.

המגזר הפרטי למגזר הציבורי באותו מגזר. במקרה של תקיפת סייבר המשפיעה על חברה פרטית ממגזר תשתית קריטית, על ה־SSA באותו מגזר לתאם את מאמצי הממשל הפרדלי, ולהבין ולאמוד את ההשפעה העסקית והתפעולית של תקיפת הסייבר על החברות הפרטיות באותו מגזר.[112]

(**3**) **מועצת הניהול הממשלתית** (Government Coordinating Council, GCC). מורכבת אף היא רק מנציגי הממשל הפדרלי הרלוונטיים לאותו מגזר תשתית קריטית. המועצה מנוהלת על ידי נציג מה־SSA ואחראית לשיתוף הפעולה הפדרלי במגזר התשתית הקריטית המסוים, וכן לשיפור שיתוף המידע בין נציגי הממשל הפדרלי לנציגי המגזר הפרטי באמצעות תקשורת בין ה־GCC ל־SCC.[113]

מודל ה־Sector Partnership Model הוא מסגרת אחידה לרגולציה שיתופית בכל אחד ממגזרי התשתיות הקריטיות. כדי לתת מענה לצרכים השונים בכל אחד מהמגזרים נקבע שנציגי הממשל הפדרלי ב־GCC ישתייכו לרשות הרגולטורית או ליחידה הפדרלית המופקדת על אותו מגזר, כך שיהיו מעורים בצרכיו הייחודיים.[114]

אפיק נוסף לרגולציה שיתופית הממוקדת בשיתוף מידע הוא המרכז הלאומי להגנת סייבר ואינטגרציית תקשורת (National Cybersecurity and Communications Integration Center, NCCIC), המנוהל על ידי ה־DHS. מרכז זה משמש כמוקד לשיתוף מידע על ידי רשויות פדרליות אחרות, חברות פרטיות וגופים בינלאומיים. המרכז מנתח את המידע המתקבל אצלו, משתף באופן עיתי במידע רלוונטי ומתאם פעולות תגובה, מזעור נזקים ומאמצי החלמה לאחר תקיפת סייבר.

הרגולציה השיתופית ב־NCCIC נשענת על מרכזי שיתוף ועיבוד מידע (Information Sharing and Analysis Centers, ISACs) שמורכבים אך ורק מנציגי חברות המפעילות תשתיות קריטיות, ולכל מגזר תשתיות קריטיות

112 דירקטיבה נשיאותית 41, **לעיל** ה"ש 42.

113 Cybersecurity & Infrastructure Security Agency, Critical Infrastructure Cross Sector Council Charter (2015)

114 דוח ה־NIAC, **לעיל** ה"ש 97, בעמ' 5–7.

ISAC משלו. ה־ISACs מיוצגים ב־NCCIC באמצעות אנליסטים מטעמם, וכך נשמר שיתוף המידע בין מסגרת הרגולציה העצמית – ה־ISAC – ובין הממשל. ה־NCCIC משתף פעולה גם עם ארגוני שיתוף ועיבוד מידע (Information Sharing and Analysis Organizations, ISAOs) המאפשרים שיתוף מידע הנוגע להגנת הסייבר גם בין חברות פרטיות שאינן משתייכות למגזרי התשתיות הקריטיות, מתוך הנחה ששיתוף שכזה חשוב להגנת הסייבר של ארצות הברית כולה.[115] ה־ISAOs מוקמים ומנוהלים בפיקוח ה־DHS.[116]

במרץ 2022 נחקק חוק הדיווח על מתקפות סייבר בתשתיות קריטיות. חוק זה קובע מסגרת להטלת חובות דיווח מנדטוריות על מפעילים ובעלים של תשתיות קריטיות בהתאם לתנאים שתקבע CISA בעתיד בתקנות.[117] חקיקתו של חוק זה מעוררת את החשד שהרגולציה השיתופית למטרות שיתוף מידע לא צלחה, ולכן בחר ממשל ביידן לפנות לאפיק רגולציית ציווי ושליטה ריכוזית ולחייב גופים מסוימים מקרב הבעלים והמפעילים של תשתיות קריטיות למסור פרטי מידע מסוימים לממשל. האפשרות לציות וולונטרי לדרישות הדיווח הקבועות בחוק על ידי גופים שאינם תשתיות קריטיות[118] מחזקת חשד זה.

III. חינוך הציבור והעלאת מודעותו לסיכונים במרחב הסייבר

מטרה נוספת שרגולציה שיתופית נועדה להשיג היא חינוך הציבור והעלאת מודעותו לאיומי הסייבר, במטרה להקטין את הסיכון הטמון בגורם האנושי. לדוגמה, ה־DHS השיקה קמפיין לאומי בשם "Stop. Think. Connect" שמטרתו

115 החלטה נשיאותית 13691, **לעיל** ה"ש 99, בסעיפים 1 ו־4.

116 **שם**, בסעיפים 2–3; חוק שיתוף המידע 2015, **לעיל** ה"ש 73, בסעיף 102(15) (הגדרת חברה פרטית) ובסעיף 103(b)(1)(B) (בנוגע למרכזי שיתוף מידע עם חברות פרטיות שאינן ממגזרי תשתיות קריטיות). Protecting Cyber Networks Act, H.R. 1560, 114th Cong. §11(13)(a) (2015); National Cybersecurity Protection Advancement Act of 2015, H.R. 1731, 114th Cong. §2(a)(9)(A) (2015)

117 חוק הדיווח על מתקפות סייבר בתשתיות קריטיות, **לעיל** ה"ש 23.

118 **שם**, בסעיף 2243.

להגביר את הערנות, המודעות וההבנה בקרב הציבור בנוגע לסכנות שבמרחב הסייבר, ולעודד את המשתמשים לאמץ התנהגות בטוחה יותר במרחב זה.[119] במסגרת הקמפיין מופצים בחינם עצות וכללים מנחים להגברת הגנת הסייבר האישית. חברות פרטיות, אוניברסיטאות ורשויות פדרליות יכולות להצטרף לקמפיין ולהעביר מסר מטעמן בנוגע לאבטחה במרחב הסייבר. אחת הפעילויות המוכרות ביותר במסגרת קמפיין זה היא חודש הערנות להגנת הסייבר הלאומית, המתקיים בכל שנה בחודש אוקטובר.[120]

IV. ניהול מאמצי ההתגוננות מפני תקיפת סייבר משמעותית בזמן אמת וההחלמה ממנה

רגולציה שיתופית תוחל רק אם היקפה ואופייה של תקיפת הסייבר המשמעותית[121] מצדיקים שיתוף פעולה עם גורמים מהמגזר הפרטי, גופים בינלאומיים וארגוני חברה אזרחית.[122]

4. רגולציה עצמית מבוססת תמריצים עקיפים או ישירים על ארגונים מהמגזר הפרטי, בין שהם תשתיות קריטיות ובין שאינם

רגולציה עצמית נועדה להשיג כמה מטרות עיקריות:

I. ניהול מאמצי ההתגוננות מפני תקיפת סייבר וההחלמה ממנה

רגולציה עצמית מקובלת כאשר תקיפת הסייבר מתמקדת בחברות בבעלות פרטית ואינה צפויה לגרום נזק כבד לביטחון הלאומי או ליציבות הכלכלית.[123]

119 *Cyber Safety*, Cybersecurity & Infrastructure Security Agency

120 שם.

121 להגדרת "תקיפת סייבר משמעותית" ראו **לעיל** ה"ש 42.

122 דירקטיבה נשיאותית 41, **לעיל** ה"ש 42, בסעיפים V(b), V(c)(1).

123 דירקטיבה נשיאותית 41, **לעיל** ה"ש 42.

II. שיתוף מידע

חוק שיתוף המידע 2015 יוצר מסגרת לרגולציה עצמית מבוססת תמריצים למטרת הגברת ניטור המערכות הממוחשבות של חברות פרטיות לשם איתור איומי סייבר ושיתוף מידע.[124] החוק מאפשר לחברה, לאו דווקא ממגזר תשתיות קריטיות, לנטר[125] למטרת הגנת סייבר[126] את מערכות המידע שלה,[127] כולל מידע המאוחסן עליהן, מועבר בהן או מעובד באמצעותן; להטמיע אמצעי הגנה[128]

124 Jamil N. Jaffer, *Carrot and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 South Carolina L. Rev. 585 (2017)

125 המונח "monitor" מוגדר כך בסעיף 102(14) לחוק שיתוף המידע 2015 (**לעיל** ה"ש 73): "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system"

126 המונח "מטרת הגנת סייבר" (cybersecurity purpose) מוגדר בחוק כך: "purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability"; **שם**, בסעיף 102(4).

127 לעניין הגדרת המונח "information system", חוק שיתוף המידע 2015 (**שם**, בסעיף 102(10)(A)), מפנה להגדרה המופיעה ב־44 U.S.C. §3502, שלשונה כדלהלן: "the term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information", כלומר צבר של מקורות מידע המשמשים לאיסוף, עיבוד, שימוש ושיתוף של מידע. בהמשך מפרט חוק שיתוף המידע 2015 סוגים שונים של מערכות מידע: "The term 'information system' includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers" (**שם**, בסעיף 102(10)(B)).

128 המונח "אמצעי הגנה" מוגדר בחוק כך:

> (A) IN GENERAL.–Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known of suspected cybersecurity threat or security vulnerability.

במערכות המידע שלה במטרה להגן עליהן מפני מתקפות סייבר; ולשתף חברות אחרות ואת רשויות הממשל הפדרלי במידע הרלוונטי להגנת הסייבר, ובלבד שאמצעי ההגנה המוטמעים אינם הורסים את מערכות המידע, מעניקים גישה לא מורשית להן או פוגעים בפונקציונליות שלהן או של המידע האישי המאוחסן בהן.[129] התמריץ לשיתוף המידע הוא החרגה מפורשת מהוראות חוק ההגבלים העסקיים בכל הקשור לשיתוף מידע בין חברות פרטיות, וחסינות מתביעות מצד הממשל או גורמים אזרחיים בגין נזקים הנגרמים עקב מתקפות סייבר. אלה יינתנו כל עוד החברה הפרטית מצייתת לקווים המנחים ולפרקטיקות נהוגות שמפרסמת ה־DHS,[130] מטמיעה אמצעי אבטחה למניעת שימוש לא מורשה במערכות המידע שלה ומבטיחה שהמידע שהיא משתפת אינו כולל פרטים אישיים שלא לצורך.[131]

(B) EXCLUSION.-The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system not belonging to-
(i) the private entity operating the measure; or
(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

שם, בסעיף (7)102.

129 **שם**, בסעיף (b)104.

130 **שם**, בסעיפים (a), (c)109; U.S. Dep't. of Homeland Security & Dep't of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 (2016); U.S. Office of the Director of National Intelligence et al., Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity information Sharing Act of 2015 (2016); U.S. Dep't of Homeland Security & Dep't of Justice, Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by Federal Government (2016); U.S. Dep't of Homeland Security & Dep't of Justice, Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 (2016)

131 Remarks on Signing an Executive Order on Promoting Private Sector Cybersecurity Information Sharing in Stanford, California,

כמו כן, חוק הדיווח על מתקפות סייבר בתשתיות קריטיות מאפשר גם לגופים שאינם כפופים לחובות הדיווח המנדטוריות הקבועות בו לדווח וולונטרית על מתקפות סייבר משמעותיות שהן חוות או על תשלום כופר בתגובה למתקפת כופרה שהופנתה נגדן.[132] הפטור מאחריות העלולה לחול בגין שיתוף המידע עם CISA מוענק גם במקרה של שיתוף מידע וולונטרי.[133]

III. אימוץ והטמעה של סטנדרטים ונורמות להגנת סייבר

במזכר ביטחון לאומי שנחתם בידי הנשיא ביידן ביולי 2021 הצביע הנשיא על כך שלדעתו האסדרה של הגנת הסייבר בתשתיות קריטיות סקטוריאלית ומורכבת על פי רוב טלאים־טלאים מחוקים שונים, ומשום כך אין דרישות אסטרטגיות קוהרנטיות להגנת הסייבר במגזר זה. לפי המזכר, לממשל אין דרך מקיפה לדרוש אימוץ של טכנולוגיות אבטחה ופרקטיקות הגנת סייבר לטיפול באיומי הסייבר הגוברים, ומשום כך מגזר התשתיות הקריטיות נעשה פגיע מאוד למתקפות סייבר. כדי לתקן מצב דברים זה נקבע במזכר שהרשויות הפדרליות, בהנהגת CISA ו־NIST, יפַתחו רשימה קוהרנטית ומקיפה של סטנדרטים או יעדים לשיפור הגנת הסייבר בתשתיות קריטיות.[134]

הרגולציה של יישום סטנדרטים אלו תהיה רגולציה עצמית מבוססת תמריצים. לפי החלטה נשיאותית 14028, גם הרגולציה של אבטחת מוצרי תוכנה, בכלל המגזרים, תהיה כזאת, בהתאם לקווים מנחים שיפרסם מזכיר ההגנה באמצעות ה־NSA.[135]

2015 Daily Comp. Pres. Doc. 97 (Feb. 13, 2015); Michael Daniel, *What You Need to Know About President Obama's New Steps on Cybersecurity*, The White House Blog (Jan. 14, 2015); חוק שיתוף המידע 2015, **לעיל** ה"ש 73, בסעיפים 104(d)(1),(2), 106; National Cybersecurity Protection Advancement Act of 2015, **לעיל** ה"ש 116, בסעיף 8(B); Eric A. Fisher, Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House 3-4 (CRS Report 7-5700, 2015)

132 חוק הדיווח על מתקפות סייבר בתשתיות קריטיות, **לעיל** ה"ש 23, בסעיף 2243.

133 **שם**, בסעיף 2245(a)(5)(a).

134 מזכר נשיאותי 2021, **לעיל** ה"ש 81.

135 החלטה נשיאותית 14028, **לעיל** ה"ש 37, בסעיף 4.

אחד התמריצים האפשריים לאימוץ רגולציה עצמית הוא זימון למתן דין וחשבון בדיון פומבי בקונגרס, כפי שהתרחש בעקבות התגובה הציבורית לאירועי סייבר רחבי היקף שאירעו במהלך השנים 2020–2019. מנהלי חברות פרטיות, שספגו הפסדים כבדים בשל מתקפות כופר, זומנו להעיד בשימוע פומבי בקונגרס בנוגע לאמצעי הגנת הסייבר שנקטו. תמריץ נוסף עשוי להיות בדמות לקוחות העלולים להיפגע מתקיפת סייבר אשר ידרשו ממנהלי ארגונים לתת דין וחשבון, לרבות פיצוי, בגין אירועי הסייבר שאירעו בארגוניהם והובילו לפגיעה בלקוחות.

תמריץ נוסף לאימוץ רמת הגנת סייבר ראויה בידי חברות פרטיות, בין שהן נתונות לרגולציית ציווי ושליטה רכה ובין שהן נתונות לרגולציה עצמית, עשוי להיות הגשת תובענות ייצוגיות. לאחרונה, ובעקבות תקיפת הסייבר על חברת הדלק Colonial Pipleline, הוגשו כמה תובענות ייצוגיות על ידי בעלים ומפעילים של תחנות דלק שספגו נזקים כבדים עקב אי־אספקת הדלק הממושכת. אף שהנושא טרם נדון בבית המשפט העליון האמריקני, ערכאות נמוכות מובילות מדיניות שלפיה מי שספג בפועל נזק ישיר וממשי מתקיפת סייבר יכול להגיש תובענה ייצוגית. לעת עתה נתבעות רבות מעדיפות לסיים את התובענות בהסכמי פשרה כדי שלא להיגרר להליכים משפטיים ארוכים ותובעניים.[136]

רגולציה עצמית יכולה להתבסס על תוכנית NIST, המשמשת בין השאר כאמצעי עזר להוכחה של נקיטת צעדים סבירים להגנת סייבר במסגרת רגולציה עצמית. חברה פרטית בכל מגזר הפועלת בהתאם למנגנון ההערכה והניהול של סיכוני הסייבר המפורט בתוכנית NIST, בשילוב עם הקווים המנחים של ה־FTC לעניין אבטחה,[137] תיחשב על ידי ה־FTC כפועלת באופן סביר, והסוכנות תימנע מלנקוט נגדה צעדי ענישה במקרה של תקיפת סייבר שהובילה לשימוש לא מורשה או

136 Gerrit De Vynck, *Ransomware Attacks, Now Come the Lawsuits*, The Washington Post (July 25, 2021); Elizabeth Casale, Layla Husen & Luke Sosnicki, *Second Circuit Rules That Risk of Future Identity Theft Not Enough to Support Standing in Data Breach Class Action*, Thompson Coburn LLP (Nov. 15, 2021)

137 Federal Trade Commission, Start with Security: A Guide for Business (2015)

לשימוש לרעה במידע אישי על לקוחות.[138] ציות לדרישות תוכנית NIST עשוי לסייע לארגון כטענת הגנה בתביעת נזיקין או בתובענה ייצוגית בגין נזק שנגרם למשתמשיו, ללקוחותיו או לצדדים שלישיים עקב תקיפת סייבר על מערכות הארגון עצמו.[139] רגולציה עצמית יכולה גם להתבסס על קווים מנחים נוספים שפרסם NIST להגנת סייבר בתעשיות ספציפיות, כמו הגנת סייבר בשרשראות אספקה בתוכנה[140] והגנת סייבר במכשירי האינטרנט של הדברים.[141]

תמריץ אפשרי נוסף לאימוץ רגולציה עצמית הוא תוכנית התוויות. בהתאם להחלטה נשיאותית 14028 ממאי 2021 פרסם NIST בפברואר 2022 קריטריונים מומלצים ליידוע הצרכנים בנוגע למידת הגנת הסייבר של מוצרי האינטרנט של הדברים (IoT) באמצעות תוויות מידע, בדומה לתוויות המוצגות על מוצרי מזון.[142] תוכנית התוויות אמורה להגשים שתי מטרות: חינוך הציבור והגברת מודעותו לסכנות במרחב הסייבר, ויצירת תמריץ לרגולציה עצמית. החיוב בציון רכיבי הגנת הסייבר במוצר על גבי תווית יהפוך את מידת הגנת הסייבר לשיקול נוסף ברכישת המוצר, כלומר ישפיע על תחרותיות המוצר בשוק. כך ייווצר תמריץ להשקעה בהגנת הסייבר. עם זאת, מידת אימוצם של הקריטריונים שקבע NIST ושל תוכנית התוויות אינה ברורה.[143] לצד יצירת התמריצים לרגולציה עצמית מופעלת גם מידה מסוימת של רגולציה שיתופית: כשנה לאחר השקת התוכנית ידונו הגורמים הרלוונטיים ב־NIST ונציגי המגזר הפרטי ביעילותה להגברת ההגנה על מרחב הסייבר.[144]

138 Arias, **לעיל** ה"ש 86.

139 Gordon Bitko, *The Emerging Biden Administration Cyber Strategy*, Forbes (June 9, 2021)

140 NIST, Software Supply Chain, **לעיל** ה"ש 92.

141 Fagan et al., **לעיל** ה"ש 93.

142 *NIST Issues Guidance on Software, IoT Security and Labeling*, NIST (Feb. 4, 2022)

143 Nat Meysenburg, *NIST's Criteria for Cybersecurity Labels Are Good. Who will Implement Them?*, New America (Feb. 9, 2022)

144 החלטה נשיאותית 14028, **לעיל** ה"ש 37, בסעיף 4.

כמו כן, חיוב כלל הרשויות הפדרליות לפעול בהתאם ל"מודל אמון אפס", שבמסגרתו יוכלו לעשות שימוש רק ברשתות מוצפנות ובתוכנות ואפליקציות העומדות בדרישות הגנת סייבר מסוימות, מהווה אף הוא תמריץ לרגולציה עצמית, שכן הוא יחייב חברת תוכנה שאינה רוצה לוותר על נתח השוק המורכב מרשויות פדרליות לאמץ את דרישות הגנת הסייבר הפדרליות.[145]

עם זאת, ממשל ביידן רמז כי אם המגזר הפרטי לא יפעל באופן רציני, מהיר וראוי להגברת הגנת הסייבר בתשתיות קריטיות, הממשל עשוי לאמץ גישת רגולציית ציווי ושליטה נוקשה בהתאם לסטנדרטים ש־CISA ו־NIST ימליצו עליהם, בהתאמה למאפייניו הייחודיים של כל מגזר.[146]

5. סיכום מודל הרגולציה להגנת מרחב הסייבר בארצות הברית

כפי שמשתקף מהסקירה שלהלן, האסדרה של הגנת מרחב הסייבר בארצות הברית ברמה הפדרלית משלבת כמה סוגי רגולציה: רגולציית ציווי ושליטה, רגולציית ציווי ושליטה רכה וביזורית, רגולציה שיתופית ורגולציה עצמית. סוג הרגולציה נקבע בהתאם למאפייני הגוף או המגזר המאוסדר, ועל בסיס הערכה וניהול של מכלול הסיכונים הצפויים לביטחון הלאומי, לביטחון הציבור ולכלכלת ארצות הברית בשל מתקפת סייבר על אותו גוף או מגזר. במסמכי המדיניות שפרסם ממשל ביידן עם כניסתו לתפקיד ניתן לזהות שאיפה להרחבת רגולציית הציווי והשליטה הריכוזית והרכה הביזורית במקרה שלא תושג רמה סבירה של הגנת סייבר באמצעות רגולציה עצמית מבוססת תמריצים.

הלוח שלהלן מסכם את סוגי הרגולציה השונים הנהוגים כיום ברמה הפדרלית בארצות הברית.

145 Off. of Mgmt. & Budget, Exec. Off. of the President, **לעיל** ה"ש 72.

146 מזכר נשיאותי 2021, **לעיל** ה"ש 81; Press Briefing, The White House, Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure (July 28, 2021)

לוח 1
האסדרה של הגנת הסייבר ברמה הפדרלית בארצות הברית

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה	כלל המגזרים בשעת חירום	בעת תקיפת סייבר משמעותית העלולה לאיים על הביטחון הלאומי או על היציבות הכלכלית, מאמצי ההתגוננות ינוהלו על ידי UCG אשר תורכב מנציגי הממשל הפדרלי בלבד.
	מפעילים ובעלים של תשתיות קריטיות שיוגדרו כגופים מאוסדרים	חובות דיווח מגובות בתמריצים לפי חוק הדיווח על מתקפות סייבר בתשתיות קריטיות.
רגולציית ציווי ושליטה רכה וביזורית	מגזרי תשתיות קריטיות	במגזר שירותי הבריאות לפי ה־HIPAA. לגוף המאוסדר ניתן שיקול דעת מסוים בבחירת אמצעי האבטחה המתאימים לו מבין אלו המנויים בתקנות, לפי הערכת סיכונים ומכלול השיקולים הקבועים בתקנות.
		במגזר הפיננסי לפי כללי האבטחה והפרטיות שקובעת ה־FTC בהתאם ל־GLBA. לגוף המאוסדר ניתן שיקול דעת בבחירת אמצעי האבטחה שיטמיע ובלבד שהם עומדים בדרישות המסגרת הקבועות בכללים.
		בשאר מגזרי התשתיות הקריטיות, הסוכנויות הפדרליות המפקחות על חברות ממגזרים אלה מחויבות לפתח כללים לניהול סיכונים ולהגנת הסייבר המחייבים את החברות המאוסדרות על ידן. CISA ו־NIST יפַתחו רשימת סטנדרטים או יעדים לביצוע לשיפור הגנת הסייבר בתשתיות קריטיות.
		חברות פרטיות המתקשרות בחוזים עם רשויות פדרליות לאספקת מוצרים ושירותים טכנולוגיים יחויבו במסגרת החוזה הנחתם עימן להגביר את שיתוף המידע על אירועי סייבר עם הממשל הפדרלי, ולעמוד בכללים לאבטחה ולהגנה של תוכנות מחשב המוגדרות "קריטיות".

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציה שיתופית על בסיס התנדבותי	כלל המגזרים	גיבוש סטנדרטים ותוכנית פעולה להגנת סייבר בשיתוף פעולה בין NIST לגורמים מהמגזר הפרטי הרלוונטי לסטנדרטים או הקווים המנחים הנדונים, האקדמיה, ורשויות פדרליות אחרות.
		שיתוף מידע.
		חינוך לשם הגברת ערנות הציבור לסכנות שבמרחב הסייבר.
		ניהול מאמצי ההתגוננות מפני תקיפת סייבר משמעותית בזמן אמת וההחלמה ממנה. רגולציה מסוג זה תוחל רק אם היקפה ואופייה של תקיפת הסייבר המשמעותית מצדיקים שיתוף פעולה עם גורמים מהמגזר הפרטי, גופים בינלאומיים וארגוני חברה אזרחית.
רגולציה עצמית	על חברות פרטיות ממגזרי התשתיות הקריטיות שאינן נתונות לרגולציית ציווי ושליטה ריכוזית או רכה וביזורית, וכן אלו שאינן תשתיות קריטיות	ניהול מאמצי ההתגוננות מפני תקיפת סייבר וההחלמה ממנה במקרה של תקיפה המתמקדת בחברה פרטית ואינה צפויה לגרום נזק משמעותי לביטחון הלאומי או ליציבות הכלכלית.
רגולציה עצמית מבוססת תמריצים		שיתוף מידע: תמרוץ חברות פרטיות לפי חוק שיתוף המידע 2015 לנטר את המערכות הממוחשבות שלהן לשם איתור איומי סייבר והגברת שיתוף מידע. מתן פטור מאחריות, משימוש במידע לצורכי אכיפה ומחוק חופש המידע למידע בנוגע למתקפות סייבר ולתשלום כופר המדווח לפי חוק הדיווח על מתקפות סייבר שנחקק במרץ 2022.
		אימוץ והטמעה של סטנדרטים ונורמות להגנת סייבר. התמריצים: 1. חברה פרטית הפועלת בהתאם למנגנון ההערכה והניהול של סיכוני סייבר המפורט בתוכנית NIST בשילוב הקווים המנחים של ה־FTC לעניין אבטחה תיחשב על ידי ה־FTC כפועלת באופן סביר, וה־FTC תימנע מלנקוט נגדה צעדי ענישה במקרה של תקיפת סייבר שהובילה לשימוש לא מורשה או לשימוש לרעה במידע אישי על לקוחותיה. 2. היישום של אמצעי הגנת הסייבר המומלצים על ידי NIST או הרשות הפדרלית הרלוונטית ייבחן בידי הקונגרס והציבור במקרה שלחברה ייגרם נזק משמעותי עקב תקיפת סייבר, ועשוי אף להשפיע על גובה הפיצוי שהחברה תידרש לשלם ללקוחותיה אם ייפגעו. 3. תובענות ייצוגיות המוגשות בידי לקוחות שנפגעו עקב תקיפת סייבר על ארגון. 4. תוכנית תוויות המידע.

ב.
אוסטרליה

אוסטרליה מדורגת במקום ה־12 במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם,[147] וזוכה ב־55 מתוך 75 נקודות במדד הגנת מרחב הסייבר של Comparitech, אשר מתמקד בהגנת הסייבר ברמת המשתמש הבודד.[148]

בשנת 2014 הוקם המרכז האוסטרלי להגנת סייבר (Australian Cyber Security Centre, ACSC), הרשות הסטטוטורית האוסטרלית להגנת הסייבר, שהפך בשנת 2018 לחלק מזרוע המודיעין האוסטרלית (Australian Signals Directorate, ASD). המרכז האוסטרלי להגנת סייבר מתפעל את צוות תגובת החירום (Computer Emergency Response Team, CERT-AU), שתפקידו להגיב לכל תקיפת סייבר, וכן משמש כגורם מנחה למתן מידע, ייעוץ וסיוע לכל המבקש זאת.[149]

באסטרטגיה להגנת הסייבר משנת 2016 הכירה ממשלת אוסטרליה בחשיבות ההגנה על מרחב הסייבר לצמיחה כלכלית ולביטחון הלאומי של המדינה, והדגישה את החשיפה הגוברת של הממשלה, המגזר הפרטי והאזרחים למתקפות סייבר, ובעיקר לפשיעת סייבר, לצד ההבנה שמרבית מרחב הסייבר מצוי בידי גופים פרטיים הנושאים אף הם באחריות על הגנתו. משום כך, האסטרטגיה הצביעה על הצורך בשיתוף פעולה בין הממשלה, המגזר העסקי והאזרחים כדי לשמר את החסינות הקיימת של מרחב הסייבר ואף להגבירה.[150]

147 Global Cybersecurity Index 2020, **לעיל** ה"ש 29.

148 Bischoff, **לעיל** ה"ש 30.

149 *About the ASCS*, ACSC – Australian Cyber Security Centre

150 Australian Government, Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity (2016) (להלן: Australia's Cyber Security Strategy 2016).

בשנת 2020 פורסמה אסטרטגיה חדשה להגנת מרחב הסייבר, אשר חזרה על מסקנות האסטרטגיה משנת 2016 בדבר הצורך בחיזוק הגנת הסייבר, כמו גם על חשיבות שיתוף הפעולה בין המדינה לחברה ולתעשייה לשם השגת האינטרס המשותף של חיזוק הגנת הסייבר. נקודות אלה הוצגו כלקחים מהשימוש הגובר במרחב הסייבר שנכפה על המדינה ואזרחיה בעקבות מגפת הקורונה, ומשיתוף הפעולה המוצלח בין הממשלה, החברה והתעשייה בהתמודדות עם המגפה. הצורך בחיזוק הגנת הסייבר הודגש בעיקר נוכח העלייה בהיקף של תקיפות סייבר ואיומי סייבר מצד מדינות שונות, וכן לאור העלייה במספרן של תקיפות סייבר שמקורן בארגוני פשיעה, אשר מאיימות על הפרט הבודד, על משפחות, על ארגונים ועסקים ואף על מכוני מחקר ושירותי רפואה.[151]

1. רגולציית ציווי ושליטה ריכוזית על כלל המגזרים בעת חירום

המרכז האוסטרלי להגנת הסייבר מרכז ומנהל את כל מאמצי הגנת הסייבר של ממשלת אוסטרליה בזמן חירום.

2. רגולציית ציווי ושליטה רכה וביזורית

I. על חלק מהתשתיות הקריטיות וספקי השירותים הדיגיטליים

חלק מהמפעילים והבעלים של התשתיות הקריטיות כפופים לאסדרה מגזרית ומחויבים במידה מסוימת לאמץ אמצעים להגנת סייבר. כך, למשל, ארגונים מהמגזר הפיננסי (בנקים, חברות ביטוח, קרנות מימון וארגונים לסילוק חובות ולגישור) כפופים לאסדרה ופיקוח מגזריים בכל הנוגע לסיכוני תפעול, לרבות הגנת סייבר. ארגונים המספקים שירותי אשראי מחויבים לניהול סיכוני סייבר כחלק מהחובות המוטלות עליהם ברישיון הפעולה שניתן להם.[152]

151 Australian Government, Australia's Cyber Security Strategy 2020 (2020) (להלן: Australia's Cyber Security Strategy 2020).

152 Australian Government, Strengthening Australia's Cyber Security Regulations and Incentives: A Call for Views 12–13 (2021) (להלן: Call for Views).

כמו כן, ספקי שירותים דיגיטלים המספקים שירות לרשות המיסים האוסטרלית (Australian Taxation Office) נדרשים למלא אחר דרישות הגנת הסייבר המפורטות ב־Digital Service Provider Framework, שנקבעו בידי רשות המיסים בשיתוף עם התאגדות התעשיינים בתחום התוכנה. הספקים נדרשים לבצע הערכה עצמית כדי להראות שהם הטמיעו מנגנוני שליטה טכניים מנדטוריים כגון הצפנה, פיקוח על כניסה ווידוא זהות המשתמש.[153]

בדצמבר 2021 התקבל התיקון לחוק אבטחת תשתיות קריטיות.[154] התיקון מרחיב את תחולת חובת הגנת הסייבר, שהתמקדה עד אז רק בארבעה מגזרים (חשמל, גז, מים ונמלים), ל־11 מגזרי תשתיות קריטיות נוספים (תקשורת, שירותים פיננסיים, אחסון ועיבוד מידע, תעשיית ההגנה, אקדמיה ומחקר, אנרגיה, מזון ורשתות מזון קמעונאות, שירותי בריאות ורפואה, טכנולוגיית חלל, תחבורה ואספקת מים וביוב). כמו כן, התיקון מטיל על בעלים ומפעילים של תשתיות קריטיות חובת הגנה חיובית, כלומר רשימת דרישות שארגון חייב למלא בהתאם לסוג הארגון וסיכוני הסייבר הצפויים לו. כך, למשל, במסגרת חובת ההגנה החיובית על הארגון לדווח מיהם הבעלים של התשתית הקריטית, מי שולט בנכסיה, למי יש גישה למערכות התשתית הקריטית ומהו הרכב הדירקטוריון שלה. דרישה נוספת היא התוכנית לניהול סיכונים: הארגון נדרש לזהות את כל הסיכונים הצפויים לו והדרכים למזער אותם באמצעות אימוץ ויישום של אמצעי הגנה מסוימים. התוכנית לניהול סיכונים תותאם לכל מגזר בתהליך של רגולציה שיתופית. דרישה נוספת שהתיקון מפרט היא דיווח על תקיפת סייבר ל־ACSC בתוך 12 שעות אם לתקיפת הסייבר יש השפעה משמעותית על זמינות נכסים בעלי חשיבות לאומית, או בתוך 72 שעות אם התקיפה עשויה להשפיע על הזמינות, המהימנות, האמינות או הסודיות של נכסים בעלי חשיבות לאומית. בדרך זו תוכל הממשלה לקבל תמונה מלאה של האיומים ושל סיכוני הסייבר שתשתיות קריטיות מתמודדות עימם, ולגבש מדיניות תגובה ומניעה מתאימה. נוסף על כל אלה, התיקון מתווה מנגנון שבמסגרתו יינתן סיוע

153 **שם**, בעמ' 21–22.

154 *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth)

ממשלתי לבעלים ולמפעילים של תשתיות קריטיות המתמודדים עם תקיפת סייבר.[155]

כמו כן, רשות הזהירות האוסטרלית (The Australia Prudential Regulation Authority, APRA), פרסמה סטנדרט זהירות החל על בנקים, חברות ביטוח וקרנות מימון, ומחייב אותם לנקוט אמצעי זהירות מסוימים לשם הגברת מוכנותם לתקיפות סייבר.[156]

II. על ארגונים גדולים שאינם תשתיות קריטיות

לצד הניסיון להחמיר את דרישות הגנת הסייבר המוטלות על תשתיות קריטיות וארגונים מהמגזר הפיננסי, ממשלת אוסטרליה מכירה בכך שיש צורך להחמיר גם את הדרישות המוטלות על ארגונים גדולים, ופנתה לשם כך לציבור לקבלת הערות לגבי כמה רעיונות אסדרה. אחד הרעיונות המוצעים הוא רגולציית ציוּוי ושליטה רכה ביזורית על ארגונים גדולים שאינם תשתיות קריטיות. אלו יחויבו להטמיע אמצעים לניהול סיכוני סייבר בתוך תקופת זמן שתיקבע בחוק. לפי הקול הקורא, רגולציית ציוּוי ושליטה רכה וביזורית כאמור תוביל לשיפור של ממש בהגנת הסייבר בקרב חלק ניכר מהתעשייה בתוך זמן קצר. אולם, לפי האמור בקול הקורא, בהיעדר רגולטור ייעודי המחזיק בידע ובמקצועיות הנדרשת לשם פיתוח סטנדרט הגנת סייבר ואכיפתו בקרב ארגונים רבים, אפיק רגולציית הציוּוי והשליטה הרכה כרוך בעלויות גבוהות מאוד שאינן סבירות בתקופת המיתון שבה אוסטרליה מצויה עתה.[157]

III. על כלל הארגונים במשק – חובות כלליות

מרבית הארגונים, לרבות ארגונים מתחומי הטכנולוגיה והסחר האלקטרוני, רשתות קמעונאיות, מפעלים ושירותי אירוח, כפופים לחובות הכלליות הקבועות בחוק הגנת הפרטיות, בחוק הגנת הצרכן ובחוק החברות, אשר רלוונטיות באופן מצומצם גם להגנת הסייבר. כך, למשל, חוק הגנת הפרטיות מחייב ארגונים

155 **שם**.

156 Call for Views, **לעיל** ה"ש 152, בעמ' 19.

157 **שם**, בעמ' 21–22.

לנקוט צעדים סבירים להגנה על מידע אישי מפני שימוש לרעה או אובדן הנגרם מגישה לא מורשית. חוק הגנת הצרכן אוסר על ארגונים להציג מצג מטעה שלפיו המוצר או השירות עומדים בסטנדרט מסוים; איסור זה עשוי לכלול גם איסור על מצג מטעה בנוגע לרמת הגנת הסייבר המוטמעת במוצר או בשירות. חובת הזהירות המוטלת בחוק החברות על דירקטורים ונושאי משרה בחברה עשויה לכלול, בדרך של פרשנות מרחיבה, גם חובה להבטיח הגנת סייבר נאותה. עם זאת, נוכח כשלי השוק הקיימים בשוק הגנת הסייבר והניסוח המרחיב של החובות בחוקים שנמנו לעיל, אין בחוקים אלו כדי לספק תמריצים משמעותיים לנקיטת הגנת סייבר ברמה נאותה על ידי ארגונים. כמו כן, לאורך השנים האכיפה של הגנת סייבר מכוח חוקים אלו הייתה מצומצמת למדי.[158]

לנוכח מצב זה, ממשלת אוסטרליה ביקשה לשמוע את עמדות הציבור, התעשייה והאקדמיה לגבי התיקון המוצע לחוק הגנת הפרטיות הקיים כך שיכלול הבהרה לגבי ה"צעדים הסבירים" שעל ארגון לנקוט כדי להגן על מידע אישי מפני שימוש לרעה או אובדן הנגרם מגישה לא מורשית. לפי ההצעה התיקון יקבע את סטנדרט הגנת הסייבר המינימלי שעל ארגון לנקוט כדי לעמוד בדרישת ה"צעדים הסבירים" הקבועה בחוק הגנת הפרטיות. תיקון כאמור יחיל חובת הגנת סייבר באמצעות שימוש בכלי הרגולטורי של ציווי ושליטה רכה, והרשות להגנת הפרטיות היא שתפקח על אכיפתו. עם זאת, חובת הגנת הסייבר באפיק זה תחול רק לגבי מידע אישי ורק על ארגונים שחוק הגנת הפרטיות חל עליהם, כלומר ארגונים שההכנסה השנתית שלהם עולה על 3 מיליון דולר אוסטרלי.[159]

3. רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים

בתחילת שנת 2020 פרסמה ממשלת אוסטרליה קוד התנהגות וולונטרי להגנת סייבר במכשירי צריכה חכמים, אולם בסקר שנערך כשנה אחר כך נמצא שרגולציה עצמית זו נכשלה ויצרנים מעטים אימצו את הקוד. היצרנים הגדולים הביעו תמיכה בקוד ונכונות לחזק את הגנת הסייבר במוצרים שהם מוכרים, אך יצרנים קטנים לא עשו דבר. הסיבות לכישלון קוד ההתנהגות הוולונטרי נעוצות

158 **שם**, בעמ' 14–16.

159 **שם**, בעמ' 26.

בכשלי השוק המרכזיים אשר גורמים להיעדר תמריצים להטמעת אמצעי הגנת סייבר נאותים.[160]

גם בנושא זה ביקשה ממשלת אוסטרליה לקבל הערות מהציבור, מהתעשייה ומהאקדמיה לגבי שינוי הכלים הרגולטוריים. אחד השינויים שהוצעו הוא לחייב על פי חוק יצרנים של מכשירים חכמים, לרבות טלפונים ניידים, להטמיע אמצעי הגנת סייבר במכשירים לפי הסטנדרט האירופי בנושא,[161] או לחלופין לחייב אותם להציג תווית אשר תפרט "תאריך פקיעה", כלומר המועד שבו היצרן יפסיק לספק למכשיר עדכוני אבטחה, כמדד לרמת הגנת הסייבר של המכשיר. הממשלה במקביל תקבע, תוך היוועצות עם התעשייה, מהן החולשות או סוגי החולשות שעל היצרן לתקן במהלך התקופה שבה הוא התחייב לספק עדכוני אבטחה ומהו פרק הזמן שבו על היצרן להוציא עדכון לחולשה מרגע היוודע לו דבר קיומה.[162]

4. רגולציה שיתופית

I. למטרת שיתוף מידע

באוסטרליה פועל מנגנון תלת־שכבתי לשיתוף מידע בין המגזר הציבורי לפרטי על איומי סייבר ומתקפות סייבר.[163] בשכבה העליונה מבוצע שיתוף מידע, בעיקר מידע רגיש על מתקפות סייבר, בין המרכז האוסטרלי להגנת סייבר לבין בעלים ומפעילים של תשתיות קריטיות. באסטרטגיה לשנת 2020 נרמז שבעתיד יחויבו בעלים ומפעילים של תשתיות קריטיות לשתף עם הממשל מידע על תקיפות ואיומי סייבר בדרך של ציווי ושליטה.[164]

160 **שם**, בעמ' 9–11.

161 ETSI, Cyber Security for Consumer Internet of Things: Baseline Requirements (ETSI EN 303 645 v2.1.1, 2020) (להלן: ETSI IoT Requirements).

162 Call for Views, **לעיל** ה"ש 152, בעמ' 32–33, 39–40.

163 Australia's Cyber Security Strategy 2016, **לעיל** ה"ש 150, בעמ' 30–32.

164 Australia's Cyber Security Strategy 2020, **לעיל** ה"ש 151, בעמ' 23.

בשכבה האמצעית, המרכז להגנת הסייבר הקים בשיתוף עם המגזר הפרטי מרכזי שיתוף מידע בערים מרכזיות ברחבי אוסטרליה. המרכזים נועדו לאפשר שיתוף מידע בין עסקים, מכוני מחקר מקומיים וגופי ממשל מקומיים, וכן לייעץ לעסקים פרטיים לגבי הטמעת פרקטיקות נכונות לשיפור הגנת הסייבר שלהם. בשכבה התחתונה, מרכז הגנת הסייבר הקים בשיתוף עם המגזר הפרטי אתר אינטרנט ייעודי לשיתוף מידע הנוגע למתקפות סייבר. אתר זה מאפשר הן לעסקים קטנים ובינוניים והן לעסקים המשתתפים במרכזי שיתוף המידע לשתף במהירות מידע על איומי סייבר ועל אמצעי ההתגוננות מפניהם. השתתפות ארגונים מהמגזר הפרטי בכל אחת משכבות שיתוף המידע היא וולונטרית.[165]

II. למטרת גיבוש אסטרטגיה וקביעת קווים מנחים וולונטריים להגנת סייבר

האסטרטגיה להגנת הסייבר לשנת 2020 התקבלה לאחר הליך היוועצות עם הציבור. ממשלת אוסטרליה פרסמה קול קורא לקבלת עמדות הציבור בנוגע לנושאים מרכזיים בתחום הגנת הסייבר, ו־215 אנשים פרטיים וארגונים שלחו את תגובותיהם לקול הקורא. כחלק מההכנות לכתיבת האסטרטגיה ערכה ממשלת אוסטרליה גם מפגשי היוועצות פיזיים עם 1,400 אנשים ברחבי המדינה, וכן התקיימו סדנאות בהשתתפות נציגים של חברות טכנולוגיה גדולות, האקדמיה, תעשיית ההגנה ומשרדי הממשלה. השר לענייני פנים אף הקים פאנל ייעוץ (Industry Advisory Panel) שהורכב מאנשי תעשייה בולטים והופקד על ייעוץ אסטרטגי בנוגע לגיבוש האסטרטגיה להגנת הסייבר לשנת 2020. ההתנסות המוצלחת בשיתוף הציבור בגיבוש האסטרטגיה הובילה להקמת ועדה מייעצת קבועה המורכבת מנציגי התעשייה, שתפקידה לוודא שהתעשייה ממלאת תפקיד משמעותי בעיצוב ובמימוש של הפעולות לטווח הקצר ולטווח הארוך שנקבעו באסטרטגיה.[166]

כמו כן, מדי שנה מתקיים מפגש של שותפות סייבר לאומית המורכבת מנציגי ממשלה, נציגים מובילים מהמגזר העסקי ונציגים מהאקדמיה. במפגש נדונות

165 *ACSC Partnership Program*, ACSC – Australian Cyber Security Centre

166 Australia's Cyber Security Strategy 2020, **לעיל** ה"ש 151.

היוזמות המרכזיות באסטרטגיה להגנת מרחב הסייבר, וכן נדונים נושאים בוערים בתחום הגנת הסייבר.[167]

גם תוכנית העיצוב להגנה (Safety by Design) של נציבות הבטיחות באינטרנט (eSafety Commissioner), אשר קובעת נורמות לעיצוב והטמעה של אמצעי הגנת סייבר ושקיפות במוצרים ושירותים טכנולוגיים, גובשה בשיתוף פעולה עם נציגי התעשייה, האקדמיה והציבור הרחב.[168]

אפיק נוסף של רגולציה שיתופית הוא צוות משימה שהוקם כדי לבחון את הצורך באסדרת קודי התנהגות וולונטריים להגנת סייבר. צוות המשימה מורכב מאנשי ממשל ומנציגים מהתעשייה המקומית והבינלאומית, ותפקידו יהיה לבחון אם קודי ההתנהגות שהממשל מפרסם מספיקים כדי להביא להגברת הגנת הסייבר של מוצרי צריכה, שירותים המוצעים לציבור ושרשראות אספקה של פעולות ומוסדות כלכליים, ממשלתיים ואלו הקשורים בביטחון הלאומי.[169]

גם הקול הקורא להבעת עמדה בנוגע לאפיקי אסדרה עתידיים, שפורסם לאחר פרסום האסטרטגיה לשנת 2020, מצביע על רגולציה שיתופית למטרת גיבוש סטנדרט להגנת סייבר כאפיק יעיל אשר עשוי להביא להגברת נכונות התעשייה להטמיע את דרישות הגנת הסייבר אף אם הן וולונטריות.[170]

III. למטרת עידוד החדשנות

מרכז הצמיחה בהגנת הסייבר (Cyber Security Growth Centre) פועל כעמותה שלא למטרות רווח המתוקצבת על ידי הממשלה. מטרתו למצב את אוסטרליה בחזית העולמית של החדשנות בתחום הגנת הסייבר. תפקיד המרכז הוא ליצור שיתופי פעולה בין הממשלה, עסקים, חברות הזנק, מכוני מחקר והאקדמיה, שירצו לקחת חלק בפעילות בהתנדבות, במטרה להגדיר ולתעדף את אתגרי הגנת הסייבר שהם קריטיים להצלחה הלאומית ושלאוסטרליה יש

167 Australia's Cyber Security Strategy 2016, **לעיל** ה"ש 150, בעמ' 21–26.

168 eSafety Commissioner, *Safety by Design*

169 Australia's Cyber Security Strategy 2020, **לעיל** ה"ש 151, בעמ' 32.

170 Call for Views, **לעיל** ה"ש 152, בעמ' 21.

יתרון יחסי בהם ברמה הבינלאומית. כמו כן, המרכז מתעתד להפעיל רשת של מחקר וחדשנות באמצעות יצירת קשרים עם גופי ממשל, עסקים, חברות הזנק, מכוני מחקר ואקדמיה באוסטרליה ומחוצה לה.[171]

IV. למטרת חינוך והכשרת אנשי מקצוע בתחום הסייבר

ממשלת אוסטרליה הקימה במשותף עם האקדמיה, קהילת המחקר והמגזר העסקי מרכזים אקדמיים למצוינות בתחום הגנת הסייבר בכמה אוניברסיטאות. כמו כן, בשיתוף עם קהילת המחקר והעסקים יגובשו חומרי לימוד בתחום, ויוקצו שעות לימוד בבתי הספר כדי להבטיח שילדי אוסטרליה ילמדו את המקצועות החיוניים לפיתוח קריירה בתחום הגנת הסייבר כבר בגיל צעיר.[172]

5. רגולציה עצמית

המרכז האוסטרלי להגנת הסייבר קובע הנחיות וסטנדרטים להגנת מרחב הסייבר בקרב ארגונים קטנים.[173] כמו כן, ארגונים מהמגזר הפרטי יוכלו לפנות למרכז הגנת הסייבר כדי לקבל הערכה של איכות הגנת הסייבר של המערכות שלהם ושל הפערים הקיימים לעומת מדיניות הגנת הסייבר הוולונטרית המומלצת.[174]

ממשלת אוסטרליה השיקה תוכנית בשם Cyber Security Connect and Protect Program, שמטרתה להעניק לארגונים קטנים ובינוניים (SMEs) עזרה ועצות ממקורות אמינים לצורך שיפור הגנת הסייבר שלהם והתמודדות עם תקיפות ואיומי סייבר. נוסף על כך, ממשלת אוסטרליה העמידה לרשות עסקים

171 *Australia Launches Cybersecurity Growth Centre*, FSTMedia (Dec. 6, 2018)

172 Australia's Cyber Security Strategy 2016, **לעיל** ה"ש 150, בעמ' 39–45. הגופים המשתתפים במאמץ זה הם, בין השאר, ה־Cyber Security National Workforce Growth Program וה־Cyber Security Skills Partnerships Innovation Fund.

173 Australian Cyber Security Centre, Small Business Cyber Security Guide (2021)

174 Australia's Cyber Security Strategy 2016, **לעיל** ה"ש 150, בעמ' 27–36.

קטנים ובינוניים מערכת הכשרות מקוונת וכן מוקד תמיכה אשר יהיה זמין 24 שעות ביממה ויעניק עצות וסיוע בהגנת סייבר.[175] הממשלה גם יצרה תמריצים שיעודדו ארגונים גדולים וספקי שירות לספק לעסקים מסוג זה חבילת שירותי הגנה, כגון חסימת איומי סייבר, תוכנות אנטי־וירוס והכשרת כוח אדם לצורך הגברת ערנות לאיומי סייבר ולתקיפות סייבר.[176]

רגולציה עצמית מיושמת גם לגבי הגנת סייבר בשרשראות אספקה (supply chains). ממשלת אוסטרליה פרסמה הנחיות בנוגע לניהול סיכוני הסייבר בשרשראות אספקה, ומפתחת עקרונות לטכנולוגיה חיונית בשרשראות אספקה שמטרתם לסייע לארגונים, כמו גם לממשלה עצמה, לקבל החלטות מודעות בנוגע להגנה על טכנולוגיה קריטית בשרשראות אספקה. הציות להנחיות ולעקרונות הוא וולונטרי.[177]

באופן דומה, ממשלת אוסטרליה קבעה קוד התנהגות, שהציות לו וולונטרי, המשקף את ציפיותיה לאבטחת מכשירי צריכה פופולריים מקטגוריית "האינטרנט של הדברים".[178] המרכז להגנת הסייבר אף פרסם מדריך הפונה לציבור הרחב ולחברות קטנות ובינוניות ובו הנחיות בנוגע לקנייה של מוצרי צריכה מסוג זה, שימוש בהם ופינויים בתום השימוש,[179] במטרה להביא להגברת המודעות והערנות של הצרכנים אשר תביא להגברת הביקוש מצידם למוצרי צריכה מאובטחים כיאות.[180] ואולם, בסקר שערכו משרד הפנים ומשרד התעשייה, המדע, האנרגיה והמשאבים כחצי שנה לאחר פרסום אסטרטגיית הגנת הסייבר לשנת 2020 נמצא שמרבית יצרני מוצרי הצריכה מסוג האינטרנט של הדברים לא הטמיעו את דרישות קוד ההתנהגות. משום כך, ממשלת אוסטרליה שוקלת

175 *The ACSC On-Call 24/7*, ACSC – Australian Cyber Security Centre

176 Australia's Cyber Security Strategy 2020, **לעיל** ה"ש 151, בעמ' 30.

177 Call for Views, **לעיל** ה"ש 152, בעמ' 47.

178 Australian Government, Code of Practice: Securing the Internet of Things for Consumers (2020)

179 Australian Cyber Security Centre, Tips to Secure your Internet of Things Device (2020)

180 Australia's Cyber Security Strategy 2020, **לעיל** ה"ש 151, בעמ' 32.

בימים אלה את נקיטת הצעדים שלהלן במסגרת הכלי של רגולציה עצמית, ופנתה בעניין זה לקבלת הערות מהאקדמיה, מהתעשייה ומהצרכנים:

(**1**) אסדרה וולונטרית שתחול רק על ארגונים גדולים שאינם תשתיות קריטיות, ותכלול מתווה לניהול סיכוני סייבר בפיקוח דירקטריון החברה. תוכן האסדרה עצמו ייקבע בדרך של רגולציה שיתופית. סטנדרט ההגנה הוולונטרי ישמש ככלי פרשני לחובות הכלליות המוטלות על ארגונים מכוח חוק הגנת הפרטיות, חוק הגנת הצרכן או חוק החברות. כך, למשל, הגנת סייבר תיחשב כחלק ממילוי חובת הזהירות של דירקטורים ומנהלים בארגון וכצעד סביר שעל ארגון לנקוט כדי להגן על המידע האישי המצוי בידו. אף שהסטנדרט הוולונטרי יותאם לארגונים גדולים, גם חברות קטנות ובינוניות יכולות להפיק ממנו תועלת. ארגון שיטמיע את עקרונות הסטנדרט הוולונטרי ייחשב כמי שעשה כל שביכולתו כדי להבטיח את הגנת הסייבר במערכות הארגון ובמוצרים או בשירותים שהוא מספק.[181]

(**2**) הגברת השקיפות באמצעות חיוב בהצגת "תווית". עבור רוב הצרכנים באוסטרליה, הגנת סייבר היא שיקול חשוב במכלול השיקולים המובאים בחשבון בעת רכישת מכשיר חכם, אך כמעט 50% מהם מאמינים בטעות שאמצעי הגנת סייבר מוטמעים בכל המכשירים החכמים הנמכרים באוסטרליה.[182] לפיכך, הקול הקורא מבקש לבחון יצירת מתווה וולונטרי לדירוג רמת הגנת הסייבר של מכשיר חכם ולפרסומה בתווית. התוויות יגבירו את השקיפות בנוגע לרמת הגנת הסייבר המוטמעת במכשיר החכם, צרכנים מודעים יתחשבו במידע זה בעת ההחלטה אם לקנות את המוצר וכך התוויות יהיו תמריץ חשוב לנקיטת רמת הגנת סייבר נאותה בדרך של רגולציה עצמית.[183]

(**3**) עיגון סעדים לצרכן שזכויותיו נפגעו עקב תקיפת סייבר על מכשיר או שירות שעשה בו שימוש. יצרן שיודע שהוא עלול להיות מחויב במתן סעד לצרכן במקרה של תקיפת סייבר יפעל להגברת הגנת הסייבר כדי שלא לחוב

181 Call for Views, **לעיל** ה"ש 152, בעמ' 20–21.

182 Data61, Results of the IoT Consumer Focused Survey (Unpublished Report Produced for the Cyber Security Cooperative Research Centre 2020); Shane D. Johnson et al., *The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay*, Plos One (2020)

183 Call for Views, **לעיל** ה"ש 152, בעמ' 38–39.

באחריות למתן סעד לצרכן. הוצע לקבוע שבמקרה של מתקפת סייבר אי־מתן סעד בהתאם לאחריות להגנת הצרכן לפי החוק ייחשב עוולה אזרחית. כמו כן, בנסיבות מסוימות תוכל רשות הגנת הצרכן באוסטרליה לחייב את היצרן במתן סעדים לצרכן אם נמצא שהיצרן אחראי לנזק שנגרם לצרכן עקב מתקפת הסייבר. אפיק נוסף הנבחן כעת הוא מתן זכות לצרכן להגיש תביעה בבית משפט, ולא רק תלונה ברשות להגנת הפרטיות, בגין פגיעה בפרטיותו. כך, צרכן שפרטיותו נפגעה עקב תקיפת סייבר יוכל לתבוע סעד בבית משפט מארגון שלטענת הצרכן לא נקט אמצעי הגנה סבירים, לרבות הגנת סייבר, כדי למנוע את הפגיעה בפרטיותו.[184]

(**4**) השקת תוכנית ממשלתית ל"בריאות סייבר" בארגונים קטנים. ארגון אשר יעמוד בכל דרישות התוכנית, בהתאם לבחינה עצמית שיערוך לעצמו בבקרה קלה מצד הממשלה, יקבל "תו תקן לבריאות סייבר" ("Cyber Health Check") שאותו יוכל להציג בציבור, שתקף למשך שנה אחת בלבד. מטרת התוכנית כפולה: להציג בפני ארגונים מתווה פשוט וברור לאמצעי הגנת הסייבר שיש לנקוט, ולספק לציבור הצרכנים סמן מהיר וקל לרמת הגנת הסייבר בארגון. הנחת המוצא היא שצרכנים יעדיפו מוצרים שיוצרו בידי ארגונים המציגים את תו התקן לבריאות סייבר על פני מוצרים שאין לדעת מהי רמת הגנת הסייבר של הארגון שמייצר אותם, בעיקר בשווקים שבהם נעשה שימוש במידע רגיש או בשרשראות אספקה, וכך באמצעות התחרות בשוק תוגבר רמת הגנת הסייבר.[185]

184 **שם**, בעמ' 54.

185 **שם**, בעמ' 48–49.

6. סיכום מודל הרגולציה להגנת מרחב הסייבר באוסטרליה

לוח 2
האסדרה של הגנת הסייבר באוסטרליה

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה ריכוזית	כלל המגזרים בעת חירום	המרכז האוסטרלי להגנת הסייבר מרכז ומנהל את כל מאמצי הגנת הסייבר של ממשלת אוסטרליה בזמן חירום.
	יצרני מוצרי צריכה חכמים	הצעת חוק הממתינה להערות הציבור: הטלת סטנדרט הגנת סייבר התואם את הסטנדרט האירופי, או לחלופין רק הטלת חובה לציין את מועד הפקיעה של עדכוני אבטחה.
רגולציית ציווי ושליטה רכה וביזורית	חלק מהתשתיות הקריטיות, ספקי שירותים דיגיטליים, ארגונים גדולים	אסדרה מגזרית במגזר הפיננסי, לרבות בנקים, חברות ביטוח וקרנות מימון. ספקי שירותים דיגיטליים המתקשרים בחוזה עם רשות המיסים האוסטרלית מתחייבים בחוזה לנקוט רמת הגנת סייבר מסוימת. חובת הגנת סייבר על 11 מגזרי תשתיות קריטיות. הצעה לחייב ארגונים גדולים להטמיע אמצעים לניהול הגנת סייבר.
	כלל המגזרים	חובות כלליות, שאינן ייעודיות להגנת הסייבר, מוחלות על כלל המגזרים מכוח חוק הגנת הפרטיות, חוק הגנת הצרכן וחוק החברות.
רגולציה שיתופית	כלל המגזרים	שיתוף מידע על איומי סייבר, מתקפות סייבר ודרכי התמודדות עימם בין המגזר הציבורי לפרטי, באופן וולונטרי במודל תלת־שכבתי. הליכי שיתוף ציבור והקמת פאנל ייעוץ מקצועי לגיבוש אסטרטגיה לאומית להגנת סייבר, וכן הקמת גופים בין־מגזריים ייעודיים לקביעת סטנדרטים בתחום. יצירת שיתופי פעולה וולונטריים בין המגזר הציבורי, המגזר הפרטי והמגזר השלישי שמטרתם להגדיר ולתעדף את אתגרי הגנת הסייבר, ועידוד מחקר ופיתוח בהתאם לתעדוף.

סוג הרגולציה	תחולה	עיקרי הרגולציה
		מרכזים אקדמיים למצוינות בתחום הסייבר שהוקמו בשיתוף פעולה בין המגזר הפרטי, המגזר הציבורי, האקדמיה ומכוני מחקר. מסגרות לשיתוף פעולה בין המגזר הציבורי, המגזר הפרטי, האקדמיה והמגזר השלישי, שיפעלו באופן וולונטרי לפי הנחיות שיקבע המרכז להגנת הסייבר לשם קביעת קווים מנחים וולונטריים להגנת סייבר.
רגולציה עצמית משולבת תמריצים	ארגונים מהמגזר הפרטי שאינם תשתיות קריטיות	המרכז להגנת הסייבר קובע הנחיות וסטנדרטים להגנת מרחב הסייבר, וארגונים המבקשים לאמוד את איכות הגנת הסייבר שלהם יכולים להשתמש בהם. המרכז להגנת הסייבר פרסם עקרונות מנחים להגנת סייבר בשרשראות אספקה ובמכשירי צריכה חכמים. הצעה לעיגון בחוק של מתווה וולונטרי להגנת סייבר בארגונים גדולים; של חיוב בהצגת תוויות המפרטות את רמת הגנת הסייבר במוצר או בשירות; של חיזוק זכויות הצרכן ככלי ענישה; ושל תוכנית "בריאות סייבר" בארגונים קטנים.

ג.
האיחוד האירופי

מדיניות הגנת הסייבר של האיחוד האירופי מהווה מסגרת רגולטורית מחייבת למדינות האיחוד. משום כך, הבנתה מסייעת להבנת מדיניות הגנת הסייבר במדינות האיחוד, כמו גם באנגליה, שהייתה חלק מהאיחוד האירופי עד הברקזיט בפברואר 2020.

האיחוד האירופי החל בגיבוש מדיניות הגנת סייבר בשנת 2013, עם פרסומה של אסטרטגיית האיחוד בנושא.[186] בשנת 2016 אומץ דבר החקיקה הראשון

186 European Commission, *Joint Communication to the European Parliament, The Council, The European Economic and Social Committee*

והמרכזי בתחום – דירקטיבת NIS.[187] המדינות החברות באיחוד חויבו לאמץ את דירקטיבת NIS בחקיקה המדינתית שלהן עד מאי 2018. מטרתה המרכזית של דירקטיבת NIS הייתה להבטיח רמה מינימלית אחידה של הגנת סייבר בתשתיות קריטיות ובקרב ספקי שירותים דיגיטליים מהסוגים המנויים בדירקטיבה ברחבי האיחוד האירופי.[188] להלן נפרט כמה מההוראות המרכזיות בדירקטיבת NIS:

(**1**) מדינות האיחוד חויבו לגבש ולפרסם אסטרטגיה לאומית להגנת הסייבר ולייחד רשות לאומית אחת או יותר שתהיה האחראית להגנת מרחב הסייבר בקרב מפעילי תשתיות קריטיות וספקי שירותים דיגיטליים.[189] על האסטרטגיה הלאומית לפרט את מטרות המדיניות והכלים הרגולטוריים שישמשו להשגתן כדי להבטיח, לכל הפחות, הגנת סייבר נאותה בקרב המגזרים והשירותים המפורטים בתוספת לדירקטיבת NIS.[190] באשר לרשות הלאומית, יש להעניק לה את הסמכויות והאמצעים הנדרשים לשם פיקוח על הציות לדרישות החקיקה המדינתית המאמצת את דירקטיבת NIS ולשם אכיפת החקיקה.[191]

---

and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final (Feb. 7, 2013)

187 Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1 (להלן: דירקטיבת NIS).

188 **שם**, Annex II, III. מגזרי התשתיות הקריטיות המנויים בדירקטיבה הם אנרגיה (חשמל, שמן וגז), תחבורה (תחבורה אווירית, הובלה ברכבות, תחבורה ימית ותחבורה יבשתית), בנקאות, תשתית שווקים פיננסיים, בריאות, אספקת מי שתייה והפצתם ותשתית דיגיטלית. ספקי השירותים הדיגיטליים המנויים בדירקטיבה הם פלטפורמות סחר אלקטרוני, מנועי חיפוש ושירותי מחשוב ענן.

189 **שם**, בסעיפי הקדמה (Recital) (29)–(30), ובסעיפים (Articles) 1(2)(a), 1(2)(e), 8 לדירקטיבה.

190 **שם**, בסעיף 7.

191 **שם**, בסעיף 15.

(**2**) המדינות החברות באיחוד חויבו להחזיק ביכולות הגנת סייבר לאומיות מסוימות, כגון צוות תגובה למתקפות סייבר (Computer Security Incident Response Team, CSIRT).[192]

(**3**) הוקמה NIS Cooperation Group, שהיא מסגרת לשיתוף מידע ולשיתוף פעולה ברמה אסטרטגית בין המדינות באיחוד למטרות הגנת סייבר. חברים בה נציגים מנציבות האיחוד, ממדינות חברות ומהסוכנות האירופית לביטחון רשת ומידע (European Union Agency for Network and Information Security, ENISA), ובעת הצורך יוזמנו אליה גם נציגים מהתעשייה. מטרת NIS Cooperation Group היא לשמש כפלטפורמה לשיתוף מידע בנוגע למתקפות סייבר ולקווי הפעולה הטובים ביותר (best practices) למניעת מתקפות סייבר, התמודדות עימן והחלמה מהן, להעלאת מודעות הציבור לאיומי סייבר, להכשרת כוח אדם למטרות הגנת סייבר ולמחקר ופיתוח בנושא הגנת רשתות ומערכות מידע. ה־NIS Cooperation Group תדון גם ביכולות הגנת הסייבר ובמוכנותה של כל מדינה למתקפת סייבר, ותסייע בהערכת האסטרטגיה הלאומית להגנת מרחב הסייבר במדינות השונות.[193]

(**4**) עוגנו דרישות הגנת סייבר ממפעילי שירות חיוני וספקי שירותים דיגיטליים, שהוגדרו כפלטפורמות סחר אלקטרוני, מנועי חיפוש וספקי שירותי ענן, שעסקים רבים נשענים עליהם,[194] במתכונת של רגולציית ציווי ושליטה רכה. מפעילי שירות חיוני או ספקי שירותים דיגיטליים נדרשים לאמץ את האמצעים הטכניים והארגונים הראויים והמידתיים לניהול הסיכון הנשקף לרשתות ולמערכות המידע שלהם, לשם מניעת מתקפת סייבר, מזעור השלכותיה והבטחת המשכיות השירות שהם מספקים.

לפי דירקטיבת NIS, מפעילי שירות חיוני הם ארגונים הפועלים באחד ממגזרי התשתיות הקריטיות המנויים בתוספת השנייה לדירקטיבה, ושהמדינה החברה באיחוד מנתה אותם כמפעילי שירות חיוני. כדי לקבוע אם ארגון מסוים ממגזרי התשתיות הקריטיות המנויים בדירקטיבת NIS הוא מפעיל שירות חיוני על

192 **שם**, בסעיף הקדמה (34) ובסעיפים 9, 1(2)(c) לדירקטיבה.

193 **שם**, בסעיפי הקדמה (4),(35)–(36) ובסעיפים 11, 1(2)(b) לדירקטיבה.

194 **שם**, בסעיפי הקדמה (48), (52), (55).

המדינה החברה להביא בחשבון כמה קריטריונים: (1) הארגון מספק שירות החיוני להמשכיותה של פעילות חיונית כלכלית או חברתית; (2) השירות המסופק תלוי במערכות מידע ורשת; (3) מתקפת סייבר עלולה להיות בעלת השפעה הרסנית על מתן השירות. הקריטריונים שלהלן עשויים, לפי דירקטיבת NIS, לסייע למדינה החברה לאמוד את מידת ההשפעה של מתקפת סייבר על השירות של מפעיל מסוים ולהעריך אם מדובר בהשפעה הרסנית: (1) מספר המשתמשים המסתמכים על השירות; (2) מידת התלות של מגזרים קריטיים אחרים בשירות; (3) ההשפעה שעשויה להיות למתקפת הסייבר, מבחינת משך זמן הפגיעה ורמתה, על פעילות כלכלית או חברתית או על ביטחון הציבור; (4) נתח השוק של מפעיל השירות; (5) היקפה הגיאוגרפי של הפגיעה; (6) חשיבותו של המפעיל לשימור רמה מספקת של השירות, בהתחשב בזמינותם של אמצעים חלופיים לאספקת השירות. כמו כן על המדינות להביא בחשבון גם שיקולים הייחודיים לכל מגזר. כל מדינה החברה באיחוד סיפקה רשימה של מפעילי שירות חיוני עם כניסת דירקטיבת NIS לתוקף במאי 2018, וחויבה לעדכנה מדי שנתיים.[195]

(**5**) הוגדרה רגולציית ציווי ושליטה ריכוזית על ספק שירות דיגיטלי אשר לא התאגד במדינה ממדינות האיחוד אך מציע שירות לעסקים ותושבים באיחוד. לפי דירקטיבת NIS על ספק שירות דיגיטלי כאמור למנות נציג במדינה ממדינות האיחוד. שימוש בשפה של אחת ממדינות האיחוד, שאינה השפה במקום התאגדותו של הספק, קבלת תשלום בעבור השירות במטבע של מדינה ממדינות האיחוד או פרסום על אודות לקוחות מתחומי האיחוד יצביעו על מתן שירות בתחומי האיחוד.[196]

(**6**) רגולציית ציווי ושליטה ריכוזית נוספת שהדירקטיבה מפעילה היא החיוב של מפעיל שירות חיוני או ספק שירותים דיגיטליים לדווח ללא דיחוי לרשות הסייבר המדינתית הרלוונטית או ל־CSIRT המדינתי על כל מתקפת סייבר המשפיעה באופן משמעותי על המשכיות השירות שהוא מספק. בהערכת מידת ההשפעה על השירות החיוני או על השירות הדיגיטלי יש להביא בחשבון את מספר המשתמשים המושפעים מההפרעה לשירות, משך המתקפה והיקף

195 **שם**, בסעיפים (2) 5, (5) 5, 6.

196 **שם**, בסעיף הקדמה (65) ובסעיפים (3)–(2)18 לדירקטיבה.

השפעתה מבחינה גיאוגרפית. לגבי שירות דיגיטלי יש להתחשב גם במידת השפעתה של מתקפת סייבר על השירות על פעולות חברתיות וכלכליות. בהתאם להודעת מפעיל השירות החיוני או ספק השירותים הדיגיטליים תיידע רשות הסייבר המדינתית רשויות סייבר במדינות חברות אחרות העשויות להיות מושפעות אף הן ממתקפת הסייבר. כמו כן, רשות הסייבר המדינתית רשאית, בהתאם לשיקול דעתה ולאחר שנועצה בנושא עם מפעיל השירות החיוני או ספק השירות הדיגיטלי המותקף, ליידע את הציבור בדבר מתקפת הסייבר.[197]

עם זאת, נוכח האופי הגלובלי וחוצה הגבולות של פעולתם של ספקי שירות דיגיטליים, אשר מחייב הרמוניזציה של הרגולציה כלפיהם בין כל מדינות האיחוד האירופי, לעומת מפעילי שירות חיוני שתפקודם קשור על פי רוב לתשתיות פיזיות בשטחה של כל אחת מן המדינות החברות, קבעה דירקטיבת NIS רף מקסימלי לדרישות הגנת הסייבר שמדינה חברה יכולה להטיל על ספקי שירות דיגיטליים, לעומת רף מינימום לדרישות הגנת הסייבר ממפעילי שירות חיוני.[198] כמו כן, דירקטיבת NIS החריגה ספקי שירותים דיגיטליים קטנים או בינוניים מהצורך לעמוד בדרישות הגנת הסייבר.[199] נוסף על כך, בדירקטיבה נקבע כי הפיקוח המדינתי על תשתיות קריטיות צריך להיות פיקוח בטרם פעולה (ex-ante) ואילו הפיקוח על ספקי שירותים דיגיטליים קריטיים צריך להיות לאחר פעולה (ex-post) – כלומר הרשות האחראית תוכל לפעול נגד ספק שירותים דיגיטליים רק לאחר שיוצגו בפניה ראיות על אי־ציות מצידו לדרישות הגנת הסייבר לפי דירקטיבת NIS.[200]

בדצמבר 2020 פרסמה נציבות האיחוד האירופי את אסטרטגיית הגנת הסייבר של האיחוד לשנים 2020–2025. האסטרטגיה קראה לעדכן את דירקטיבת NIS מכמה סיבות: התגברות האיומים על מרחב הסייבר, השאיפה להבטיח הגנת סייבר נאותה בקרב מוצרים ושירותים העושים שימוש בטכנולוגיית 5G, וחוסר הבהירות בנוגע להיקף תחולתה של דירקטיבת NIS בקרב המדינות החברות

197 **שם**, בסעיפים 14, 16.

198 **שם**, בסעיף הקדמה (57).

199 **שם**, בסעיפי הקדמה (49), (53).

200 **שם**, בסעיף הקדמה (60) ובסעיף 17 לדירקטיבה.

עקב ההגדרות השונות שניתנו בכל מדינה למפעיל שירות חיוני ולספק שירותים דיגיטליים.[201]

בנובמבר 2022 אישרה מועצת האיחוד האירופי את דירקטיבת NIS המעודכנת (להלן: NIS2),[202] ולהלן כמה מהחידושים בה:

(**1**) הרחבת מעגל הגופים המאוסדרים באמצעות רגולציית ציווי ושליטה רכה, הכולל עתה גם גופים ממגזרים נוספים, כגון ספקים של רשתות ושירותי תקשורת אלקטרונית, שירותים דיגיטליים כגון פלטפורמות רשתות חברתיות, ניהול מים וביוב, יצרנים של מוצרים קריטיים כגון מכשור רפואי, תרופות ומוצרים כימיים, תעשיית המזון, שירותי הובלה ודיוור ומינהל ציבורי, לרבות גופים קטנים ובינוניים ממגזרים אלו וממגזרי תשתיות קריטיות אחרים המנויים בדירקטיבת NIS, וכן גופים השייכים לשרשאות אספקה של טכנולוגיות תקשורת ומידע, לרבות טכנולוגיית 5G ומוצרי צריכה חכמים. הרחבת תחולת דירקטיבת NIS גם למוצרים ושירותים בטכנולוגיית 5G נשענת בעיקרה על מסמך שפרסמה נציבות האיחוד בינואר 2020, המפרט את האמצעים למזעור סיכוני הסייבר הצפויים לרשתות 5G.[203] נוסף על כך, NIS2 מסמיכה את נציבות האיחוד לקבוע קטגוריות של ארגונים חיוניים שמדינות האיחוד יחויבו להטיל עליהם את דרישות NIS2. כך יובטח שבכל המדינות החברות יוגדרו ארגונים מקטגוריות מסוימות כמפעילים חיוניים, במקום זיהוי פרטני של מפעילים חיוניים בכל מדינה ומדינה. עם זאת, גופים הפועלים בתחום ההגנה, הביטחון הלאומי, ביטחון הציבור, אכיפת החוק והמשפט, וכן פרלמנטים ובנקים מרכזיים, הוחרגו מתחולת NIS2.

201 European Commission, *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, JOIN (2020) 18 final (Dec. 16, 2020)

202 Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union Repealing Directive (EU) 2016/1148 (NIS 2 Directive)

203 NIS Cooperation Group, Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures (2020)

(**2**) השוואה של דרישות הגנת הסייבר המוטלות באמצעות רגולציית ציווי ושליטה רכה על ספקי שירותים דיגיטליים לאלו המוטלות על מפעילי שירותים חיוניים, ייעול חובות הדיווח, אמצעי פיקוח ודרישות אכיפה מחמירים יותר, וקביעת רף מינימום לסנקציות שאפשר להטיל בגין אי־ציות לדרישות דירקטיבת NIS בכל המדינות החברות באיחוד.

נציבות האיחוד האירופי הציגה גם שתי יוזמות חקיקה אשר ישתלבו עם חקיקת NIS2. היוזמה הראשונה היא עדכון הדירקטיבה משנת 2008[204] בנושא החוסן של מפעילי תשתיות קריטיות פיזיות ממגזרי האנרגיה, התחבורה, הבנקאות, תשתיות השווקים הפיננסיים, הבריאות, מי השתייה, הביוב, התשתיות הדיגיטליות והחלל, המספקות שירותים חיוניים שפרנסתם של אזרחי האיחוד והתפקוד הראוי של השוק המשותף תלויים בהם.[205] בעוד עדכון דירקטיבת החוסן עוסק בהגנה על ארגוני תשתיות קריטיות מפני איומים פיזיים, NIS2 עוסקת בהגנה על ארגונים ממגזרים אלו, וממגזרים נוספים, מפני איומים במרחב הסייבר.[206] היוזמה השנייה היא הצעת חוק חוסן הפעילות הדיגיטלית במגזר הפיננסי (Digital Operational Resilience Act for the Financial Sector, להלן: DORA) העוסקת בהרמוניזציה של דרישות הגנת הסייבר בקרב ארגונים מהמגזר הפיננסי בכל מדינות האיחוד תוך הבטחת שיתוף מידע הנוגע להגנת סייבר ביניהם.[207] DORA מבוססת על דירקטיבות NIS ו־NIS2 ועוסקת

204 Council Directive 2008/114 of 8 December 2008, on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, 2008 O.J. (L 345) 75

205 *Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities*, COM (2020) 829 final (Dec. 16, 2020)

206 Council of the EU Press Release 1009/21, Strengthening EU Resilience: Council Adopts Negotiating Mandate on the Resilience of Critical Entities (Dec. 20, 2021)

207 *Porposal for a Regulation of the European Parliament and of the Concil on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (DORA)*, 10581/22 (June 23, 2022)

בנושאים שאינם מאוסדרים בדירקטיבות אלו בכל הקשור לארגונים מהמגזר הפיננסי.[208]

ו. אנגליה[209]

אנגליה מדורגת במקום התשיעי במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם.[210] במדד הגנת מרחב הסייבר של Comparitech, אשר מתמקד בהגנת הסייבר ברמת המשתמש הבודד, זכתה אנגליה ב־36 מתוך 75 נקודות אפשריות.[211]

אסדרת ההגנה על מרחב הסייבר באנגליה מבוססת אף היא על הערכת הסיכון האפשרי הנשקף מתקיפת סייבר על חברה, רשות או תשתית מסוימת לביטחון הציבור, לביטחון המדינה או ליציבותה הכלכלית,[212] וכן על עקרון האחריות משותפת אך שונה.

208 Council of the EU Press Release 433/22, Digital Finance: Provisional Agreement Reached on DORA (May 11, 2022)

209 מדיניות הגנת הסייבר המפורטת להלן תקפה לרחבי אנגליה, ובכל מסמכי המדיניות מובהר שממשלת אנגליה תעבוד בשיתוף פעולה עם ממשלות סקוטלנד, ויילס וצפון אירלנד כדי להבטיח רמת הגנת סייבר דומה בכולן. ראו למשל, HM Government, National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK, 21 (2022) (להלן: האסטרטגיה לשנים 2025–2022).

210 Global Cybersecurity Index 2020, **לעיל** ה"ש 29.

211 Bischoff, **לעיל** ה"ש 30.

212 UK Prime Minister, A Strong Britain in an Age of Uncertainty: The National Security Strategy 10–11, 14, 22, 27, 29–30 (2010); UK Prime Minister, Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review 3, 47 (2010) (להלן: Securing Britain); UK Prime Minister Office, Fact Sheet 18: Cyber Security (2011) (להלן: Fact Sheet 18); UK Cabinet Office, Cyber Security Strategy: Statement 1 Year On (2012) (להלן: Statement 1 Year On); UK Cabinet Office, The UK Cyber Security Strategy Report on Progress – December 2012 Forward Plans (2012) (להלן: 2012 Forward Plans); UK Cabinet Office, Progress Against the Objectives of the National Cyber Security Strategy – December 2013 (2013) (להלן: Progress Against Objectives 2013); UK Cabinet Office, The UK Cyber Security Strategy Report on Progress – December 2013 Our Forward Plans (2013) (להלן: 2013 Forward Plans); UK Cabinet

בהתאם, באנגליה נהוג שילוב של רגולציית ציווי ושליטה, רגולציית ציווי ושליטה רכה, רגולציה שיתופית ורגולציה עצמית. קיים מתאם בין הערכת הסיכון האפשרי מתקיפת סייבר על מגזר מסוים והשפעתה על הביטחון הלאומי, יציבותה הכלכלית של המדינה וביטחון הציבור בה, ובין מרחב שיקול הדעת והיקף הרגולציה העצמית של הגוף המאוסדר.[213]

על מגזרי תשתיות קריטיות וספקי שירותים דיגיטליים, כגון שירותי ענן וחנויות אפליקציות,[214] חלה רגולציה שונה מזו החלה על חברות, רשויות ותשתיות אחרות שאינן נמנות עם מגזרים אלו. עם מגזרי התשתיות הקריטיות נמנים כיום 13 מגזרים: כימיקלים, מפעלי גרעין אזרחיים, תקשורת, הגנה, שירותי חירום, אנרגיה, המגזר הפיננסי, מזון, ממשל, בריאות, חלל, תחבורה ומים.[215]

גישת האסדרה התפתחה לאורך השנים. הגישה השלטת עד 2016 הייתה רגולציה עצמית בקרב חברות במגזר הפרטי שאינן תשתיות קריטיות, ורגולציה שיתופית על בסיס התנדבותי בקרב מפעילי תשתיות קריטיות. בשלהי שנת 2016 חל שינוי מהותי בגישה הרגולטורית להגנת הסייבר של ממשלת אנגליה, נוכח ההבנה שהשוק לבדו אינו מספק תמריצים הולמים להגברת הגנת הסייבר על ידי המגזר הפרטי, ומשום כך נדרשת מעורבות מוגברת של הממשלה. תובנה זו הובילה להעדפת רגולציה מסוג ציווי ושליטה (ריכוזית או רכה וביזורית) על פני רגולציה שיתופית או עצמית.[216] בפברואר 2022 התפרסמה אסטרטגיית

Office et al., Policy Paper: 2010 to 2015 Government Policy: Cyber Security (2015)

213 Securing Britain, **לעיל** ה"ש 212, בעמ' 47; Fact Sheet 18, **לעיל** ה"ש 212; Progress Against Objectives 2013, **לעיל** ה"ש 212; UK Intelligence and Security Committee, Foreign Involvement in the Critical National Infrastructure: The Implications for National Security (2013); HM Government, National Cyber Security Strategy 2016-2021, 14 (2017) (להלן: האסטרטגיה לשנים 2016–2021).

214 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209.

215 ראו *Critical National Infrastructure*, Centre for the Protection of National Infrastructure

216 The Joint Committee on the National Security Strategy, Cyber Security of the UK's Critical National Infrastructure 13 (3rd Report of Session 2017-19, 2018) (להלן: אבטחת סייבר של תשתיות לאומיות באנגליה). ראו דיון בסעיף II.2 **להלן**.

הסייבר הלאומית לשנים 2025–2022. לצד שימור המתווה הרגולטורי שהונהג באסטרטגיה לשנים 2021–2016, התובנה המרכזית של האסטרטגיה החדשה היא שבמרחב הסייבר מתנהלת תחרות תמידית בין כוחות דמוקרטיים לכוחות דיקטטוריים, המיוצגים בעיקר על ידי מדינות כמו רוסיה וסין, ולכן נדרשת הגנה על מרחב הסייבר לשם שמירה על משטר דמוקרטי וזכויות יסוד. כדי להתמודד עם תחרות זו ולהבטיח שהסטנדרטים המקובלים במרחב הסייבר לא ייקבעו על ידי מדינות שאינן דמוקרטיות וחופשיות ויהיו מנוגדים לערכים המקובלים באנגליה, על אנגליה לפתח יכולת להגן ולקדם את האינטרסים הלאומיים שלה במרחב הסייבר – יכולת המכונה "כוח סייבר".[217]

כחלק מגיבושו של כוח הסייבר, האסטרטגיה מדגישה את הצורך לחזק את יכולת ההרתעה של אנגליה באמצעות פעולות הגנתיות והתקפיות. לפיכך, בשלהי שנת 2020 הוקם כוח הסייבר הלאומי (National Cyber Force, NCF) שמאחד תחת קורת גג אחת מומחי הגנה ומודיעין ממטה התקשורת הממשלתי (Government Communications Headquarters, GCHQ) וממשרד ההגנה. כמו כן, ביחידות המשטרה האזוריות והמקומיות הוקמו יחידות המתמחות באכיפה נגד פשעי סייבר. יחידות אלו מנוהלות על ידי ה־National Crime Agency (NCA) ותפקידן לתת מענה מקיף לפשיעת סייבר.[218] זאת ועוד, כוח הסייבר שונה מיכולות או מכוחות אחרים שיש בידי המדינה שכן זוהי יכולת מבוזרת יותר והממשלה חייבת לשתף פעולה עם מגזרים אחרים כדי להשיגה ולעשות בה שימוש. משום כך, מדיניות נאותה להגנת מרחב הסייבר מחייבת אימוץ גישה כלל־חברתית מתוך הבנה שכל שחקן, מהמגזר הציבורי, מהמגזר הפרטי או מהמגזר השלישי, וכן האזרחים עצמם, חייב לתרום את חלקו להגנת מרחב הסייבר, ושנדרש שיתוף פעולה בין השחקנים השונים תוך הבנת הקשר ביניהם.[219]

217 **שם**, בעמ' 10.

218 UK Cabinet Office, Policy Paper: Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy 41-42 (2021); האסטרטגיה לשנים 2025-2022, **לעיל** ה"ש 209, בעמ' 17, 24, 36-38, 42.

219 **שם**, בעמ' 36-38.

1. רגולציית ציווי ושליטה בעת תקיפת סייבר

המרכז הלאומי להגנת סייבר (National Cyber Security Centre, NCSC), יחידה טכנולוגית הפועלת במסגרת ה־GCHQ שהוקמה בשנת 2016, קבע בשנת 2018 שיטה לסיווג מתקפות סייבר לשש דרגות חומרה: מצב חירום לאומי, תקיפת סייבר משמעותית מאוד, תקיפת סייבר משמעותית, תקיפת סייבר ממשית, תקיפת סייבר בינונית ותקיפת סייבר מקומית.[220]

בעת מצב חירום לאומי, תקיפת סייבר משמעותית מאוד ותקיפת סייבר משמעותית נהוגה רגולציית ציווי ושליטה בניהול ה־NCSC.[221] רגולציה מסוג זה הייתה נהוגה לפני 2016 ונהוגה גם כיום.

מצב חירום לאומי במרחב הסייבר, הקטגוריה החמורה ביותר של תקיפות סייבר, מוגדר כהתרחשותה של מתקפת סייבר הגורמת להפרעה ממושכת לשירותים חיוניים באנגליה או משפיעה על הביטחון הלאומי של אנגליה או על יציבותה הכלכלית, או שעלולות להיות לה השלכות חברתיות או שהיא עלולה להביא לפגיעה בחיי אדם. תקיפת סייבר משמעותית מאוד מוגדרת כתקיפת סייבר שיש לה השפעה משמעותית על הממשלה, על שירותים חיוניים, על חלק ניכר מאוכלוסיית המדינה או על כלכלת המדינה. תקיפת סייבר משמעותית, הקטגוריה השלישית של תקיפות סייבר, מוגדרת ככזו שיש לה השפעה משמעותית על ארגונים גדולים או על גופי ממשל מקומיים, או שהיא מסכנת סיכון משמעותי את הממשלה או שירותים חיוניים במדינה.[222]

בעת תקיפת סייבר ממשית, המוגדרת כתקיפת סייבר בעלת השלכות חמורות על ארגונים בגודל בינוני או כתקיפת סייבר המטילה סיכון רב על ארגונים גדולים או על השלטון המקומי, מנוהלת התגובה על ידי ה–NCSC או רשויות אכיפת החוק (ה־NCA או רשות אכיפת חוק אחרת). בעת תקיפת סייבר בינונית,

220 *New Cyber Attack Categorisation System to Improve UK Response to Incidents*, NSCS (Apr. 11, 2018) (להלן: *New Cyber Attack Categorisation*).

221 HM Government, Prospectus: Introducing the National Cyber Security Centre 7 (2016) (להלן: Introducing the NCSC); האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 40.

222 *New Cyber Attack Categorisation*, **לעיל** ה"ש 220.

המוגדרת כתקיפת סייבר על ארגונים קטנים, או תקיפה החושפת ארגונים בינוניים לסיכון רב, או אינדיקציה ראשונית לפעולת סייבר נגד ארגונים גדולים או השלטון, מנוהלים מאמצי התגובה על ידי רשויות אכיפת החוק, כגון המשטרה, תוך היוועצות, במידת הצורך, עם ה־NCA. בעת תקיפה מקומית, המוגדרת כתקיפת סייבר על אדם מסוים או אינדיקציה ראשונית לפעולות סייבר נגד ארגונים קטנים ובינוניים, התגובה מנוהלת על ידי רשות אכיפת החוק המקומית או על ידי הנפגע עצמו, שיכול להיעזר גם במענה האוטומטי הניתן בנושא על ידי רשויות אכיפת החוק (למשל, המשטרה המקומית).[223]

2. רגולציית ציווי ושליטה בעת שגרה

I. עד שנת 2016: רגולציית ציווי ושליטה רכה וביזורית במגזרי תשתיות קריטיות מסוימים

עד שנת 2016 התמקדה רגולציית הציווי והשליטה הרכה והביזורית במגזרי תשתיות קריטיות מסוימים. לדוגמה, הרגולטור האחראי במגזר הפיננסי (Financial Conduct Authority, FCA) השתמש ברגולציה מסוג זה מתוך הבנה שהאחריות להגנת הסייבר משותפת ל־FCA, לממשלה, לרגולטורים אחרים ולגופים נוספים במישור הבינלאומי. לפיכך, ה־FCA קבעה, בדרך של רגולציית ציווי ושליטה רכה, שעל חברה במגזר הפיננסי לאמץ תרבות הגנת סייבר שבמסגרתה תיקבע רמת הגנת הסייבר הדרושה לכל אחד מנכסי המידע של החברה, ויינקטו הפעולות הנדרשות כדי להגן על מערכותיה מפני איומי סייבר ולמזער את הפגיעה של תקיפת סייבר בתפקודה התקין.[224] עם זאת, ה־FCA לא חייבה את החברות לאמץ אמצעי הגנה מסוימים ולא פירטה כיצד על חברה ליישם את חובתה להגנת הסייבר, אלא התמקדה בשיתוף פעולה ובקבלת תובנות בנוגע לפרקטיקות ההגנה המתאימות מהתעשייה עצמה. כך, למשל, ה־FCA מנהלת קבוצות תיאום המכונות Cyber Coordination Groups, המשמשות פלטפורמה לשיתוף מידע בנושאים אלו בין החברות השונות במגזר

223 שם.

224 *Operational Resilience*, FCA (Mar. 31, 2022)

הפיננסי ובינן לבין ה־FCA. אחד מתוצרי שיתוף המידע הוא דוח המרכז את תובנות התעשייה בנוגע לפרקטיקות הגנת הסייבר הנהוגות בה.[225]

כמו כן, ה־FCA מבצעת מבדקי חדירוּת לבחינת רמת הגנת הסייבר בחברות המאוסדרות. מבדק החדירות מבוסס על המידע המודיעיני הרלוונטי בנוגע לאיומי הסייבר הצפויים לחברה הנבדקת ומותאם למאפייניה. מבדקי החדירות הם מנגנון לבחינה ולשיפור של מידת החוסן של החברה הנבדקת לאיומי הסייבר הצפויים לה, והם גם כלי לרגולציה שיתופית: ה־FCA מעבדת את המידע המודיעיני הנאסף מהממשלה ומהמגזר הפרטי כדי לגבש צפי בנוגע לאיומי הסייבר האפשריים ובוחנת את היתכנותם בחברה המאוסדרת, והיא מצידה משתפת פעולה ומשנה את רמת הגנת הסייבר שלה בהתאם לממצאי המבדק. עם זאת, מבדקי החדירות מוגבלים לשימוש באמצעים חוקיים ואתיים לתקיפה, והדבר עשוי לפגוע באותנטיות ובשימושיות של הסימולציה ועל כן בתוצאותיה.[226]

II. החל משנת 2016

בשלהי שנת 2016 חל שינוי מהותי בגישה הרגולטורית של ממשלת אנגליה להגנת הסייבר, וגברה הנטייה להעדפת רגולציה מסוג ציווי ושליטה, בעיקר רגולציית ציווי ושליטה רכה וביזורית, על פני רגולציה שיתופית או עצמית. שינוי המדיניות הרגולטורית נשען על ממצאי ביקורת שביצעה הממשלה באותה השנה, שמהם עלה כי לחברות פרטיות במגזרים שאינם תשתיות קריטיות ואף לחברות פרטיות המפעילות תשתיות קריטיות אין די תמריצים להטמעת רמת הגנת סייבר מתאימה ורצויה בראייה מדינתית. לפיכך, נוכח העלייה באיומי הסייבר וההשלכות הקשות שיש לכך על אמון הצרכנים ועל אבטחת המידע שלהם, וכן על ביטחון הציבור והשגשוג הכלכלי, הביקורת מצאה שייתכן שיהיה

225 FCA, Cyber Security – Industry Insights (2019)

226 אבטחת סייבר של תשתיות לאומיות באנגליה, **לעיל** ה"ש 216, בעמ' 28–30.

צורך ברגולציה מסוג ציווי ושליטה או בחיזוק התמריצים הניתנים לחברות פרטיות במסגרת הרגולציה העצמית או השיתופית.[227]

אם כן, האסטרטגיה לשנים 2021–2016 דחתה במפורש את ההנחה שעמדה בבסיס האסטרטגיה הקודמת, לשנים 2016–2011, שלפיה הביקוש להגנת סייבר מצד לקוחות הקצה והעלות האפשרית של תקיפת סייבר יוצרים תמריצים מספיקים להגברת רמת הסייבר בידי בעלים ומפעילים של תשתיות קריטיות.[228] באסטרטגיה לשנים 2021–2016 נקבע כי המגזר הפרטי, על אף חלקו המשמעותי במרחב הסייבר, אינו מסוגל למלא את התפקיד המצופה ממנו להגברת ההגנה של מרחב זה, ואין לצפות מאזרחים ומעסקים קטנים לנקוט את צעדי ההגנה המספיקים למזעור מתקפות סייבר. משום כך נקבע שעל ממשלת אנגליה למלא תפקיד מרכזי ומקיף יותר מזה שלכאורה היה עליה למלא לאור חלקה המצומצם במרחב הסייבר יחסית לחלקו של המגזר הפרטי.[229]

אחד הצעדים להגברת מעורבות המדינה שתוארו באסטרטגיה לשנים 2016–2021 היה הקמת ה־NCSC. בשנים שחלפו מאז הקמתו חל שיפור באחידות ובעקביות של ההנחיות והסטנדרטים הממשלתיים להגנת הסייבר. כאמור, ה־NCSC הוא יחידה טכנולוגית הפועלת במסגרת מטה התקשורת הממשלתי (GCHQ), ותפקידו לשמש כמקור הידע המרכזי והמייעץ לממשלה ולמגזר הפרטי בכל הקשור בהגנת הסייבר. ה־NCSC הוא הגוף הטכנולוגי המוביל בתחום הגנת הסייבר, והוא מעניק שירות דיגיטלי המספק דרגות הגנת סייבר שונות, מנהל את התגובה המדינתית לתקיפת סייבר משמעותית,[230] מספק יכולות טכנולוגיות וידע לאזרחים, לעסקים ולארגונים ברחבי אנגליה במטרה לסייע להם לנקוט את הצעדים המתאימים לשיפור הגנת הסייבר שלהם, מספק לממשלה מידע טכני והערכות בנוגע לאיומי סייבר כדי לסייע לה בפיתוח ויישום

227 HM Government, Cyber Security Regulation and Incentives Review 4–5 (2016)

228 אבטחת סייבר של תשתיות לאומיות באנגליה, **לעיל** ה"ש 216, בעמ' 18–19.

229 האסטרטגיה לשנים 2016–2021, **לעיל** ה"ש 213, בעמ' 26–29.

230 לעניין הגדרת "תקיפת סייבר משמעותית" ראו הדיון בטקסט הנלווה לה"ש 222 **לעיל**.

מדיניות ורגולציה, שמטרתן להגן על האינטרסים של אנגליה במרחב הסייבר, מספק הגנה על מידע ושירותים קריטיים המשמשים את צבא אנגליה, ותומך בפיתוח יכולות הגנת סייבר באמצעות סיוע למסגרות חינוך ותמיכה ביוזמות שמטרתן הגברת ההשקעות במגזר הסייבר. אולם לצד מגוון יכולות אלו, ל־NCSC אין סמכויות אכיפה והוא אינו עוסק כלל בקביעת רגולציה.[231]

צעד נוסף של האסטרטגיה לשנים 2021–2016 להגברת מעורבות המדינה היה הוספה של "קבוצת פרימיום" (Premium Group) לרשימת 13 מגזרי התשתיות הקריטיות: קבוצת חברות פרטיות שאינן משתייכות ל־13 מגזרי התשתיות הקריטיות, אך פעילותן מחייבת רמה גבוהה יותר של תמיכה ממשלתית לשם הבטחת רמת הגנת סייבר מספקת. לקבוצה משתייכות החברות המצליחות ביותר באנגליה, אשר מבחינת ערך הקניין הרוחני והמחקר המבוצע בהן יש להן חלק חשוב בעוצמה הכלכלית העתידית של המדינה; חברות המחזיקות במידע אישי או רגיש על אזרחים באנגליה ומחוצה לה, כמו עמותות צדקה; חברות שעלולות להיות מטרה לתקיפות סייבר משמעותיות, כגון חברות תקשורת, שתקיפת סייבר עליהן עלולה לפגוע במוניטין של המדינה, לפגוע באמון הציבור בממשלה או לסכן את חופש הביטוי; ספקי שירותים דיגיטליים, כמו שירותי מחשוב ענן, המאפשרים מסחר וכלכלה דיגיטלית וששירותיהם תלויים באמון לקוחותיהם; וכן כל ארגון שבאמצעות כוחות השוק או סמכותו לפי חוק עשוי להשפיע על הכלכלה הלאומית ולשפר את רמת הגנת הסייבר כולה, למשל חברות ביטוח, משקיעים, רגולטורים ויועצים מקצועיים.[232]

אסטרטגיית הסייבר הלאומית לשנים 2025–2022 המשיכה במתווה הרגולטורי של הגברת מעורבות המדינה, כפי שנקבע באסטרטגיה לשנים 2021–2016, ואף הוצהר בה על הכוונה להרחיב את רגולציית הציווי והשליטה הרכה והביזורית לכלל מגזרי התשתיות הקריטיות וכן להטיל אחריות רגולטורית להגנת סייבר על ארגונים נוספים מהמגזר הפרטי ומהמגזר הציבורי.[233]

231 **שם**, בעמ' 20, 43; האסטרטגיה לשנים 2025–2022, **לעיל** ה"ש 209, בעמ' 40–41.

232 האסטרטגיה לשנים 2021–2016, **לעיל** ה"ש 213, בסעיף 5.4.1.

233 האסטרטגיה לשנים 2025–2022, **לעיל** ה"ש 209, בעמ' 17, 24, 36–38.

i. רגולציית ציווי ושליטה רכה וביזורית על ספקי שירותים דיגיטליים ותשתיות קריטיות

בשנת 2018 הותקנו תקנות הרשת ומערכות המידע לשנת 2018 (The Network and Information Systems Regulations 2018, להלן: תקנות NIS)[234] כחלק מיישום דירקטיבת NIS של האיחוד האירופי. תקנות NIS חלות על חברות שאינן ממגזרי התשתיות הקריטיות ואינן חברות בינוניות או קטנות,[235] אך עונות להגדרה של "ספקי שירותים דיגיטליים רלוונטיים" הכוללת ספקי פלטפורמות סחר אלקטרוני, ספקי מנועי חיפוש וספקי שירותי ענן.[236] כמו כן, תקנות NIS חלות על 5 מתוך 13 מגזרי התשתיות הקריטיות – אנרגיה, תחבורה, בריאות, אספקה והפצה של מי שתייה ותשתיות דיגיטליות.[237]

תקנות NIS נועדו להביא לשינוי התנהגותי בקרב בעלים ומפעילים של תשתיות קריטיות שעליהן מוחלות התקנות, שיוביל למעבר מחשיבה צרה המתמקדת אך ורק בציות לרשימה של אמצעי אבטחה מומלצים אל בחינה מעמיקה ומיפוי של מכלול האיומים הצפויים למערכת או התשתית שעליה הם מופקדים, ואימוץ אמצעי אבטחה מתאימים ומידתיים.[238]

מגזרי התשתיות הקריטיות וספקי השירותים הדיגיטליים הרלוונטיים מוינו כך שכל מגזר שויך לרשות לאומיות מתאימה, בהתאם למפורט בנספח 1 לתקנות NIS. לפי התקנות, שר המופקד על מגזר מסוים מהמגזרים שעליהם חלות התקנות נדרש לקבוע מדיניות לאומית להגנת הסייבר בתחומו, תוך הצבת

234 The Network and Information Systems Regulations 2018, SI 2018/506 (Eng.) (להלן: תקנות NIS).

235 הכוונה לחברות המעסיקות פחות מ־250 עובדים ושמחזור המסחרי השנתי שלהן לא עולה על 50 מיליון אירו. ראו Commission Recommendation 2003/361 of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises (Notified under Document Number C(2003) 1422), tit. I, art. 2, 2003 O.J. (L 124) 36 (EC)

236 תקנות NIS, **לעיל** ה"ש 234, הגדרת "digital service provider" ו-"digital service" בסעיף 1, וחלק 4.

237 **שם**, בלוח 1.

238 **שם**.

מטרות וקביעת סדר עדיפויות למימושן במטרה להשיג ולשמר הגנת סייבר ברמה גבוהה. על השר לבחון את הרלוונטיות של המדיניות באופן עיתי. כמו כן, על המדיניות להתייחס לכל הפחות לנושאים המפורטים בתקנות NIS, ובהם אמצעי הרגולציה ומנגנון האכיפה להבטחת השגת מטרות המדיניות; האמצעים להשגת מוכנות לתקיפת סייבר, לתגובה למתקפה ולהחלמה ממנה, לרבות שיתוף פעולה בין המגזר הציבורי לפרטי בנושאים אלה; פירוט בעלי התפקידים המופקדים על יישום המדיניות; תוכניות להעלאת מודעות הציבור הרלוונטי במגזר שעליו מופקד השר ולחינוכו להגנת הסייבר; תוכנית להערכה ולניהול סיכונים ותוכניות למחקר ולפיתוח בנושאים הקשורים למדיניות.[239]

תקנות NIS גם מחייבות מפעילים של שירותים חיוניים או ספקים של שירותים דיגיטליים רלוונטיים לנקוט אמצעים טכנולוגים וארגוניים מתאימים ומידתיים, בהתחשב באמצעים העדכניים ביותר הקיימים ובמדריכי ההפעלה המפורסמים על ידי הרשות האחראית, ולהבטיח שספקי השירות שעימם הם מתקשרים נוקטים אף הם אמצעים דומים לניהול הסיכונים הצפויים למערכות המידע שברשותם, המשמשות את השירותים החיוניים או הדיגיטליים שהם מספקים, ולמזעור ההשפעה של תקיפת סייבר עליהן.[240] תקנות NIS אינן נוקבות באמצעי טכנולוגי או ארגוני מסוים; אלו ייקבעו בהתאם לשיקול דעתו של מפעיל השירות החיוני או השירות הדיגיטלי הרלוונטי, אך המפעיל יכול להיעזר ברשימת 14 העקרונות שפרסם ה־NCSC, המפרטת את התוצאות שיש להשיג כדי לעמוד בדרישת הגנת הסייבר ולהשיג חוסן סייבר. על בסיס עקרונות אלו התווה ה־NCSC את מסגרת הערכת הסייבר (Cyber Assessment Framework, CAF) – מסגרת סיסטמטית ומקיפה להערכת ניהול סיכוני הסייבר לשירותים ולתשתיות חיוניות על ידי הארגון עצמו או הרגולטור האחראי עליו. לפי האסטרטגיה לשנים 2025–2022, בכוונת המדינה לפעול להרחבת אימוץ ה־CAF לכלל מגזרי התשתיות הקריטיות.[241]

239 תקנות NIS, **לעיל** ה"ש 234, בסעיף 2.

240 **שם**, בסעיפים (2)–(1)12 ,10.

241 האסטרטגיה לשנים 2025–2022, **לעיל** ה"ש 209, בעמ' 68.

כמו כן, תקנות NIS מחייבות מפעיל שירות חיוני או ספק שירות דיגיטלי רלוונטי לדווח לרשות המתאימה על תקיפת סייבר המשפיעה באופן משמעותי על המשכיות השירות החיוני או הדיגיטלי שהוא מספק, לא יאוחר מ־72 שעות מרגע שנודע לו על המתקפה. בקביעה אם תקיפת הסייבר היא בעלת השפעה משמעותית על תשתית קריטית, על מפעיל התשתית להתחשב בגורמים שלהלן: מספר המשתמשים הנפגעים עקב ההפרעה בשירות, משך המתקפה והשטח הגיאורפי המושפע מהמתקפה. כאשר מדובר בספק שירות דיגיטלי רלוונטי, עליו לבחון את מספר המשתמשים שהושפעו מתקיפת הסייבר, ובייחוד מספר המשתמשים שנשענו על השירות הדיגיטלי שהוא מספק לשם מתן שירות אחר מטעמם; וכן את משך תקיפת הסייבר, היקף השפעתה הגיאוגרפי, מידת ההפרעה הנגרמת לפונקציונליות השירות ומידת ההשפעה של התקיפה על פעילות חברתית וכלכלית. לאחר קבלת הדיווח על תקיפת הסייבר, על הרשות המתאימה לבחון מהן הפעולות הדרושות ולהעביר את הדיווח בהקדם האפשרי לצוות התגובה למתקפות סייבר (CSIRT, ראו להלן). הרשות המתאימה וה־CSIRT רשאים להעביר לאותו מפעיל תשתית קריטית או ספק שירות דיגיטלי מידע העשוי לסייע לו בהתמודדות עם המתקפה, וכן לדווח לציבור על תקיפת הסייבר בתנאי שדיווח כאמור עשוי לסייע להתמודדות עם המתקפה או למנוע מתקפה נוספת בעתיד. כאשר מדובר בתקיפת סייבר על ספק שירות דיגיטלי רלוונטי, על הרשות המתאימה וה־CSIRT להיוועץ זו בזה לפני הדיווח לציבור.[242] באסטרטגיה לשנים 2025–2022 הובהר שחובת הדיווח המוטלת על גופים מאוסדרים תורחב כך שתכלול גם אירועי סייבר שלו היו מתרחשים היו עשויים לגרום לנזק משמעותי, אך זוהו ונמנעו בזמן ("near misses").[243]

אכיפת רגולציית הציווי והשליטה הרכה, כלומר המדיניות שנקבעת על ידי השר בהתאם לתקנות NIS, מבוצעת באופן ביזורי באמצעות הרשות המגזרית המתאימה בשילוב תמריצים עונשיים. על הרשות המגזרית להכין ולפרסם מדריכי פעולה העולים בקנה אחד עם המדיניות שקבע השר ולבחון אותם באופן עיתי;[244]

242 תקנות NIS, **לעיל** ה"ש 234, בסעיפים 11, (3)12–14.

243 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 74.

244 תקנות NIS, **לעיל** ה"ש 234, בסעיף 3.

לבחון ולקבוע אם חברה מסוימת צריכה להיחשב ספקית שירותים חיוניים[245] או ספקית שירות דיגיטלי רלוונטית; להחזיק רשימה של חברות הנחשבות ספקיות שירותים חיוניים או ספקיות שירות דיגיטלי רלוונטיות; להיוועץ ולשתף פעולה עם נציבות הגנת הפרטיות (Information Commissioner) בכל הקשור לטיפול בתקיפת סייבר שהביאה לפגיעה במידע אישי; להיוועץ ולשתף פעולה עם רשויות אכיפת חוק, עם רשויות מקבילות באנגליה ובמדינות אחרות באיחוד האירופי ועם ה־GCHQ. במשימותיה אלו על הרשות המתאימה לפעול בהתאם למדיניות הלאומית שקבע השר האחראי הרלוונטי.[246] כמו כן, הרשות המתאימה מוסמכת לדרוש מידע מאדם או מחברה אם הדבר דרוש באופן סביר כדי לקבוע אם יש להגדיר את החברה כספק שירות חיוני או כספק שירות דיגיטלי רלוונטי, וכן כדי להעריך את מידת הגנת הסייבר של מערכותיו או את מידת היישום של מדיניות אבטחה.[247] כן מוסמכת הרשות המתאימה לבצע חקירה כדי לבחון אם החברה המאוסדרת מקיימת את חובות ההגנה והדיווח המוטלות עליה מכוח תקנות NIS ולנקוט צעדי אכיפה, לרבות הטלת קנסות עד לגובה של מיליון לירות שטרלינג, אם נמצא כי חובות אלו הופרו.[248]

לפי תקנות NIS, ה־CSIRT משמש כצוות התגובה למתקפות סייבר, ותפקידו לנטר מתקפות סייבר ברחבי אנגליה; לפרסם ולהפיץ התראות ואזהרות על איומי סייבר ומידע רלוונטי לכלל בעלי העניין; להגיב לכל תקיפת סייבר שדווח לו עליה; לספק ניתוח דינמי לאיומים ולמתקפות סייבר; להשתתף ברשת של מרכזי תגובה דומים; ליצור קשרים עם המגזר הפרטי כדי לאפשר שיתוף פעולה עימו במגזר הרלוונטי; לקדם את השימוש בפרקטיקות ובסטנדרטים מקובלים לניהול איומי סייבר ומתקפות סייבר ולמיון שלהם; ולשתף פעולה עם רשויות האכיפה לשם אכיפת תקנות NIS.[249]

245 **שם**, בסעיף 8.

246 **שם**, בסעיף 12.

247 **שם**, בסעיף 15.

248 **שם**, בסעיפים 16–18.

249 **שם**, בסעיף 5.

כאשר נבחנה היעילות של תקנות NIS כשנתיים לאחר כניסתן לתוקף נמצא שאף שמוקדם לאמוד את ההשפעה ארוכת הטווח שלהן, הארגונים הכפופים להן אכן נקטו אמצעים להגברת ההגנה על המערכות והמידע שבבעלותן באופן שהביא למזעור סיכוני הסייבר לשירותים הניתנים על ידם.[250]

ii. רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים

בשנת 2018 פרסמה ממשלת אנגליה קוד התנהגות וולונטרי להגנת סייבר במוצרי צריכה חכמים,[251] אך הקוד לא אומץ באופן רחב, ועל כן לא הביא לחיזוק מהותי של הגנת הסייבר במוצרים אלו. משום כך, באפריל 2021 הגישה הממשלה הצעת חוק אשר מחייבת יצרנים של מוצרי צריכה חכמים לאמץ את הסטנדרט האירופי להגנת סייבר במוצרים אלה, שמפורט גם בקוד ההתנהגות הוולונטרי.[252]

אחד הזרזים להגשת הצעת החוק היה ההבנה שכשלי השוק המאפיינים את מרחב הסייבר, כגון החצנות שליליות וא־סימטריה במידע,[253] מונעים מכוחות השוק לבדם להביא לאימוץ רמת הגנת סייבר נאותה במכשירים חכמים – אף שכ־28% מהצרכנים באנגליה העידו שאין בכוונתם לרכוש במהלך שנת 2020 מוצר צריכה חכם מחשש שהגנת הסייבר שלו נמוכה.[254]

250 Secretary of State for Digital, Culture, Media and Sport, Post Implementation Review of the Network and Information Systems Regulation 2018 (2020)

251 Department for Digital, Culture, Media & Sport, Code of Practice for Consumer IoT Security (2018) (להלן: IoT Code of Practice).

252 ETSI IoT Requirements, **להלן** ה"ש 161; IoT Code of Practice, **לעיל** ה"ש 251; Product Security and Telecommunications Infrastructure Bill (Originated in the House of Commons, Sessions 2021-22. 2022-23 Nov. 1, 2022); האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 86.

253 להרחבה בנוגע למאפייני מרחב הסייבר וכשלי השוק שבו ראו **מהו סייבר א**, **לעיל** ה"ש 9.

254 RSM UK Consulting LLP, Evidencing the Cost of the UK Government's Proposed Regulatory Interventions for Consumer IoT (2020)

החובה לאמץ את עקרונות הגנת הסייבר הקבועים בקוד ההתנהגות חלה על היצרנים של מוצרי צריכה חשמליים ביתיים בעלי יכולת להתחבר לרשת האינטרנט, כגון רמקולים חכמים, טלוויזיות חכמות, מכשירי טלפון ניידים, צעצועים חכמים, גלאי עשן חכמים, שעוני כושר חכמים, מקרר חכם ומכונת כביסה חכמה, ועל השירותים הנלווים למכשיר. החובה אינה חלה על יצרנים של מכשירים המוחרגים במפורש מהחוק, כמו מונים חכמים, רכבים אוטונומיים, מחשבים ניידים, מחשבים נייחים וטאבלטים.

יצרני המכשירים החכמים נדרשים, בין השאר, שלא להשתמש בסיסמאות אוניברסליות או בסיסמאות שקל לגלות בכל המכשירים החכמים: על היצרן לספק סיסמה ייחודית ומורכבת לכל מכשיר חכם. כמו כן, על יצרן מוצרי צריכה חכמים להתוות מנגנון לדיווח על חולשות, שיאפשר לחוקרי סייבר לדווח ליצרן על גילוי חולשה במכשיר מבלי לחשוש שהיצרן יתבע אותם בגין פריצה או שימוש לרעה במכשיר. שלישית, על היצרנים להקפיד על שקיפות – עליהם לגלות לצרכן מהו פרק הזמן שבמהלכו יש בדעת היצרן לספק לצרכן עדכוני אבטחה למכשיר החכם שבידו. עקרונות ההגנה עשויים להתעדכן מעת לעת לפי החלטת השר האחראי. כמו כן, החוק המוצע מסמיך את השר האחראי לקבוע בעתיד קטגוריות של מוצרי צריכה שיצרניהם יחויבו לעמוד בתהליך בדיקה ויקבלו אישור בנוגע לרמת הגנת הסייבר במכשיריהם.[255]

המגמה של הרחבת רגולציית הציוּוי והשליטה הרכה ממשיכה גם באסטרטגיה לשנים 2025–2022. נקודת המוצא של האסטרטגיה, אשר קיבלה חיזוק מהתעשייה עצמה, היא שארגונים רבים כלל אינם מבינים את סיכוני הסייבר שאליהם הם חשופים, התמריצים הכלכליים להשקעה בהגנת סייבר אינם ברורים להם ולרוב יש להם מוטיבציה מעטה לדווח לרשויות על אירועי סייבר שחוו. ביטוי נוסף להרחבת הרגולציה קשור לחשש מפני הגברת החשיפה למתקפות סייבר בשל ההתקשרויות של תשתיות קריטיות וספקי שירותים דיגיטליים עם צדדים שלישיים שאינם כפופים לתקנות NIS. בהקשר זה הובהר באסטרטגיה

255 Dep't for Digital, Culture, Media & Sport, Policy Paper: Government Response to the Call for Views on Consumer Connected Product Cyber Security Legislation (2021)

כי מגמת המדיניות לשנים הקרובות תהא הטלת אחריות רגולטורית על יצרנים, משווקים, ספקי שירותים וגופים במגזר הציבורי, לניהול יעיל של סיכוני הסייבר שאליהם הם חשופים, להגברת חוסן הסייבר שלהם ולמתן תמיכה ללקוחותיהם בעת אירועי סייבר המתרחשים במערכותיהם. כמו כן, חברות טכנולוגיות גדולות המספקות שירותים דיגיטליים צריכות, לפי האסטרטגיה, להבטיח הגנת סייבר כברירת מחדל (secure by default) מתוך הנחה שלקוחות הקצה אינם צריכים לנקוט צעדים פרואקטיביים כדי לזכות בהגנת סייבר נאותה.[256]

3. רגולציה שיתופית על בסיס התנדבותי

רגולציה שיתופית הייתה נהוגה באנגליה עוד לפני 2016 והיא נהוגה גם היום. המגזר הפרטי, שהוא המפעיל והבעלים העיקרי במרחב הסייבר, לרבות בתשתיות קריטיות, נהנה מהמידע המודיעיני שהממשלה מספקת לו; עבור הממשלה הרגולציה השיתופית היא כלי להגברת הציות לרגולציה, גם כאשר מדובר ברגולציה וולונטרית, ובאמצעותה אפשר להגביר את הגנת הסייבר גם בתשתיות שאינן בבעלותה או בשליטתה הישירה מבלי לפגוע בהמשך תפקודו התקין של המגזר הפרטי כמנוע החדשנות וההשקעות במרחב הסייבר. הרגולציה השיתופית מבוססת על השתתפות התנדבותית של חברות מהמגזר הפרטי, בנימוק שרק כך אפשר ליצור ולשמר יחסי אמון בין הצדדים, החיוניים להתוויה של הגנת סייבר מתאימה.[257] כדי לעודד רגולציה שיתופית יעילה בכל רחבי אנגליה, אשר תוביל לקִדמה טכנולוגית בתחום, לחינוך הציבור ולהגברת ההשקעה בתעשיית הגנת הסייבר, הוקמה, לפי האסטרטגיה לשנים 2022–2025, שותפות אשכולות הסייבר האנגלית (UK Cyber Cluster Collaboration, UKC3). מרכזי חוסן סייבר אזוריים העומדים בדרישות מסגרת התפעול של ה־UKC3, מבחינת עקרונות פעולה, יעדים ותוצאות, זוכים להכרת ה־UKC3. הכרה זו מאפשרת למרכזי חוסן הסייבר האזוריים להיות חלק מקהילת הגנת הסייבר האנגלית, לנהל שיח פורה בין שחקנים מהמגזר הפרטי, מהמגזר השלישי ומהמגזר הציבורי, ליהנות מגישה לרשתות שיתוף מידע וסטנדרטים שחברים בהן מרכזי סייבר מאזורים שונים, ולזכות במימון המדינה ליוזמות

256 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 23, 29, 37, 66, 70.

257 Securing Britain, **לעיל** ה"ש 212; Statement 1 Year On, **לעיל** ה"ש 212.

שונות בתחום הקשורות בהגנת הסייבר, כגון מחקר ופיתוח, הכשרות מקצועיות וחינוך הציבור.[258]

הרגולציה השיתופית רלוונטית לכלל המגזרים, ונועדה לשרת כמה מטרות מרכזיות:

I. שיתוף מידע על איומי סייבר, דרכי התגוננות ואופני החלמה ממתקפת סייבר

המטרות המוצהרות של שיתוף במידע באנגליה דומות לאלו המוזכרות במסמכי המדיניות של ארצות הברית: להגביר את ערנות השחקנים מהמגזר הציבורי ומהמגזר הפרטי לסכנות הטמונות במרחב הסייבר ולדרכי ההתגוננות מפניהן, ולשמש פלטפורמה להחלפת דעות ורעיונות בנוגע לפעולות היעילות ביותר למניעת מתקפות סייבר, להתגוננות מפניהן ולהתמודדות עימן.[259]

לדוגמה, השותפות לשיתוף המידע להגנת סייבר (The Cyber Security Information Sharing Partnership, CiSP) הוקמה בשנת 2013 כפלטפורמה לשיתוף מידע בין המגזר הפרטי למגזר הציבורי בנוגע לאיומי סייבר ומתקפות סייבר בזמן אמת. המידע מועבר תוך שמירה על סודיות מה־CiSP למרכז עיבוד (Fusion Cell) המורכב מנציגי ממשלה ואנליסטים מהתעשייה. בסיום בחינת המידע וניתוחו מפורסם לכל חברי ה־CiSP דוח מסכם.[260] הרציונל שבבסיס פעולת ה־CiSP הוא ששיתוף המידע בין כלל חברי השותפות יאפשר לכולם לקבל מידע אמיתי וקריטי לשם התגוננות מפני מתקפות סייבר, ללמוד מניסיונם של אחרים ולהישאר מעודכנים בנוגע לאסטרטגיות הטובות ביותר למניעת מתקפות סייבר ולהתמודדות עימן.[261]

258 האסטרטגיה לשנים 2025-2022, **לעיל** ה"ש 209, בעמ' 50-53; *About: Our Mission*, UKC3, UK Cyber Cluster Collaboration (להלן: *UKC3 Mission*).

259 Fact Sheet 18, **לעיל** ה"ש 212; האסטרטגיה לשנים 2021-2016, **לעיל** ה"ש 213, בעמ' 26.

260 Progress Against Objectives 2013, **לעיל** ה"ש 212; Forward Plans 2013, **לעיל** ה"ש 212.

261 Statement 1 Year On, **לעיל** ה"ש 212; Cyber Security Information Sharing Partnership, GOV.UK (Speech by Francis Maude delivered at Chatham House, London, UK, Mar. 27, 2013)

מסגרת נוספת לשיתוף מידע היא צוות תגובת החירום (Computer Emegency Response Team, CERT-UK) שהוקם בשנת 2014. CERT-UK פונה לחברות מכל המגזרים והגדלים ולאקדמיה, ומטרתו לקדם את הבנת איומי הסייבר ולהגביר את המודעות אליהם בקרב שחקנים מהמגזר הפרטי ומהמגזר הציבורי, ולספק ייעוץ והנחיות לחברות בשוק הפרטי כדי לסייע להן להתכונן למתקפת סייבר, לחזק את הגנת הסייבר שלהן ולהתמודד עם מתקפת סייבר בזמן אמת.[262]

דוגמה נוספת לרגולציה שיתופית היא ההבהרה באסטרטגיה לשנים 2025–2022 שיש לפעול לחיזוק שיתוף הפעולה עם בעלים ומפעילים של תשתיות קריטיות כדי לשפר את הגישה למידע בנוגע לאיומי סייבר וסכנות סייבר, ולהגיע להסכמה בנוגע להגדרת סיכון סביר למתקפת סייבר.[263]

באסטרטגיה לשנים 2025–2022 הוכרזה הקמתה של פלטפורמה נוספת לשיתוף ידע ורעיונות הנוגעים להגנת מרחב הסייבר, שאינם קשורים בהכרח למידע על תקיפות או על איומי סייבר בזמן אמת – ועדת הייעוץ הלאומית לסייבר (National Cyber Advisory Board). מטרת הוועדה היא ליצור שיח מקיף עם התעשייה, האקדמיה והאזרחים בנוגע להגנת סייבר, בהתבסס על מסגרות קיימות של שותפויות בין המגזר הציבורי, האקדמיה התעשייה ומרכזי מצוינות וחינוך להגנת מרחב הסייבר.[264]

II. גיבוש רגולציה וכללי התנהגות טכניים מנחים

גיבוש הכללים המנחים הטכניים, הפצתם ומתן מענה וייעוץ לשחקנים מהמגזר הציבורי או הפרטי נעשים על ידי ה־NCSC על בסיס המידע והתובנות שהתקבלו משיתוף המידע הבין־מגזרי.[265]

262 Forward Plans 2012, **לעיל** ה"ש 212.

263 האסטרטגיה לשנים 2025–2022, **לעיל** ה"ש 209, בעמ' 68, 75, 83.

264 **שם**, בעמ' 50.

265 Introducing the NCSC, **לעיל** ה"ש 221, בעמ' 17; UK Dep't for Digital, Culture, Media & Sport, UK Digital Strategy, ch. 5 (2017) (להלן: UK Digital Strategy).

כמו כן, ממשלת אנגליה פונה לתעשייה, לאקדמיה ולבעלי עניין לשם היוועצות במסגרת גיבוש יוזמות חקיקה או כללי התנהגות מנחים. למשל, לשם גיבוש הצעת החוק המחייבת יצרני מכשירים חכמים לאמץ סטנדרטים של הגנת סייבר התקיימו שני סבבי היוועצות עם התעשייה והאקדמיה.[266]

III. קידום מחקר ופיתוח (R&D) בתחום הגנת הסייבר

אחת הדוגמאות לקידום מחקר ופיתוח בתחום הגנת הסייבר היא מענקי המחקר שמחלקת המועצה הבריטית למחקר במדעי ההנדסה והפיזיקה (British Engineering and Physical Sciences Research Council) לאוניברסיטאות ולמוסדות מחקר המבצעים מחקרים בתחום הגנת מרחב הסייבר.[267] המדינה קובעת באמצעות המועצה את תחומי המחקר שברצונה לקדם ואת תקופת המחקר שאותה תממן כתמריץ לביצוע המחקר על ידי המוסד האקדמי.[268] דוגמה נוספת לרגולציה שיתופית לשם עידוד מחקר ופיתוח וחדשנות היא שותפות ה־UKC3.[269]

באסטרטגיה לשנים 2025–2022 הוצע לשקול הקמה של שיתופי פעולה בין התעשייה במגזר הרלוונטי, האקדמיה, המגזר השלישי והמגזר הציבורי, שתפקידם יהיה לבחון את התגובה לאירועי סייבר בעלי השלכה על המגזר כולו, לרבות בחינת טכנולוגיות חדשניות בתחום. כך, למשל, בתחום הטלקומוניקציה הוקמה UK Telecoms Lab, שותפות המורכבת מהממשלה, הרגולטור האחראי וחברות מתעשיית הטלקומוניקציה, שמטרתה להתוות מסגרת חדשה לאבטחת שירותי טלקומוניקציה תוך הבטחת הגיוון והחדשנות בתחום. במגזר הפיננסי

266 UK Dep't for Digital, Culture, Media & Sport, Consultation Outcome: Consultation on Regulatory Proposals on Consumer IoT Security (2019); UK Dep't for Digital, Culture, Media & Sport, Proposals for Regulationg Consumer Smart Product Cyber Security – Call for Views (2020)

267 Scecuring Britain, **לעיל** ה"ש 212, בעמ' 3, 47.

268 Engineering and Physical Science Research Council, Code of Practice for Council Members 9-10 (2006)

269 האסטרטגיה לשנים 2025-2022, **לעיל** ה"ש 209, בעמ' 50-53; *UKC3 Mission*, **לעיל** ה"ש 258.

פועל בהצלחה המרכז לשותפות סייבר במגזר הפיננסי (Financial Sector Cyber Collaboration Centre).[270]

IV. חינוך הציבור והגברת ערנותו לסיכונים הטמונים במרחב הסייבר

אחת ממטרות הרגולציה השיתופית היא להגביר את מודעות הציבור לסיכונים שבמרחב הסייבר כדי לעודד התנהגות זהירה ונקיטת אמצעי אבטחה והגנה מתאימים, מתוך הכרה בסיכון הטמון בגורם האנושי.[271]

כך, למשל, ה־Cyber Essentials scheme נועדה להעלות מודעות ולחנך את הציבור במטרה להגביר את האמון במרחב הסייבר. התוכנית מספקת הנחיות ברורות לגבי הצעדים הטכניים הבסיסיים וההכרחיים שעל חברה לנקוט כדי למזער את סיכוני הסייבר בעלות נמוכה. ההנחיות גובשו בשיתוף פעולה בין גורמים מהממשלה ומהתעשייה בהליך של רגולציה משותפת. יישום ההנחיות על ידי חברה פרטית נעשה בדרך של רגולציה עצמית בשילוב תמריץ – "תג" (cyber essential badge) שהחברה מציגה בפומבי והוא מסמל לציבור שהחברה נקטה את האמצעים הטכנולוגים המומלצים להתגוננות במרחב הסייבר.[272]

פלטפורמה נוספת לחינוך הציבור היא שותפות הכישורים הדיגיטליים (Digital Skills Partnership), שהוקמה במרץ 2017 על בסיס ההבנה שלשם הגברת היעילות והחדשנות יש להבטיח שלכל אחד יהיו הכישורים המתאימים לפעולה במרחב הסייבר. ממשלת אנגליה הגדירה לפיכך את המטרה ואת כללי הניהול של הפלטפורמה, לרבות המנהלים, תדירות הפגישות והדרכים שיבטיחו ייצוג הולם בדירקטוריון, וחברות פרטיות – דוגמת גוגל, חברות הבנקאות Barclays

270 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 68, 75, 83.

271 Scecuring Britain, **לעיל** ה"ש 212, בעמ' 3, 47; Statement 1 Year On, **לעיל** ה"ש 212.

272 National Cyber Security Centre, Cyber Essentials Scheme Leaflet (2014) (להלן: Cyber Essentials).

ו־Lloyds Banking וענקית התקשורת British Telecom – מציעות באמצעות הפלטפורמה הזדמנויות להכשרה לתעשייה לציבור הרחב.[273]

תוכנית CyberFirst עוסקת גם היא בתחום החינוך: זוהי תוכנית ממשלתית בהנהגת ה־NCSC בשותפות עם משרדי ממשלה וחברות מהתעשייה, שמטרתה קידום הכשרת מומחים בתחום הגנת הסייבר מקרב הדור הצעיר. התוכנית כוללת הכשרה בבתי ספר ובאוניברסיטאות וקורסים קצרים לבני נוער.[274]

כמו כן, במרץ 2021 הוקמה מועצת הגנת הסייבר של אנגליה (UK Cyber Security Council) המשמשת כארגון המייצג של בעלי המקצוע בתחום הגנת הסייבר. המועצה מופעלת על ידי נציגים מהמגזר הציבורי אך חברים בה גם נציגים מהתעשייה. בדומה להתאגדויות מקצועיות כמו לשכת עורכי הדין או הסתדרות הרופאים, המועצה אמורה לקבוע את הסטנדרטים והדרישות המקצועיות מהעוסקים בתחום הגנת הסייבר ואת הנורמות האתיות של המקצוע, וכן להבטיח כי בתחום יועסקו אנשי מקצוע מכל המגזרים בחברה.[275]

4. רגולציה עצמית

בארגונים שאינם תשתיות קריטיות או ספקי שירותים דיגיטליים הכפופים לרגולציית הציווי והשליטה הרכה, נהוגה רגולציה עצמית בשילוב תמריצים. למשל, ה־Cyber Essentials scheme שהוזכרה לעיל מציעה תמריץ לאימוץ סטנדרט של הגנת סייבר בדמות "תג" (cyber essential badge) שמסמל לציבור שהחברה נקטה את האמצעים הטכנולוגיים המומלצים להתגוננות במרחב הסייבר.[276]

כאמור, ב־2018 ניסתה ממשלת אנגליה להחיל סטנדרטים של הגנת סייבר בקרב יצרני מוצרי צריכה חכמים באמצעות רגולציה עצמית, עם פרסום קוד התנהגות

273 UK Digital Strategy, **לעיל** ה"ש 265, בפרק 2.

274 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 55; *CyberFirst Overview*, National Cyber Security Centre

275 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 56–57.

276 Cyber Essentials, **לעיל** ה"ש 272.

וולונטרי ליצרני מוצרים אלה.[277] ואולם, בסקר שנערך כשנתיים לאחר מכן נמצא שרק אחד מכל שישה ארגונים טרח לאמץ את קוד ההתנהגות הוולונטרי ולהטמיע אמצעים להגנת סייבר כמוצע בו.[278] ממשלת אנגליה החליטה שאין די בכלי הרגולטורי של רגולציה עצמית, ובהצעת חוק שפורסמה באפריל 2021 הציעה להחיל רגולציית ציווי ושליטה ריכוזית המחייבת יצרני מכשירים חכמים, לרבות טלפונים חכמים, לאמץ סטנדרטים של הגנת סייבר הקבועים בקוד ההתנהגות ותואמים את הדרישות הבינלאומיות בתחום.[279]

ממשלת אנגליה השיקה גם כמה יוזמות שתפקידן לסייע בהגנת סייבר בדרך של רגולציה עצמית, כגון cyber PROTECT network, יחידת הסיוע לקורבנות פשעי סייבר כלכליים (Economic Crime Victims Care Unit) ומרכזי חוסן סייבר אזוריים (Cyber Resilience Centres). תפקידן של יוזמות אלו לשמש כמקור ידע וכישורי סייבר וככתובת להיוועצות בעבור יחידים וארגונים בינוניים וקטנים (SMEs).[280]

אמצעי נוסף של רגולציה עצמית הוא הנחיות שפרסם ה־NCSC להגנה על ארגונים מפני מתקפת כופר ולצעדים שיש לנקוט במקרה של מתקפת כופר. נוסף על כך, לפי האסטרטגיה לשנים 2022–2025, ה־NCSC אמור לפרסם אחת לכמה זמן רשימה של חברות המספקות שירותים למגזר הציבורי אשר עומדות בדרישות הגנת הסייבר שלו. הגבלת ההתקשרויות של המגזר הציבורי לחברות מרשימה זו בלבד אמורה להוביל לאימוץ סטנדרט הגנת סייבר ראוי בקרב יותר חברות מהמגזר הפרטי.[281]

277 IoT Code of Practice, **לעיל** ה"ש 251.

278 IoT Security Foundation, Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure – 2020 Progress Report (2020)

279 להרחבה ראו דיון בסעיף ג.ii.II.2.I **לעיל**, "רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים".

280 האסטרטגיה לשנים 2022–2025, **לעיל** ה"ש 209, בעמ' 22.

281 **שם**, בעמ' 27, 58.

יוזמה נוספת להגברת הגנת הסייבר בדרך של רגולציה עצמית היא תוכנית הגנת סייבר האקטיבית (Active Cyber Defense, ACD), שבמסגרתה ניתנים בחינם מגוון שירותים לבחינת רמת מוכנות הארגון למתקפת סייבר ולזיהוי וגילוי מתקפת סייבר. תוכנית ה־ACD נועדה לסייע במניעה ובגילוי של מתקפות סייבר שגרתיות הפוגעות במשתמשי הקצה ברמה היום־יומית, ומטרתה לנסות ליצור מרחב סייבר בטוח יותר לאזרחים.[282]

באסטרטגיה לשנים 2025–2022 נקבע גם כי במגזר הציבורי יאומצו סטנדרטים (best practices) להגנת סייבר אשר הממשלה מצפה גם מארגונים וחברות מרכזיות במגזר הפרטי לאמץ, כך שהמגזר הציבורי ישמש דוגמה להגנת סייבר נאותה. עוד הובהר באסטרטגיה שהממשלה תספק לחברות מהמגזר הפרטי תמריצים לשם עידוד הטמעתה של הגנת סייבר נאותה, ובכל הנוגע לחברות ממגזרים שלמתקפת סייבר עליהם עשויה להיות השפעה גדולה, בעיקר חברות המספקות שירותים דיגיטליים חיוניים וחברות גדולות, יעוגנו התמריצים בחקיקה.[283]

5. סיכום מודל הרגולציה להגנת מרחב הסייבר באנגליה

מאז שנת 2016 גוברת נטיית הממשלה באנגליה להחיל רגולציה מסוג ציווי ושליטה רכה וביזורית, לא רק על תשתיות קריטיות אלא גם על חברות אחרות שלפעילותן יש השפעה ניכרת על כלכלת המדינה ועל הציבור בכללותו. בכל הנוגע להגנת הסייבר במוצרים שיש להם השלכה ישירה על משתמשי הקצה אף מוצע להחיל רגולציית ציווי ושליטה ריכוזית, והצעת החוק בנושא תלויה ועומדת. לצד נטייה זו קיימות גם מסגרות של רגולציה שיתופית ורגולציה עצמית לנושאים מסוימים וביחס לארגונים מסוימים. האסטרטגיה לשנים 2025–2022 מצביעה על השלב הבא במדיניות הגנת הסייבר באנגליה: לצד הרחבת התחולה של רגולציית הציווי והשליטה הרכה והביזורית ואסדרה רגולטורית של תמריצים לרגולציה עצמית, אנגליה מאמצת ראייה רחבה המשלבת בין שיפור הגנת הסייבר בקרב גופים ציבוריים וארגונים מהמגזר הפרטי ובין ההבנה שנדרש מענה מקיף, הכולל

282 **שם**, בעמ' 70.

283 **שם**, בעמ' 35–38, 65, 70, 78.

לצד מאמצי ההגנה גם פעולות הרתעה – באמצעות הקשחת האכיפה הפלילית של פשיעת סייבר, בין השאר באמצעות חקיקה ייעודית בנושא, וכן באמצעות פעולות סייבר התקפי שייעשו בשקיפות ככל האפשר.

לוח 3
האסדרה של הגנת הסייבר באנגליה

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה	בעת חירום על כלל המגזרים	בעת מצב חירום לאומי, תקיפת סייבר משמעותית מאוד ותקיפת סייבר משמעותית, ולעיתים בעת תקיפת סייבר ממשית, ה־NCSC מוביל את מאמצי ההתגוננות וההחלמה, ומנהל ומתאם את הפעולות של הגורמים השונים מהמגזר הציבורי ומהמגזר הפרטי. בעת תקיפת סייבר בינונית ומקומית ינהלו רשויות אכיפת החוק את פעולות ההתגוננות, ההחלמה והתגובה.
רגולציית ציווי ושליטה רכה ריכוזית	יצרני מוצרי צריכה חכמים	נכון לכתיבת מסמך זה תלויה ועומדת הצעת חוק להחלת עקרונות הגנת סייבר מסוימים על יצרני מוצרי צריכה חכמים. בשנים הקרובות תיתכן הרחבה של רגולציית הציווי והשליטה הרכה כך שתכלול גם חברות טכנולוגיה גדולות, יצרנים, משווקים וספקי שירותים דיגיטליים.
רגולציית ציווי ושליטה רכה ביזורית	המגזר הפיננסי, חמישה מגזרי תשתיות קריטיות נוספים וחברות המוגדרות כ"ספקי שירותים דיגיטליים רלוונטיים"	על בעלים ומפעילים של תשתיות קריטיות וגם על חברות פרטיות שאינן תשתיות קריטיות אך לתפקודן התקין יש השפעה משמעותית על כלכלת המדינה וחוסנה הציבורי ("קבוצת הפרימיום"). לפי תקנות NIS, על כל שר המופקד על מגזר מסוים לקבוע מדיניות לאומית להגנת הסייבר בתחומו בהתאם לדרישות התקנות. לכל אחד מספקי השירותים הדיגיטליים ומחמשת מגזרי התשתיות הקריטיות צוותה רשות לאומית מתאימה שתפקידה לאכוף את יישום תקנות NIS בהתאם להנחיות שקבע השר האחראי.

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציה שיתופית על בסיס התנדבותי	כלל המגזר הפרטי	מסגרות שונות לשיתוף מידע בנוגע לתקיפות ואיומי סייבר וכן ידע הקשור להגנת סייבר, למשל CERT-UK ו־National Cyber Advisory Board.
	המגזר הציבורי והפרטי	גיבוש כללי התנהגות טכניים מנחים לשם מזעור סיכוני הסייבר בשיתוף פעולה בין גורמים במגזר הציבורי והפרטי. היוועצות עם התעשייה, האקדמיה ובעלי עניין בטרם גיבוש רגולציה מסוג ציווי ושליטה.
	כלל המגזר הפרטי והאקדמיה	קידום מחקר ופיתוח, למשל באמצעות מענקי מחקר לאוניברסיטאות.
	כלל המגזר הפרטי	חינוך הציבור, למשל באמצעות ה־Cyber Essentials scheme ושותפות הכישורים הדיגיטליים.
רגולציה עצמית בשילוב תמריצים	כלל המגזר הפרטי	תוכנית ה־The Cyber Essentials scheme. יוזמת ACD למתן שירותים חינמיים לבחינת רמת מוכנות הארגון למתקפת סייבר ולזיהוי וגילוי מתקפת סייבר. מרכזי חוסן סייבר וקווים מנחים המפורסמים על ידי ה־NCSC המשמשים ככתובת להיוועצות בכל הנוגע להגנת הסייבר. בעתיד ייתכן שיעוגנו בחקיקה תמריצים לרגולציה עצמית בנוגע לחברות ממגזרים שלמתקפת סייבר עליהם עשויה להיות השפעה גדולה, בעיקר חברות המספקות שירותים דיגיטליים חיוניים וחברות גדולות.

II. דנמרק

דנמרק מדורגת במקום ה־32 במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם.[284] עם זאת, היא זוכה במלוא הנקודות במדד הגנת מרחב הסייבר של Comparitech, אשר בוחן את הגנת הסייבר ברמת המשתמש הבודד.[285] דירוגים אלו תואמים את הערכת סיכוני הסייבר שמבצעת הרשות הדנית הלאומית לאבטחת טכנולוגיות מידע, שלפיה נכון לשנת 2021

284 Global Cybersecurity Index 2020, **לעיל** ה"ש 29.

285 Bischoff, **לעיל** ה"ש 30.

הסיכון לפשיעת סייבר בדנמרק גבוה מאוד, אולם הסיכון לתקיפות סייבר אשר יאיימו על תשתיות קריטיות של המדינה, לרבות כחלק מטרור מאורגן, נמוך יחסית.[286]

מדיניות הגנת הסייבר בדנמרק מורכבת מאסטרטגיה לאומית המתעדכנת מדי כמה שנים, אשר מכוחה מתקינות הרשויות האחראיות על מגזרים שונים אסטרטגיות הגנת סייבר מגזריות, וכן מחקיקה התואמת את דירקטיבת NIS של האיחוד האירופי, אשר מחייבת מפעילי תשתיות קריטיות להטמיע אמצעי אבטחה טכנולוגיים וארגוניים כדי להבטיח הגנה המותאמת לסיכון לתקיפות סייבר במערכות המידע.[287]

בדצמבר 2021 פרסמה ממשלת דנמרק אסטרטגיה ממשלתית לאבטחת מידע ולהגנת מרחב הסייבר במדינה לשנים 2024–2022, אשר החליפה את האסטרטגיה הקודמת לשנים 2021–2018.[288] הנחת המוצא של האסטרטגיה לשנים 2021–2018 הייתה שכל אחד מהגורמים הרלוונטיים במרחב הסייבר – האזרחים, המגזר העסקי ורשויות הממשלה – אחראי להגנת הסייבר שלו, בהתאם להערכה וניהול של סיכוני הסייבר הצפויים לו, וכי יש צורך בשיתוף פעולה בין כלל גורמים אלו.[289] האסטרטגיה לשנים 2024–2022 ממשיכה בקו זה, ומתמקדת בהגנת הסייבר של הממשקים הדיגיטליים בתשתיות קריטיות המספקות או תומכות בפונקציות חיוניות לחברה (vital societal functions). אלו מוגדרות כפעולות, סחורות ושירותים המהווים את הבסיס לניהול הכללי של החברה בדנמרק.[290]

286 Center for Cyber Security, The Cyber Threat Against Denmark 2021 (1st ed. 2021)

287 Gorrissen Federspiel, *Cybersecurity in Denmark*, Lexology (Feb. 25, 2019)

288 The Danish Government, Danish Cyber and Information Security Strategy 2018–2021 (2018) (להלן: האסטרטגיה לשנים 2021–2018); The Danish Government, The Danish National Strategy for Cyber and Information Security 2022–2024 (2021) (להלן: האסטרטגיה לשנים 2024–2022).

289 האסטרטגיה לשנים 2021–2018, **לעיל** ה"ש 288, בעמ' 13, 21.

290 האסטרטגיה לשנים 2024–2022, **לעיל** ה"ש 288, בעמ' 12.

1. רגולציית ציווי ושליטה ריכוזית

I. במגזר הציבורי למטרות הגנת סייבר

רשויות השלטון בדנמרק חייבות לציית לדרישות הסטנדרט הבינלאומי ISO 27001 ולדרישות מינימום טכניות נוספות במטרה להטמיע מדיניות הגנת סייבר המושתתת על ניהול סיכונים. הסוכנות הדנית לממשל דיגיטלי (The Danish Agency fo Digital Government) אחראית למתן ייעוץ והנחיה בנוגע לעמידה בדרישות אלו.

רשויות ממשל האחראיות על תשתיות המספקות פעולות, מוצרים או שירותים החיוניים לניהול הכללי של החברה בדנמרק, או תומכות בפעולות, מוצרים או שירותים כאלה, מחויבות להפעיל יחידה סקטוריאלית ביזורית להגנת סייבר ומידע (Decentralised Cyber and Information Security Unit, DCIS) ולפתח אסטרטגיית הגנת סייבר בתשתיות המאוסדרות על ידן.[291]

כמו כן, גופי ממשל האחראים על מערכות מידע ותקשורת טכנולוגיות קריטיות לחברה חייבים לציית לדרישות רגולטוריות הנוגעות למערכות אלו, לרבות הוראות בנוגע לחוזים וניהול ספקים. מערכות מידע ותקשורת טכנולוגיות קריטיות לחברה מוגדרות ככאלו שהרס משמעותי שלהן ייצור אתגר משמעותי עבור החברה כולה, או שחוסר זמינותן או הפרעה לפעילותן עשויים להיות בעלי השלכות משמעותיות על החברה ועל פעילויות קריטיות לה.[292]

II. למטרות ניטור ומעקב אחר איומי סייבר

משרד ההגנה הדני מפעיל במשך 24 שעות ביממה מרכז לאומי למצבי סייבר (National Cyber Situation Centre), אשר מנטר באופן קבוע רשתות, מערכות ממוחשבות של מערכות חיוניות וקריטיות בבעלות ציבורית או פרטית, ואף פורומים ואמצעי תקשורת, בחיפוש אחר מידע על איומי סייבר ומתקפות סייבר. הניטור מבוצע לפי סדר עדיפויות שנקבע בהתאם להערכת הסיכון הצפוי לכל מערכת או תשתית קריטית מנוטרת. עסקים פרטיים מסוימים מחויבים לדווח

291 **שם**, בעמ' 11, 13.

292 **שם**, בעמ' 13.

למרכז הניטור על כל אירוע אבטחה. מערכת הדיווחים היא אוטומטית וביכולתה גם לספק למדווח פרטים ועצות על אופני ההתגוננות מפני איום הסייבר שעליו דיווח, אולם עצם הדיווח הוא תנאי מקדים לקבלת הייעוץ.[293]

III. למטרות חינוך והגברת האוריינות הדיגיטלית

האסטרטגיה לשנים 2021–2018 הצביעה על הצורך בהגברת האוריינות הדיגיטלית בקרב כלל הציבור, הארגונים ומשרדי הממשלה ככלי להתמודדות עם תקיפות סייבר. לפיכך, אחת המטרות המרכזיות של האסטרטגיה היא שיפור ההכשרה של כוח אדם מומחה בתחום הגנת הסייבר. לשם כך משולבים שיעורים בנושא אוריינות דיגיטלית ופיתוח יכולות דיגיטליות לצד התנהלות מבוקרת וביקורתית במרחב הסייבר בתוכנית הלימוד המחייבת, החל משנות הלימוד המוקדמות ובאופן רציף עד לסיום לימודי התיכון. כמו כן מוצעים קורסים בנושא התנהלות בטוחה במרחב הסייבר במסגרת הלימודים האקדמיים וההכשרות המקצועיות של עובדי הממשלה. הממשלה גם התחייבה להשקיע משאבים כדי להבטיח שלפחות 20% מכלל הצעירים יפנו ללימודים אקדמים בתחום הטכנולוגיה והגנת מרחב הסייבר. מגמה זו ממשיכה גם באסטרטגיה לשנים 2022–2024.[294]

2. רגולציית ציווי ושליטה רכה ביזורית במגזרי התשתיות הקריטיות ובמגזרים האחראים על אספקת שירות או מוצר חיוני לחברה

האסטרטגיה לשנים 2021–2018 קבעה מסגרת לרגולציית ציווי ושליטה רכה וביזורית על מגזרי תשתיות קריטיות: מגזר האנרגיה, הבריאות, התחבורה, התקשורת, הפיננסים והמגזר הימי. השר האחראי למגזר מתווה את האסטרטגיה להגנת מרחב הסייבר, לאבטחת מידע ולהגברת המוכנות הטכנולוגית במגזר הרלוונטי, תוך שיתוף פעולה ושיתוף במידע בין גופי הביטחון, רשויות הממשל הרלוונטיות ובעלים ומפעילים של תשתיות קריטיות מהמגזר הפרטי. בגיבוש

293 האסטרטגיה לשנים 2021–2018, **לעיל** ה"ש 288, בעמ' 20–21.

294 האסטרטגיה לשנים 2024–2022, **לעיל** ה"ש 288, בעמ' 15.

האסטרטגיה מסתייע השר הרלוונטי ביחידה סקטוריאלית ביזורית להגנת סייבר ומידע (DCIS) הרלוונטית למגזר.[295] כך, למשל, במגזר הבריאות פרסם משרד הבריאות בשנת 2019 אסטרטגיה להגנת סייבר במגזר לשנים 2022–2019. האסטרטגיה סוקרת את המאפיינים החושפים את מגזר הבריאות למתקפות סייבר, כמו למשל מספר רב של נותני שירות השונים בגודלם ובמורכבותם, הטרוגניות בחברות המאוסדרות, תלות גדולה בתשתיות דיגיטליות, שימוש בטכנולוגיות ובמכשירים לבישים כחלק ממתן השירות הרפואי ואיסוף מידע אישי רגיש בהיקפים נרחבים. כחלק מהצעדים לחיזוק הגנת הסייבר במגזר חויב ה־DCIS המגזרי למפות ולדרג את הסיכונים לארגונים המאוסדרים, לזהות את הגופים הקריטיים, לקבוע קווים מנחים להגנת סייבר שהציות להם יהיה מנדטורי, לקבוע מסגרת ברורה לאחריותו של כל אחד מהשחקנים במגזר להגנת הסייבר ולהבטיח זרימת מידע חופשית ביניהם בנוגע להערכת הסיכונים.[296]

האסטרטגיה לשנים 2024–2022 הרחיבה את תחולת רגולציית הציווי והשליטה הרכה והביזורית לכל תשתית, לרבות מתקן, מערכת, רשת, טכנולוגיה, נכס או שירותים, המספקת פונקציה חיונית לחברה או תומכת בפונקציה כאמור. פונקציה חיונית מוגדרת כפעולה, מוצר או שירות המהווים את הבסיס לתפקוד הכללי של החברה. האחריות להגדרת אסטרטגיית הגנת הסייבר המתאימה, לפיקוח על הטמעת מדיניות הגנת סייבר נאותה בקרב הגופים המאוסדרים ולהתנהלות בעת מתקפת סייבר מוטלת גם במקרה זה על הרשות הממשלתית האחראית על המגזר הרלוונטי.[297]

מתווה הגנת הסייבר הקבוע בשתי האסטרטגיות מהווה יישום של דירקטיבת NIS של האיחוד האירופי, ולפיו מפעילי תשתיות קריטיות נדרשים להטמיע דרישות אבטחה טכניות וארגוניות כדי להבטיח שרמת ההגנה תואמת את הסיכון לפִּרצות אבטחה ברשתות או במערכות מידע שבהן הם עושים שימוש לצורך פעילותם. כן נדרשים מפעילי תשתיות קריטיות לדווח על פרצת אבטחה

295 האסטרטגיה לשנים 2021-2018, **לעיל** ה"ש 288, בעמ' 13-14, 16.

296 Ministry of Health, Strategy for Cyber and Information Security in the Healthcare Sector (2019)

297 האסטרטגיה לשנים 2024-2022, **לעיל** ה"ש 288, בעמ' 12-13.

לרשויות מייד לאחר שנודע להם על קיומה, אם היא משפיעה על המשכיות שירותיהם.[298]

נוסף על כך, ספקי שירותים דיגיטליים שאינם נחשבים תשתיות קריטיות נדרשים להטמיע הגנה טכנית וארגונית המתאימה לסיכון שלו הם חשופים. מדובר בספקים גדולים של שירותי סחר אלקטרוני, מנועי חיפוש או מחשוב ענן.[299]

מתווה רגולציית הציווי והשליטה הרכה והביזורית עומד בעינו גם בעת מתקפת סייבר. הרשות האחראית על המגזר או התשתית הרלוונטית היא שאחראית גם לקביעת ההוראות להתמודדות עם מתקפת סייבר וכן על ניהול ההתגוננות בעת מתקפת סייבר. ואולם, בעת מתקפת סייבר משמעותית המשפיעה על כמה מגזרים, רשויות הממשל הרלוונטיות רשאיות לדווח, להיוועץ ולבקש סיוע מהצוות האופרטיבי הלאומי (National Operative Staff, NOST), המורכב, בין השאר, מנציגים של המשטרה, שירותי הביון ושירותי ההגנה הדנים.[300]

3. רגולציה שיתופית על כלל המגזרים

I. למטרות שיתוף מידע

השיתוף בידע ובניסיון בנוגע להתמודדות עם תקיפות סייבר הוא חיוני לשם שיפור רמת הגנת הסייבר, וכדי לעשות זאת הוקמו מסגרות לשיתוף ידע וניסיון בין סקטורים שונים בתעשייה ובין חברות מהמגזר הפרטי, נציגים ממוסדות מחקר ואקדמיה ורשויות הממשל.[301] כמו כן, ומתוך הבנה שהגנת הסייבר בקרב עסקים קטנים ובינוניים היא נמוכה, הוקמה מסגרת ייעודית לשיתוף

298 Federspiel, **לעיל** ה"ש 287.

299 The Network and Information Security Act for Domain Name Systems and Certain Digital Services (Act No. 436 of 8 May 2018)

300 האסטרטגיה לשנים 2022–2024, **לעיל** ה"ש 288, בעמ' 37.

301 **שם**, בעמ' 27.

מידע הנוגע למתקפות סייבר, התגוננות מפניהן וטיפול בהן בין חברות בינוניות וקטנות וגורמי ממשל.[302]

לצד אלה פועלת שותפות במודל של מאמץ משותף (joint effort), המורכבת מנציגים של רשויות הממשלה הרלוונטיות ובעלי עניין מקרב ארגונים פרטיים, האחראית להגדרה ולעדכון תדיר של אמצעים למניעת תקיפות סייבר, וכן לעידוד עסקים פרטיים לאמץ סטנדרטים בינלאומיים לאבטחת מידע ולהגנת מרחב הסייבר.

II. למטרות גיבוש סטנדרטים להגנת סייבר

המועצה הדנית להגנת הסייבר (the Danish Cyber Security Council) מורכבת מנציגים מהמגזר הציבורי ומהתעשייה ותפקידה להבטיח שיתוף במידע בנוגע למתקפות סייבר והתמודדות עימן בין הממשלה, התעשייה ומוסדות מחקר, וכן לייעץ בגיבוש אסטרטגיית הגנת הסייבר הלאומית.[303]

הפורום העסקי לאבטחה דיגיטלית (the Business Forum for Digital Security), שגם הוא שותפות בין המגזר הציבורי והמגזר הפרטי, מסייע לממשלה בעידוד ובחיזוק הגנת הסייבר בתעשייה, מספק לממשלה ולמגזר העסקי המלצות בנוגע להגנת הסייבר, ומהווה שותף אסטרטגי לממשלה ביוזמות שונות להגנת הסייבר.[304]

4. רגולציה עצמית על חברות פרטיות שאינן תשתיות קריטיות בשילוב הנחיה מהמדינה

הסוכנות הדנית לממשל דיגיטלי אחראית להפעלת קו חם להגנת סייבר וקו חם לפשעי גנבת זהות, המספק הנחיה וייעוץ לאזרחים, לחברות ולרשויות ממשל בכל הקשור להתגוננות במרחב הסייבר, להתמודדות עם איומי סייבר ותקיפות

302 **שם**, בעמ' 29.

303 **שם**, בעמ' 30.

304 **שם**, בעמ' 30.

סייבר ולהתנהלות בטוחה במרחב הסייבר, וכן מידע בנוגע לפרשנות ולאופני הציות לחקיקה המסדירה את הגנת מרחב הסייבר.[305]

כמו כן, המרכז הדני להגנת סייבר (the Danish Centre for Cyber Security), שהוא הרשות הממשלתית להגנת הסייבר בדנמרק ופועל במשרד שירותי ההגנה והמודיעין, ורשות הדיגיטיזציה (the Danish Agency for Digitisation), שהיא זרוע במשרד האוצר, פרסמו קווים מנחים להתמודדות עם איומי סייבר. הציות לקווים מנחים אלו הוא על בסיס התנדבותי בקרב ארגונים מהמגזר הפרטי.[306]

המרכז הדני להגנת סייבר גם מעודד ארגונים מהמגזר הפרטי וכן יחידים לדווח לו על תקיפות ואיומי סייבר, שלא כחלק ממערך הניטור. התמריצים לדיווח אינם משפטיים או כלכליים אלא מתבססים על עקרון הערבות ההדדית. לפי המרכז דיווחים כאמור יובילו לשיפור ביכולות שלו עצמו לתת ייעוץ וסיוע לארגונים מהמגזר הפרטי וליחידים המתמודדים עם תקיפות ואיומי סייבר. כמו כן, דיווחים על תקיפות ואיומי סייבר פטורים מחובות לפי חוק חופש המידע.[307]

גורם נוסף בהקשר זה הוא שירות ההגנה והביון הדני (the Danish Security and Intelligence Service), רשות אבטחה לאומית המספקת ייעוץ וסיוע לרשויות ממשל ולעסקים פרטיים בכל הנושאים הקשורים לאבטחה, לרבות לגבי טיפול במסמכים רגישים ואחסונם.[308]

חברות תעשייה פרטיות, בעיקר חברות בינוניות וקטנות, יכולות להסתייע גם ברשות העסקים הדנית (the Danish Business Authority), האחראית על פיתוח ויצירת ידע, קווים מנחים וכלים לחיזוק הגנת הסייבר בקרב הקהילה העסקית, בעיקר בקרב חברות בינוניות וקטנות, כמו גם על ניהול שיתוף הפעולה ביניהן למטרות אלו.[309]

305 **שם**, בעמ' 29.

306 Federspiel, **לעיל** ה"ש 287.

307 **שם**.

308 האסטרטגיה לשנים 2022–2024, **לעיל** ה"ש 288, בעמ' 39.

309 **שם**.

5. סיכום מודל הרגולציה להגנת מרחב הסייבר בדנמרק

לוח 4
האסדרה של הגנת הסייבר בדנמרק

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה ריכוזית	במגזר הציבורי, ולמטרות ניטור וחינוך בכלל מרחב הסייבר	רשויות הממשל בדנמרק נדרשות לציית לסטנדרט בינלאומי להגנת סייבר. רשויות ממשל האחראיות על מגזרי תשתיות קריטיות או על חברות המספקות שירותים החיוניים לחברה מחויבות לפתח אסטרטגיית הגנת סייבר מגזרית. משרד ההגנה הדני מפעיל 24 שעות ביממה מרכז לאומי לניטור ומעקב אחר איומי סייבר בתשתיות קריטיות. הממשלה מפעילה תוכניות לחינוך והכשרה בקרב עובדי מדינה, באקדמיה ובבתי הספר לשם העלאת המודעות לאיומי סייבר והגברת האוריינות הדיגיטלית.
רגולציית ציווי ושליטה רכה ביזורית	תשתיות קריטיות וחברות המספקות או תומכות בפונקציה חיונית לחברה	רשות הממשל הרלוונטית למגזר קובעת את אסטרטגיית ההגנה, וה־DCIS (יחידות סקטוריאליות ממשלתיות) אחראיות ליישום האסטרטגיה תוך שיתוף פעולה ושיתוף מידע בין כלל הגורמים הרלוונטיים.
רגולציה שיתופית	משרדי ממשלה ובעלי עניין מהמגזר הפרטי	שיתוף מידע בין המגזר הפרטי למגזר הציבורי הן בקרב תשתיות קריטיות והן בקרב חברות בינוניות וקטנות שאינן תשתיות קריטיות. קביעה משותפת של סטנדרט הגנת הסייבר המומלץ ועידוד ארגונים מהמגזר הפרטי לאמצו.
רגולציה עצמית	ארגונים במגזר הפרטי שאינם תשתיות קריטיות	ציות וולונטרי לקווים מנחים המפורסמים על ידי המרכז הדני להגנת סייבר ורשות הדיגיטיזציה. עידוד דיווח על תקיפות ואירועי סייבר, שלא דרך מערך הניטור, כדרך לחיזוק הערבות ההדדית. ייעוץ ומתן קווים מנחים לחברות בינוניות וקטנות על ידי רשות העסקים הדנית.

III. צרפת

צרפת מדורגת במקום השני במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם.[310] היא זוכה ב־68 מתוך 75 נקודות אפשריות במדד הגנת מרחב הסייבר של Comparitech, אשר מתמקד בהגנת הסייבר ברמת המשתמש הבודד.[311]

האסדרה של הגנת מרחב הסייבר בצרפת החלה בשנת 2008 עם הקמת הרשות הלאומית להגנת הסייבר (National Cybersecurity Agency, להלן: ANSSI)[312] המדווחת לשר ההגנה (Secretary General for Defence and National Security). ANSSI הופקדה על גיבוש מדיניות לאסדרת ההגנה של מרחב הסייבר, שתכלול אמצעים לאיתור איומי סייבר, למניעת תקיפות סייבר, להתמודדות עם תקיפת סייבר בעת התרחשותה ולמזעור נזקיה, וכן הכשרת כוח אדם מקצועי בתחום הגנת הסייבר לרווחת משרדי הממשלה ומפעילים של תשתיות קריטיות.[313]

1. רגולציית ציווי ושליטה בעת מתקפת סייבר

ANSSI אחראית לניהול התגובה למתקפת סייבר על תשתית קריטית, וכן לניהול ההחלמה ממנה. רק במקרה קיצון תתערב המדינה באירוע של תקיפת סייבר על חברות פרטיות שאינן שייכות למגזר התשתיות הקריטיות.[314]

310 Global Cybersecurity Index 2020, **לעיל** ה"ש 29.

311 Bischoff, **לעיל** ה"ש 30.

312 הכינוי המקוצר נגזר משם הרשות בצרפתית: Agence nationale de la sécurité des systèmes d'information.

313 The French White Paper on Defence and National Security (2008)

314 **שם;** Antonio Calcara & Raffaele Marchetti, *State-Industry Relations and Cybersecurity Governanace in Europe*, 29(4) Rev. of Int'l Pol. Econ. 1237, 1245-1246 (2022)

2. רגולציית ציווי ושליטה ריכוזית על תשתיות קריטיות, מפעילי שירותי טלקומוניקציה וספקי שירות דיגיטליים

המדינה מחויבת לפי חוק להבטיח שמערכות המידע הקריטיות של מפעיל במגזר חיוני (Operator of Vitally Important Sector) מאובטחות כראוי. מפעיל במגזר חיוני מוגדר ככל ארגון, פרטי או ציבורי, שמעורב בפעילות בסקטור חיוני, כלומר בייצור או הפצה של טובין או שירות חיוניים, דהיינו טובין או שירות שפגיעה באספקתם התקינה והפסקתה עלולות לפגוע באופן משמעותי במצבה הכלכלי או הצבאי של המדינה, או בביטחון הציבור וחוסנו, ושקשה להחליפם.[315] עד כה זוהו כ־200 ארגונים מ־12 מגזרי תשתיות קריטיות כמפעילים במגזר חיוני. מערכות המידע הקריטיות במגזר חיוני הן אלו התומכות בפונקציות קריטיות לפעולה השגרתית של הארגון, ושאי־זמינותן עלולה לאיים משמעותית על חוסנה הלאומי של צרפת, כוחה הצבאי או כוחה הכלכלי.[316] ארגון הנחשב מפעיל שירות חיוני מקבל על כך הודעה מ־ANSSI.[317] על ארגונים אלו מוחלת רגולציית ציווי ושליטה ריכוזית בכל הנוגע להגנת הסייבר במערכות המידע הקריטיות

315 Code de la défense [Defence Code] art. L.1332-1

316 Code de la défense [Defence Code] art. L.1332-1; LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale [Act No. 2013-1168 of December 18, 2013, on Military Programming for 2014 to 2019], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Dec. 19, 2003, p. 20570, art. 22 (להלן: Military Programming Act 2013).

317 LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité [Act No. 2018-133 of February 26, 2018, on implementing various provisions of European Union law in the field of security and its implementing decrees and orders], J.O., Feb. 27, 2018 (להלן: Implementing EU Law Act); Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique [Decree No. 2018-384 of May 23, 2018, on the networks and information systems security of essential and digital services providers], J.O., May 25, 2018

שלהם. במסגרת רגולצייה זו הם מחויבים לאמץ כללי אבטחה המוגדרים על ידי ANSSI, להטמיע מנגנוני ניטור המופעלים על ידי ANSSI או על ידי ספק מוסמך אחר, וכן לדווח ל־ANSSI על כל תקיפת סייבר גדולה המכוונת נגד מערכות המידע הקריטיות שלהם. ANSSI גם מוסמכת לבצע ביקורות בארגונים אלו כדי לבחון את רמת האבטחה בהם, ובמקרה של תקיפת סייבר רחבת היקף היא מוסמכת לחייב הטמעה של אמצעי הגנה נחוצים שיוגדרו על ידי הממשלה.[318]

מפעילי שירותי טלקומוניקציה כפופים גם הם לרגולציית ציווי ושליטה ריכוזית שבמסגרתה, בכפוף לקבלת מידע מקדים מ־ANSSI, הם מורשים לעשות שימוש במערכת ניטור לשם זיהוי וגילוי מתקפות סייבר העלולות להשפיע על רמת האבטחה של מערכות המידע של לקוחותיהם. אם ANSSI מודעת לאיום סייבר העלול להשפיע על האבטחה של מערכות מידע, היא מורשית לדרוש ממפעיל שירות הטלקומוניקציה לעשות שימוש במערכת ניטור המסופקת לו מטעמה. אם האיום עלול להשפיע על מערכות מידע של רשות ציבורית, ANSSI מוסמכת להטמיע מערכת ניטור מטעמה במערכות מפעיל שירות הטלקומוניקציה. כן חלה על מפעילי שירותי טלקומוניקציה החובה לדווח ל־ANSSI ללא דיחוי על כל איום סייבר שהם מזהים ושעלול להשפיע על אבטחת מערכות מידע של לקוחותיהם, ו־ANSSI מוסמכת לחייבם במתן הודעה ללקוחותיהם על חולשה או מתקפת סייבר במערכותיהם.[319]

318 The French White Paper on Defence and National Security, **לעיל** ה"ש 313; Code de la défense [Defence Code] art. L.1332-1; Military Programming Act 2013, **לעיל** ה"ש 316, בסעיף 22.

319 Code des postes et des communications électroniques [Post and Electronic Communication Code] art. L33-14; LOI n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense [Act No. 2018-607 of July 13, 2018, on Military Programming for 2019 to 2025], J.O., July 14, 2018 (להלן: Military Programming Act 2018); Code de la défense [Defence Code] art. L.2321-2-1

כחלק מהטמעת דירקטיבת NIS, ספקי שירות דיגיטליים[320] חייבים למנות נציג בצרפת אם הם אינם מאוגדים או מחזיקים בנציג בתחומי האיחוד, לבצע ניהול והערכה של הסיכון לתקיפת סייבר נגדם, להטמיע אמצעים טכניים וארגוניים הדרושים כדי למנוע תקיפות סייבר ולדווח ל־ANSSI על תקיפות סייבר.[321]

מפעיל במגזר חיוני, ספק שירותי טלקומוניקציה או ספק שירות דיגיטלי שאינם עומדים בדרישות הרגולציה צפויים לקנסות כספיים בהתאם לחוק.[322]

3. רגולציה שיתופית בכלל המגזרים

צרפת נוקטת גם את גישת הרגולציה השיתופית, מתוך הבנה שכל אחד מהשחקנים במרחב הסייבר – גופים ציבוריים, רשויות רגולטוריות, משרדי ממשלה, ארגונים פרטיים עסקיים, אקדמיה, ארגונים שלא למטרות רווח, ארגוני החברה האזרחית ואף האזרחים – אחראי להגנת מרחב הסייבר.[323]

הרגולציה השיתופית נהוגה לשם הגשמת המטרות שלהלן:

I. קביעת מדיניות

ההגדרה בחוק של מפעיל במגזר חיוני[324] גובשה בהליך היוועצות עם המגזר העסקי בניהול ANSSI. כך גם גובש סעיף החוק המתיר לארגונים להטמיע מערכות ניטור לשם זיהוי וגילוי מוקדם של איומי סייבר, ואשר במקרים מסוימים מאפשר ל־ANSSI להטמיע מערכות ניטור שכאלו לתקופה קצובה

320 ספק שירותים דיגיטליים (digital service) הוא כל ספק של שירות המסופק בשגרה מרחוק באמצעים אלקטרוניים לבקשתו של מקבל השירות, לרבות מנוע חיפוש, פלטפורמת סחר אלקטרוני ושירותי ענן. הגדרה זו שאובה מדירקטיבת NIS של האיחוד האירופי. ראו דירקטיבת NIS, **לעיל** ה"ש 187, בסעיפים 4(5)–(6).

321 Implementing EU Law Act, **לעיל** ה"ש 317.

322 **שם**; Military Programming Act 2018, **לעיל** ה"ש 319; Code de la défense [Defence Code] art. L.2321-2-1

323 Premier Ministre, French National Digital Security Strategy, 7 (2015) (להלן: National Strategy 2015).

324 ראו **לעיל** ה"ש 316.

בארגונים פרטיים המוגדרים כחיוניים. בגיבוש הסעיף השתתפו נציגים של חברות תקשורת וארגונים חיוניים אחרים, במטרה להבטיח ניטור אפקטיבי של המערכות לצד מזעור הפגיעה בזכות לפרטיות.[325]

II. העלאת מודעות לסיכוני סייבר, חינוך ועידוד מחקר ופיתוח

ANSSI הקימה ועדה מדעית שמטרתה לחזק את הקשר עם קהילת המחקר בתחום הסייבר, כחלק משיתוף פעולה בין־מגזרי שמטרתו העלאת מודעות לסיכוני הסייבר ועידוד המחקר המדעי בתחום.[326]

כמו כן, הוקם פאנל מומחים לאמון דיגיטלי (Expert Panel for Digital Trust), שמורכב מנציגים ממשרדי הממשלה השונים (החינוך, המחקר וההשכלה הגבוהה, המשפטים, ההגנה, הרווחה, הבריאות וזכויות הנשים, הכלכלה, התעשייה, הטכנולוגיה הדיגיטלית, הפנים ומשרד ראש הממשלה), מנציבות ההשקעות, מרשות המחקר הלאומית ומארגוני מחקר רלוונטים. בפאנל יכולים להשתתף גם נציגים מהמגזר העסקי שהם מומחים בתחומם. מטרת הפאנל לזהות תחומים שבהם נדרשת הכשרה בהגנת סייבר, לפקח על מחקרים ויישומם בתעשייה, וכן להתוות תוכנית ממשלתית לתמיכה כלכלית במחקר ולסיוע במימון מלגות דוקטורט בתחום הגנת הסייבר. על הפאנל לדווח מדי שנה לראש הממשלה על פעילותו.[327]

נוסף על כך, בשיתוף פעולה בין ANSSI למוסד המחקר הלאומי למדע דיגיטלי וטכנולוגיה (Inria) הושקה בפברואר 2022 תוכנית ההעברה של קמפוס הסייבר (Cyber Campus Transfer Programme). התוכנית, המנוהלת על ידי Inria, היא מסגרת לעידוד שיתוף פעולה בין המגזר הציבורי, המגזר הפרטי והאקדמיה,

325 Agence nationale de la sécurité des systèmes d'information, Report Annuel 2018, 20 (2018) (להלן: ANSSI Annual Report 2018).

326 **שם**, בעמ' 48.

327 National Strategy 2015, לעיל ה"ש 323, בעמ' 14–15.

למטרות מחקר ופיתוח בתחום טכנולוגיית ההעברה בהקשר של הגנת הסייבר, לעידוד הטמעת טכנולוגיות חדשניות ולעידוד הקמת חברות הזנק בתחום.[328]

III. שיתוף מידע במגזרי תשתיות קריטיות

שיתוף המידע על מתקפות סייבר, איומי סייבר וההתמודדות עימם מוגבל כרגע למסגרות של שותפות ציבורית–פרטית בין ANSSI לארגונים ממגזרי התשתיות קריטיות, דהיינו מפעילים חיוניים ומפעילים במגזר חיוני.[329]

4. רגולציה עצמית על ארגונים פרטיים ממגזרים שאינם תשתיות קריטיות

המגזר הפרטי נתפס כאחראי להגנת הסייבר בתשתיות שבשליטתו, ורשויות המדינה מתערבות רק במקרי קיצון. ואולם, ANSSI מספקת לארגונים פרטיים שאינם מפעילים או בעלים של תשתיות קריטיות תמריצים שונים, כמו למשל Security Visa – אישור ש־ANSSI נותנת למוצרים או לספקי שירותים דיגיטליים המוכיחים שהם מצייתים לדרישותיה;[330] ו־French Cybersecurity – אישור לספקי מוצרי הגנת סייבר. כמו כן מפעילה ANSSI מרכזים לבחינת רמת המוכנות לתקיפת סייבר של מוצרים או שירותים דיגיטליים, לרבות שירותי מחשוב ענן, ומרכז להכשרת עובדי ציבור ועובדים בארגונים חיוניים או מפעילי שירות חיוני בתחום ההגנה על מערכות מידע (Information Systems Security Training

328 Hubert Duault, *Inria and ANSSI Key Players in Cyber Security in France*, Inria (Feb. 15, 2022)

329 שיתוף הפעולה הציבורי־פרטי נעשה למשל במסגרת הפלטפורמה האינטרנטית Cybermalveillance.gouv.fr או במסגרת הקמפיין SecNumEco, פרי שיתוף פעולה בין ANSSI וה־DGE (Directorate General for Enterprise), האחראי לתכנון ויישום מדיניות ציבורית התורמת לפיתוח עסקים, במסגרת משרד הכלכלה, האוצר והתעשייה הדיגיטלית. הקמפיין נועד להעלות מודעות להגנת סייבר בכל הקשור לניירות ערך דיגיטליים. ראו גם ANSSI Annual Report 2018, **לעיל** ה"ש 325, בעמ' 20–21.

330 Matthieu Duault, *What is the Security Visa issued by the ANSSI?*, You Sign

Centre), ומפרסמת הנחיות לשיפור הגנת הסייבר בארגון.[331] עם זאת, עלויות העמידה בדרישות ANSSI, למשל במסגרת ה־French Cybersecurity, גבוהות מאוד, ולכן חברות קטנות ובינוניות בתחום הגנת הסייבר לא פנו כלל לקבלת האישור או העדיפו לפעול מחוץ לצרפת.[332]

היעדר סיוע לעסקים בינוניים וקטנים, לעצמאים ולאנשים פרטיים החווים תקיפת סייבר הוביל להקמתו בשנת 2015 של מערך סיוע ייעודי המופעל בשיתוף פעולה בין משרדי הממשלה השונים (משרד הפנים, משרד המשפטים, משרד הכלכלה, ANSSI ומשרד ההגנה). המערך מעניק עצות מעשיות להתמודדות עם תקיפת סייבר בשיתוף עם גורמים מומחים מהתעשייה, וכן מעמיד לרשות הנפגעים מנגנון להגשת תלונות.[333]

5. סיכום מודל הרגולציה להגנת מרחב הסייבר בצרפת

לוח 5
האסדרה של הגנת הסייבר בצרפת

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה	תשתיות קריטיות בעת חירום	ANSSI אחראית לניהול התגובה למתקפת סייבר על תשתית קריטית ולניהול ההחלמה ממנה. רק במקרה קיצון תתערב המדינה גם באירוע של מתקפת סייבר על חברות פרטיות שאינן שייכות למגזר התשתיות הקריטיות.

331 בשנת 2021, למשל, פרסמה ANSSI 48 מסמכים המהווים מקור למידע בתחומי הגנת הסייבר. ראו ANSSI, Annual Review 2021 (2022).

332 Calcara & Marchetti, **לעיל** ה"ש 314, בעמ' 1247.

333 National Strategy 2015, **לעיל** ה"ש 323, בעמ' 20–23.

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה ריכוזית	ארגונים המוגדרים כמפעיל במגזר חיוני, מפעיל שירות טלקומוניקציה וספקי שירות דיגיטליים	רגולציית ציווי ושליטה ריכוזית המוטלת ונאכפת בידי ANSSI.
רגולציה שיתופית	כלל השחקנים במרחב הסייבר	ANSSI בשיתוף עם גורמים מהמגזר הציבורי, המגזר הפרטי, האקדמיה והמגזר השלישי פועלים כדי לגבש רגולציה, להגביר את המודעות לסיכוני סייבר, לשפר את החינוך וההכשרה בתחום הגנת הסייבר החל מבתי הספר, לקדם את המחקר והפיתוח של טכנולוגיות חדשניות להגנת סייבר ולשתף מידע (המוגבל לתשתיות קריטיות).
רגולציה עצמית	ארגונים במגזר הפרטי שאינם תשתיות קריטיות	רגולציה עצמית בשילוב תמריצים והנחיות לא מחייבות של ANSSI. למשל, תוכנית Security Visa שבמסגרתה מעניקה ANSSI אישורים למוצרים ולספקי שירות דיגיטלי המוכיחים שהם עומדים בדרישותיה בתחום הגנת הסייבר. ANSSI מפרסמת באופן תדיר הנחיות והמלצות בנוגע להגנת הסייבר לרווחת כלל הארגונים במשק. ANSSI מפעילה מרכז להכשרת עובדי ציבור ועובדים בארגונים חיוניים או מפעילי שירות חיוני בתחום ההגנה על מערכות מידע.

ד. ישראל

ישראל מדורגת במקום ה־36 במדד הגנת הסייבר העולמי לשנת 2020 של איחוד הטלקומוניקציה הבינלאומי של האו"ם,[334] והיא זוכה ב־61 מתוך 75 נקודות

334 Global Cybersecurity Index 2020, **לעיל** ה"ש 29. זאת בהתחשב בכך שאף נציג רשמי לא ענה על השאלות במדד.

אפשריות במדד הגנת מרחב הסייבר של Comparitech, אשר מתמקד בהגנת הסייבר ברמת המשתמש הבודד.[335]

1. האסדרה של הגנת הסייבר לאורך השנים

ישראל הכירה בצורך להתמודד עם איומים שמקורם במרחב הסייבר כבר בשנת 1997. תחילה התמקדה האסדרה בהגנה על המערכות הממוחשבות של משרדי ממשלה במסגרת פרויקט תהיל"ה ("תשתית הממשלה לעידן האינטרנט"). בשנת 1998 התרחבה רגולציית הסייבר גם אל המגזר הפרטי, עם חקיקת החוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998. חוק זה השית רגולציית ציווי ושליטה על תשתיות קריטיות מהמגזר הציבורי ומהמגזר הפרטי, מתוך הערכת סיכונים וההבנה שפגיעה בתשתיות קריטיות עלולה לגרום לפגיעה חמורה בביטחון המדינה. החלטת ממשלה ב/84 משנת 2002 הסמיכה את הרשות לאבטחת מידע (רא"מ), יחידה בשב"כ, לתפקיד המנחה המקצועי של גופי התשתיות הקריטיות בכל הנוגע לאבטחת סייבר.[336]

רא"מ הוסמכה לקבוע אילו ארגונים ייחשבו גופי תשתיות מדינה קריטיות (להלן: גופי התמ"ק) ויידרשו לפעול בהתאם להנחייתה ולפי החוק להסדרת הביטחון בגופים ציבוריים. רשימת גופי התמ"ק מעודכנת מזמן לזמן ונכון ל־2020 כוללת כ־80 גופים.[337] ארגונים שהוגדרו כגופי תשתיות קריטיות נדרשו למנות קצין ציות לעבודה מול רא"מ, חויבו לתת לרא"מ גישה לכל המידע שבידי הארגון, למערכותיו ולנכסיו כדי להעריך את הסיכונים האפשריים ולוודא ציות לדרישותיה, ונאלצו לשאת בעלות ההנחיה הרגולטורית של רא"מ. ארגונים

335 Bischoff, **לעיל** ה"ש 30.

336 החלטה ב/84 של ועדת השרים לענייני ביטחון לאומי, הממשלה ה־29 "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" (19.12.2002); עמיר רפפורט "השב"כ בעידן הקיברנטי: מבט מבפנים" **IsraelDefence** (11.4.2014).

337 תוספת ראשונה עד תוספת חמישית לחוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח–1998.

מסחריים שהוגדרו כגופי תשתיות קריטיות הביעו מורת רוח מכך שנדרשו לשאת בעלויות ההנחיה וכן מהיעדר שקיפות מצד רא״מ.[338]

בשנת 2011 שינתה ממשלת ישראל את גישתה לאסדרת ההגנה של מרחב הסייבר, והחלה לתת את הדעת לצורך לפעול גם מול ארגונים מהמגזר האזרחי הפרטי, שאינם בהכרח תשתיות קריטיות, תוך העברת סמכויות מסוכנויות המודיעין (רא״מ) למטה הסייבר הלאומי, שהוקם כגוף מטה הכפוף לראש ממשלת ישראל. המניע להחלטת הממשלה היה הרצון ליצור אינטגרציה מוצלחת יותר עם חברות במשק ולאמץ תפיסה הוליסטית רחבה לעיסוק במרחב הסייבר.[339]

כארבע שנים אחר כך החליטה הממשלה על הקמת הרשות הלאומית להגנת הסייבר, כיחידת סמך במשרד ראש הממשלה שייעודה הוא הגנת מרחב הסייבר האזרחי והגנה על נכסים קריטיים במטרה לשמור על רציפות תפקודית של תשתיות המדינה הקריטיות. הרשות הלאומית להגנת הסייבר פעלה גם כגוף מנחה מול כלל המשק באמצעות הרגולטורים השונים, והיה עליה לפקח על פעולותיהם בתחום ההגנה על מרחב הסייבר ולתאם בין הפעולות השונות. מטה הסייבר המשיך בפעילותו לפתח מסגרת רגולטורית להגנת הסייבר במדינת ישראל. ביולי 2017 קיבלה הרשות הלאומית להגנת הסייבר את סמכויותיה של רא״מ בכל הקשור לחברות פרטיות שהן בעלים או מפעילים של תשתיות קריטיות אזרחיות.[340]

338 עידו סיון סביליה **הרגולציה בתחום הגנת הסייבר בישראל: שינוי משטרי מדיניות 1997 – 2018** 86 (2022).

339 מטה הסייבר הלאומי הוקם לפי החלטה 3611 של הממשלה ה־32 "קידום היכולת הלאומית במרחב הקיברנטי" (7.8.2011).

340 החלטה 2443 של הממשלה ה־33 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" (15.2.2015) (להלן: החלטת ממשלה 2443); החלטה 2444 של הממשלה ה־33 "קידום ההיערכות הלאומית להגנת הסייבר" (15.2.2015) (להלן: החלטת ממשלה 2444); ס' 21ב לחוק להסדרת הביטחון בגופים ציבוריים; הרשות הלאומית להגנת הסייבר **סיכום שנות ההקמה 2016–2017** 25 (2017) (להלן: **סיכום 2016–2017**); סעיפים 1–2 להחלטה 3270 של הממשלה ה־34 "איחוד יחידות מערך הסייבר הלאומי" (17.12.2017) (להלן: החלטת ממשלה 3270).

בסוף שנת 2017 אוחדו מטה הסייבר הלאומי והרשות הלאומית להגנת הסייבר לגוף אחד – מערך הסייבר הלאומי.[341] המערך אחראי להגנת מרחב הסייבר האזרחי, למתן שירותים לניהול מתקפות סייבר והדרכה לכל החברות האזרחיות ולהגנת הסייבר בחברות פרטיות שהן בעלים או מפעילים של תשתיות קריטיות אזרחיות, וכן בחברות פרטיות שאינן תשתיות קריטיות אך נחשבות תשתית חיונית שכן פגיעה בהן עשויה להוביל לפגיעה חמורה בכלכלת המדינה, בביטחונה או בביטחון אזרחיה. עוד אחראי מערך הסייבר לייעץ לחברות פרטיות ולאזרחים פרטיים באמצעות הקו החם שהוא מפעיל.[342]

ביוני 2018 פורסם תזכיר חוק הגנת הסייבר, שמטרתו לעגן בחקיקה את המסגרת הרגולטורית לפעילותו של מערך הסייבר הלאומי תוך מימוש החלטות הממשלה בנושא.[343] פרסום התזכיר הוא צעד חשוב, שכן יש להסדיר את סמכויותיו, מטרותיו והמבנה הארגוני של מערך הסייבר בחקיקה ראשית של הכנסת.

בהמשך ולאחר קבלת הערות מהציבור בוצעו במהלך השנים 2020–2019 סבבי דיונים בהשתתפות משרדי הממשלה הרלוונטיים, ותזכיר חוק הסייבר תוקן. עם זאת, תזכיר חוק סייבר מתוקן לא פורסם בציבור וכל הידוע עליו נשאב מפרסום תקציר התיקונים.[344]

נכון לכתיבת מסמך זה תזכיר חוק הסייבר תלוי ועומד ואינו בשל לכדי חוק. במרץ 2021 נעשה ניסיון לחוקק הוראת שעה אשר תסדיר את הסמכויות האופרטיביות של מערך הסייבר, ולדברי מערך הסייבר תיתן מענה לחסר המרכזי בטיפול ב"סרבנים", כלומר ארגונים מהמגזר הפרטי שאינם מסכימים לשתף פעולה עם דרישות מערך הסייבר. הוראת השעה הייתה אמורה להסמיך את מערך הסייבר

341 החלטת ממשלה 3270, **לעיל** ה"ש 340.

342 Dimitry Adamsky, *The Israeli Odyssey toward Its National Cyber Security Strategy*, 40(2) The Washington Quarterly 113, 120 (2017); החלטת ממשלה 3270, **לעיל** ה"ש 340.

343 תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח–2018 (להלן: תזכיר חוק הסייבר).

344 "תקציר תזכיר חוק הגנת הסייבר" **מערך הסייבר הלאומי** (12.7.2018; עודכן 5.7.2020) (להלן: תקציר התזכיר).

לחייב ארגון שמותקף לשתף עימו פעולה אם לדעת המערך תקיפת הסייבר על אותו ארגון עלולה לסכן אזרחים רבים ואינטרסים חיוניים.[345] גם הוראת שעה זו לא בשלה לכדי חוק.[346]

2. מערך הסייבר הלאומי – פנים רבות לו

תפקידיו של מערך הסייבר הם:[347]

(**1**) לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים והאופרטיביים מפני תקיפות סייבר.

(**2**) לקדם את יכולת ההתמודדות של ישראל עם תקיפות סייבר. יש לציין שתקציר התזכיר משנה במעט מהקבוע בתזכיר חוק הסייבר, וקובע שמערך הסייבר הלאומי יופקד על קידום יכולת ההתמודדות של **מדינת ישראל**, ולא של **ארגונים** במדינת ישראל, עם תקיפות סייבר.

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

(**4**) לקדם שיתופי פעולה בינלאומיים בתחום הסייבר שיבשילו לכדי הסכמי שיתוף פעולה.

(**5**) לייעץ לממשלה ולוועדותיה בתחום הסייבר.

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

מדובר אפוא בטווח רחב מאוד של תפקידים, שחלקם מוגדרים באופן שמשאיר פתח רחב לפרשנות, ומשלב, ואולי יש לומר מערבב, בין הסמכות לקבוע סטנדרטים להגנת סייבר, שצריכה להיות מופקדת בידיו של גוף מקצועי בעל ידע, מומחיות וגישה למידע מודיעיני רלוונטי, ובין סמכויות אופרטיביות,

345 טל שחף "'איבד את הדרך': מה קורה במערך הסייבר?" **ynet** (29.10.2021) (להלן: שחף "איבד את הדרך").

346 תזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי (סמכויות לשם חיזוק הגנת הסייבר) (הוראת שעה), התשפ"א–2021 (להלן: תזכיר הוראת השעה).

347 סעיף 2א לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343, וכן תקציר התזכיר, **לעיל** ה"ש 344.

סמכויות אכיפה, סמכויות בתחום החינוך, ההכשרה וקידום החדשנות וסמכות שיורית.

זאת ועוד, בתזכיר חוק הסייבר ובתקציר התזכיר מערך הסייבר מוצג בראש ובראשונה כגוף ביטחוני־מבצעי, וככזה הוא בעל סמכויות אופרטיביות לפעול לשם מניעת מתקפות סייבר והתמודדות עימן. לצד היותו גוף ביטחוני, מערך הסייבר הוא גם המאסדר הלאומי בתחום הגנת הסייבר, וכן גוף מקצועי שבידו הידע הדרוש להנחיית רגולטורים אחרים בתחום זה. בתקציר התזכיר מוסבר שכובעיו הרבים של מערך הסייבר, בדמות סמכויותיו האופרטיביות והרגולטוריות, הם שמאפשרים לו לעמוד במשימת ההגנה הלאומית בתחום הסייבר.[348]

אולם לדעתנו, עירוב הסמכויות השונות – ההנחיה, קביעת הסטנדרטים, האכיפה והפיקוח, החינוך וההכשרה והסמכות השיורית – לצד העובדה שמערך הסייבר הוקם כגוף מודיעיני, הובילו את מערך הסייבר לאמץ פרקטיקות מעולם המודיעין שאינן מתאימות להתנהלות מול גופים פרטיים שאינם תשתיות קריטיות.

יתרה מכך, מערך הסייבר הלאומי נמצא בניגוד עניינים מובנה, שכן מחד גיסא עליו לפעול למימוש האינטרס הלאומי שבהבנת זהות מבצע התקיפה לשם גיבוש התגובה המדינתית לתקיפת הסייבר, ומאידך גיסא עליו לתת מענה לחברות מהמגזר הפרטי, שאינן מתעניינות בזהות התוקף ומטרותיו ברמה הלאומית אלא מצפות לקבל מהמערך סיוע מקצועי למניעת תקיפת סייבר ולהתמודדות עימה לשם מזעור נזקיה.

לאור כל אלה, גורמים במגזר הפרטי מותחים ביקורת קשה על מערך הסייבר הלאומי ותפקודו, והתפרסמו בתקשורת עדויות על התנהגות כוחנית מצד אנשי מערך הסייבר הלאומי, המנסים לכאורה להשיג שיתוף הפעולה מצד חברות פרטיות באמצעות הפחדה מפני מתקפות סייבר, אך בה בעת נמנעים מגילוי ושיתוף מידע עם חברות אלה.[349]

348 תקציר התזכיר, **לעיל** ה"ש 344.

349 שחף "איבד את הדרך", **לעיל** ה"ש 345.

מערך הסייבר, מצידו, אינו תופס את הסיוע לארגונים בעת תקיפת סייבר כחלק עיקרי מתפקידו. אזרח, או כל ארגון שאינו תשתית קריטית, שמערכות המידע שלו מותקפות יכול ליצור קשר עם המוקד הלאומי 119 שהמערך מפעיל ולדווח על מתקפת הסייבר. בחלק מהמקרים המערך יזהה את החולשה שאפשרה את המתקפה ויַפנה את הפונה המותקף לאתרים שבהם יוכל למצוא את המפתח למתקפה או העדכון לחולשה. אם המערך יזהה שמקור המתקפה הוא פלילי, יופנה המותקף למשטרה. במקרים אחרים ינסה המערך לסייע למותקף כדי למנוע את התפשטות מתקפת הסייבר לארגונים נוספים.[350] ואכן, לדבריו של יגאל אונא, ראש מערך הסייבר לשעבר, תפקיד מערך הסייבר אינו למנוע תקיפות אלא למנוע "מגפה". כלומר הוא אינו אחראי לטיפול בגוף הספציפי המותקף, "החולה הבודד" שעל פי רוב נדרש לשיקום, אלא תפקידו למנוע את התפשטות תקיפת הסייבר לגופים חיוניים אחרים במשק הישראלי.[351]

לתוך הריק שנוצר בתחום הסיוע לחברות פרטיות שאינן תשתיות קריטיות בהגנה מפני מתקפות סייבר החלו להיכנס חברות פרטיות. באוקטובר 2021 הכריזה חברת הגנת הסייבר קונפידס על הקמת חמ"ל סייבר הזמין לאורך כל שעות היממה לשם מתן מענה לחברות שמגלות שנחשפו לתקיפת סייבר. גם התאחדות התעשיינים הכריזה על הקמת מטה סייבר פנימי לשם מתן מענה בזמן אמת לחברות שהותקפו.[352]

כמו כן, גוברות הקריאות לשנות את מודל האסדרה של הגנת מרחב הסייבר, להחזיר את האחריות להגנת מרחב הסייבר בתשתיות קריטיות לידי השב"כ ולהשאיר את מערך הסייבר הלאומי כגוף אזרחי ולא ביטחוני, האחראי על קביעת סטנדרטים מינימליים לשוק הפרטי וכפוף לחוק חופש המידע, בדומה לגופי רגולציה אזרחיים אחרים. הרגולטורים הייעודיים כמו רשות הגנת

350 יואב לימור "סייבר קינג: הדור הבא של ההגנה על הארץ" **ישראל היום** (10.9.2020).

351 שחף "איבד את הדרך", **לעיל** ה"ש 345.

352 **שם.**

הפרטיות, הממונה על שוק ההון ואחרים, יאכפו את הסטנדרטים שיקבע מערך הסייבר.[353]

היעדר מסגרת חקיקתית ברורה להסדרת פועלו ותפקידיו של מערך הסייבר הלאומי, אשר תיקבע לאחר תיאום ציפיות בין המגזרים השונים ובין המדינה, מחריף את הפערים בין תפקודו של המערך בפועל והציפיות ממנו בציבור, בעיקר נוכח העלייה המתמדת במתקפות הסייבר על גופים וארגונים במדינת ישראל.[354]

3. המסגרת הרגולטורית של הגנת מרחב הסייבר בישראל

כאמור, נכון למועד כתיבת מסמך זה תזכיר חוק הסייבר תלוי ועומד וכך גם תזכיר הוראת השעה. מערך הסייבר ועימו הגנת הסייבר במדינת ישראל מתנהלים בהתאם להחלטות הממשלה בנושא ולפי החוק להסדרת הביטחון בגופים ציבוריים. בשל כך, מערך הסייבר מתפקד בעיקר כגוף מנחה ומייעץ לרגולטורים המגזריים ולארגונים פרטיים מסוימים, אך לבד מרגולטורים מגזריים מסוימים אין בנמצא גוף כלשהו – המערך או גוף אחר – המחזיק בסמכויות פיקוח ואכיפה של הגנת סייבר נאותה בקרב ארגונים מהמגזר הפרטי.

הבעייתיות שבמצב זה מומחשת במתקפות סייבר שונות שאירעו בשנים האחרונות. כך, למשל, בדצמבר 2020 כוונה מתקפת סייבר נגד חברת הביטוח שירביט. התוקפים, שהזדהו כהאקרים מקבוצת BlackShadow, הצליחו לחדור למערכות חברת הביטוח, על פי ההערכות דרך כתובת דוא"ל שנותרה פעילה אף שהעובד שהחזיק בה עזב את החברה. הם הצליחו לשים את ידם על מאגרי מידע אישי שכללו, בין השאר, צילומים של תעודות זהות, רישיונות נהיגה, פוליסות ביטוח של כלי רכב ודירות, תיעוד שיחות עם שירות הלקוחות ומידע אישי על עובדי החברה. התוקפים דרשו משירביט כמיליון דולר בביטקוין בתוך 24 שעות, ולא – יוכפל סכום הכופר. בהמשך איימו המוכרים כי אי־תשלום הכופר

353 שם.

354 יהודה קונפורטס "מניעת מתקפת סייבר: המדינה צריכה לחשב מסלול מחדש" **אנשים ומחשבים** (1.8.2022).

הדרוש יביא למכירת המידע בשוק השחור למרבה במחיר. להוכחת רצינותם פרסמו התוקפים חלק מהמסמכים שיש בידם בפומבי, אולם ברגע ששירביט הכריזה שאין בכוונתה לשלם את הכופר ירדו התוקפים בחזרה למחשכים, וסביר שמכרו או שהם מנסים למכור את מאגרי המידע שברשותם ברשת האפלה (Darknet).[355]

שירביט הודיעה על התקיפה ללקוחותיה במסרון רק כשלוש שעות לאחר הדיווח הראשוני בתקשורת. מידע נוסף בדבר המתקפה פורסם על ידי מערך הסייבר הלאומי בדף הפייסבוק שלו. נציג שירביט ניהל משא ומתן עם התוקפים בערוץ טלגרם, אך המשא ומתן לא הניב כל תוצאה. בפרסומים בתקשורת ובתגובתה לבית המשפט בבקשה לתביעה ייצוגית נגדה שבה והדגישה שירביט כי גורמים ממלכתיים מעורבים בניהול האירוע, וכי נציגי מערך הסייבר והשב"כ נמצאים במשרדי החברה. יתרה מכך, הובהר שהחברה פועלת בתיאום עם מערך הסייבר הלאומי, רשות שוק ההון, ביטוח וחיסכון, משטרת ישראל, הרשות להגנת הפרטיות וגורמים ממלכתיים נוספים.[356]

אולם דווקא טענתה של שירביט שהיא פועלת בתיאום עם מכלול הרגולטורים המעורבים מבהירה עד כמה היעדר חקיקה מתאימה מוביל בסופו של דבר לחולשת גורמי הפיקוח והאכיפה. רשות שוק ההון, הרגולטור האחראי על חברות הביטוח, התוותה בשנת 2016 מסגרת כללית לעקרונות הגנת סייבר בחברות שבפיקוחה, ועל פי הדיווחים קיימה ביקורת בשירביט כמה שבועות לפני תקיפת הסייבר. אולם בהיעדר חובת דיווח ושקיפות לציבור וללא סמכויות

355 אסף שמואלי "טעות ללא הזדמנות: שירביט יכולה הייתה לנהוג אחרת גם אחרי הפריצה" **גלובס** (3.12.2020); עירית אבישר "שירביט על הפריצה: 'ההחלטה לא לשלם להאקרים אינה נובעת משיקול כספי'" **כלכליסט** (5.12.2020); שירות גלובס "שירביט החליטה: לא נשלם את דרישות הכופר לתוקפי הסייבר" **גלובס** (4.12.2020); אמיתי זיו ואפרת נוימן "שירביט החזירה לפעילות 90% מהמערכות, 2,000 מסמכים הודלפו" **TheMarker** (6.12.2020).

356 שמואלי, **לעיל** ה"ש 355; אמיתי זיו "האקרים פרצו למערכות המידע של שירביט ופירסמו פרטים אישיים של מבוטחים" **TheMarker** (1.12.2020); ליטל דוברוביצקי "שירביט לביהמ"ש: 'הפרטים המלאים של כרטיסי האשראי לא נגנבו'" **כלכליסט** (4.12.2020); אורי ברקוביץ' "צוות המשא ומתן של שירביט להאקרים: 'אחי, תהיה מענטש'" **גלובס** (4.12.2020).

ענישה מיידיות ומחמירות לא ברור עד כמה הנחיות רשות שוק ההון והביקורות שהיא מבצעת הובילו לשינוי של ממש.[357] רק כשנה לאחר מתקפת הסייבר, בדצמבר 2021, החליט הממונה על שוק ההון להטיל על שירביט עיצום כספי בגובה של 10.72 מיליון שקל בגין ממצאי אותה ביקורת, שקדמה לתקיפת הסייבר וחשפה הפרות של הוראות ניהול סיכוני הסייבר בגופים מוסדיים שקבע הממונה.[358]

רגולטור נוסף הרלוונטי במקרה זה הוא הרשות להגנת הפרטיות, האחראית להגנת הפרטיות במידע אישי ואמורה לקיים ביקורות ולאכוף את דרישות החוק בנושא בקרב חברות ציבוריות ופרטיות. ואולם, חלפו כ־40 שנים מאז נחקק חוק הגנת הפרטיות, ואף שנעשו בו תיקונים לאורך השנים הכוללים גם התייחסות למאגרי מידע ולשימוש במידע אישי והותקנו תקנות ייחודיות לאבטחת מידע, דיני הגנת הפרטיות ואכיפתם בישראל לוקים בחסר.[359] כך, למשל, הסכמת נושא המידע מכשירה כל שימוש במידע אישי, גם כאשר מטרת השימוש מוגדרת באופן רחב ומעורפל.[360] התוצאה היא שדיני הגנת הפרטיות בישראל אינם מחייבים מחיקת מידע אישי כאשר אין בו צורך עוד, וכך יכלו ההאקרים בפרשת שירביט – וגם בפרשת "אטרף", אתר ההיכרויות של קהילת הלהט"ב –[361] לפרסם גם מידע עודף, לרבות מסמכים על לקוחות לשעבר של שירביט או משתמשים לשעבר של אטרף.[362] כמו כן, סמכויות הפיקוח והאכיפה של הרשות להגנת

357 חוזר לגופים מוסדיים 2016-9-14 "ניהול סיכוני סייבר בגופים מוסדיים" (31.8.2016); מייקי לוי "רשות שוק ההון ערכה ביקורת סייבר בשירביט שבועות ספורים לפני הפריצה" **וואלה!** (3.12.2020); טל שחף "פרשת שירביט ושתיקת הרגולטורים / דעה" **ynet** (9.12.2020) (להלן: שחף "פרשת שירביט").

358 רועי ויינברגר "שירביט נקנסה ב־10 מיליון שקל לאחר פריצה לשרתיה והדלפת המידע" **גלובס** (30.11.2021).

359 רחל ארידור הרשקוביץ ותהילה שוורץ אלטשולר **הצעת חוק הגנת הפרטיות, התשע"ט-2019** 7–19 (המכון הישראלי לדמוקרטיה 2019).

360 ס' 1 לחוק הגנת הפרטיות, התשמ"א-1981.

361 זיו "ההאקרים", **לעיל** ה"ש 13.

362 מחיקת מידע עודף היא אחד הדגשים שצוינו בהמלצות שפרסמה הרשות להגנת הפרטיות לחברות ולארגונים בעקבות תקיפת הסייבר על חברת הביטוח שירביט. ראו

הפרטיות מוגבלות מאוד ומתמצות בהטלת קנסות נמוכים שאינם מהווים תמריץ מספק לנקיטת רמה מתאימה של אבטחת מידע והגנת פרטיות. תיקון 13 לחוק הגנת הפרטיות, שאמור להעניק לרשות להגנת הפרטיות סמכויות אכיפה ופיקוח רחבות יותר לצד סמכות להטיל סנקציות עונשיות חמורות יותר, תלוי ועומד כבר משנת 2011. גם תיקון 14, המבוסס על תיקון 13, ושוועדת החוקה החלה לדון בו בכנסת ה־24, לא התגבש עדיין לכדי חוק.[363] ללא תיקון מהותי לחוק המיושן תידרש להטוטנות פרשנית כדי להביא לשינוי של ממש בסמכויות האכיפה והפיקוח של הרשות להגנת הפרטיות ובתמריצים לשיפור הגנת הפרטיות.[364] עד אז תישאר הרשות להגנת הפרטיות גוף מנחה ומייעץ, אך "חסר שיניים".[365]

מערך הסייבר הלאומי הוא הרשות השלישית הרלוונטית לתקיפת סייבר, אך בהיעדר חוק מסמיך הוא משמש כגורם מנחה ומייעץ בלבד.[366] לראיה, המערך הנחה כבר לפני זמן רב את משרדי הממשלה להפסיק את השימוש בתאריך הנפקת תעודת זהות כאמצעי זיהוי, נוכח הסכנה של התחזות וגנבת זהות במקרה שצילום תעודת זהות יגיע לידיים הלא נכונות – כפי שאכן קרה בתקיפת הסייבר על חברת שירביט. אך למרות הנחיית המערך, הממשלה פעלה באיטיות ובהדרגתיות, וגופים מטעמה עדיין עושים שימוש באמצעי זה כתנאי לאימות זהות.[367]

ניכר אפוא שהמצב הקיים בעייתי מכמה בחינות: אין ביקורת חיצונית על קיום ההנחיות של הרגולטור המגזרי או של מערך הסייבר; לעיתים אין לרגולטור

"דגשים לאבטחת מידע בחברות וארגונים והמלצות לציבור בעקבות אירוע אבטחת מידע חמור בחברת שירביט" **הרשות להגנת הפרטיות** (6.12.2020).

363 הצעת חוק הגנת הפרטיות (תיקון מס' 14), התשפ"ב–2022, ה"ח הממשלה 420.

364 הצעת חוק הגנת הפרטיות (תיקון מס' 13), התשע"ח–2018, ה"ח הממשלה 692.

365 עמיר קורץ "הסנקציות שחוק הגנת הפרטיות מאפשר להטיל לא מרתיעות מספיק" **כלכליסט** (6.12.2020).

366 שחף "פרשת שירביט", **לעיל** ה"ש 357.

367 אורי ברקוביץ' "'לסגור מייל של עובדים בחופשה': ההמלצות הדרמטיות בעקבות פריצה הסייבר הגדולה" **גלובס** (9.12.2020).

המגזרי סמכויות אכיפה להבטחת קיום הנחיותיו; הרשות להגנת הפרטיות, האחראית על הגנת הפרטיות במידע בישראל, פועלת באמצעות פרשנויות משפטיות מרחיבות של חוק בן 40 שנה בעידן שבו מאגרי המידע הפכו כבר מזמן לנכס סחיר; מערך הסייבר פועל, מנחה ומסייע אך חסר גם הוא סמכויות אכיפה של ממש; ואין בנמצא גוף מתכלל אשר יפעל כמתאם פעולות הרשויות השונות, יבהיר את חלוקת הסמכויות ביניהן וייצור מסגרת חוקית מחייבת לעניין ההתנהלות הרצויה בעת תקיפת סייבר.

במצב דברים זה האסדרה של הגנת הסייבר נשענת על החוק להסדרת הביטחון בגופים ציבוריים, המתווה את סמכויות הגנת מרחב הסייבר בכל הקשור בתשתיות קריטיות (גופי התמ"ק), וכן על החלטות הממשלה בנושא. עם זאת, אפשר וחשוב ללמוד על המסגרת הרגולטורית שהמחוקק מציע זה מספר שנים לפי תזכיר חוק הסייבר, תקציר התזכיר ותזכיר הוראת השעה, לבחון אותה ולהעיר עליה במטרה להביא לשיפורה.

I. רגולציית ציווי ושליטה ריכוזית על תשתיות קריטיות

בשגרה ובחירום נתונים גופי התמ"ק לרגולציית ציווי ושליטה ריכוזית בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, וכפופים בעניין זה למערך הסייבר הלאומי.[368]

II. רגולציה של גופים שאינם תשתיות קריטיות – המסגרת הכללית

החלטת ממשלה 2443 הורתה על הקמת יחידות להכוונה מקצועית מגזרית בתחום הגנת הסייבר במשרדי הממשלה. על מערך הסייבר הוטל לסווג את הרגולטורים המגזריים השונים בממשלה לפי סמכויותיהם והמגזר שבו הם פועלים, ובהתאמה לקבוע את גודל היחידה להכוונה מקצועית ואת כוח האדם הדרוש להם. תפקיד יחידות מגזריות אלו הוא לספק הכוונה והנחיה מקצועית

368 החלטת ממשלה 2443, **לעיל** ה"ש 340; החלטת ממשלה 2444, **לעיל** ה"ש 340; ס' 21ב לחוק להסדרת הביטחון בגופים ציבוריים; **סיכום 2016–2017**, **לעיל** ה"ש 340, בעמ' 25; סעיפים 1–2 להחלטת ממשלה 3270, **לעיל** ה"ש 340.

בתחום הגנת הסייבר למשק האזרחי בהתאם לסמכויות הרגולטוריות של המשרד הממשלתי או במסגרתו, ובהתאם להנחיות שתקבל אותה יחידה מהמערך.[369]

תזכיר חוק הסייבר ממשיך במתווה זה, והנחת המוצא שבבסיסו היא שהשוק לבדו אינו יכול לתקן את כשלי השוק הקיימים בתחום הגנת הסייבר, הנובעים בעיקר מחוסר מודעות, חוסר ידע או חוסר יכולת להגביר את רמת הגנת הסייבר בארגונים. לפיכך, לפי תזכיר חוק הסייבר, יש צורך חיוני בהתערבות ממשלתית. אולם מאחר שהגנת הסייבר הוא תחום דינמי שמשתנה באופן תדיר, התערבות ממשלתית בו חייבת להיות גמישה דייה ולהיעשות, עד כמה שאפשר, תוך צמצום של הנטל הבירוקרטי ושל הפגיעה בתמריצים חיוביים ובחדשנות. לפי תזכיר חוק הסייבר, התערבות ממשלתית הבאה לידי ביטוי בשילוב של כלים רגולטוריים של ציווי ושליטה ריכוזית וביזורית, שנשענת על הרגולטורים המגזריים, עונה על דרישות אלו. הכלי הרגולטורי ייקבע בהתאם להערכת הסיכון הצפוי ל"אינטרס החיוני" מתקיפת סייבר אפשרית על אותו ארגון או סוגי ארגונים.[370] קביעת סוג הרגולציה בהתאם למידת הסיכון הנשקפת לאינטרס הציבורי מקובלת במדינות אחרות בעולם. עם זאת, "אינטרס ציבורי" מוגדר באופן שונה במדינות שונות, ועל כן בנסיבות דומות מדינות עשויות לבחור כלים רגולטוריים שונים, שכן ההתאמה של הכלי הרגולטורי הנבחר והמידתיות שלו תלויות במידה רבה בהגדרת האינטרס הציבורי.

ככלל, לפי תזכיר חוק הסייבר "האינטרס החיוני" אינו מוגבל לתשתיות קריטיות בלבד, וזהו שם כולל למכלול של אינטרסים:

- ביטחון המדינה, ביטחון הציבור או בטיחותו;
- חיי אדם;
- כלכלת המדינה;

369 רועי גולדשמידט **הסדרת האחריות להגנת הסייבר בממשלה ובגופים הציבוריים** (הכנסת, מרכז מחקר ומידע 2017).

370 תזכיר חוק הסייבר, **לעיל** ה"ש 343, בעמ' 5 ובסעיף 1 לחוק המוצע בתזכיר חוק הסייבר; מערך הסייבר הלאומי – משרד ראש הממשלה **הערכת השפעות רגולציה: פרק האסדרה בחוק הסייבר** 2–3, 8, 12 (2018) (להלן: **הערכת השפעות רגולציה**).

- תפקודן התקין של תשתיות, מערכות או שירותים חיוניים בשגרה או בחירום, ובכלל זה שירותי האינטרנט והתקשורת;
- תפקודם התקין של ארגונים המספקים שירותים בהיקף משמעותי;
- מניעת סכנה ניכרת לסביבה או לבריאות הציבור;
- מניעת פגיעה משמעותית בפרטיות בהיקף שיקבע שר המשפטים, או מניעת פגיעה בנכס מידע משמעותי;
- אינטרס שקבע ראש הממשלה בצו לאחר התייעצות עם השר הנוגע בדבר.[371]

בתזכיר הוראת השעה מופיעה הגדרה שונה מעט של "אינטרס ציבורי חיוני", הכוללת את האינטרסים שלהלן:[372]

- מניעת פגיעה חמורה בשלום הציבור;
- חיי אדם;
- כלכלת המדינה;
- הגנה על הסביבה;
- בריאות הציבור או בטיחותו;
- מניעת אירוע אבטחה חמור במאגר שחלה עליו רמת האבטחה הגבוהה, כהגדרתם בתקנות אבטחת מידע;[373]
- התפקוד התקין של תשתיות, מערכות או שירותים חיוניים;
- תפקודו התקין והבטוח של מרחב הסייבר.

לעניין האינטרס החיוני, מערך הסייבר הגדיר שלוש רמות סיכון עבור ארגונים שאינם תשתיות קריטיות, בהתאם לחומרת הפגיעה באינטרס החיוני והמשקל שיש לתת לפגיעה שכזו, והארגונים יסווגו לפיהן:[374]

371 סעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

372 בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346, ההפניה היא ל"אינטרס ציבורי חיוני".

373 תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 (להלן: תקנות אבטחת מידע).

374 **הערכת השפעות רגולציה, לעיל** ה"ש 370, בעמ' 2–3, 8, 12.

- ארגונים ברמה **A** – ארגונים שפגיעה בהם מהווה סיכון **חמור לכל אחד** מהאינטרסים המנויים ב"אינטרס החיוני".
- ארגונים ברמה **B** – ארגונים אשר פגיעה בהם מהווה סיכון **מהותי לאחד** מהאינטרסים המנויים ב"אינטרס החיוני".
- ארגונים ברמה **C** – ארגונים שפגיעה בהם מהווה סיכון **נמוך לאחד** מהאינטרסים המנויים ב"אינטרס החיוני". ארגונים ברמה C הם בפועל **כל הארגונים במשק שאינם** עונים לסיווג **A** או **B**.[375]

החלוקה לשלוש רמות תתבסס על מיפוי של חשיפת המשק למתקפות סייבר העשויות לפגוע באינטרס חיוני. שיטת המיפוי תיקבע בידי ראש מערך הסייבר, ועיקריה יפורסמו באופן שלדעת ראש מערך הסייבר אין בו כדי לסכן אינטרס חיוני.

שיטה זו צריכה להתבסס, בין השאר, על מגוון השיקולים המנויים בתזכיר חוק הסייבר:

(**1**) לעניין חומרת הפגיעה באינטרס החיוני תיבחן רמת השירות הנדרשת מסוגי ארגונים בשגרה ובחירום וטיב השירות; היקף הפגיעה האפשרית בחיי אדם; גודל הציבור המשתמש בשירותי הארגון; הנזק הכלכלי הצפוי מהפגיעה; היקף המידע המצוי בארגון ורגישותו; היקף הפגיעה בסביבה; פגיעה משמעותית בפרטיות; השפעת תקיפת סייבר נגד הארגון על תפקודם התקין של שירותי המחשוב והאינטרנט בישראל; השפעתה של תקיפה כאמור על גורמי ייצור, משאבים, שירותים, תהליכים ומוצרים החיוניים לקיום האוכלוסיה, לכלכלת המדינה ולפעילות הגורמים המיוחדים בשגרה ובחירום; ועמדת הרגולטור המגזרי בנוגע לאיומי סייבר בארגונים המפוקחים על ידו.

(**2**) לעניין החשיפה למתקפות סייבר ייבחנו סוגי איומי הסייבר הרלוונטיים לפעילות הארגון וההסתברות להתרחשותם.[376]

375 **שם**, בעמ' 13.

376 סעיף 46 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

אם כן, המסגרת הרגולטורית שתזכיר חוק הסייבר מתווה חלה על כל הארגונים שאינם תשתיות קריטיות, על בסיס ההנחה שגם תקיפת סייבר המתמקדת בארגונים אזרחיים שאינם מוגדרים כתשתיות קריטיות עשויה לפגוע ברציפות התפקודית המשקית, ולכך יש פוטנציאל ממשי לפגיעה חמורה בביטחון הלאומי. למשל, תחנות כוח קטנות, שפגיעה בכל אחת מהן בנפרד אינה צפויה לסכן באופן קריטי את ביטחון המדינה, יוגדרו כארגון בסיווג סיכון גבוה מאחר שאיום הסייבר מתאפיין ביכולת לתקוף בו בזמן ארגונים רבים בעלי מאפיינים דומים. באותו אופן, גם ארגונים מהמגזר האזרחי שמהווים צומת לשרשרות אספקה של תשתיות קריטיות יוגדרו כארגונים ברמה A.[377]

כמו כן, רגולציה מסוג זה מיישמת את עקרון האחריות המשותפת אך שונה, המבוסס על הערכת סיכונים, ושלפיו אסדרת הגנת הסייבר חלה על כלל המגזרים במשק, אך הכלי הרגולטורי הנבחר להגנת הסייבר בכל מגזר הוא הכלי הנחוץ והמידתי כדי להתמודד עם הסיכון הצפוי.[378]

בהמשך נרחיב על הכלים הרגולטוריים המוצעים בתזכיר בתוך מסגרת רגולטורית כללית זו. כפי שנסביר בפרק השלישי, אומנם מסגרת הרגולציה הכללית המוצעת בתזכיר חוק הסייבר היא נכונה ותואמת את המקובל בעולם, אך בחינתה צריכה להתמקד בכלי הרגולטורי הנבחר ובמידת התאמתו לתפיסת הערכת הסיכונים. המידתיות וההתאמה של הכלי הרגולטורי תלויות במידה רבה בהגדרתו של ה"אינטרס החיוני" ובמידת שקיפותה של השיטה למיפוי ודירוג חשיפת הארגונים במשק למתקפות סייבר שיש בהן כדי לפגוע באינטרס חיוני.

III. רגולציית ציווי ושליטה ריכוזית

i. על ארגונים מרמה A בעת שגרה

ארגון מרמה A, בין שהוא פועל בתחום שמופקדת עליו רשות מאסדרת אחראית ובין שאינו פועל בתחום כזה, יהיה נתון לרגולציית ציווי ושליטה ריכוזית,

377 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 10–11.

378 "החלטות הממשלה והחוק להסדרת הביטחון בגופים ציבוריים" **מערך הסייבר הלאומי** (16.7.2018).

שתתבצע על ידי מערך הסייבר בהתאם לרמת הסיכון הנשקפת לאינטרס החיוני מתקיפת סייבר נגדו.[379]

ii. על מגזר משקי שייקבע בידי ראש הממשלה

ראש הממשלה רשאי להורות על הכפפת מגזר משקי, המוגדר כארגון יחיד או כקבוצת ארגונים בעלי פעילות עסקית עיקרית דומה, לרגולציית ציווי ושליטה ריכוזית ישירה של מערך הסייבר, בהתקיים מכלול התנאים שלהלן:

(**1**) במגזר המשקי המדובר מצויים ארגונים שפעילותם חשופה לתקיפות סייבר העלולות להביא לפגיעה באינטרס חיוני. הגדרת "אינטרס חיוני" רחבה ומעורפלת, וכוללת, למשל, גם את תפקודם התקין של ארגונים המספקים שירותים בהיקף משמעותי. כך, לכאורה, מערך הסייבר יכול להפוך למאסדר הישיר, באמצעות רגולציית ציווי ושליטה ריכוזית, של רשתות האופנה הגדולות בישראל, במקרה שמערכות המחשוב שלהן ייחשפו לתקיפת סייבר העשויה לפגוע בתפקודן; זאת אף שהן אינן מספקות שירותים חיוניים.

(**2**) במגזר המשקי אין רגולטור מגזרי בעל סמכות, משאבים ויכולת ארגונית להנחות פעילות הגנת סייבר או לפקח על פעילות כזאת בארגונים השייכים למגזר. לפי דברי ההסבר מטרת הסעיף היא להבטיח "שלא ייוותר 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".[380] תנאי זה עלול להיות בעייתי, שכן לא ברור כיצד ייקבע שרגולטור מגזרי מסוים אינו אפקטיבי באופן המצדיק את העברת הפיקוח ישירות לידי מערך הסייבר.

(**3**) היעדרה של רשות מאסדרת כאמור מקים חשש סביר להתממשות הפגיעה באינטרס החיוני.[381]

379 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 2–3, 8, 12.

380 דברי ההסבר לסעיף 57 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

381 **שם**, בסעיף 57 לחוק המוצע בתזכיר חוק הסייבר.

iii. על ארגון מסוים לפרק זמן של עד 3 חודשים

החוק המוצע בתזכיר מסמיך את ראש מערך הסייבר להטיל רגולציית ציווי ושליטה ריכוזית על ארגון לפי שיקול דעתו ולתקופה מוגבלת בזמן אם מתקיימים שני תנאים: (1) הארגון מקיים פעילות שחשופה לתקיפות סייבר העלולות להביא לפגיעה חמורה באינטרס החיוני; (2) הארגון אינו כפוף על פי דין להנחיה ופיקוח של רגולטור מגזרי, ובשל כך אינטרס חיוני עלול להיפגע פגיעה קשה עקב תקיפת סייבר נגדו.[382]

iv. על ההכשרה הנדרשת לעיסוק במקצועות הגנת סייבר

בשנת 2015 פורסמה מדיניות האסדרה של מקצועות הגנת הסייבר, הקובעת דרישות סף ותנאי העשרה להתמקצעות בכמה מקצועות בתחום הגנת הסייבר, כדי להבטיח את הרמה המקצועית, המהימנות והאתיקה של העוסקים בתחום.[383]

v. סמכויות אופרטיביות שונות לטיפול בתקיפות סייבר ובאיומי סייבר בכלל המגזרים בתנאים מסוימים

לפי תזכיר חוק הסייבר, תקציר התזכיר ותזכיר הוראת השעה, מערך הסייבר הלאומי מוסמך להפעיל סמכויות אופרטיביות לשם מניעת מתקפת סייבר, הכלתה או צמצום הנזקים שנגרמה.[384]

סמכויות אופרטיביות לפי תזכיר חוק הסייבר

הפעלת אי אילו מהסמכויות האופרטיביות המנויות בתזכיר חוק הסייבר מותנית בקיום התנאים הכלליים שלהלן, המתווספים לתנאים הקבועים לגבי הפעלת כל סמכות בנפרד:

382 **שם**, בסעיף 62 לחוק המוצע בתזכיר חוק הסייבר.

383 מטה הסייבר הלאומי **מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל** (2015).

384 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 8.

(**1**) הפעלת הסמכות תיעשה רק בידי מי שהוסמך לכך בחוק.

(**2**) הארגון יעודכן לפני ביצוע פעולה בדבר הצורך בביצועה והשפעותיה עליו.

(**3**) סביר להניח שמתבצעת או שעלולה להתבצע תקיפת סייבר העלולה לגרום לפגיעה באינטרס חיוני, והפעולה נדרשת לצורך איתור תקיפת הסייבר, התמודדות עימה או מניעתה.

(**4**) טרם הפעלת הסמכות נשקלה השפעת הפעלתה על הארגון ועל הזכות לפרטיות ונמצא כי היא מידתית.[385]

הסמכויות האופרטיביות המוקנות במסגרת זו למערך הסייבר הן אלה:

(**1**) **סמכות לדרוש מסמכים ומידע**. עובד מוסמך[386] רשאי לדרוש מכל ארגון הנוגע בדבר למסור לו כל מידע ומסמך, לרבות עותק של חומר מחשב, הנדרשים לשם איתור תקיפת סייבר, התמודדות עימה או מניעתה.[387]

(**2**) **סמכות לדרוש מינוי איש קשר בארגון שהופעלה נגדו תקיפת סייבר**. עובד מוסמך במערך הסייבר מוסמך להורות לארגון למנות איש קשר שיקבל הוראות מהמערך ויעביר אליו מידע.[388]

(**3**) **סמכות כניסה למקום**. גורם אחראי[389] במערך הסייבר רשאי להיכנס או להורות לעובד מוסמך להיכנס למקום אם יש לו יסוד סביר להניח שבמקום קיים מחשב או חומר מחשב שיש בו "מידע בעל ערך אבטחתי" הדרוש לאיתור תקיפת סייבר, מניעתה או טיפול בה. לפי תזכיר חוק הסייבר, אם המקום הוא מקום מגורים יש לקבל את הסכמת מחזיק המקום לכניסה. לעומת זאת, בתקציר

385 סעיף 19 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

386 בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **שם**, "עובד מוסמך" מוגדר כעובד מערך הסייבר שהוא בעל הכשרה מתאימה לפעולה, מהסוג שקבע ראש המערך בכללי המערך.

387 **שם**, בסעיף 20 לחוק המוצע בתזכיר חוק הסייבר.

388 **שם**, בסעיף 21 לחוק המוצע בתזכיר חוק הסייבר.

389 בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **שם**, "גורם אחראי במערך" מוגדר כ"עובד מערך בכיר שהוסמך לפי חוק זה לבצע את הפעולות הקבועות בחוק זה או לפיו".

התזכיר צוין שההסכמה נדרשת ללא קשר להיות המקום בית מגורים.[390] בהיעדר הסכמה יש לפנות לקבלת צו מבית משפט שלום.

ראש מערך הסייבר רשאי להורות לגורם אחראי או לעובד מוסמך להיכנס למקום המשמש למגורים גם ללא צו אם לדעתו סביר שיש במקום מחשב או חומר מחשב שיש בו "מידע בעל ערך אבטחתי",[391] ומידע זה דרוש למניעת סכנה ממשית ומיידית לשלום הציבור או לביטחון הציבור, ובנסיבות העניין אין דרך אחרת להשיג מידע זה.[392]

(**4**) סמכות **תפיסת חפץ**. עובד מוסמך במערך הסייבר רשאי לתפוס חפץ אם יש יסוד סביר להניח שיש בחפץ "מידע בעל ערך אבטחתי" שבדיקתו המיידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עימה או מניעתה.

תנאי למימוש הסמכות לתפיסת חפץ הוא שניתנה למחזיק בחפץ ההזדמנות להשמיע את טענותיו. אם הגורם האחראי סבור שמתן ההזדמנות למחזיק בחפץ להשמיע את טענותיו תפגע באופן משמעותי ביכולת לאתר תקיפת סייבר, להתמודד עימה או למנוע אותה, ויש סכנה ממשית ומיידית לשלום הציבור או לביטחונו, הגורם האחראי רשאי לתפוס את החפץ ורק אחר כך לתת למחזיק בו הזדמנות להשמיע את טענותיו.[393]

(**5**) סמכות **מתן הוראות**. עובד מוסמך במערך הסייבר מוסמך לתת לארגון הוראות לפעולה, לרבות הוראות לעניין פעולות בחומר מחשב, לשם איתור תקיפת סייבר, התמודדות עימה או מניעתה. מתן ההוראה מותנה בכך שיינתן לארגון רקע תמציתי עובדתי ומקצועי שהביא להחלטה בנוגע לפעולה הנדרשת,

390 תקציר התזכיר, **לעיל** ה"ש 344.

391 בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343, "מידע בעל ערך אבטחתי" מוגדר כ"מידע שיש בו כדי לסייע לאיתור תקיפת סייבר, התמודדות עמה או מניעתה ובכלל זה אחד מאלה: (1) סממנים (indicatiors) – 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".

392 **שם**, בסעיף 22(ב) לחוק המוצע בתזכיר חוק הסייבר.

393 **שם**, בסעיף 23 לחוק המוצע בתזכיר חוק הסייבר.

ככל שהדבר אפשרי מבלי לפגוע באיתור, בטיפול ובמניעה של תקיפת הסייבר או להביא לחשיפת מקורות או שיטות עבודה של המערך. מרגע מתן ההוראה חובה על הארגון לפעול לפיה ולדווח למערך הסייבר על ביצועה. יתרה מכך, על הארגון חל איסור לגלות את תוכן ההוראה. הסודיות עשויה לחול לא רק כלפי חוץ, אלא גם כלפי עובדים בארגון.[394]

(**6**) סמכות **לביצוע פעולות בחומר מחשב לפי צו בית משפט שלום**. עובד מוסמך במערך רשאי לבצע פעולות במחשב או בחומר מחשב של ארגון בתנאי ששופט בית משפט שלום התיר לו לעשות כן, לאחר ששוכנע שיש יסוד סביר להניח שמתרחשת תקיפת סייבר או שיש איום סייבר ו"האינטרס החיוני" עלול להיפגע. תזכיר חוק הסייבר מתווה את השיקולים שעל בית משפט השלום לשקול בעת מתן צו לביצוע פעולות: ההסתברות להתרחשות תקיפת הסייבר וחומרת הנזק הצפויה מהתרחשותה, השפעת הפעולות המבוקשות על הארגון וגורמים נוספים שעשויים להיות מושפעים מהצו לביצוע פעולות, ומידת הפגיעה בפרטיות או פגיעה אחרת בארגון או באדם עקב ביצוע הפעולות.[395] לשם תמיכה בבקשה לצו רשאי מערך הסייבר להציג חומר חסוי לעיני בית המשפט בלבד.[396]

(**7**) **סמכות לביצוע פעולות בחומר מחשב לצורך בקרה מדגמית לפי צו בית משפט**. שופט בית משפט שלום רשאי להתיר למערך הסייבר לבקשת גורם אחראי בו, בדיון בדלתיים סגורות, לבצע פעולות בחומר מחשב של ארגון לצורך בקרה מדגמית אם לדעתו יש סיכוי של ממש, בהתחשב במאפייני הארגון, לאתר באמצעות הפעולות תקיפת סייבר. בקבלת ההחלטה על בית המשפט להביא בחשבון את נחיצות הצו לצורכי הגנת סייבר, את השפעת הפעולות שיבוצעו מכוח הצו על הארגון וגורמים נוספים העשויים להיות מושפעים מהן, ואת מידת הפגיעה בפרטיות או פגיעה אחרת בארגון או באדם.[397]

(**8**) **סמכות לביצוע פעולות בהסכמת הארגון**. גורם אחראי במערך הסייבר רשאי לבצע פעולות גם ללא צו בית משפט ובלבד שגורם מוסמך בארגון נתן

394 **שם**, בסעיף 26 לחוק המוצע בתזכיר חוק הסייבר.

395 **שם**, בסעיף 27 לחוק המוצע בתזכיר חוק הסייבר.

396 **שם**, בסעיף 29 לחוק המוצע בתזכיר חוק הסייבר.

397 **שם**, בסעיפים 32 ו־33 לחוק המוצע בתזכיר חוק הסייבר.

את הסכמתו לכך לאחר שהוסברו לו, בשפה מובנת, הנסיבות המצדיקות את הפעולה, השפעת ביצוע הפעולה על הארגון וארגונים נוספים, מידת הפגיעה בפרטיות או האפשרות לפגיעה אחרת באדם או בארגון בשל ביצוע הפעולה, קיומה של אפשרות לצמצם את הפגיעה והדרכים לעשות כן וזכותו של הארגון לסרב לביצוע הפעולה. לארגון הזכות לחזור בו מהסכמתו לביצוע פעולה.[398]

(**9**) **סמכות לבצע פעולת סייבר דחופה**. ראש המערך רשאי להורות בכתב על כניסה למקום, תפיסת חפץ, מתן הוראות, ביצוע פעולות בחומר מחשב או ביצוע פעולה בחומר מחשב לצורך בקרה מדגמית אף ללא צו בית משפט, ובלבד שהתקיימו התנאים המצטברים שלהלן: (1) הפעולה נדרשת בדחיפות לצורך מניעת נזק ממשי ל"אינטרס חיוני" בשל תקיפת סייבר, אין דרך אחרת למנוע את הנזק ואין די זמן לפנות לבית המשפט בבקשה לצו; (2) התקיימו יתר הדרישות לעניין ביצוע פעולות לפי צו בית משפט, ככל שהדבר אפשרי מבלי לסכל את ביצוע הפעולה. אישור ראש המערך לביצוע פעולה כאמור יעמוד בתוקפו 24 שעות בלבד. על ראש המערך לדווח ליועץ המשפטי לממשלה על ביצוע הפעולה לא יאוחר משש שעות מביצועה, ועל המערך לפנות לבית המשפט בבקשה לצו לא יאוחר מ־24 שעות מביצועה.[399]

סמכויות אופרטיביות לפי תזכיר הוראת השעה

(**1**) **סמכות למתן הנחיות מקצועיות להיערכות לתקיפת סייבר**.[400] גורם אחראי במערך רשאי לתת לארגון הנחיות מקצועיות להיערכות לתקיפת סייבר, לרבות הוראות לביצוע "פעולות הגנת סייבר": מתן הוראות למחשב בשפה קריאת מחשב, בחינה של חומר מחשב או תקשורת, לרבות סריקה ממוכנת שלהם, העתקה של חומר מחשב, התקנת מחשב או תוכנת מחשב לשם ביצוע פעולות אלו, וכן כניסה למקום ותפיסת חפץ,[401] ובלבד שהתקיימו התנאים האלה:

398 **שם**, בסעיף 35 לחוק המוצע בתזכיר חוק הסייבר.

399 **שם**, בסעיף 36 לחוק המוצע בתזכיר חוק הסייבר.

400 סעיף 4 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346.

401 ראו הגדרת "פעולות הגנת סייבר" בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **שם**.

(א) לגורם האחראי יש יסוד סביר להניח שהתקיימו התנאים המצטברים שלהלן:

i. הארגון מקיים פעילות חיונית, כלומר מתקיימים לפחות אחד מהשניים: (1) פעילות הארגון בעלת מאפיינים ציבוריים הנוגעים לכלל הציבור או לחלק ניכר ממנו, והיא נדרשת לקיום אספקה חיונית או שירותים חיוניים לציבור בשגרה או בחירום, או למניעת פגיעה חמורה בענף החשוב למשק המדינה; (2) שירותי הארגון מהווים תשתית מחשובית או תשתית תקשורת לניהול נכסי המדינה ומשאביה, או לצורך פעילותו התקינה של ארגון שפעילותו חיונית לפי הסיבה הראשונה או של גוף המנוי בתוספת החמישית לחוק להסדרת הביטחון בגופי ציבור.[402]

ii. בארגון קיימת חשיפה קריטית, המוגדרת כחולשה היוצרת סיכון לתקיפת סייבר חמורה או בהיקף נרחב, והארגון אינו נוקט את הפעולות הדרושות לצורך טיפול בה. תקיפת סייבר חמורה מוגדרת כאחת מאלה: (1) תקיפה העלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני; (2) יש יסוד סביר להניח שהתקיפה תגרום לפגיעה ממשית באינטרס ציבורי חיוני לנוכח חומרת הסכנה להתפשטותה למחשבים אחרים ולפגיעה נרחבת בהם או במידע השמור בהם; (3) התקיפה אותרה בארגון שמקיים פעילות חיונית או שיש יסוד סביר להניח שהיא מכוונת כלפי ארגון שכזה או כלפי גוף המנוי בתוספת החמישית לחוק להסדרת הביטחון בגופי ציבור; (4) יש יסוד סביר להניח שהתקיפה נועדה לפגוע בביטחון הלאומי של המדינה.[403]

iii. תקיפת סייבר נגד הארגון עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני.[404]

(ב) הגורם האחראי הודיע על הכוונה לתת הנחיות מקצועיות לארגון מבעוד מועד ונתן לארגון הזדמנות להשמיע את טענותיו.

ארגון המקבל הנחיות מקצועיות חייב לבצען בהקדם ולדווח על כך למערך הסייבר.

402 שם.

403 שם.

404 שם.

(**2**) **סמכות למתן הנחיות מקצועיות למניעת תקיפת סייבר חמורה.**[405] גורם אחראי במערך רשאי לתת לארגון הנחיות מקצועיות להיערכות לתקיפת סייבר, לרבות הוראות לביצוע "פעולות הגנת סייבר", ובלבד שהקיימו התנאים שלהלן:

א. לגורם האחראי יסוד סביר להניח שהתקיימו התנאים המצטברים שלהלן:

i. מתרחשת או עומדת להתרחש תקיפת סייבר חמורה בארגון.

ii. הארגון אינו נוקט את הפעולות הנדרשות כדי להתמודד עם התקיפה ולמנוע פגיעה באינטרס ציבורי חיוני שהתקיפה עלולה לגרום.

ב. הגורם האחראי הודיע על הכוונה לתת הנחיות מקצועיות לארגון מבעוד מועד ונתן לארגון הזדמנות להשמיע את טענותיו.

ארגון המקבל הנחיות מקצועיות חייב לבצען בהקדם ולדווח על כך מערך הסייבר.

(**3**) **סמכות לביצוע פעולות הגנת סייבר בצו בית משפט.** גורם אחראי במערך הסייבר רשאי לפנות לבית המשפט לעניינים מינהליים בבקשה להתיר לעובד מוסמך במערך לבצע "פעולת הגנת סייבר" מסוימת או לתת הוראה הנוגעת לביצוע פעולה כאמור. בית המשפט ייעתר לבקשה אם שוכנע שהפעולות נדרשות למניעת פגיעה באינטרס ציבורי חיוני, והתקיים אחד מהתנאים שלהלן: (1) לארגון ניתנו הנחיות מקצועיות להיערכות לתקיפת סייבר או למניעת תקיפת סייבר חמורה והוא לא ביצע אותן; (2) לא ניתן להשיג את תכלית הפעולות המבוקשות בצו באמצעות הנחיה מקצועית בלבד.[406]

בקבלת החלטה בנוגע למתן הנחיות מקצועיות להיערכות לתקיפת סייבר או למניעת תקיפת סייבר, או בעת מתן צו שיפוטי לביצוע פעולות הגנת סייבר על ידי עובד מוסמך במערך, על הגורם האחראי או בית המשפט לשקול, בין השאר, את השיקולים האלה: (1) מאפייני הארגון ומידת הסיכון שנשקף לאינטרס ציבורי חיוני מתקיפת סייבר נגדו; (2) התאמת הפעולה המבוקשת לאיתור

405 **שם**, בסעיף 5 לחוק המוצע בתזכיר הוראת השעה.

406 **שם**, בסעיפים 1 ו־6 לחוק המוצע בתזכיר הוראת השעה.

תקיפת הסייבר, להיערכות לה, לטיפול בה או למניעתה; (3) היכולת להשיג את תכלית הפעולה באמצעות אדם בעל ידע ומומחיות מטעם הארגון.[407]

(**4**) **סמכות לקבלת מידע מספק גישה לאינטרנט או מעובד השב"כ.** גורם אחראי רשאי, לאחר קבלת הסכמה לכך בכתב מראש הממשלה או ממי שהוסמך על ידו, לקבל מספק גישה לאינטרנט או מעובד השב"כ מידע על זהותו של לקוח ופרטי ההתקשרות עימו, אם לפי מידע שיש בידי הגורם האחראי קיימת חשיפה קריטית במחשבי הלקוח, או שמחשבי הלקוח נתונים לתקיפת סייבר או לתקיפת סייבר חמורה, ובלבד שהלקוח אינו אדם יחיד. על ספק הגישה לספק את המידע הדרוש בתוך 72 שעות מהפנייה אליו או בתוך 24 שעות אם קיים חשש מתקיפת סייבר חמורה. עם זאת, לפי דברי ההסבר, ברירת המחדל תהא פנייה לשב"כ לקבלת המידע הדרוש.[408]

IV. רגולציית ציווי ושליטה רכה ביזורית

ארגונים מרמה B וארגונים מרמה C, שנתונים לאסדרה באמצעות רגולטור מגזרי (מכונה בתזכיר חוק הסייבר "רשות מאסדרת"), יהיו נתונים לרגולציית ציווי ושליטה רכה. ברירת המחדל היא האצלת סמכויות לרשויות מאסדרות קיימות, ויהיה עליהן לפעול באופן אחיד ובהתאם לתורת ההגנה בסייבר שפרסמה הרשות הלאומית להגנת הסייבר בשנת 2017.[409] במסגרת זו תינתן עדיפות לאסדרה בהתאם לתקינה בינלאומית, תוך התאמת האסדרה למאפייני המגזר הספציפי, קביעת הסדר מידתי לסיכון הצפוי והתחשבות בעלויות הישירות של ההסדר ובהשפעתו על התחרות במגזר.[410]

לפיכך, הרגולציה שתוטל על ידי הרשויות המאסדרות הקיימות תהיה מסוג של ציווי ושליטה רכה תוך השארת שיקול דעת נרחב יחסית להנהלת הארגון המאוסדר באשר לאופן יישומה של תורת ההגנה בארגון.[411]

407 **שם**, בסעיף 8 לחוק המוצע בתזכיר הוראת השעה.

408 **שם**, בסעיף 9 לחוק המוצע בתזכיר הוראת השעה.

409 מערך הסייבר הלאומי **תורת ההגנה בסייבר לארגון** (גרסה 1.0, יוני 2017).

410 סעיף 43 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

411 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 25–26.

כבר היום מפרסמים חלק מהרגולטורים המגזריים הנחיות, חלקן מחייבות וחלקן וולונטריות, לנושא הגנת הסייבר בארגונים הנתונים לאסדרתם. כך, למשל, רשות ניירות ערך, שהיא והגופים הכפופים לה, למעט הבורסה לניירות ערך, אינם מוגדרים כיום כתשתיות קריטיות,[412] הטילה על התאגידים הנתונים לאסדרתה חובות הקשורות להגנת סייבר, כגון גילוי נאות במקרי תקיפת סייבר. רשות ניירות ערך אף בחנה את מידת המוכנות לאיומי סייבר בקרב מנהלי תיקי השקעות.[413]

משרד הבריאות אחראי למעטפת הגנת הסייבר הלאומית בבתי חולים ובשירותי הבריאות הפרטיים והציבוריים, שאינם מוגדרים כיום כתשתיות חיוניות.[414] במסגרת זו דורש משרד הבריאות מבתי החולים ליישם הגנת סייבר בהתאם לתקן בינלאומי בנושא. משרד הבריאות הזהיר כי מערכות המחשוב בבתי החולים אינן ערוכות כלל למתקפות סייבר בשל היעדר תקציבים מספיקים.[415]

בתחום הפיננסי, בנק ישראל מוגדר כתשתית קריטית אך התאגידים הבנקאיים וחברות האשראי אינם מוגדרים כך.[416] לפיכך, המפקח על הבנקים בבנק ישראל חייב תאגידים בנקאיים וחברות כרטיסי אשראי לנהל הגנת סייבר אפקטיבית. במסגרת זו הטיל המפקח על הבנקים חובה למנות מנהל הגנת סייבר, הגדיר את אחריות הדירקטוריון לניהול הגנת הסייבר בתאגיד וחייב את הבנקים להתוות

412 גופים אלו אינם מופיעים בתוספות לחוק להסדרת הבטחון בגופים ציבוריים.

413 רפאל קאהאן "הרשות לניירות ערך מצפה מארגונים לגילוי נאות במקרי מתקפות סייבר" **כלכליסט** (21.10.2018); מחלקת השקעות ברשות ניירות ערך "תובנות מניתוח מענה לשאלון בנושא סיכוני אבטחת מידע וסייבר שהופץ בקרב חברות ניהול תיקים בחודש יולי 2018" (6.3.2019).

414 הם אינם מופיעים בתוספות לחוק להסדרת הבטחון בגופים ציבוריים.

415 מערכת ישראל היום "חשש: התקפות סייבר בבתי החולים יעלו בחיי אדם" **ישראל היום** (31.12.2018); יהודה קונפורטס "שי אמיר, משרד הבריאות: 'מערכת הבריאות אינה ערוכה למתקפת סייבר כוללת על בתי החולים'" **אנשים ומחשבים** (11.5.2014). מבקר המדינה אף מתח ביקורת נוקבת על הכשלים בהגנת הסייבר במשרד הבריאות, ראו עומר כביר "כשלים של משרדי הבריאות והחינוך מסכנים מידע של מיליוני ילדים בישראל" **כלכליסט** (6.5.2019).

416 תוספת שנייה לחוק להסדרת הבטחון בגופים ציבוריים.

תוכנית עבודה רב־שנתית לניהול סיכוני סייבר. בידי הבנקים נותר שיקול הדעת בנוגע לאופן הביצוע של חובת התוויית התוכנית. דירקטוריון הבנק הוא שאמון על התוויית האסטרטגיה לניהול הגנת הסייבר ואישורה, והנהלת התאגיד הבנקאי אחראית לגיבוש המדיניות, ליישומה, להקצאת משאבים נאותים להפעלתה ולניהול פיקוח מתאים לשם קבלת תמונת מצב עיתית על הנעשה.[417] כמו כן, בחודש מאי 2019 נחתם מסמך עקרונות לשיתוף פעולה בתחום הגנת הסייבר על המערכת הבנקאית בין המפקח על הבנקים ומערך הסייבר הלאומי.[418]

גם הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר פרסמה הנחיות בנוגע להגנת הסייבר בקרב הגופים הכפופים לפיקוחה, שאינם מוגדרים כתשתיות קריטיות.[419] במסגרת הנחיה זו חויבו הגופים המאוסדרים לגבש מדיניות לניהול סיכוני סייבר שתתייחס, בין השאר, לעקרונות הגנת הסייבר בכל המערכות והתשתיות של הארגון המאוסדר, ליישום הגנת הסייבר בהיבט של מחשוב ענן וכן להכשרת כוח האדם בארגון בנושא הגנת סייבר. ההנחיה כוללת דרישות נוספות, כגון מינוי מנהל להגנת סייבר שהוא בעל מומחיות בתפקיד ניהול בתחום זה, הקמת גוף פנים־ארגוני שירכז את הטיפול בהגנת הסייבר בארגון, עריכת סקר סיכונים וביצוע מבחני חדירות. האחריות ליישום ההנחיה מוטלת על מנכ"ל הארגון.[420]

עם זאת, בהיעדר סמכויות אכיפה ייעודיות בנושא הגנת סייבר בידי מערך הסייבר או הרשות המאסדרת, הסבירות לשיפור הגנת הסייבר בקרב הגופים המאוסדרים נמוכה. כך, למשל, כחמישה חודשים לפני תקיפת הסייבר ששיתקה את המערכות הממוחשבות בבית החולים הלל יפה בחודש אוקטובר 2021 הזהיר מערך הסייבר את משרד הבריאות ואת בית חולים הלל יפה כי יש במערכותיהם

417 חוזר המפקח על הבנקים ח-06-2457 "ניהול הגנת סייבר" (16.3.2015).

418 "הפיקוח על הבנקים ומערך הסייבר הלאומי חתמו על מסמך עקרונות לשיתוף פעולה" **מערך הסייבר הלאומי** (30.5.2019).

419 הגופים המוסדיים הנתונים לפיקוח הממונה על שוק ההון אינם מופיעים ברשימת התשתיות הקריטיות שבחוק להסדרת הבטחון בגופים ציבוריים.

420 חוזר גופים מוסדיים 2016-117 "ניהול סיכוני סייבר בגופים מוסדיים – טיוטה שנייה" (4.4.2016).

חולשה העשויה להוביל לתקיפת כופר על בית החולים, וכי יש אף התראה ממוקדת על תקיפת עתידית שכזו. נראה כי על אף אזהרה ממוקדת זו לא תוקנה החולשה.[421]

נציין שתזכיר חוק הסייבר מבקש למנוע מצב שבו הרשות המאסדרת תהיה חסרת סמכויות אכיפה ופיקוח בכל הנוגע להגנת הסייבר. לכן מוצע בתזכיר חוק הסייבר שרשות מאסדרת שאינה מצוידת בסמכויות כאמור תוסמך לתת הוראות בתחום הגנת הסייבר ולפקח על ביצוען, בדומה לסמכויות הנתונות למערך הסייבר ביחס לארגונים הנתונים להנחייתו הישירה.[422]

רגולציית הציווי והשליטה הרכה הנתונה לפי תזכיר חוק הסייבר בידי הרשויות המאסדרות הקיימות מזכירה את רגולציית הציווי והשליטה הרכה והביזורית בארצות הברית[423] ובאנגליה.[424] עם זאת, יש הבדל חשוב בין המודלים: במודל האנגלי ובמודל האמריקני התקינה נקבעת בידי גוף אזרחי מקצועי ולאחר הליך שקוף של היוועצות עם בעלי עניין מהמגזר הפרטי, ואילו התקינה המנחה בישראל נקבעת על ידי מערך הסייבר, שהוא בראש ובראשונה גוף ביטחוני ומתנהל כך מבחינת מידת השקיפות שלו כלפי המגזר הפרטי. כמו כן, לאותו גוף ביטחוני – מערך הסייבר – ניתנות אף סמכויות אופרטיביות.

יתרה מכך, הביזוריות של רגולציית הציווי והשליטה היא מוגבלת. מערך הסייבר שומר לעצמו את תפקיד "מאסדר־העל": הוא המנחה את הרשויות המאסדרות בנוגע לאופן יישום הוראות החוק המוצע בתזכיר חוק הסייבר בתחום הגנת הסייבר, אישורו נדרש לכל אסדרה הנקבעת על ידי הרשות המאסדרת וכן למינוי עובדים בתחום הגנת הסייבר אצל הרשות המאסדרת, והוא גם משמש כפוסק

421 אריק בנדר "משרד הבריאות: 'אנחנו נמצאים במלחמת עולם שלישית בעניין הסייבר'" **מעריב** (8.11.2021).

422 סעיף 61 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

423 ראו דיון בסעיף א.2 בפרק 2 **לעיל**.

424 ראו דיון בסעיף ג.I.2.II בפרק 2 **לעיל**.

האחרון – הרואה עצמו נפגע מהחלטה של רשות מאסדרת בתחום הגנת הסייבר רשאי לבקש בחינה חוזרת של ההחלטה בידי ראש מערך הסייבר.[425]

נוסף על כך, ראש הממשלה רשאי להחליט על הפקעת הטיפול בהגנת הסייבר במגזר משקי מסוים מידי הרשות המאסדרת והעברתו לידי מערך הסייבר אם לדעתו הרשות המאסדרת אינה אפקטיבית.[426] בדרך זו מחזיק מערך הסייבר בסל כלים רב עוצמה אשר יאפשר לו להתערב ביעילות ובמהירות אם יימצא שהרשות המאסדרת אינה מתפקדת כראוי בנושא הגנת הסייבר. בתקציר התזכיר הובהר שאומנם מערך הסייבר הוא המאסדר הלאומי בתחום הגנת הסייבר, אולם אין הכוונה שמערך הסייבר ישמש כ"רגולטור־על", אלא רק ישתלב וינחה את הרשויות המאסדרות הקיימות כגוף בעל הידע המקצועי בכל הקשור להגנת סייבר.[427] עם זאת, בהיעדר הנוסח הרשמי של התיקונים המוזכרים בתקציר התזכיר אין בידנו להעריך אם אכן בוצע שינוי של ממש המבטל את תפיסתו של מערך הסייבר כ"רגולטור־על", כפי שנלמד מתזכיר חוק הסייבר.

V. רגולציה שיתופית

i. למטרות שיתוף מידע ביחס לכלל המגזרים

ה־CERT-IL, שהוקם לפי החלטת ממשלה 2444, נועד לאפשר שיתוף מידע בין חברות פרטיות וגופי מודיעין כדי לשפר את הביטחון והחוסן של מרחב הסייבר בישראל.[428] מכניזם שיתוף המידע בו דומה לזה המקובל בפלטפורמות לשיתוף מידע בנושא הגנת סייבר הפועלות בארצות הברית ובאנגליה. רשות ממשלתית – מערך הסייבר הלאומי – היא שאחראית לתפעולו ולמיצובו כמוקד לקליטת מידע. הרשות הממשלתית מנתחת את המידע ומחליטה עם מי לשתף אותו. המידע המשותף מועבר תוך שימוש בטכנולוגיות התממה (אנונימיזציה) שונות.

425 סעיפים 44, 49 ו־53(ד) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343; סיון סביליה, **לעיל** ה"ש 338, בעמ' 93–94.

426 סעיף 57 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

427 תקציר התזכיר, **לעיל** ה"ש 344.

428 החלטת ממשלה 2444, **לעיל** ה"ש 340.

נוסף על שיתוף מידע, CERT-IL מציע לארגונים פרטיים גם שירותי תגובה, המנחים את הקורבנות של תקיפת סייבר לגבי אופן התגובה הרצוי למתקפה, וכן שירותים פרו־אקטיביים, כגון בקרת אבטחה והערכת סיכונים ורמת אבטחה. תזכיר חוק הסייבר מבהיר שבנסיבות מסוימות שיתוף מידע במסגרת CERT-IL יבוצע באופן התנדבותי,[429] אך עשוי להיות מנדטורי במקרים אחרים.[430]

ii. באופן מוגבל במסגרת היוועצות בלבד למטרות גיבוש תורת ההגנה

תורת הגנת הסייבר בארגון, שלפיה תבוצע רגולציית הציווי והשליטה הרכה הביזורית והרגולציה העצמית, גובשה גם היא בדרך של רגולציה שיתופית במידה מסוימת. אנשי מערך הסייבר נפגשו, בכמה סבבי היוועצות, עם מנהלים בארגונים מכל אחת מרמות הארגונים A, B ו־C, עם מומחים בתחום הסייבר, עם חברות המציעות מוצרים ושירותים בתחום הסייבר ועם נציגי התאחדות התעשיינים. יתרה מכך, לפי עמדת מערך הסייבר ההיוועצות היא תהליך מתמשך שהוא חלק מיישום המדיניות בפועל ואין לו תאריך סיום מוגדר.[431]

iii. למטרת עידוד המחקר והפיתוח

קיימות יוזמות שונות לעידוד מחקר ופיתוח בנושא הגנת הסייבר. למשל, תוכנית קֶדמה ביוזמת מערך הסייבר הלאומי והמדען הראשי היא תוכנית מקיפה שתפקידה לקדם מחקר, פיתוח ויזמות בתחום הגנת הסייבר, במטרה לשמר ולחזק את הפוטנציאל התחרותי של התעשייה בישראל בשוק העולמי.[432] חברות פרטיות המקבלות מימון מרשות החדשנות דרך פרויקט קֶדמה חייבות לציית לתנאי התוכנית, הכוללים למשל דרישות בנוגע למיקום הגיאוגרפי של העסק ולבעלות בזכויות הקניין הרוחני בפיתוח תוצר המימון, או הגבלה של היכולת

429 סעיף 18(5) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

430 **שם**, בסעיפים 16–18.

431 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 32.

432 חוזר המדען הראשי 2012–02 "תוכנית קידמ"ה (קידום מו"פ הגנת הסייבר לקידום יכולות התעשייה הישראלית בתחום הגנת הסייבר" (21.11.2012).

להעביר זכויות אלו לצדדים שלישיים. מערך הסייבר גם מספק מימון להקמה ולתפעול של מרכזי מחקר בתחום הגנת הסייבר באוניברסיטאות – אוניברסיטת בן־גוריון, האוניברסיטה העברית, אוניברסיטת בר־אילן, אוניברסיטת תל אביב, אוניברסיטת חיפה והטכניון.

VI. רגולציה עצמית בארגונים מרמה C שאינם כפופים לרשות מאסדרת

בארגונים מרמה C שאינם כפופים לאף רשות מאסדרת מגזרית תונהג רגולציה עצמית המבוססת על תורת ההגנה בארגון, ומערך הסייבר ישמש כגורם מנחה ומייעץ בלבד.[433]

כאמצעי לתמרוץ ארגונים מרמה C לנקוט את אמצעי ההגנה הראויים הכריז מערך הסייבר על תוכנית "תו חוסן סייבר לחברות אחסון אתרים". מערך הסייבר הלאומי השיק את התוכנית בעקבות ההבנה שמתקפות סייבר לא מעטות הצליחו לגרום נזק לאתרים רבים באמצעות חדירה לחברות לאחסון אתרים. תוכנית "תו החוסן" מציגה שלוש רמות הגנה – כסף, זהב ופלטינה, המוענקות לחברות אחסון אתרים שיעמדו בביקורת אבטחה שבה ייבדקו קריטריונים שהגדיר המערך (בקרת גישה, הגנה על עמדות קצה ושרתים, הגנה היקפית, ניטור ובקרה, פיתוח מאובטח וענן להגנה על סביבת המידע של הלקוח). ביקורת האבטחה תיערך על ידי בודקי ספקים שיאושרו בידי המערך, והתו יעמוד בתוקפו במשך שנה. בדרך זו תעניק התוכנית ללקוחות חברות האחסון כלי שיאפשר להם לשפוט את רמת ההגנה של השירות ולבחור בשירות המתאים להם. כך תייצר התוכנית תמריץ כלכלי עבור ספקי שירות אחסון האתרים לנקוט רמת הגנה ראויה.[434]

433 **הערכת השפעות רגולציה**, **לעיל** ה"ש 370, בעמ' 25–26.

434 "תוכנית חדשה של מערך הסייבר הלאומי תעניק 'תו חוסן' סייבר לחברות אחסון אתרים" **מערך הסייבר הלאומי** (21.4.2021).

4. סיכום מודל הרגולציה להגנת מרחב הסייבר בישראל

נכון לכתיבת מסמך זה, תזכיר חוק הסייבר שפורסם ביוני 2018 ותזכיר הוראת השעה משנת 2021 טרם הפכו לחוק. במצב דברים זה הרגולציה של הגנת מרחב הסייבר מותווית בהתאם לחוק להסדרת הביטחון בגופים ציבוריים, הקובע את סמכויות הגנת מרחב הסייבר בכל הקשור בתשתיות קריטיות (גופי התמ״ק), וכן בהתאם להחלטות הממשלה בנושא. הלוח שלהלן מסכם את המסגרת הרגולטורית המוצעת בתזכיר חוק הסייבר, בתקציר התזכיר ובתזכיר הוראת השעה.

לוח 6
האסדרה של הגנת הסייבר בישראל

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה ריכוזית	משרדי ממשלה, תשתיות קריטיות וארגונים מרמה A	תשתיות קריטיות נתונות לאסדרת מערך הסייבר הלאומי לפי החוק להסדרת הביטחון בגופים ציבוריים. ארגונים מרמה A נתונים לאסדרת מערך הסייבר הלאומי. לפי תזכיר חוק הסייבר – למערך או לשב"כ יש סמכויות אופרטיביות לביצוע הפעולות הנחוצות לצורך איתור תקיפת סייבר, מניעתה או התמודדות עימה; הסמכויות יופעלו בהתאם לעקרון המידתיות ובכפוף לחובת יידוע בתנאים מסוימים, כלפי כלל הארגונים במשק. לפי תזכיר הוראת השעה – למערך הסייבר הלאומי או לשב"כ יש סמכויות אופרטיביות שאפשר להפעילן כלפי ארגון המקיים פעילות חיונית לשם היערכות לתקיפת סייבר, וכלפי כל ארגון לשם מניעת תקיפת סייבר חמורה או מניעת פגיעה באינטרס ציבורי חיוני.

סוג הרגולציה	תחולה	עיקרי הרגולציה
רגולציית ציווי ושליטה רכה ביזורית	ארגונים מרמה B ו־C הכפופים לרשות מאסדרת	האסדרה תיעשה על ידי הרשויות המאסדרות המגזריות בהנחיית מערך הסייבר. המסגרת הרגולטורית תתבסס על תורת ההגנה בארגון שפרסם מערך הסייבר, תוך התאמה לתקינה בינלאומית, למאפייני המגזר הספציפי ולעלויות הישירות של ההסדר. לדוגמה: הנחיות רשות ניירות ערך לתאגידים הנתונים לאסדרתה; דרישות משרד הבריאות מבתי החולים בתחום הגנת הסייבר; הרגולציה שמטיל המפקח על הבנקים על תאגידים בנקאיים וחברות כרטיסי אשראי; והנחיות שפרסמה הממונה על שוק ההון, ביטוח וחיסכון במשרד האוצר.
רגולציה שיתופית	כלל המגזרים	למטרות שיתוף מידע ועידוד מחקר ופיתוח בתחום הגנת הסייבר; למטרות חינוך והכשרה.
רגולציה עצמית	ארגונים מרמה C שאינם כפופים לרשות מאסדרת	ארגונים אלה יפעלו בהתאם לתורת ההגנה בסייבר לארגון שפרסם מערך הסייבר, ויכולים לפנות לקבלת ייעוץ והנחייה ממערך הסייבר. חברות אחסון אתרים יכולות לקבל "תו חוסן סייבר" ממערך הסייבר.

ה.
סיכום המודלים הרגולטוריים להגנת מרחב הסייבר – משפט משווה

ממשלות רבות ברחבי העולם עוסקות באסדרת ההגנה על מרחב הסייבר. כפי שהראינו בסקירה לעיל, מדינות שונות החלו לנקוט פעולות מדיניות לאסדרת ההגנה על מרחב הסייבר בנקודות זמן שונות, אך לכולן משותפת ההבנה שהחיוניות של מרחב הסייבר לכלכלת המדינה ולחיי היום־יום בה, לצד החולשות הקיימות בו, מציבות סכנות רבות בפני המגזר הציבורי, המגזר הפרטי והציבור

בכללותו. הבנה זו הובילה גם לאימוץ התפיסה כי האחריות להגנת מרחב הסייבר היא אחריות משותפת, המוטלת על כלל השחקנים במרחב הסייבר בהתאם לעקרון האחריות המשותפת אך שונה.

כלל המדינות שנסקרו במחקר זה עושות שימוש במגוון כלים רגולטוריים לשם הגנת מרחב הסייבר במדינה: רגולציית ציווי ושליטה ריכוזית, רגולציית ציווי ושליטה רכה וביזורית, רגולציה שיתופית ורגולציה עצמית. מידת האחריות של כל אחד מהשחקנים במרחב הסייבר, וכנגזרת ממנה הכלי הרגולטורי שבו ייעשה שימוש לאסדרת הגנת הסייבר, נקבעים לפי הערכת הסיכון הנשקף לאינטרסים לאומיים חשובים מתקיפת סייבר על ארגון מסוים או על ארגונים ממגזר מסוים. קיים מתאם בין רמת הסיכון לבין מידת ההתערבות של המדינה בשוק החופשי, כפי שבאה לידי ביטוי בכלי הרגולטורי שבו נעשה שימוש: ככל שהסיכון גדול יותר המדינה נוטה להשתמש בכלי רגולטורי "מתערב" יותר. הנגזרת הברורה ביותר מהערכת הסיכון לאינטרסים לאומיים חשובים היא ההבחנה המקובלת בכל המדינות בין ארגונים המשתייכים למגזרי התשתיות הקריטיות ובין אלו שאינם מפעילים או בעלים של תשתיות קריטיות, ולכן הרגולציה של הגנת הסייבר במגזרי תשתיות קריטיות שונה מהרגולציה במגזרים אחרים.

אם כן, ההגדרה של אינטרסים לאומיים חשובים אלו היא המפתח להבנת היקפה של התערבות המדינה בשוק לשם הגנת מרחב הסייבר. באופן כוללני הכוונה היא לאינטרסים הקשורים לביטחון הציבור, לביטחון המדינה ולמצבה הכלכלי. אולם ההגדרה של אינטרסים לאומיים חשובים בישראל שונה מהגדרתם במדינות האחרות שנסקרו במחקר זה. שׁוֹנוּת זו משפיעה על הכלים הרגולטוריים שבהם נעשה שימוש כלפי ארגונים ממגזרים שונים, ובאה לידי ביטוי בעיקר בהיקף של רגולציית ציווי ושליטה ריכוזית או רכה וביזורית.

בארצות הברית, באנגליה ובאוסטרליה האינטרסים הלאומיים החשובים קשורים לביטחון המדינה, יציבותה הכלכלית, בריאות הציבור וביטחונו. גם בצרפת מדובר על מצבה הכלכלי או הצבאי של המדינה, או ביטחון הציבור וחוסנו. בדנמרק אין התייחסות ברורה לאינטרסים אלו, אך מודגשת בטיחות השימוש של פרטים ועסקים במרחב הסייבר והביצוע התקין של פעולות בעלות חשיבות חברתית באמצעות מרחב הסייבר. באיחוד האירופי אינטרסים לאומיים חשובים מוגדרים כשמירה על תפקוד תקין של גורמים המספקים שירותים החיוניים

לביצוע פעילויות קריטיות מבחינה חברתית או כלכלית, ושתקיפת סייבר עליהם תביא לפגיעה הרסנית משמעותית במתן השירות על ידם. ההערכה אם הפגיעה עלולה להיות הרסנית מבוססת על כמה קריטריונים, ובהם מספר המשתמשים בשירות, תלות של ארגון ממגזר תשתיות קריטי אחר בשירות וההשפעה שעשויה להיות לתקיפה, במונחים של חומרה ומשך זמן, על פעולות כלכליות או חברתיות או על ביטחון הציבור.[435]

בישראל ההגדרה של אינטרס לאומי חשוב, המכונה בתזכיר חוק הסייבר "אינטרס חיוני", רחבה אך גם מעורפלת יותר. ראשית, נעשה שימוש במושגים שמשמעותם אמורה להיות זהה. בתזכיר חוק הסייבר לא ברור אם קיים הבדל בין "ביטחון המדינה, ביטחון הציבור או בטיחותו", ובין "חיי אדם" או "סכנה ניכרת לסביבה או לבריאות הציבור". גם בתזכיר הוראת השעה מופיעים זה לצד זה "מניעת פגיעה חמורה בשלום הציבור", "חיי אדם", "הגנה על הסביבה" ו"בריאות הציבור או בטיחותו" – מבלי שמוגדרים ההבדלים ביניהם. שנית, נראה שיש בלבול בין אינטרס חיוני לבין יעד הגנה שתִּפקודו התקין חיוני לשם הגנה על אינטרס לאומי חשוב: הן תזכיר חוק הסייבר והן תזכיר הוראת השעה כוללים במסגרת "אינטרס חיוני" את תִּפקודם התקין של "ארגונים המספקים שירותים בהיקף משמעותי" (בתזכיר חוק הסייבר) או "תשתיות, מערכות או שירותים חיוניים" (בתזכיר הוראת השעה). לטעמנו אלו הם יעדי הגנה – תקיפת סייבר על ארגונים מסוג זה עלולה לפגוע באינטרסים לאומיים חשובים כמו ביטחון המדינה, כלכלתה או ביטחון הציבור, אך אין אלה אינטרסים העומדים בפני עצמם. הגדרתם כאינטרסים חיוניים מביאה לכך שרגולציית הציווי והשליטה הרכה והריכוזית או הביזורית בישראל רחבה ביותר ומעורפלת. כמו כן, הן תזכיר חוק הסייבר והן תזכיר הוראת השעה מאפשרים הכללת אינטרסים נוספים שכלל אינם ידועים או ברורים: לפי תזכיר חוק הסייבר ראש הממשלה רשאי להוסיף אינטרסים לאחר היוועצות עם השר הנוגע בדבר, ובתזכיר הוראת השעה נכלל "תִּפקודו התקין והבטוח של מרחב הסייבר" ברשימת האינטרסים הציבוריים החיוניים. בשל ההגדרה הרחבה והמעורפלת של אותם אינטרסים לאומיים חיוניים, היקפה של הרגולציה המדינתית ושל התערבות הממשלה בשוק החופשי אינו ברור כלל ועלול להיות רחב ביותר.

435 דירקטיבת NIS, **לעיל** ה"ש 187, בסעיפים 5–6.

בחינת אסטרטגיות הרגולציה של המדינות שנבדקו מגלה שעם השנים הרחיבו המדינות את השימוש ברגולציית ציווי ושליטה ריכוזית או ביזורית ורכה: תחילה הוחלה הרגולציה רק על מגזרי תשתיות קריטיות, אך בשנים האחרונות מרבית המדינות מרחיבות את רגולציית הציווי והשליטה גם לארגונים ממגזרים נוספים, כגון ספקי שירות דיגיטליים, חברות שהן חלק משרשראות אספקה טכנולוגיות ויצרני מוצרי צריכה חכמים. זאת מתוך הבנה שתקיפת סייבר על ארגונים אלו עשויה לפגוע בארגונים ממגזרי התשתיות הקריטיות ובסופו של דבר גם באינטרסים הלאומיים החשובים. הרחבת הרגולציה לא נבעה משינוי בהגדרת האינטרסים הלאומיים החשובים, אלא מההבנה שככל שגוברת התלות של הממשל, התעשייה והציבור במרחב הסייבר כך פעילותם השגרתית של ארגונים רבים יותר נעשית קריטית ויש להגן עליה, באמצעות הכפפת ארגונים אלו לרגולציה מסוג ציווי ושליטה רכה ריכוזית או ביזורית.

במרבית המדינות הרחבת הרגולציה של הגנת הסייבר כך שתחול על ארגונים נוספים נעשתה באופן ברור. למשל, בארצות הברית הייתה נהוגה מאמצע שנות התשעים של המאה העשרים רגולציית ציווי ושליטה רכה וביזורית על שירותי הבריאות והמגזר הפיננסי. בהחלטה נשיאותית 13636 משנת 2016 ובהמשך בדירקטיבה נשיאותית 21 משנת 2021 הוחלט על הרחבת רגולציית הציווי והשליטה הרכה והביזורית גם למגזרי תשתיות קריטיות נוספים. במאי 2021 הוחלה רגולציית ציווי ושליטה רכה וביזורית גם על מפעילים ובעלים של צינורות המובילים נוזלים מסוכנים וגז טבעי, וחובות להגנת הסייבר הוטלו גם על ספקי שירותים דיגיטליים המספקים שירותים לרשויות הממשל. באנגליה הורחבה רגולציית הציווי והשליטה והביזורית בשנת 2018 ל"ספקי שירותים דיגיטליים רלוונטיים", הכוללים ספקי פלטפורמות סחר אלקטרוני, ספקי מנועי חיפוש וספקי שירותי ענן. באפריל 2021 פורסמה הצעת חוק המבקשת להחיל רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים, נוכח הסיכון הנשקף מתקיפת סייבר על מכשירים אלו בהיבטים של פגיעה במידע אישי רגיש ובהתנהלות הציבור בחיי היום־יום. גם בצרפת ובדנמרק הורחבה התחולה של רגולציית הציווי והשליטה הרכה והריכוזית לספקי שירותים דיגיטליים, כחלק מיישום דירקטיבת NIS של האיחוד האירופי, ודירקטיבת NIS2 הרחיבה לאחרונה את היקף רגולציית הציווי והשליטה הריכוזית בכל הנוגע לחובות דיווח, ואת היקף רגולציית הציווי והשליטה הרכה לארגונים ומגזרים נוספים, כגון אלו

הנמנים עם שרשראות אספקת של טכנולוגיות תקשורת ומידע. באוסטרליה הוצע באסטרטגיה משנת 2020 להרחיב את רגולציית הציווי והשליטה הרכה והריכוזית ולהחילה גם על ספקי שירותים דיגיטליים וכן על יצרני מוצרי צריכה חכמים. צעד זה ננקט לנוכח השימוש הגובר במרחב הסייבר שנכפה בעקבות מגיפת הקורונה, לצד העלייה בתקיפות סייבר ובאיומי סייבר שמקורם במדינות שונות וכן בארגוני פשיעה, אשר מאיימים על הפרט הבודד, על משפחות, על ארגונים ועסקים ואף על מכוני מחקר ושירותי רפואה.

בישראל, לעומת זאת, ההבחנה בין ארגונים הנתונים לרגולציית ציווי ושליטה רכה ריכוזית או ביזורית אינה ברורה שכן היא תלויה בהבחנה בין ארגונים מרמות A, B ו־C, והבחנה זו מבוססת על דרגת הסיכון לאחד מהאינטרסים המנויים בהגדרת "אינטרס חיוני", שהיא הגדרה רחבה ומעורפלת. כך, גם ארגונים שמתקיפתם נשקף סיכון נמוך לביטחון המדינה, לכלכלתה או לביטחון הציבור ובריאותו יכולים להיות נתונים לרגולציית ציווי ושליטה רכה ביזורית או ריכוזית, עקב סיכון העשוי להיגרם לאינטרס רחב ומעורפל כמו "תפקודו התקין והבטוח של מרחב הסייבר".

הבדל נוסף ומהותי בין המדינות שנבדקו נוגע להיקף רגולציית הציווי והשליטה הריכוזית בעת שגרה. בצרפת מוחלת בעת שגרה רגולציית ציווי ושליטה ריכוזית על תשתיות קריטיות, ארגונים המספקים שירות החיוני לשמירה על פעילות חברתית או כלכלית קריטית, מפעילי שירותי טלקומוניקציה וספקי שירות דיגיטליים. בדנמרק, רגולציית ציווי ושליטה ריכוזית מוחלת על כלל המגזרים אך היא מצומצמת לכדי ניטור וזיהוי של איומי סייבר ומבוצעת בידי המרכז הלאומי לניטור איומי סייבר שבמשרד ההגנה הדני. לעומת זאת, בישראל נדמה כי רגולציית הציווי והשליטה הריכוזית היא הרחבה ביותר: היא חלה על תשתיות קריטיות לפי החוק להסדרת הביטחון בגופים ציבוריים, וכן על ארגונים מרמה A, המוגדרים כארגונים שפגיעה בהם מהווה סיכון חמור לאחד מהאינטרסים החיוניים המנויים בתזכיר וסווגו כך לאחר היוועצות עם הרשות המאסדרת האחראית על האינטרס החיוני הרלוונטי. ההגדרה הרחבה והמעורפלת של אינטרס חיוני מובילה גם לתחולה אפשרית רחבה של רגולציית הציווי והשליטה הריכוזית.

הבדל נוסף בין המדינות שנבדקו הוא זהות הגוף האחראי לקביעת סטנדרט ההגנה, להנחיה ולייעוץ בכל הקשור להגנת הסייבר, וכן לזהות הגוף בעל סמכויות האכיפה והפיקוח על הגנת הסייבר בעת שגרה. בישראל ובצרפת מוטלים תפקידים אלה על אותו הגוף. בצרפת מדובר על ANSSI, רשות לאומית אזרחית המדווחת לשר ההגנה. בישראל – מערך הסייבר, שהוא גוף ביטחוני במהותו, אחראי לקביעת הסטנדרטים המקצועיים ודרישות ההגנה ולמתן הייעוץ וההנחיה, והוא גם בעל סמכויות אופרטיביות של פיקוח ואכיפה. בכל שאר המדינות הגופים הביטחוניים או המקצועיים אחראים לקביעת סטנדרט ההגנה ומתן הייעוץ וההנחיה, מתוך הבנה שלשם ביצוע תפקידים אלו יש צורך בידע מקצועי ואף מודיעיני שאינו מנת חלקם של ארגונים אחרים, אולם אכיפת הוראות הגנת הסייבר נתונה בידי רגולטורים אזרחיים מגזריים.

יתרה מכך, המבנה של רגולציה ביזורית הוא בעייתי. אומנם מבנה זה מאפשר את התאמת הרגולציה לצרכיו של כל מגזר, אולם ביזוריות זו עלולה להקשות על שיתוף פעולה חוצה מגזרים וליצור כפילות סמכויות בין הרגולטורים השונים. כמו כן, רגולציה ביזורית מציבה רשויות שעדיין לא התמקצעו בהגנת סייבר בתפקיד מתוות מדיניות הגנת הסייבר במגזר הרלוונטי. משום כך, יש חשיבות לזהות הגורם הממשלתי חוצה המגזרים האחראי לקביעת המדיניות והאסטרטגיה המדינית הכוללת שלפיה על הרגולטורים המגזריים לפעול, וכן למידת מעורבותו בפעילותם.

הרגולטורים המגזריים בארצות הברית רשאים להיעזר במסגרת להגנת הסייבר שפרסם המכון הלאומי לסטנדרטים וטכנולוגיה (NIST), שהוא סוכנות פדרלית לא רגולטורית הפועלת כמקור חסר פניות למידע ולפרקטיקות מדעיות, לרבות בתחום הגנת הסייבר. ל־NIST יש ניסיון מוכח בהתמודדות עם נושאים הקשורים בתשתיות קריטיות ובעבודה בשיתוף פעולה בין המגזר הציבורי, האקדמיה והמגזר האזרחי הפרטי. באנגליה מוסמך כל שר המופקד על מגזר מסוים מהמגזרים שעליהם חלות תקנות NIS לקבוע מדיניות לאומית להגנת הסייבר בתחומו, תוך הצבת מטרות וקביעת סדר עדיפויות למימושן כדי להשיג ולשמר הגנת סייבר ברמה גבוהה. על המדיניות להתייחס לכל הפחות לנושאים המפורטים בתקנות NIS, אשר נקבעו בהתאם לדירקטיבת NIS של האיחוד האירופי לאחר היוועצות עם התעשייה והאקדמיה. בדנמרק הממשלה קובעת את אסטרטגיית ההגנה ועל הרגולטורים המגזריים לפעול לפיה. בצרפת, הרשות

הלאומית להגנת הסייבר (ANSSI) קובעת בשיתוף פעולה עם הרגולטורים המגזריים ועם התעשייה הנחיות להגנת סייבר בכל מגזר. גם בהיבט זה המצב בישראל אינו ברור: האסדרה במגזרים מרמות B ו־C, הכפופים לרשות מאסדרת, נתונה בידי הרגולטורים המגזריים, אך מערך הסייבר, אשר פועל כגוף ביטחוני, שומר לעצמו סמכויות־על רגולטוריות להתערבות בפעולות הרגולטור המגזרי.

לצד ההבדלים באסדרה של הגנת הסייבר במדינות השונות יש גם כמה נקודות דמיון. ראשית, בעת חירום יש נטייה לרגולציית ציווי ושליטה: בארצות הברית מוקם שיתוף פעולה המורכב מנציגי הממשל הפדרלי הרלוונטיים; בצרפת אחראים לחקירת מתקפת סייבר ולניהול התגובה אליה משרד הפנים ומשרד ההגנה, בהתאמה; באוסטרליה בעל הסמכות הוא המרכז האוסטרלי להגנת הסייבר (ACSC), שהוא חלק מזרוע המודיעין האוסטרלית; באנגליה המרכז הלאומי להגנת סייבר, ה־NCSC, הוא בעל הסמכות; ובישראל ניתנת הסמכות להתמודדות עם מתקפות סייבר משמעותיות בעת חירום לצה"ל.

נקודת דמיון נוספת היא שבמרבית המדינות הרגולציה השיתופית מוגבלת לזמן שגרה ולמטרות של שיתוף מידע, חינוך הציבור, העלאת מודעות הציבור ועידוד מחקר ופיתוח. באוסטרליה, באנגליה ובדנמרק נראה כי קיימת תרבות מבוססת של רגולציה שיתופית למטרת גיבוש סטנדרטים וחוקים הנוגעים להגנת הסייבר. מבין המדינות שנסקרו, רק בארצות הברית תיתכן רגולציה שיתופית מוגבלת בעת תקיפת סייבר משמעותית, במקרה שהיקפה ואופייה של תקיפת הסייבר מצדיקים שיתוף פעולה עם גורמים מהמגזר הפרטי.

באשר לרגולציה העצמית, במרבית המדינות הארגונים הנתונים לרגולציה עצמית (לעיתים מבוססת תמריצים) הם אלה שעל פי ההערכות לא נשקף מפגיעה בהם סיכון משמעותי לאינטרסים לאומיים חשובים. עם זאת, חשוב להצביע על שינוי המסתמן גם באפיק זה: באנגליה ובאוסטרליה כשל הניסיון להגביר את הגנת הסייבר במוצרי צריכה חכמים באמצעות רגולציה עצמית וקוד התנהגות וולונטרי, וכעת מדינות אלו מציעות רגולציית ציווי ושליטה ריכוזית רכה כדי להביא לתוצאות המצופות בנוגע להגנת הסייבר במוצרי צריכה חכמים.

לוח 7
סיכום המודלים לרגולציית הגנת הסייבר

	ארצות הברית	אוסטרליה	אנגליה	דנמרק	צרפת	ישראל
דירוג לפי מדד הגנת הסייבר העולמי	מקום ראשון	מקום 12	מקום שני	מקום 32	מקום 9	מקום 36
דירוג לפי מדד הגנת מרחב הסייבר של Comparitech	31 נקודות מתוך 75	55 נקודות מתוך 75	68 נקודות מתוך 75	75 נקודות מתוך 75	36 נקודות מתוך 75	61 נקודות מתוך 75
הגוף המגבש את סטנדרט הגנת הסייבר	המכון הלאומי לסטנדרטים וטכנולוגיה (NIST), סוכנות פדרלית, מקצועית, לא רגולטורית. סטנדרט הגנת הסייבר בתשתיות קריטיות ייקבע בשיתוף פעולה בין NIST לסוכנות להגנת הסייבר ולאבטחת תשתיות (CISA), יחידה במחלקה לביטחון המולדת (DHS).	המרכז האוסטרלי להגנת הסייבר (ACSC), שהוא חלק מזרוע המודיעין האוסטרלית.	המרכז הלאומי להגנת סייבר (NCSC), יחידה טכנולוגית הפועלת במסגרת מטה התקשורת הממשלתי (GCHQ). ה־NCSC הוא הגוף המקצועי המוביל בתחום הגנת הסייבר, אך אין לו סמכויות אכיפה.	השר הרלוונטי למגזר המאוסדר בשיתוף פעולה והיוועצות עם היחידה המגזרית המבוזרת להגנת סייבר ומידע (DCIS).	ANSSI, המדווח לשר ההגנה.	מערך הסייבר הלאומי, גוף ביטחוני הכפוף למשרד ראש הממשלה.
הגוף בעל סמכויות האכיפה והפיקוח	רגולטורים מגזריים	רגולטוריים מגזריים	רגולטורים מגזריים	רגולטורים מגזריים	ANSSI	מערך הסייבר הלאומי
הגדרת אינטרס לאומי חשוב	ביטחון המדינה, יציבותה הכלכלית, בריאות הציבור וביטחונו	ביטחון המדינה, יציבותה הכלכלית, בריאות הציבור וביטחונו	ביטחון המדינה, יציבותה הכלכלית, בריאות הציבור וביטחונו	בטיחות השימוש במרחב הסייבר על ידי פרטים ועסקים, הביצוע התקין של פעולות בעלות חשיבות חברתית במרחב הסייבר	מצבה הכלכלי או הצבאי של המדינה, ביטחון הציבור וחוסנו	לפי תזכיר חוק הסייבר: ביטחון המדינה, ביטחון הציבור או בטיחותו; חיי אדם; כלכלת המדינה; תפקודן התקין של תשתיות, מערכות או שירותים חיוניים בשגרה או בחירום ובכלל זה שירותי התקשורת; תפקודם התקין של ארגונים המספקים שירותים בהיקף גדול; מניעת סכנה ניכרת לסביבה או לבריאות הציבור; מניעת פגיעה משמעותית בפרטיות בהיקף שיקבע שר המשפטים, או מניעת פגיעה בנכס מידע משמעותי; אינטרס שקבע ראש הממשלה בצו לאחר התייעצות עם השר הנוגע בדבר.

	ארצות הברית	אוסטרליה	אנגליה	דנמרק	צרפת	ישראל
						לפי תזכיר הוראת השעה: מניעת פגיעה חמורה בשלום הציבור; חיי אדם; כלכלת המדינה; הגנה על הסביבה; בריאות הציבור או בטיחותו; מניעת אירוע אבטחה חמור; תפקודם התקין של תשתיות, מערכות או שירותים חיוניים; תפקודו התקין והבטוח של מרחב הסייבר.
סמכות ניטור	ניטור וולונטרי בלבד	ניטור וולונטרי בלבד. ייתכן שבעתיד יחויבו מגזרי התשתיות הקריטיות בדיווח על מתקפות סייבר.	ל־GCHQ סמכות לנטר את מרחב הסייבר במטרה לחשוף מתקפות סייבר.	משרד ההגנה מפעיל מרכז לאומי למצבי סייבר שמנטר רשתות, מערכות ממוחשבות של מערכות חיוניות וקריטיות בבעלות ציבורית או פרטית, ואף פורומים ואמצעי תקשורת. עסקים פרטיים מסוימים מחויבים לדווח למרכז הניטור על כל אירוע אבטחה.	ניטור מנדטורי על מפעיל במגזר חיוני, מפעיל שירות טלקומוניקציה וספקי שירות דיגיטליים.	מערך הסייבר מוסמך להפעיל מערך ניטור וזיהוי רציף, שבמסגרתו ייאסף ויעובד מידע למטרת גילוי מוקדם של תקיפות סייבר וסיוע בהתמודדות עימן מרשימה רחבה ביותר של ארגונים.
רגולציית ציווי ושליטה ריכוזית בעת חירום	מאמצי ההתגוננות מפני תקיפת סייבר ינוהלו בידי שותפות המורכבת מהרשויות הפדרליות הרלוונטיות ויחולו על כלל המגזרים.	מאמצי ההתגוננות מפני תקיפת סייבר ינוהלו בידי המרכז האוסטרלי להגנת הסייבר.	בעת מצב חירום לאומי, תקיפת סייבר משמעותית מאוד ותקיפת סייבר משמעותית, מאמצי ההתגוננות מפני תקיפת סייבר ינוהלו בידי ה־NCSC ויחולו על כלל המגזרים.		במקרה של תקיפת סייבר נגד תשתיות קריטיות, ההתגוננות מפני התקיפה תנוהל בידי ANSSI. רק במקרה קיצון תתערב המדינה גם בהתגוננות מפני תקיפת סייבר על חברות פרטיות שאינן תשתיות קריטיות.	מאמצי ההתגוננות מפני תקיפת סייבר ינוהלו בידי צה"ל.

	ארצות הברית	אוסטרליה	אנגליה	דנמרק	צרפת	ישראל
רגולציית ציווי ושליטה רכה ריכוזית בעת שגרה	חובות דיווח על מפעילים ובעלים של תשתיות קריטיות שיוגדרו כגופים מאוסדרים.	תלויה ועומדת הצעת חוק להחלת רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים.	תלויה ועומדת הצעת חוק להחלת רגולציית ציווי ושליטה רכה ריכוזית על יצרני מוצרי צריכה חכמים. יש רצון להרחיב את רגולציית הציווי והשליטה הרכה גם לחברות טכנולוגיה גדולות, יצרנים, משווקים וספקים של שירותים דיגיטליים.	המרכז הלאומי למצבי סייבר שבמשרד ההגנה הדני מפעיל רגולציה מסוג זה על כלל המגזרים לשם מעקב אחר איומי סייבר, חינוך והגברת מודעות הציבור והכשרת עובדי מדינה.	ANSSI מפקחת על הגנת הסייבר בארגונים המוגדרים כמפעיל במגזר חיוני, מפעיל שירות טלקומוניקציה וספק שירותים דיגיטליים.	למערך הסייבר הלאומי כפופים גופי תמ"ק, ארגונים מרמה A, כל מגזר משקי נוסף שייקבע בידי ראש הממשלה, ארגונים מסוימים באופן זמני וארגונים שמוחלות עליהם הסמכויות האופרטיביות.
רגולציית ציווי ושליטה רכה ביזורית	רגולציה מגזרית על התשתיות הקריטיות, על מפעילים ובעלים של צינורות המובילים נוזלים מסוכנים וגז טבעי ועל חברות פרטיות מכלל המגזרים המתקשרות בחוזים עם רשויות פדרליות לאספקת מוצרים ושירותים טכנולוגיים.	רגולציה מגזרית על 11 מגזרי תשתיות קריטיות. תלויה ועומדת הצעת חוק להטיל רגולציית ציווי ושליטה רכה וביזורית על ארגונים גדולים שאינם תשתיות קריטיות, ועל כלל הארגונים מכוח חובות כלליות בחוק הגנת הפרטיות, חוק הגנת הצרכן וחוק החברות.	רגולציה מגזרית על חלק ממגזרי התשתיות הקריטיות, על חברות פרימיום ועל חברות המוגדרות כ"ספקי שירותים דיגיטליים רלוונטיים".	רגולציה מגזרית על כל תשתית קריטית התומכת בפונקציה חיונית לחברה ועל ספקי שירותים דיגיטליים.		בארגונים מרמות B ו־C המאוסדרים בידי רגולטורים מגזריים, האסדרה של הגנת הסייבר תיעשה על ידי הרשויות המאסדרות המגזריות, בהנחיית מערך הסייבר. למערך הסייבר מעמד של רגולטור־על.
רגולציה שיתופית	נהוגה בכלל המגזרים לשם גיבוש סטנדרטים להגנת סייבר, לשם חינוך ושיתוף מידע, ובעת חירום – רק אם היקפה ואופייה של תקיפת הסייבר המשמעותית מצדיקים שיתוף פעולה עם גורמים מהמגזר הפרטי.	נהוגה בכל המגזרים לשם שיתוף מידע, גיבוש אסטרטגיה לאומית להגנת סייבר, עידוד החדשנות, חינוך והכשרה מקצועית והעלאת מודעות הציבור.	נהוגה במגזר הפרטי לשם שיתוף מידע, גיבוש סטנדרטים להגנת סייבר, קידום מחקר ופיתוח וחינוך הציבור.	נהוגה בכל המגזרים למטרות קביעת סטנדרט הגנת סייבר ושיתוף מידע.	נהוגה בכל המגזרים לשם גיבוש נוסח הרגולציה, הגברת מודעות לסיכוני סייבר, חינוך והכשרה החל מבתי הספר, קידום מחקר ופיתוח, ובמגזרי התשתיות הקריטיות גם לשם שיתוף מידע.	נהוגה בכל המגזרים למטרות שיתוף מידע, מחקר ופיתוח, חינוך והכשרה.

	ארצות הברית	אוסטרליה	אנגליה	דנמרק	צרפת	ישראל
רגולציה עצמית ועצמית בליווי תמריצים	על ארגונים פרטיים ממגזרי התשתיות הקריטיות שאינם נתונים לרגולציית ציווי ושליטה ריכוזית או רכה וביזורית, ועל ארגונים פרטיים שאינם ממגזרי התשתיות הקריטיות, למטרת התמודדות עם תקיפת סייבר, שיתוף מידע ואימוץ והטמעה של סטנדרטים להגנת סייבר. הרגולציה העצמית מבוססת תמריצים. עם זאת, מהחלטותיו האחרונות של הנשיא ביידן עולה שיש בדעתו להטיל רגולציית ציווי ושליטה רכה אם הרגולציה העצמית לא תביא לאימוץ רמת הגנת סייבר נאותה בקרב בעלים ומפעילים של תשתיות קריטיות.	המרכז האוסטרלי להגנת הסייבר (ACSC) קובע הנחיות וסטנדרטים להגנת מרחב הסייבר בכלל המגזרים, לשימושם של ארגונים המבקשים לאמוד את חוזקת הגנת הסייבר שלהם. כן פורסמו הנחיות להגנת סייבר בשרשראות אספקה ולגבי יצרני מוצרי צריכה חכמים. הרגולציה העצמית על יצרני מוצרי צריכה חכמים כשלה והובילה לפרסום הצעת חוק להחלת רגולציית ציווי ושליטה ריכוזית רכה עליהם.	על ארגונים פרטיים שאינם תשתיות קריטיות או ספקי שירותים דיגיטליים למטרת אימוץ סטנדרטים להגנת סייבר, שנקבעים בשיתוף פעולה בין הממשלה לתעשייה. הרגולציה העצמית על יצרני מכשירי צריכה חכמים כשלה והובילה להצעת חוק להחלת רגולציית ציווי ושליטה רכה ריכוזית עליהם.	על ארגונים פרטיים שאינם תשתיות קריטיות. הממשלה מספקת הנחיה בנוגע להגנת הסייבר וההנחיה מיושמת באמצעות רגולציה עצמית.	רגולציה עצמית בשילוב תמריצים והנחיות לא מחייבות של הסוכנות הלאומית להגנת הסייבר על ארגונים שאינם מפעיל במגזר חיוני, מפעיל שירות טלקומוניקציה או ספק שירותים דיגיטליים.	ארגונים מרמה C שאינם נתונים לאסדרת רגולטור מגזרי יכולים להשתמש בתורת ההגנה בסייבר לארגון שנכתבה על ידי מערך הסייבר לשם רגולציה עצמית. אחרי אחסון נהנים מתמריץ בדמות תוכנית "תו החוסן".

פרק 3

המודל הרגולטורי להגנת מרחב הסייבר בישראל - הערות והארות

בפרק הקודם סקרנו את המודל הרגולטורי להגנת מרחב הסייבר בישראל כפי שעולה מתזכיר חוק הסייבר, מתקציר התזכיר ומתזכיר הוראת השעה, והצגנו את קווי הדמיון ונקודות השוני בין המודל הישראלי למודלים בארצות אחרות, על סמך סקירת המשפט המשווה. בפרק זה נבקש לבקר את המודל הרגולטורי להגנת מרחב הסייבר בישראל ולהצביע על הבעייתיות הטמונה בסמכויות הרחבות שהמדינה מבקשת ליטול לעצמה במסגרתו.

א.
ריבוי הכובעים של מערך הסייבר

מערך הסייבר הוא בראש ובראשונה גוף ביטחוני מבצעי אשר מעניק סיוע בזמן אמת לארגונים אשר נפגעים מתקיפת סייבר בהתאם לסמכויות האופרטיביות המוענקות לו. ואולם, לצד זאת הוא גם המאסדר הלאומי, רגולטור־העל והגוף המקצועי אשר קובע את התקינה המתאימה להשגת הגנת סייבר ברמה נאותה.

ריבוי הכובעים של מערך הסייבר מציב אותו בניגוד עניינים מובנה ומוביל לבלבול באשר לתפקידו וסמכויותיו. מחד גיסא עליו לפעול למימוש האינטרס הלאומי של חשיפת זהות מבצע התקיפה לשם גיבוש התגובה המדינתית לתקיפת הסייבר ומניעת תקיפת סייבר חמורה; מאידך גיסא עליו לתת מענה לחברות מהמגזר הפרטי, ואלו אינן מתעניינות בזהות התוקף ובמטרותיו ברמה הלאומית אלא מצפות שמערך הסייבר הלאומי יזהיר אותן מפני מתקפות סייבר ויסייע להן כאשר הן מתרחשות.

ואולם, מבחינת מערך הסייבר תפקידו אינו לסייע לארגונים בעת תקיפת סייבר אלא למנוע "מגפה" – כלומר הוא אינו אחראי לטיפול בגוף הספציפי המותקף, שעל פי רוב נדרש לשיקום, אלא תפקידו למנוע את התפשטות תקיפת הסייבר לגופים חיוניים אחרים במשק הישראלי.

ריבוי הכובעים של מערך הסייבר והבלבול בקשר לתפקידו גם יוצרים רתיעה ממנו וחשדנות כלפיו, בעיקר מצד ארגונים שאינם תשתיות קריטיות, ומשפיעים על נכונותם לשתף עימו פעולה ולהסכים להפעלת הסמכויות האופרטיביות על ידו בעת הצורך.

יתרה מכך, המצב שבו מערך הסייבר הוא הגוף המקצועי אשר קובע את התקינה המתאימה וגם הגוף בעל סמכויות האכיפה האופרטיביות הוא ייחודי למדי ומקבילה לו אפשר למצוא רק בצרפת, אם כי ANSSI היא רשות לאומית אזרחית ואינה גוף ביטחוני. במדינות אחרות הגופים הביטחוניים או המקצועיים אחראים לקביעת סטנדרט ההגנה ולמתן הייעוץ וההנחיה, מתוך ההבנה שלשם ביצוע תפקידים אלו יש צורך בידע מקצועי ואף מודיעיני שאינו מנת חלקם של ארגונים אחרים, אולם אכיפת הוראות הגנת הסייבר נתונה בידי רגולטורים אזרחיים מגזריים.

התקינה צריכה להיקבע בידי גוף מקצועי, בלתי תלוי וחסר יכולות אכיפה. כך יובטח שהסטנדרטים ייקבעו באופן מקצועי ולא יתעורר חשד כי אכיפתם נגועה בשיקולים זרים שאינם שקופים או גלויים הנובעים מכך שהגוף האוכף – מערך הסייבר באמצעות סמכויותיו האופרטיביות – הוא בראש ובראשונה גוף ביטחוני מבצעי.

ב.
היעדר סעיף מטרות ברור

בחקיקה המבקשת להסדיר את סמכויותיו הרחבות של מערך הסייבר, את המבנה הארגוני שלו ואת מטרותיו יש הכרח בהגדרת מטרות ברורה אשר תתחום את מרחב הפרשנות שיינתן לסמכויותיו. ואולם, בתזכיר חוק הסייבר נקבע ש"ייעוד המערך הוא הגנת מרחב הסייבר וקידום ישראל כמובילה עולמית

בתחום הסייבר".[436] זוהי מטרה רחבה, דו־ראשית, שתוכנה לא ברור ומעורפל ושממנה נגזרות גם סמכויותיו הרחבות והמעורפלות של מערך הסייבר.

ג. רגולציית־על לצד רגולציה על רגולטורים: הצורך בהידוק, שיפור ואִזרוח של המודל

תזכיר חוק הסייבר מתווה מסגרת של רגולציית ציווי ושליטה רכה וביזורית על ארגונים מרמות B ו־C הנתונים לאסדרה באמצעות רשות מאסדרת, אולם מקים בפועל רגולציית־על, רגולציה על רגולטורים. לפי מתווה זה ראש מערך הסייבר הוא המאסדר הלאומי: במגזרים הנתונים לסמכות רשות מאסדרת לפי דין[437] יקבעו הרשויות המאסדרות את ההוראות להגנת הסייבר בהתאם לעקרונות המנויים בתזכיר חוק הסייבר, אולם ראש מערך הסייבר הוא שינחה את הרשויות המאסדרות בנוגע לאופן יישום עקרונות אלו,[438] והוא הסמכות העליונה לאישור הוראותיהן של הרשויות המאסדרות בתחום הגנת הסייבר.[439] כמו כן, ראש מערך הסייבר משמש כערכאת ערעור על הוראות הרשות המאסדרת.[440]

בתקציר התזכיר מובהר שמערך הסייבר הוא המאסדר הלאומי בתחום הגנת הסייבר, אך מוסבר גם שמערך הסייבר אינו רגולטור נוסף אלא הוא משתלב בפעילותן של הרשויות המאסדרות הקיימות ומנחה אותן, כגוף בעל הידע

436 סעיף 2(ב) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

437 סעיף 47(א) לחוק המוצע בתזכיר חוק הסייבר, **שם**, מגדיר "רשות מאסדרת" כ"שר, רשות או ממונה שנתונות לו סמכויות בדין להסדרת פעילות בתחומים משקיים המופיעים בתוספת השנייה".

438 **שם**, בסעיף 44(א) לחוק המוצע בתזכיר חוק הסייבר.

439 **שם**, בסעיפים 44(ב), 49(א)–(ב) לחוק המוצע בתזכיר חוק הסייבר.

440 **שם**, בסעיף 44(ג) לחוק המוצע בתזכיר חוק הסייבר.

המקצועי בכל הקשור להגנת סייבר.[441] עם זאת, בהיעדר נוסח רשמי של שינוי משמעותי זה, חשוב להצביע על הבעייתיות והקשיים הטמונים במתווה של רגולטור־על.

מתווה של רגולציית־על, רגולציה על רגולטורים, הוא מבנה חדש וייחודי יחסית לישראל, כפי שעולה מסקירת המשפט המשווה. באנגליה, לפי מודל הרגולציה של הגנת הסייבר שאומץ ב־2016, מדיניות הגנת הסייבר המגזרית נקבעת על ידי השר האחראי על המגזר בהתאם לתקנות NIS, והרשות הרגולטורית הכפופה לאותו שר אחראית לאכיפה של אותה מדיניות. המשטר הרגולטורי באנגליה לפיכך הוא רגולציית ציווי ושליטה רכה וביזורית ללא רשות־על רגולטורית, כמוצע בתזכיר.[442] גם בארצות הברית נהוגה רגולציית ציווי ושליטה רכה ביזורית: הרגולטורים המגזריים נעזרים בתוכנית NIST לשם קביעת דרישות הגנת הסייבר בארגונים הכפופים להם. אולם תוכנית NIST היא תוצר של עבודה משותפת של המכון הלאומי לסטנדרטים וטכנולוגיה (NIST), שהוא גוף מקצועי אזרחי ללא יכולות אכיפה ופיקוח, ושל בעלי עניין מהמגזר הפרטי; NIST אינו רגולטור של הרגולטורים המגזריים בנושא הגנת הסייבר.[443] גם בדנמרק מוחלת רגולציית ציווי ושליטה רכה ביזורית באמצעות יחידות סקטוריאליות שהוקמו במגזרים מסוימים של תשתיות קריטיות, אולם היחידות הסקטוריאליות מוסמכות לפעול לפי אסטרטגיה להגנת מרחב הסייבר שהממשלה קובעת ואין רגולטור־על המפקח על פעולתן.[444]

המתווה של רגולציית־על מעורר כמה חששות:

(**1**) חוסר התאמה לתרבות הפוליטית והרגולטורית בישראל, המאופיינת בהיעדר שיתוף פעולה בין רגולטורים שונים. למשל, בשוק התקשורת הרגולטורים

441 תקציר התזכיר, **לעיל** ה"ש 344.

442 ראו דיון בסעיף ב בפרק 2 **לעיל**.

443 ראו דיון בסעיף א.2 בפרק 2 **לעיל**.

444 ראו דיון בסעיף ג.II.2 בפרק 2 **לעיל**.

השונים נדרשים לשתף פעולה אך מתקשים מאוד לעשות זאת.[445] כמו כן, כפי שעולה מדוח מבקר המדינה, כבר היום מערך הסייבר אינו מצליח לשתף פעולה ביעילות עם הרשות להגנת הפרטיות.[446]

(**2**) התרבות הארגונית של כל אחד מהרגולטורים בישראל שונה ותקשה על יישום מוצלח של מודל רגולציית־העל.

(**3**) רמת האוריינות הדיגיטלית של כל אחד מהרגולטורים שונה ועלולה להכשיל את היישום המוצלח של המודל הייחודי והחדש של "רגולציה על רגולטורים". יהיה צורך באיגום משאבי ההדרכה והפיקוח כדי להבטיח רמת אוריינות דיגיטלית זהה.

(**4**) סכנה של פוליטיזציה (או סקיוריזציה). במסגרת המתווה המוצע רשאי ראש הממשלה להוסיף מגזרים משקיים לרגולציית ציווי ושליטה ישירה של מערך הסייבר, כפי שפורט לעיל. באמצעות אפיק זה מערך הסייבר עלול להרחיב את הפיקוח וההנחיה הישירה למגזרים משקיים מסוימים מטעמי ביטחון.

גם המתווה של רגולציית ציווי ושליטה ביזורית מעורר כמה קשיים. נטען שמדובר במבנה שביר שמידת יעילותו אינה ברורה, וכי הביזוריות אף עלולה להיות מכשול שכן היא עשויה ליצור כפילויות בסמכויות ולהעניק לרשויות המאסדרות סמכויות בתחום שבו אין להן די ידע או מקצועיות. כמו כן, אם הרשות המאסדרת חסרת סמכויות אכיפה אין כל דרך להבטיח שהגופים המאוסדרים יאמצו סטנדרטים ראויים להגנת סייבר. תזכיר חוק הסייבר מנסה לתקן כשל זה באמצעות ההוראה המעניקה לרשות המאסדרת סמכויות פיקוח ואכיפה זהות לאלו שבידי מערך הסייבר, בכובעו כמאסדר ישיר של ארגונים במשק, אם אין בידה סמכויות אכיפה ופיקוח מתאימות.[447]

בכך מניח תזכיר חוק הסייבר שהרשות המאסדרת תפעל בתחום הגנת הסייבר בדומה לאופן פעילותה בתחומים הרלוונטיים למגזר שעליו היא ממונה. כך,

445 ראו למשל נתי טוקר "מי הבוס של שוק התקשורת?" **TheMarker** (9.12.2019); תהילה שוורץ אלטשולר "בואו נעשה סדר" **מגזין TheMarker** (2.12.2018).

446 מבקר המדינה "היבטים בהגנה על הפרטיות במאגרי מידע" 6, 20–21 (דו"ח שנתי 69ב, 2019).

447 סעיף 61 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

למשל, הרשות המאסדרת מוסמכת להפעיל את סמכויות הפיקוח המוקנות לה בדין המסמיך אותה גם לשם פיקוח על ביצוע ההוראות לפי תזכיר חוק הסייבר.[448] אולם לא ברור אם ההפעלה של סמכויות פיקוח אלו מוגבלת בידי דרישות הדומות לאלו המנויות בתזכיר חוק הסייבר בנוגע לטיפול בתקיפות ובאיומי סייבר.[449] למשל, האם מפקח ברשות מאסדרת המוסמך לתפוס חפץ לפי החוק המסמיך הרלוונטי לו יוכל לעשות זאת בהקשר של הגנת סייבר רק אם יש לו יסוד סביר להניח שיש בחפץ "מידע בעל ערך אבטחתי, שבדיקתו המיידית נדרשת לצורך איתור תקיפת הסייבר, התמודדות עמה או מניעתה"? האם המפקח יידרש לאפשר למחזיק בחפץ הזדמנות לטעון את טענותיו לפני תפיסת החפץ?[450]

כמו כן, במקרה של הפרת הוראות החוק המוצע בתזכיר חוק הסייבר הרשות המאסדרת מוסמכת להטיל סנקציות עונשיות המוקנות לה בחוק המסמיך אותה. למשל, אם הרשות המאסדרת רשאית להתלות רישיון, לבטלו או להגבילו במקרה שהגוף המאוסדר מפר את הוראות הדין או את תנאי הרישיון, הרי היא מוסמכת לנקוט את אותן הפעולות גם במקרה של הפרת הוראות החוק המוצע בתזכיר. עם זאת, לא ברור שהתליית רישיון פעולה היא סנקציה מתאימה או מידתית במקרה של הפרת כל הוראה הנוגעת להגנת סייבר.[451]

ד. הרחבת מעגל המטרות של הגנת סייבר: שימוש נרחב ברגולציית הציווי והשליטה הריכוזית וסכנת הפוליטיזציה

לאורך השנים התמקדה הגנת הסייבר בישראל בהגנה מפני תקיפות סייבר אשר עלולות להוביל לפגיעה מוחשית בתשתיות קריטיות. זוהי הגנת הסייבר

448 **שם**, בסעיף 55 לחוק המוצע בתזכיר חוק הסייבר.

449 **שם**, בסעיפים 19–35 לחוק המוצע בתזכיר חוק הסייבר.

450 **שם**, בסעיף 23 לחוק המוצע בתזכיר חוק הסייבר.

451 **שם**, בסעיף 56 לחוק המוצע בתזכיר חוק הסייבר.

(cybersecurity) הקלאסית המבוססת על מודל ה־CIA, המגדיר שלושה סוגי נזקים שתקיפת סייבר עשויה לגרום:

- Confidentiality – פגיעה בחסיון המידע: בדרך כלל הכוונה לפגיעה לתכלית של איסוף מידע למטרות מודיעין צבאי, אזרחי או מסחרי.
- Integrity – פגיעה באמינות המידע: בדרך כלל הכוונה לפגיעה לתכלית של שיבוש ושינוי נתונים במטרה לגרום פגיעה תפקודית פיזית.
- Availability – פגיעה בזמינות המידע: בדרך כלל הכוונה לפגיעה לתכלית של מניעת גישה למידע.

תזכיר חוק הסייבר מרחיב את מעגל מטרות הגנת הסייבר מעבר למודל ה־CIA המקובל. כפי שמוסבר בתקציר התזכיר, פוטנציאל הנזק היום התרחב אל מעבר לשמירה על סודיות המידע, מניעת הגעתו לידיים הלא נכונות או שיבושו. כיום תקיפת סייבר עלולה להוביל לפגיעה בכל מרחב הנשען על מערכות טכנולוגיות וכך, למשל, לשבש את האספקה של שירותים חיוניים, לפגוע בתשתיות ולגרום נזק לאדם ולסביבה.[452]

אין מחלוקת על הצורך בהרחבת ההגדרה של הגנת סייבר מעבר להגדרה המצומצמת של אבטחת מידע. מתקפות הסייבר שהובילו להפסקת אספקת הדלק בארצות הברית[453] או לפגיעה באספקת החשמל באוקראינה[454] ממחישות צורך זה. אולם, לצד הרחבת ההגדרה של הגנת הסייבר, ועימה הרחבת תחולת ההתערבות הממשלתית לתיקון כשלי השוק הקשורים בהגנת מרחב הסייבר, יש צורך בהתאמת הכלי הרגולטורי למגזר הרלוונטי; אין דין תשתיות קריטיות הנתונות לרגולציית ציווי ושליטה ישירה וריכוזית כדין אתר סחר מקומי או רשת קוסמטיקה.

452 תקציר התזכיר, **לעיל** ה"ש 344.

453 William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, Bloomberg (June 3, 2021)

454 Donghui Park & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, The Henry M. Jackson School of International Studies, University of Washington (Oct. 11, 2017)

וכאן, לדעתנו, טמונה הבעיה בתזכיר חוק הסייבר – נראה שהשימוש ברגולציית ציווי ושליטה ריכוזית ישירה בידי מערך הסייבר רחב מדי, כפי שניתן להסיק מהמפורט להלן:

(**1**) ההצדקה העיקרית להחלת רגולציית ציווי ושליטה ריכוזית ישירה היא פגיעה ב"אינטרס חיוני", כלומר מערך הסייבר מוסמך להפעיל את סמכויותיו כאשר הדבר נדרש לשם הגנה על "אינטרס חיוני" מפני תקיפת סייבר. "אינטרס חיוני" מוגדר בתזכיר חוק הסייבר ככל 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".[455]

תזכיר הוראת השעה מגדיר "אינטרס ציבורי חיוני" ככל אחד מאלה: "(1) מניעת פגיעה חמורה בשלום הציבור; (2) חיי אדם; (3) כלכלת המדינה; (4) הגנה על הסביבה; (5) בריאות הציבור או בטיחותו; (6) מניעת אירוע אבטחה חמור במאגר שחלה עליו רמת האבטחה הגבוהה כהגדרת בתקנות אבטחת מידע; (7) תפקודם התקין של תשתיות, מערכות או שירותים חיוניים; (8) תפקודו התקין והבטוח של מרחב הסייבר".[456]

ניכר כי רשימת האינטרסים רחבה ומעורפלת. כך, למשל, האם מערך הסייבר יוכל להפעיל את סמכויותיו במקרה של תקיפת סייבר הפוגעת בתפקוד התקין של רשתות קמעונאיות למכירת בגדים, שהן "ארגונים המספקים שירותים בהיקף משמעותי"? למשל, תקיפת סייבר על מערכות המחשוב של קבוצת פוקס, החולשת על 18 מותגי אופנה ועיצוב הבית, או על מערכות חברת ביג, החולשת על עשרות מרכזי קניות וקניונים בישראל, עשויה להיחשב פגיעה באינטרס

455 סעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343, הגדרת "אינטרס חיוני".

456 סעיף 1 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346.

חיוני אף שהשירות שחברות אלה מספקות אינו חיוני לבריאות הציבור, לביטחון המדינה או לכלכלתה.

כמו כן, מה ההבדל בין "ביטחון הציבור ובטיחותו", "חיי אדם" ו"מניעת סכנה ניכרת לסביבה או לבריאות הציבור", המוזכרים בתזכיר חוק הסייבר? או בין "מניעת פגיעה חמורה בשלום הציבור", "חיי אדם" ו"בריאות הציבור או בטיחותו" בתזכיר הוראת השעה? יתרה מזו, תחת הסעיפים "אינטרס שקבע ראש הממשלה" בתזכיר חוק הסייבר או "תפקודו התקין והבטוח של מרחב הסייבר" בתזכיר הוראת השעה אפשר לכלול, לכאורה, גם פגיעה בתודעה, ולהביא לפוליטיזציה של מערך הסייבר.

(**2**) מיפוי המשק וסיווג הארגונים לרמות שונות של סיכון בהתאם לחומרת הפגיעה ב"אינטרס חיוני" ייעשו לפי שיטה שיקבע ראש מערך הסייבר. תזכיר חוק הסייבר מציג רשימה פתוחה של שיקולים שעליהם השיטה צריכה להתבסס, אך ראש מערך הסייבר יכול גם להביא בחשבון שיקולים נוספים שאינם חשופים או ידועים לציבור. גם השיטה עצמה אינה שקופה לחלוטין לציבור: עיקרי השיטה יפורסמו רק באופן שלדעת ראש מערך הסייבר לא יסכן את האינטרס החיוני, שכאמור הגדרתו רחבה. התוצאה היא שסיווג הארגונים במשק, הקובע את הרגולציה שתוחל עליהם, מתבסס על שיטה שעשויה להיות חסויה ברובה ונקבעת בדרך שמתאימה לגופים ביטחוניים ולא לאסדרת משק אזרחי.

מסקירת המשפט המשווה עולה שישראל אינה המדינה היחידה אשר הרחיבה את תחולת רגולציית הציווי והשליטה אל מעבר לתשתיות קריטיות. עם זאת, במדינות שבהן הורחבה תחולת הרגולציה לארגונים נוספים ההרחבה מוגבלת יחסית, ואינה נובעת מהרחבת ההגדרה של האינטרסים הלאומיים החיוניים אלא מההבנה שהתלות הגוברת בפעילותם של ארגונים מסוימים במרחב הסייבר עשויה להביא לפגיעה באינטרס לאומי חשוב במקרה של תקיפת סייבר. לדוגמה, בצרפת מוחלת רגולציית ציווי ושליטה ריכוזית על המערכות הממוחשבות של ארגונים שפגיעה בפעילותם התקינה עלולה לפגוע באופן משמעותי במצבה הכלכלי או הצבאי של המדינה או בביטחון הציבור וחוסנו. ואולם, לעומת רשימת האינטרסים המוצעת בתזכיר החוק, בצרפת מדובר ברשימה מצומצמת יותר – אם כי חוסנו של הציבור הוא אינטרס מעורפל למדי.

באנגליה הורחבה התחולה של רגולציית הציווי והשליטה הרכה והביזורית וכעת היא כוללת גם "ספקי שירותים דיגיטליים רלוונטיים", הכוללים ספקי פלטפורמות סחר אלקטרוני, ספקי מנועי חיפוש וספקי שירותי ענן. רגולציה מסוג זה הוחלה גם על חברות הנמנות עם "קבוצת הפרימיום": קבוצה של חברות פרטיות שאף שאינן משתייכות למגזרי התשתיות הקריטיות, הן כוללות את החברות המצליחות ביותר באנגליה המחזיקות בעוצמה הכלכלית העתידית של המדינה, מבחינת ערך הקניין הרוחני שלהן והמחקר שהן מבצעות; חברות המחזיקות במידע אישי או רגיש על אזרחים באנגליה ומחוצה לה, כמו עמותות צדקה; חברות שעלולות להיות מטרה לתקיפות סייבר משמעותיות, כגון חברות תקשורת, שתקיפת סייבר נגדן עלולה לפגוע במוניטין של המדינה, לפגוע באמון הציבור בממשלה או לסכן את חופש הביטוי; ספקי שירותים דיגיטליים המאפשרים מסחר וכלכלה דיגיטלית ושירותיהם תלויים באמון לקוחותיהם; וכל ארגון שבאמצעות כוחות השוק או סמכותו לפי חוק עשוי להשפיע על הכלכלה הלאומית ולשפר את רמת הגנת הסייבר כולה, למשל חברות ביטוח, משקיעים, רגולטורים ויועצים מקצועיים. עם זאת, ההגדרה הרחבה של קבוצת הפרימיום יצרה קשיים רבים בהבנת תחולת הרגולציה, ובשנת 2018 נעשה ניסיון למפות את המערכות באותן חברות ואת רמת הקישוריות ביניהן כדי לתעדף את רמת המעורבות הממשלתית ברגולציית הגנת הסייבר במגזרי התשתיות הקריטיות ובקבוצת הפרימיום.

ה. סמכויות רחבות ומעורפלות

1. סמכות שיורית וסכנה לפוליטיזציה

למערך הסייבר נתונה סמכות שיורית "לבצע כל תפקיד אחר בתחום הגנת הסייבר שיקבע ראש הממשלה".[457] "הגנת הסייבר" מוגדרת בהרחבה כ"מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום

457 סעיף 3(6) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע".[458] "תקיפת סייבר" מוגדרת כרשימה פתוחה של פעולות שמטרתן לפגוע בשימוש במחשב או בחומר מחשב השמור בו, לרבות "אחסון או הצגה של מידע או פלט כוזב, או שיש בהם כדי להטעות, בהתאם למטרות השימוש בהם".[459] הגדרה רחבה זו מאפשרת הסמכה של מערך הסייבר לפעול גם בכל הקשור להשפעה על תודעה ודעת קהל; באופן זה גוברת הסכנה לפוליטיזיציה של מערך הסייבר.

2. סמכות רחבה לאיסוף מידע ולעיבודו

I. לפי תזכיר חוק הסייבר

מערך הסייבר רשאי לקבל, לאסוף, לעבד, להעביר, להפיץ ולשתף "מידע בעל ערך אבטחתי" ו"מידע שעשוי לשמש להפקת מידע בעל ערך אבטחתי".[460] "מידע בעל ערך אבטחתי" מוגדר בצורה רחבה.[461] מנגד, "מידע שעשוי לשמש להפקת מידע בעל ערך אבטחתי"[462] אינו מוגדר כלל בתזכיר חוק הסייבר, ולא ברור אם הוא עשוי לכלול גם מידע אישי. בתקציר התזכיר הוסבר שיש שלושה

458 **שם**, בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, הגדרת המונח "הגנת סייבר".

459 **שם**, סעיף קטן (3) בהגדרת המונח "תקיפת סייבר" בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר.

460 **שם**, בסעיפים 16(א)(1)–(3) לחוק המוצע בתזכיר חוק הסייבר.

461 "מידע בעל ערך אבטחתי" מוגדר בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **שם**, כך:

> 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.

462 **שם**, בסעיף 16(א)(1) לחוק המוצע בתזכיר חוק הסייבר.

סוגים עיקריים של מידע המצוי במחשבים וברשתות: מידע טכנולוגי טהור שאי־אפשר להסיק ממנו מסקנות על אדם; מידע טכנולוגי טהור שאפשר להסיק ממנו, במישרין או בצירוף מידע אחר, מידע על אדם מזוהה או ניתן לזיהוי; ומידע טכנולוגי המתעד מסרים אנושיים, כלומר התבטאויות ותקשורת בין בני אדם. בעוד עיקר פעילות הגנת הסייבר שמערך הסייבר מבצע או מנחה לבצע קשור למידע בעל ערך אבטחתי המצוי בעיקר בשני הסוגים הראשונים, תקציר התזכיר מכיר בכך שלעיתים גם מידע המתעד מסרים אנושיים, דהיינו תוכן, עשוי להיות בעל ערך אבטחתי – למשל כאשר שיטת החדירה של תקיפת הסייבר היא שיטוי של עובד בארגון ללחוץ על קישור זדוני.[463]

זאת ועוד, מערך הסייבר מוסמך לעשות מגוון פעולות במידע שיאסוף: לקבל, לאסוף, לעבד,[464] להעביר, להפיץ ולשתף אותו, אך המונח "עיבוד" כלל אינו מוגדר בתזכיר חוק הסייבר ולא ברור מהו מגוון הפעולות הנופלות בגדר סמכות עיבוד זו.

במציאות של נתוני עתק נעשה קל יותר לזקק פרטי מידע אישי ממידע שלכאורה אינו מזוהה. סכנה זו קיימת גם במקרה של שיתוף של "מידע בעל ערך אבטחתי", ולפיכך יש לתת את הדעת להגדרתו המדויקת של המידע הרלוונטי לשיתוף, ולסכנה לחשיפת מידע אישי הנלווית לשיתופו.[465]

463 תקציר התזכיר, **לעיל** ה"ש 344.

464 סעיף 16(א)(2) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

465 Daniel M. Best et al., *Improved Cyber Threat Indicator Sharing by Scoring Privacy Risk*, IEEE (2017). הכותבים מצביעים על הצורך באימוץ הארכיטקטורה המוצעת על ידם כדי להקטין את הסיכון לפגיעה בפרטיות עקב שיתוף מידע בעל ערך אבטחתי.

II. לפי תזכיר הוראת השעה

תזכיר הוראת השעה מגביל במידת מה את הפעולות שמערך הסייבר רשאי לבצע במידע. ראשית, האיסוף של "מידע מוגן פרטיות"[466] מותר אך ורק בהתקיים אחד מהתנאים האלה:[467]

(**1**) מדובר ב"מידע בעל ערך הגנתי" הכולל "מאפיינים טכנולוגיים של תקיפת סייבר, ובכלל זה כתובת המחשב שממנו בוצעה התקיפה או של המחשב שנתקף" או "נתונים בשפת קריאת מחשב המעידים על תבנית תקיפת סייבר".[468]

(**2**) האיסוף מותר לפי דין.

(**3**) בית המשפט שוכנע שהפגיעה בפרטיותו של אדם מידתית לשם הגנה על "אינטרס ציבורי חיוני" והתיר את איסוף המידע בהחלטה מנומקת. כפי שכבר ציינו לעיל,[469] אף שהוראה זו מבקשת לצמצם את היקף המידע הנאסף בשם הגנת הפרטיות, חולשתה נעוצה בהגדרה המרחיבה של "אינטרס ציבורי חיוני", הכוללת, למשל, את האינטרס הרחב והמעורפל של "תפקודו התקין והבטוח של מרחב הסייבר".

השימוש ב"מידע מוגן פרטיות" מוגבל רק למידע שהתקבל או נאסף בהתאם לתזכיר הוראת השעה ורק למטרות "הגנת סייבר", והותר על ידי בית משפט אשר שקל את הפגיעה בפרטיותו של אדם וקבע שהיא מידתית לשם הגנה על "אינטרס ציבורי חיוני". "הגנת סייבר" מוגדרת בתזכיר הוראת השעה כמכלול הפעולות הדרושות לאיתור תקיפת סייבר, היערכות לתקיפה, מניעתה, טיפול

466 "מידע מוגן פרטיות" מוגדר בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346, כ"מידע כהגדרתו בסעיף 7 לחוק הגנת הפרטיות וכן ידיעות על ענייניו הפרטיים של אדם אף אם אינן בגדר מידע כאמור". "מידע" מוגדר בסעיף 7 לחוק הגנת הפרטיות כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".

467 סעיף 7 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346.

468 **שם**, בסעיפים 1 ו־7(א).

469 ראו הטקסט הנלווה להערת שוליים 456.

בה וצמצום נזקים והחלמה ממנה.[470] בניגוד לתזכיר חוק הסייבר, "תקיפת סייבר" בתזכיר הוראת השעה מוגדרת באופן מצומצם יותר כ"פעולה המבוצעת בחומר מחשב שנועדה לפגוע במחשב, בחומר מחשב המאוחסן בו, בתקשורת הנתונים מהמחשב או אליו" או פעולה המהווה "גישה לחומר מחשב או לתקשורת נתונים בלא הרשאה".[471] אולם "אינטרס ציבורי חיוני" מוגדר בהרחבה ובאופן מעורפל, והמונח "שימוש" כלל אינו מוגדר בתזכיר הוראת השעה. המשמעות היא שמערך הסייבר רשאי לעשות מגוון פעולות העשויות להיחשב "שימוש" למטרת הגנת סייבר, ובלבד שיהיו מידתיות לדעת בית המשפט ומיועדות להשגת תכלית רחבה ומעורפלת של אינטרס ציבורי חיוני.

העברה של "מידע מוגן פרטיות" מותרת בכמה מקרים:

(**1**) למטרת "הגנת סייבר" לאחד מהגופים האלה: משרדי ממשלה, מוסדות מדינה אחרים, רשות מקומית וגוף אחר הממלא תפקיד ציבורי לפי דין. בדרך זו נוצר **צינור רחב ביותר של העברת מידע לגופים שלאו דווקא מחזיקים במומחיות הנדרשת להגנת סייבר ולהחזקת מידע ואבטחתו.** כך, למשל, ניסיון העבר מלמד שמשרד החינוך והרשויות המקומיות אינם מצטיינים, בלשון המעטה, באבטחה של מאגרי המידע המצויים כבר עתה ברשותם.[472] ראוי על כן לצמצם את רשימת הגופים הציבוריים שהעברת מידע מוגן אליהם מותרת, להתנות את היקף המידע המועבר במבחן מידתיות ולקבוע כללים לשימוש במידע כאמור, להחזקתו ולאבטחתו.

(**2**) לארגון כאשר מדובר במידע שהוא "מאפיינים טכנולוגיים של תקיפת סייבר, ובכלל זה כתובת המחשב שממנו בוצעה התקיפה או של המחשב שנתקף" או

470 "הגנת סייבר" מוגדרת בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346, כ"פעולות להגנה על מחשב, על חומר מחשב השמור בו ועל תקשורת הנתונים אליו וממנו מפני תקיפת סייבר, ובכלל זה פעולות לאיתורה, היערכות לה, מניעתה, או טיפול בה ומצמום הנזקים הנגרמים ממנה, במהלכה או לאחריה".

471 "תקשורת נתונים" מוגדרת בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **שם**, כ"מעבר של חומר מחשב ממחשב אחד למחשב אחר באמצעות התקשרות או התחברות של מחשב עם מחשב אחר".

472 מבקר המדינה אף מתח ביקורת נוקבת על הכשלים בהגנת הסייבר במשרדים אלו, ראו כביר, **לעיל** ה"ש 415.

"נתונים בשפת קריאת מחשב המעידים על תבנית תקיפת סייבר", ואם ההעברה נחוצה לשם הגנת הסייבר.[473] מוצע להגביל את האפשרות להעביר מידע ולהבטיח שהעברת המידע נחוצה לצורך הגנת הסייבר בארגון המקבל.

(**3**) לגוף מיוחד בהתאם לסמכויותיו לפי כל דין, למעט העברת מידע לפי המנגנון הקבוע בחוק הגנת הפרטיות להעברת מידע לגופים ציבוריים.[474] זהו צינור העברה נוסף ורחב ביותר, המתיר העברת מידע ללא תנאים ברורים לגופים ביטחוניים שונים לצורך שאינו ברור. לדעתנו יש להבהיר מתי ולשם מה נדרשת העברת מידע כאמור ואילו סוגי מידע מותרים בהעברה.

כמו כן, תזכיר הוראת השעה מעגן את דרישת הנחיצות בקבעו שיש למחוק מידע מוגן פרטיות ברגע שאין בו צורך עוד.[475] עם זאת, תזכיר הוראת השעה אינו כולל הוראות לעניין מפקח פרטיות פנימי בארגון או ועדה מייעצת, בדומה לאלו המצויות בתזכיר חוק הסייבר.

לצד הוראות אלו, תזכיר הוראה השעה מסמיך את מערך הסייבר לקבל מעובד השב"כ, כברירת מחדל, או מספק גישה לאינטרנט, מידע אישי מזהה של לקוח קצה, ובלבד שאין מדובר באדם פרטי. מידע זה כולל את זהות הלקוח ופרטי ההתקשרות עימו, הכוללים את שמו, מענו, מספר הטלפון וכתובת הדוא"ל שלו. קבלת המידע מותנית בכך שבהתאם למידע המצוי בידי המערך יש "חשיפה קריטית" במחשבי הלקוח, או שמחשבי הלקוח נתונים ל"תקיפת סייבר" או ל"תקיפת סייבר חמורה". לפי תזכיר הוראת השעה, השימוש במידע מזהה כאמור יהא אך ורק לשם יצירת קשר עם הלקוח לצורך הגנת הסייבר. אולם גם במקרה זה, ההגדרות הרחבות והמעורפלות של המונחים מכרסמות ביעילותם של אמצעי הגנת הפרטיות המוצעים בתזכיר הוראת השעה. "חשיפה קריטית" מוגדרת כחולשה שיוצרת סיכון לתקיפת סייבר בהיקף נרחב או לתקיפת סייבר חמורה. תזכיר הוראת השעה מסתפק בחשש לסיכון ואינו דורש כי הסיכון יהיה ממשי. "תקיפת סייבר חמורה" מוגדרת כתקיפת סייבר שמתקיימים לגביה

473 סעיף 7(ג) לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346.

474 **שם**, בסעיף 7(ה).

475 **שם**, בסעיף 7(ד).

מגוון תנאים,[476] ובהם פגיעה ממשית באינטרס ציבורי חיוני. הגדרתו הרחבה והמעורפלת של "אינטרס ציבורי חיוני" יוצרת גם כאן פתח לאיסוף מידע אישי מזהה על לקוח קצה בנסיבות מעורפלות.

יתרה מכך, עצם מתן ההרשאה לקבלת מידע מזהה על לקוח קצה, שאינו אדם יחיד, מהשב"כ, כברירת המחדל, או מספק שירותי אינטרנט היא חריגה ובעייתית ביותר, ולדעתנו אינה נחוצה כלל. יש לאמץ הסדר דומה לזה המעוגן בחוק נתוני תקשורת, אשר קובע מנגנון שבמסגרתו רשויות אכיפה כגון משטרת ישראל יקבלו פרטים אישיים של יחיד בצו בית משפט, ובמקרים דחופים יפנו לקבלת היתר ללא צו שתוקפו 24 שעות, בנסיבות המנויות בחוק ובין השאר כאשר הפרטים דרושים לשם הצלת חיי אדם או הגנה עליהם.[477] מדוע טיפול בתקיפת סייבר חמורה או מניעתה מצדיק מנגנון אחר, חודרני ונעדר איזונים כמו זה המוצע בתזכיר הוראת השעה? מדוע אי־אפשר לקבוע מנגנון זהה לזה המצוי בחוק נתוני תקשורת, שנתקבל לאחר דיונים רבים ותוך שימת לב לפגיעה בפרטיות לצד דחיפות הטיפול, בין השאר לשם הצלת חיים?

3. סמכויות רחבות ומעורפלות למערך הניטור

לפי תזכיר חוק הסייבר מערך הסייבר מוסמך להפעיל מערך ניטור וזיהוי הפועל 24 שעות ביממה, לשם איסוף ועיבוד של "מידע" למטרת גילוי מוקדם של

476 "תקיפת סייבר חמורה" מוגדרת בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **שם**, כ"תקיפת סייבר שמתקיים לגביה אחד מאלה: (1) התקיפה עלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני; (2) יש יסוד סביר להניח שהתקיפה תגרום לפגיעה ממשית באינטרס ציבורי חיוני לנוכח חומרת הסכנה להתפשטותה למחשבים אחרים ולפגיעה נרחבת בהם או במידע השמור בהם; (3) התקיפה אותרה בארגון שמקיים פעילות חיונית או שיש יסוד סביר להניח שהיא מכוונת כלפי ארגון כאמור או כלפי גוף המנוי בתוספת החמישית לחוק להסדרת הביטחון; (4) יש יסוד סביר להניח שהתקיפה נועדה לפגוע בביטחון הלאומי של המדינה".

477 סעיפים 3 ו־4 לחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח–2007.

תקיפות סייבר וסיוע בהתמודדות עימן,[478] והמידע ייאסף מרשימה רחבה ביותר של ארגונים.[479]

סמכות איסוף המידע ועיבודו על ידי מערך הניטור מוגבלת אך במעט בהתאם לעקרונות אלה:[480] (1) איסוף המידע ימוקד במידע בעל ערך אבטחתי; (2) עיבוד המידע למידע בעל ערך אבטחתי יבוצע ככל האפשר בזמן אמת, באופן ממוחשב ואוטומטי; (3) המידע ייאסף ויעובד בהתאם לחובת "עיצוב לפרטיות" (Privacy by Design) המצומצמת הקבועה בחוק המוצע בתזכיר; (4) המידע ייאסף ויעובד אך ורק למטרת גילוי מוקדם של תקיפות סייבר וסיוע בהתמודדות עימן.[481]

עם זאת, היעדר הגדרות למונח "מידע" שמערך הסייבר מוסמך לאסוף,[482] ולמונח "עיבוד" בהתייחס למגוון הפעולות שהמערך רשאי לעשות במידע שנאסף,[483] לא רק יוצרים חשש לפגיעה בזכות לפרטיות, אלא גם מתווים סמכות רחבה שגבולותיה אינם ברורים. הוראות מדויקות באשר לאופן הפעלת הסמכות בכל הקשור לאיסוף המידע, עיבודו, שמירתו וביעורו הותרו לקביעה בתקנות.[484]

4. הסמכויות האופרטיביות והסכנה ליצירת "דלת אחורית"

לפי תזכיר חוק הסייבר, כחלק מהסמכויות האופרטיביות המוענקות למערך הסייבר, עובד מוסמך במערך הסייבר רשאי לתת לארגון הוראות לביצוע פעולות בחומר מחשב לשם איתור תקיפת סייבר, התמודדות עימה או מניעתה.[485]

478 סעיף 17(א) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

479 **שם**, בסעיף 17(ב).

480 העקרונות מפורטים בסעיף 17(ג) לחוק המוצע בתזכיר חוק הסייבר, **שם**.

481 חובת העיצוב לפרטיות מפורטת בסעיף 38 לחוק המוצע בתזכיר חוק הסייבר, **שם**.

482 **שם**, בסעיף 16(א)(1).

483 **שם**, בסעיף 16(א)(2).

484 **שם**, בסעיף 17(ה).

485 **שם**, בסעיף 26.

"פעולה בחומר מחשב" מוגדרת כאחת מהפעולות האלה: חדירה לחומר מחשב, העתקה של חומר מחשב, הקלטה או ניטור של תקשורת בין מחשבים, מתן הוראות למחשב בשפת קריאת מחשב, שינוי חומר מחשב ובלבד שאין בו שינוי של מידע שהוא רשומה מוסדית או מידע הניתן לפענוח חזותי בידי אדם, דיווח למערך בשפה קריאת מחשב על איתור סממנים ומאפייניהם, והתקנת מחשב או התקן אחר ברשת תקשורת או במחשב של ארגון לשם ביצוע פעולות אלו.[486] "תקיפת סייבר" מוגדרת באופן רחב כרשימה פתוחה של פעולות, לרבות "אחסון או הצגה של מידע או פלט כוזב, שיש בהם כדי להטעות, בהתאם למטרת השימוש בהם". הגדרה זו עלולה לאפשר למערך הסייבר לפעול גם בכל הקשור להשפעה על תודעה ודעת קהל. ארגון המקבל הוראה כאמור מחויב לבצעה ללא יכולת ערעור,[487] ואסור לו לגלות את תוכן ההוראות שקיבל ממערך הסייבר.[488]

כמו כן, עובד מוסמך במערך הסייבר מוסמך לבצע פעולה במחשב או בחומר מחשב לפי צו בית משפט שלום אם השופט שוכנע שסביר שמתרחשת או שעומדת להתרחש תקיפת סייבר העלולה לפגוע ב"אינטרס החיוני". ההגדרה הרחבה של "אינטרס חיוני" בתזכיר חוק הסייבר הופכת את מרחב הסכנה שעל השופט להביא בחשבון לרחב ומעורפל. בשילוב עם העובדה שהצו יכול להינתן במעמד צד אחד ואף על בסיס ראיות חסויות,[489] מדובר בסמכות רחבה ומעורפלת.

עובד מערך הסייבר אף מוסמך לבצע בהתאם לצו בית משפט שלום פעולה במחשב או בחומר מחשב לצורך בדיקה מדגמית, אם מערך הסייבר סבור שיש סיכוי של ממש לאתר באמצעות הדגימות תקיפות סייבר. במתן הצו על בית המשפט להתחשב בין השאר בנחיצות הצו לצורכי "הגנת סייבר". "הגנת סייבר" מוגדרת כמגוון פעולות לשם מניעה של תקיפת סייבר או איום סייבר, התמודדות

486 הגדרת "פעולה בחומר מחשב" מפורטת בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **שם**.

487 **שם**, בסעיפים 26(א)–(ג).

488 **שם**, בסעיפים 26(ד), 39 ו־72.

489 **שם**, בסעיפים 27–29.

עימם וטיפול בהם. מאחר שזוהי הגדרה רחבה, כפי שהוסבר לעיל,[490] גם כאן הסמכות עשויה להיות רחבה ומעורפלת. יתרה מכך, בית המשפט יכול לתת צו לביצוע פעולה במחשב במעמד צד אחד אם הוא סבור שהארגון המשיב הוזמן כדין ולא התייצב לדיון, ובכל מקרה ברירת המחדל היא שהדיון יהיה בדלתיים סגורות.[491]

גורם אחראי במערך הסייבר מוסמך גם להורות על ביצוע פעולות הדורשות אישור בית משפט אף ללא אישור בית משפט, אם קיבל את הסכמת הארגון לכך.[492] כמו כן, ראש מערך הסייבר רשאי להורות על ביצוע פעולות הדורשות אישור בית משפט אף ללא אישור בית משפט או הסכמת הארגון למשך תקופה מוגבלת של 24 שעות, אם ביצוע הפעולה נדרש בדחיפות לשם מניעת נזק ממשי ל"אינטרס החיוני".[493] עם זאת, המונח "נזק ממשי" אינו מוגדר בחוק המוצע והגדרת "אינטרס חיוני רחבה ומעורפלת.[494]

תזכיר הוראת השעה מעניק לגורם אחראי במערך הסייבר את הסמכות לתת הנחיה מקצועית לארגון לביצוע "פעולות הגנת סייבר" לשם היערכות לתקיפת סייבר או מניעת תקיפת סייבר חמורה, ובלבד שלגורם האחראי יש יסוד סביר להניח שהארגון מקיים פעילות חיונית ושקיימת במערכותיו חשיפה קריטית, המוגדרת כחולשה היוצרת סיכון לתקיפת סייבר חמורה או בהיקף נרחב, והארגון אינו נוקט בפעולות לטיפול בה.

רשימת הפעולות המוגדרות כ"פעולות הגנת סייבר" בתזכיר הוראת השעה מצומצמת מזו שבתזכיר חוק הסייבר, אך עדיין כוללת מתן הוראות למחשב בשפת קריאת מחשב, העתקה של חומר מחשב, התקנת תוכנה במחשב של ארגון לשם ביצוע פעולות שונות במחשב, בחינה וסריקה ממוכנות של חומר

490 ראו הטקסט הנלווה להערות שוליים 485–487.

491 סעיפים 32–33 לחוק המוצע בצזכיר חוק הסייבר, לעיל ה"ש 343.

492 **שם**, בסעיף 35 לחוק המוצע בתזכיר חוק הסייבר.

493 **שם**, בסעיף 36 לחוק המוצע בתזכיר חוק הסייבר.

494 ראו דיון בטקסט הנלווה להערות שוליים 455–456.

מחשב ודיווח על איתור מידע בעל ערך הגנתי למערך הסייבר.[495] תקיפת סייבר חמורה מוגדרת, בין השאר, כתקיפה העלולה לגרום לפגיעה ממשית באינטרס ציבורי חיוני, המוגדר אף הוא בהגדרה רחבה.[496] בשל כך, מדובר בסמכות רחבה שגבולותיה מעורפלים; נוסף על כך, גם לפי תזכיר הוראת השעה ארגון המקבל הוראה כאמור מחויב לבצעה ללא אפשרות ערעור.

תזכיר הוראת השעה אינו מגדיר מנגנון לביצוע פעולות הגנת סייבר בהסכמת הארגון.[497] כמו כן, גורם אחראי במערך הסייבר מוסמך לבצע פעולות הגנת סייבר לפי צו בית משפט לעניינים מינהליים. עם זאת, תזכיר הוראת השעה אינו מפרט את סדרי הדין בבקשת צו כאמור אלא מותיר זאת לתקנות שיתקין שר המשפטים.[498]

השילוב בין ההגדרה הרחבה של "פעולה בחומר מחשב" בתזכיר חוק הסייבר ובין הסמכויות האופרטיביות הרחבות האלו, שאפשר לבצען ללא צו לתקופה מוגבלת או בצו שיכול להינתן במעמד צד אחד, מעורר שאלות וחששות: באילו נסיבות יפנה גורם ממערך הסייבר לקבלת צו, ובאילו נסיבות ינסה קודם לפנות לקבלת הסכמת הארגון? וככלל, מהי תקפותה של הסכמת הארגון הניתנת נוכח פערי הכוחות, הידע והמומחיות בין הצדדים? בדיווחים חדשותיים נטען כי חלק מהחברות חשו שמערך הסייבר נהג עימן בבריונות ובהפחדה, באופן שלא הותיר להן שיקול דעת רב כשנדרשו להחליט אם להסכים או לסרב לדרישת המערך לבצע פעולות במערכות המחשב שלהן.[499] בתנאים אלו גובר החשש מפני יצירת "דלת אחורית" הרחק מעין הציבור, בדומה לדלת האחורית שיצרה הסוכנות

495 "פעולות הגנת סייבר" מוגדרות בסעיף 1 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346, כ"פעולות מחשב שהן אחת מאלה: (1) מתן הוראות למחשב בשפה קריאת מחשב; (2) בחינה של חומר מחשב או תקשורת נתונים לצורך ביצוע הפעולה המנויה בפסקה (2); (3) דיווח על איתור מידע בעל ערך הגנתי למערך הסייבר הלאומי; (5) התקנת מחשב או תוכנה במחשב של ארגון לשם ביצוע הפעולות המנויות בפסקאות (1) עד (4)".

496 ראו דיון בטקסט הנלווה להערות שוליים 455–456.

497 סעיפים 4–5 לחוק המוצע בתזכיר הוראת השעה, **לעיל** ה"ש 346.

498 **שם**, בסעיף 6(ה).

499 שחף "איבד את הדרך", **לעיל** ה"ש 345.

האמריקנית לביטחון לאומי (NSA) באמצעות תוכנת PRISM, כפי שחשף אדוארד סנודן בשעתו.[500]

גם השילוב בין ההגדרה המצומצמת יותר של "פעולות הגנת סייבר" בתזכיר הוראת השעה לסמכויות האופרטיביות המוענקות למערך הסייבר מעורר חששות דומים. אומנם תזכיר הוראת השעה אינו מחייב את הארגון לשמור על סודיות ההנחיות המקצועיות שהוא מקבל ממערך הסייבר לביצוע פעולות הגנת סייבר ואינו מאפשר ביצוע פעולות הגנת סייבר בהסכמת הארגון ללא צו בית משפט, אך העובדה שהארגון מחויב לבצע את הפעולות מרגע מתן ההנחיה המקצועית היא בעייתית ומעוררת אף היא חשש מיצירת "דלת אחורית".

5. אי־בהירות לגבי הגורם המפעיל את הסמכות ודרישות הכשירות שלו

ראש מערך הסייבר רשאי להאציל מסמכויותיו ל"עובד בכיר",[501] אולם תזכיר חוק הסייבר אינו כולל הגדרה למונח זה או התייחסות להגדרת תנאי הכשירות לתפקיד "עובד בכיר".

כמו כן, לפי תזכיר חוק הסייבר הסמכויות האופרטיביות נתונות בידי "עובד מוסמך" או "גורם אחראי", ותנאי הכשירות לתפקידים אלו ייקבעו בידי ראש מערך הסייבר עצמו ואינם מוגדרים בתזכיר חוק הסייבר.[502]

תזכיר הוראת השעה נעדר הוראה דומה לעניין האצלת הסמכות, אך כולל הגדרה ברורה לעובד מוסמך ולתנאי כשירותו. עם זאת, בתזכיר הוראת השעה אין הגדרה ברורה של תנאי הכשירות למינוי עובד בכיר ל"גורם אחראי".

500 ראו למשל Levy, **לעיל** ה"ש 14.

501 סעיף 4(ד) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

502 **שם**, בסעיף 5(ד) לחוק המוצע בתזכיר חוק הסייבר.

ו.
מנגנוני פיקוח והגנה על הזכות לפרטיות בפעולות מערך הסייבר

1. מפקח פרטיות פנימי והוועדה המפקחת

בתזכיר חוק הסייבר מוגדרים שני גופים שייחודם בכך שתפקידם מתמקד בהגנה על הזכות לפרטיות.

הגוף הראשון הוא מפקח פרטיות פנימי המפקח על יישום הוראות חוק הגנת הפרטיות במערך.[503] המינוי של מפקח פרטיות פנימי הוא צעד חיובי וחשוב לשמירה על הזכות לפרטיות בפעילות מערך הסייבר, אולם נבקש להצביע על שני חסרונות מרכזיים בהגדרת מיהות המפקח ופועלו שיש בהם כדי לפגום ביעילות מנגנון זה. ראשית, נראה שמערך הסייבר הוא שממנה את המפקח וגם קובע את תנאי הכשירות שלו, והמשקל הניתן לעמדתו של רשם מאגרי המידע נמוך. זאת משום שהמפקח הוא עובד מערך הסייבר הממונה מבין עובדי המערך בידי ראש המערך, בהתייעצות עם רשם מאגרי המידע ובהתאם לתנאי כשירות והכשרה שיורה עליהם רשם מאגרי המידע, אולם אלו ייקבעו בהתייעצות עם ראש המערך.[504]

חיסרון נוסף הוא שמפקח הפרטיות הפנימי אינו עצמאי בעבודתו. דרישת העצמאות היא דרישה חיונית וחשובה שיוצרת מעין "הפרדת רשויות" פנימית, והיא נהוגה כיום בתקנות החדשות להגנה על הפרטיות במידע של האיחוד האירופי, המחייבות מינוי ממונה על הגנת פרטיות בארגון שעצמאותו היא מדד לכשירותו.[505] אולם מפקח הפרטיות הפנימי במערך כפוף ישירות לראש המערך

503 **שם**, בסעיף 11 לחוק המוצע בתזכיר חוק הסייבר.

504 **שם**, בסעיף 10(א) לחוק המוצע בתזכיר חוק הסייבר.

505 סעיף 38 ל־GDPR, **לעיל** ה"ש 20.

או לעובד בכיר במערך הכפוף ישירות לראש המערך, אך מונחה מקצועית על ידי רשם מאגרי המידע.[506] המפקח אינו עצמאי, ולא זו בלבד אלא הוא עשוי למצוא עצמו מתמודד עם הנחיות סותרות מצד ראש מערך הסייבר מחד גיסא ורשם מאגרי המידע מאידך גיסא.

הגוף השני המוגדר בתזכיר חוק הסייבר כבעל תפקיד לעניין הגנת הפרטיות הוא הוועדה המפקחת הממונה על ידי ראש הממשלה. גם כאן מדובר במינוי חשוב להגנת הפרטיות, בעיקר בגוף הרואה בעצמו גוף ביטחוני, ויש לברך על כך. עם זאת, גם המבנה והפעילות של הוועדה המייעצת, כפי שהם מוגדרים בתזכיר חוק הסייבר, לוקים בכמה חסרונות העלולים לגרוע מחשיבותה ומיעילותה. ראשית, בראש הוועדה יעמוד שופט בדימוס או משפטן בכיר הכשיר לכהן כשופט מחוזי, אך מלשון תזכיר חוק הסייבר לא ברור מהן דרישות הכשרות משופט בדימוס –[507] האם גם עליו להיות שופט מחוזי בדימוס? שנית, על הוועדה המפקחת להגיש דוח מטעמה מדי שנה, אולם תזכיר חוק הסייבר אינו מפרט כלל מהן הפעולות האופרטיביות שיבוצעו לאחר קבלת הדוח.[508] מכאן שעבודות הפיקוח והבקרה של הוועדה עשויות להיות לריק, שכן אין כל חובה לנקוט פעולה כלשהי בעקבות דוח הוועדה. כמו כן, אם הוועדה מוצאת שיש סיכוי שהופר הדין בידי גורם או אדם מסוים עליה לחדול מהטיפול בעניין ולהעביר את המשך הטיפול לגורם המוסמך לכך – אולם תזכיר חוק הסייבר אינו מפרט מיהו אותו גורם מוסמך, מהן דרישות כשירותו ומהן סמכויותיו.[509]

2. עיצוב לפרטיות

חובת העיצוב לפרטיות בתזכיר חוק הסייבר חלה על סוגים רבים של מידע, וכוללת "הגנה על הפרטיות" וכן על "מידע מוגן",[510] שכולל לא רק מידע

506 סעיף 10(ד) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

507 **שם**, בסעיף 13(ג)(1) לחוק המוצע בתזכיר חוק הסייבר.

508 **שם**, בסעיף 14(א) לחוק המוצע בתזכיר חוק הסייבר.

509 **שם**, בסעיף 15(ב) לחוק המוצע בתזכיר חוק הסייבר.

510 **שם**, בסעיף 38 לחוק המוצע בתזכיר חוק הסייבר.

שחוק הגנת הפרטיות חל עליו אלא גם מידע בעל ערך כלכלי, לרבות סודות מסחריים.[511]

חובת העיצוב לפרטיות חשובה להגנת הפרטיות ויש לברך על הכללתה בתזכיר חוק הסייבר. עם זאת, אופן הגדרתה עלול לרוקן אותה מתוכן, משתי סיבות. ראשית, חובת העיצוב לפרטיות דורשת הטמעה של אמצעים טכנולוגיים שיבטיחו שייאסף ויישמר רק המידע המוגן "המינימלי הנדרש לקיום ייעוד המערך".[512] ואולם, "ייעוד המערך" מוגדר בהרחבה כ"הגנת מרחב הסייבר וקידום ישראל כמובילה עולמית בתחום הסייבר".[513] "הגנת מרחב הסייבר" מוגדרת כ"מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ולאחריהם, ובכלל זה פעולות אבטחת מידע",[514] אך המטרה של "קידום ישראל כמובילה עולמית בתחום הסייבר" היא מטרה רחבה ומעורפלת שאינה מוגדרת בתזכיר חוק הסייבר. במסגרת קידום ישראל כמובילה עולמית בתחום הסייבר ניתן למשל לכלול איסוף ושמירה של מידע אישי לשם פיתוח באמצעות בינה מלאכותית של מערכות זיהוי של פעולות אנושיות העלולות להוביל למתקפת סייבר.

שנית, חובת העיצוב לפרטיות בתזכיר חוק הסייבר מתמצה בחובת הטמעת אמצעים טכנולוגיים, והיא מצומצמת מזו המקובלת במשפט המשווה, הדורשת גם הטמעת אמצעים ארגוניים. כך, למשל, ב־GDPR נדרש בעל השליטה במידע להטמיע אמצעים טכניים וארגוניים כחלק מחובת העיצוב לפרטיות.[515]

511 סעיף 1 לחוק המוצע בתזכיר חוק הסייבר, **שם**, מגדיר "מידע מוגן" כ"כל אחד מאלה: (1) מידע שחוק הגנת הפרטיות חל עליו; (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".

512 **שם**, בסעיף 38(א)(1) לחוק המוצע בתזכיר חוק הסייבר.

513 **שם**, בסעיף 2(ב) לחוק המוצע בתזכיר חוק הסייבר.

514 **שם**, בסעיף 1 לחוק המוצע בתזכיר חוק הסייבר.

515 סעיף 25 ל־GDPR, **לעיל** ה"ש 20.

3. חובת סודיות

תזכיר חוק הסייבר מטיל חובת סודיות בכמה הקשרים.

ראשית, עובד המערך או הפועל מטעם המערך מחויב בחובת סודיות לגבי "מידע מוגן", הכולל הן מידע שחוק הגנת הפרטיות חל עליו והן מידע בעל ערך כלכלי. ואולם, חובת הסודיות המוטלת על עובד המערך או הפועל מטעם המערך נסוגה על פי דין או על פי "היתר בכתב בהתאם להוראות שקבע ראש המערך".[516] הוראות ראש המערך צריכות להינתן לפי תזכיר חוק הסייבר,[517] אך זהו פתח רחב מאוד להתרת פגיעה בפרטיות בנסיבות שונות ובחוסר שקיפות.

שנית, לראש מערך הסייבר, לעובדים הכפופים לו או למי שפועל מטעמו אסור לגלות ידיעה או מסמך שהגיעו לידיו מתוקף תפקידו. אך גם במקרה זה האיסור מוגבל, והוא נסוג כאשר גילוי המידע נעשה לפי הוראות תזכיר חוק הסייבר, לצורך הליך פלילי בשל "עבירה חמורה" או בשל הפרעה לעובד ציבור.[518] המונח "עבירה חמורה" אינו מוגדר בתזכיר חוק הסייבר, ועל כן היקפו וגבולותיו של החריג לאיסור הגילוי אינם ברורים או ידועים. כמו כן, עלולה להיות סתירה בין אפשרויות הפרת חובת הסודיות לבין ההוראה הקובעת שמידע שהגיע לידי המערך בהסכמה לא ישמש כראיה נגד מוסרו בהליך פלילי, אזרחי או מינהלי, אלא בעבירות שיקבע השר.[519]

שלישית, לצד חובת הסודיות המוטלת על עובד המערך או הפועל מטעם המערך, לאדם או לארגון אסור לגלות מידע שנמסר לו על הוראה או מידע אחר הקשור בפעילות המערך שסומן כמידע מוגן, מידע בעל ערך אבטחתי רגיש או מידע בעל סיווג ביטחוני. רק בית משפט מוסמך להורות על עקיפת איסור זה.[520] לאיסור זה מצטרף גם האיסור על גילוי פעילות מערך הסייבר, אלא בהתאם להוראות תזכיר

516 סעיף 6(א) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

517 **שם**.

518 **שם**, בסעיף 40 לחוק המוצע בתזכיר חוק הסייבר.

519 **שם**, בסעיף 41(א) לחוק המוצע בתזכיר חוק הסייבר.

520 **שם**, בסעיף 39 לחוק המוצע בתזכיר חוק הסייבר.

חוק הסייבר או להוראות שיקבעו ראש הממשלה ושר המשפטים.[521] לכאורה, איסורים אלו הם חלק ממכלול ההגנה על הזכות לפרטיות הקבוע בתזכיר חוק הסייבר, אך לפי דברי ההסבר נראה שהכוונה היא להגן על הסודיות של שיטות, אמצעים ומידע הרלוונטיים להגנת סייבר שהמערך עושה בהם שימוש, ואין מדובר כלל על הגנה על הזכות לפרטיות במידע אישי.[522] בהקשר זה, הכפפת ארגון לסודיות בנוגע להוראות שהוא מקבל מהמערך בעייתית בהיבט השקיפות והפיקוח על פעולות המערך.

4. סיכום: הגנת הפרטיות בתזכיר חוק הסייבר ובתזכיר הוראת השעה

תזכיר חוק הסייבר ותזכיר הוראת השעה כוללים הוראות חשובות לעניין ההגנה על הזכות לפרטיות בפעולות מערך הסייבר, ויש לברך על כך. אולם הוראות אלו אינן מעניקות הגנה מספקת על הזכות לפרטיות.

באשר לתזכיר חוק הסייבר, מערך הסייבר מוסמך לעשות מגוון רחב של פעולות, חלקן לא מוגדר, במידע שהגדרתו רחבה ושעשוי לכלול גם מידע מזוהה או ניתן לזיהוי. כמו כן, נוכח ההגדרה הרחבה והמעורפלת של "ייעוד המערך", מנגנוני ההגנה שהתזכיר מבקש להטמיע, דוגמת עיצוב לפרטיות, עשויים להיות "חסרי שיניים" בחלק מהמקרים.

תזכיר הוראת השעה מציג לכאורה מסגרת מהודקת יותר למגוון הפעולות שמערך הסייבר רשאי לבצע במידע. אולם אין בכך די; גם כאן חולשת מנגנוני הגנת הפרטיות נעוצה בהגדרות הרחבות או בהיעדר ההגדרות של מונחי מפתח, דוגמת "שימוש" ו"אינטרס ציבורי חיוני". כמו כן, תזכיר הוראת השעה אינו כולל את מנגנוני ההגנה הנוספים והחשובים המוצעים בתזכיר חוק הסייבר – מפקח פרטיות פנימי והוועדה המפקחת.

521 **שם**, בסעיף 72 לחוק המוצע בתזכיר חוק הסייבר.

522 **שם**, בדברי ההסבר לסעיפים 39 ו־72 לחוק המוצע בתזכיר חוק הסייבר.

ז. פטורים רחבים או לא ברורים בתזכיר חוק הסייבר

בתזכיר חוק הסייבר יש כמה סעיפי פטור המעוררים חשש מחסינות רחבה מדי מפני אחריות משפטית.

1. סייג לאחריות

תזכיר חוק הסייבר קובע שני סייגים לאחריות עובד המערך או מי מטעמו:

(**1**) עובד מערך הסייבר או מי שפועל מטעם המערך בתפקידים שקבע ראש הממשלה לא יישא באחריות פלילית או אזרחית למעשה או למחדל אם נעשה בתום לב ובאופן סביר במסגרת תפקידו ולשם מילויו.[523]

(**2**) פטור ייחודי מאחריות לפגיעה בפרטיות, ולפיו עובד המערך או מי שפועל מטעמו לא יישא באחריות לפי חוק הגנת הפרטיות לפגיעה בפרטיות ובלבד שהפגיעה נעשתה באופן סביר במסגרת תפקידו ולשם מילויו.[524]

שני סעיפי הסייג מאחריות מעוררים כמה קשיים:

(**1**) אמת המידה של סבירות המעשה אינה אמת המידה המקובלת במשפט המשווה. ב־GDPR, למשל, המבחן לקיומו של פטור מאחריות בגין פגיעה בפרטיות הוא מבחן מידתיות ונחיצות, כלומר הפגיעה בפרטיות הייתה נחוצה ומידתית להשגת מטרה לגיטימית.[525]

523 **שם**, בסעיף 8 לחוק המוצע בתזכיר חוק הסייבר.

524 **שם**, בסעיף 65(ב) לחוק המוצע בתזכיר חוק הסייבר.

525 רחל ארידור הרשקוביץ **הצעת חוק הגנת הפרטיות, התשע"ט-2019: השלמות בנושא עיבוד מידע אישי על ידי גופי ביטחון והתנאים להכרת הנציבות האירופית בתאימות הדין המקומי (adequacy): סקירת משפט משווה** (המכון הישראלי לדמוקרטיה 2019).

(**2**) היחס בין שני סעיפי הסייג מאחריות אינו ברור. בעוד שני סעיפי הפטור קובעים פטור מאחריות אזרחית או פלילית, התנאים לתחולת הפטור מאחריות למעשה או מחדל הם תום לב וסבירות, ואילו לתחולת הפטור מאחריות לפגיעה בפרטיות די בהתקיים מבחן הסבירות בלבד.

2. פטור "נמל הביטחון"

תזכיר חוק הסייבר קובע שמידע שנמסר למערך הסייבר בהסכמה לפי הוראות פרק ג, העוסק בסמכויות האופרטיביות של המערך, לא ישמש כראיה נגד מוסרו בהליך אזרחי, מינהלי או פלילי, למעט במקרה שמדובר בעבירות שקבע שר המשפטים.[526] תחולת הפטור אינה ברורה. למשל, האם במקרה שמותקן בארגון מערך ניטור יחול הפטור על כל מידע הנקלט במערך הניטור, שאמור לפעול באופן אוטומטי, או רק על מידע שבעל תפקיד או עובד בארגון מוסר למערך בהסכמה?

3. פטור לפעולה המיועדת ל"הגנת סייבר"

תזכיר חוק הסייבר קובע פטור רחב במיוחד, שלפיו פעולה המבוצעת על ידי ארגון ומיועדת ל"הגנת סייבר" במחשבי הארגון לא תיחשב כפגיעה בפרטיות, האזנת סתר או חדירה אסורה לחומר מחשב, אם מתקיימות הדרישות שלהלן: (1) לארגון יש מדיניות הגנת סייבר בהתאם להוראות או לתקן מקובל הרלוונטי לצורכי הגנת הסייבר בארגון ולאיומי 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, ומסר להם פרטים על הפעילות, על מטרותיה ועל השימוש במידע.[527]

526 סעיף 41(א) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

527 **שם**, בסעיף 64 לחוק המוצע בתזכיר חוק הסייבר.

4. פטור לשם שיתוף מידע

תזכיר חוק הסייבר פוטר ארגון מאחריות בגין הפרת חוק הגנת הפרטיות במקרה של שיתוף מידע שנאסף בארגון עם ארגונים אחרים או עם מערך הסייבר, בהתקיים התנאים שלהלן: (1) המידע הוא מידע בעל ערך אבטחתי; (2) הארגון מסר פרטים על שיתוף המידע, מטרותיו והשימוש שיעשה במידע לעובדיו וללקוחותיו; (3) השימוש במידע הוא למטרת הגנת סייבר.[528]

ח.
חלוקת הסמכויות בין מערך הסייבר לרשויות ביטחון אחרות

בתזכיר חוק הסייבר הובהר שהחוק המוצע אינו מיועד "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".[529]

אולם מלשון תזכיר חוק הסייבר נראה שחלוקת הסמכויות בין מערך הסייבר לגופי ביטחון אחרים, ובעיקר השב"כ, אינה ברורה. תזכיר חוק הסייבר מסמיך את ראש מערך הסייבר להחליט אם לערב בעלי סמכות נוספת לשם מניעת פגיעה באינטרס חיוני.[530] מנגד, תזכיר חוק הסייבר מתיר לראש השב"כ להסמיך עובד בסמכויות האופרטיביות הנתונות לעובד מערך הסייבר בנוגע לטיפול בתקיפה

528 **שם**, בסעיף 65(א) לחוק המוצע בתזכיר חוק הסייבר.

529 **שם**, בעמ' 2.

530 **שם**, בסעיף 37 לחוק המוצע בתזכיר חוק הסייבר: "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 לאוצו בעל סמכות; בעל הסמכות יקבע איש קשר לסיוע למניעת הפגיעה האמורה ולהיערכות להתמודדות עמה".

ובאיומי סייבר, אם הדבר דרוש לצורך סיכול איומי טרור וריגול, כמשמעותם בסעיף 7 לחוק השב"כ.[531]

ואולם, המונח "סיכול איומי טרור וריגול" אינו מוגדר בסעיף 7 לחוק השב"כ, שאליו מפנה תזכיר חוק הסייבר. אותו סעיף 7 מגדיר את ייעוד השב"כ ותפקידיו וקובע, בין השאר, שהשב"כ יופקד גם על "שמירת [...] **סדרי המשטר הדמוקרטי ומוסדותיו, מפני איומי טרור**, **חבלה**, **חתרנות**, ריגול וחשיפת סודות מדינה, וכן יפעל השירות לשמירה ולקידום של אינטרסים ממלכתיים חיוניים אחרים לביטחון הלאומי של המדינה, והכל כפי שתקבע הממשלה ובכפוף לכל דין" (ההדגשות בציטוטים מהחוק הן שלנו).[532] אחד מתפקידי השב"כ הוא "סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע [...] **בסדרי המשטר הדמוקרטי או במוסדותיו**".[533] תפקיד נוסף הוא "**פעילות בתחום אחר שקבעה הממשלה**, באישור ועדת הכנסת לענייני השירות, שנועדה **לשמור ולקדם אינטרסים ממלכתיים חיוניים לביטחון הלאומי של המדינה**";[534] זאת ועוד, חוק

531 **שם**, בסעיף 71 לחוק המוצע בתזכיר חוק הסייבר:
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.

(א) 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;

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

532 חוק שירות הביטחון הכללי, התשס"ב–2002 (להלן: חוק השב"כ).

533 **שם**, בסעיף 7(ב)(1).

534 **שם**, בסעיף 7(ב)(6).

השב"כ מסמיך את עובדי השב"כ לקבל ולאסוף מידע, וכן להעביר מידע לגופים אחרים.[535]

נראה כי תפקידים אלו של השב"כ חופפים את תפקידי מערך הסייבר כפי שהם מוגדרים בתזכיר חוק הסייבר:[536]

תפקידי המערך הם:

(**1**) לנהל, להפעיל ולבצע בהתאם לצורך את מאמצי ההגנה הלאומיים והאופרטיביים כנגד תקיפות סייבר;

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

(**3**) לקדם מדיניות ומובילות ישראלית בתחום הגנת 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 מרחב הסייבר שיקבע ראש הממשלה.

תזכיר הוראת השעה כולל אף הוא הוראה המצביעה על כפילות סמכויות, בהסמיכה עובד שב"כ לתת הנחיות מקצועיות להיערכות לתקיפת סייבר או למניעת תקיפת סייבר חמורה, בתנאי שמתקיימים שני תנאים: (1) הנחיות אלו נחוצות למילוי תפקידי השירות המנויים בסעיף 7(ב)(1) לחוק השב"כ, כלומר לשם "סיכול ומניעה של פעילות בלתי חוקית שמטרתה לפגוע בביטחון המדינה, בסדרי המשטר הדמוקרטי או במוסדותיו"; (2) ראש השב"כ התיר את השימוש בסמכויות לאחר ששוכנע שהשימוש בהן דרוש לצורך מניעת תקיפת סייבר חמורה או התמודדות איתה בארגון באירוע נתון. אותן סמכויות אופרטיביות למתן הנחיות מקצועיות מוקנות בתזכיר הוראת השעה גם לגורם אחראי במערך.[537]

535 **שם**, בסעיף 8(א).

536 סעיף 3 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

537 סעיף 10 לתזכיר הוראת השעה, **לעיל** ה"ש 346.

אומנם ההוראה המסמיכה את עובד השב"כ בתזכיר הוראת השעה ממוקדת יותר מזו המופיעה בתזכיר חוק הסייבר, שכן היא מתמקדת בשתי סמכויות אופרטיביות מסוימות (מתן הנחיות מקצועיות להיערכות לתקיפת סייבר או למניעת תקיפת סייבר חמורה) ככל שהדבר נדרש לשם מילוי תפקיד אחד מבין תפקידי השב"כ. אולם כפילות הסמכויות נותרת בעינה, משום שגורם אחראי במערך מוסמך לתת הנחיות מקצועיות להיערכות לתקיפת סייבר או למניעת תקיפת סייבר חמורה בתנאים מסוימים, ובהם סכנה ל"אינטרס ציבורי חיוני". הגדרתו הרחבה והמעורפלת של "אינטרס ציבורי חיוני" בהחלט עשויה להתיר את הפעלת הסמכות גם למטרות שהן בגדר מטרותיו של השב"כ: מניעת פגיעה בביטחון המדינה, בסדרי המשטר הדמוקרטי או במוסדותיו.

כמו כן, הסמכת עובד שב"כ בסמכויות האופרטיביות הנתונות למערך הסייבר, בין לפי תזכיר חוק הסייבר ובין לפי תזכיר הוראת השעה, משמעה שגוף הביטחון החשאי של מדינת ישראל מוסמך לתת הוראות לביצוע פעולות להגנת סייבר גם לארגונים שאינם מורגלים באסדרה שכזו, ותוך פגיעה, שאינה שקופה ואינה כפופה למבחן מידתיות, בזכות לפרטיות.

בידי השב"כ נתונות כבר כיום סמכויות מעקב נרחבות, המופעלות לפי דינים חסויים וכפופות לפיקוח חיצוני, שיפוטי ופרלמנטרי חלקי וחסר, הנעשה ברובו על ידי גופים החסרים מומחיות טכנולוגית ומודיעינית מספקת לבחינה אמיתית של פרקטיקות המעקב המקוון.[538] לדוגמה, השב"כ מוסמך ליירט נתוני תקשורת בכפוף לדינים חסויים וליירט נתוני תוכן הנדרשים מטעמי ביטחון המדינה. במקרים שאינם דחופים מותנה יירוט נתוני התוכן באישור ראש הממשלה או שר הביטחון, אך במקרים דחופים הוא מותר אף באישור ראש השב"כ בלבד בכפוף להסכמת היועמ"ש.[539] משום כך, ההצדקה להקניית סמכויות נוספות לשב"כ במסגרת תזכיר חוק הסייבר או תזכיר הוראת השעה אינה ברורה.

538 עמיר כהנא ויובל שני "מתחת לרדאר: מעקב מקוון בישראל" **בלוג סיווג ביטחוני, המכון הישראלי לדמוקרטיה** (13.3.2017); עמיר כהנא בשיתוף עם יובל שני **פיקוח על מעקב מקוון בישראל** (מחקר מדיניות 149, המכון הישראלי לדמוקרטיה 2020).

539 סעיף 11 לחוק השב"כ.

יתרה מכך, בעוד תזכיר הוראת השעה מגביל את סמכויות מערך הסייבר בכל הנוגע לפגיעה בפרטיות ולאיסוף מידע ולהחזקתו, ההסמכה המוקנית בתזכיר הוראת השעה לעובד שב"כ אינה כפופה לאותן מגבלות. זאת ועוד, לשב"כ פטור רחב מאחריות לפגיעה בפרטיות במקרים שבהם הפגיעה נעשתה לפי הסמכה בדין או באופן סביר ובמסגרת התפקיד ולשם מילויו.[540]

ט.
כשירות ראש המערך ועובדיו

תזכיר חוק הסייבר מאפשר לראש הממשלה לעקוף את דרישות חוק המינויים ולקבוע תקנות או כללים לעניין "ארגון וניהול כוח האדם במערך". בדברי ההסבר מוסבר שמערך הסייבר הוא גוף ביטחוני מבצעי, ומאפיינים ייחודיים אלו מחייבים שינויים בהיבטים הארגוניים שלו, כפי שיקבע ראש הממשלה.[541] זוהי הוראה כללית ומעורפלת שיש בה אף פתח להעסקת עובדי קבלן לביצוע עבודה כה רגישה.

540 סעיף 19 לחוק הגנת הפרטיות.

541 סעיף 5 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343, ודברי ההסבר לסעיף.

פרק 4

סיכום והמלצות מדיניות

השילוב בין הנזקים העצומים העשויים להיגרם ממתקפות סייבר ובין היעדר תמריצים מספקים להשקעה בהגנת מרחב הסייבר, כפי שנסקרו במחקר המדיניות על מרחב הסייבר,[542] מצדיק התערבות ממשלתית לשם אסדרת המרחב הזה. עם זאת, אסדרת ההגנה על מרחב הסייבר כרוכה בכמה אתגרים. הראשון שבהם הוא העובדה שלמדינה כובעים רבים, ולפעמים סותרים, במרחב הסייבר: המדינה היא הבעלים של תשתיות קריטיות; האחראית לביטחון הלאומי ואמורה להגן על התשתית הקריטית עצמה; פועלת כרגולטור עבור גופי המגזר הפרטי המחזיקים בתשתיות במרחב הסייבר ואחראים להגנתו; שחקנית הלוקחת חלק בשיתופי פעולה ציבוריים ופרטיים להגנת מרחב הסייבר; נציגה במישור הבינלאומי ופועלת עם ומול מדינות אחרות במטרה להגן על מרחב הסייבר, שהגבולות הגיאוגרפיים בו מטושטשים; יצרנית ומפיצה של ידע ומידע בנוגע להגנת מרחב הסייבר; ולבסוף, המדינה יכולה לשמש גם כתוקפת במרחב הסייבר היוצרת בעצמה איומים.

אתגרים נוספים העומדים בפני גיבוש אסדרה להגנת מרחב הסייבר הם אתגרים טכנולוגיים הקשורים בא־סימטריה בין התוקף למגן, היעדר היכולת להעריך את מידת האפקטיביות של פעולות להגנת מרחב הסייבר ואת הרצף הנכון שלהן, והצורך בשילוב גורמים מתחומים שונים, לאו דווקא טכנולוגיים, היות שהגנת מרחב הסייבר היא נושא מורכב המחייב מומחיות בתחומים נוספים כגון כלכלה, פסיכולוגיה, משפטים וסוציולוגיה. כמו כן, מתווה הגנת סייבר צריך להיות חוצה מגזרים, משום שהסכנות במרחב הסייבר אינן ייחודיות למגזר מסוים או לתעשייה מסוימת. ההתמודדות עם סכנות אלו מחייבת מדיניות כוללנית מצד הרגולטור לצד הבנת המאפיינים הייחודיים לכל מגזר. לבסוף, הגנת מרחב הסייבר מחייבת רמה מינימלית של אוריינות דיגיטלית בקרב המשתמשים במרחב הסייבר וקובעי המדיניות.

542 **מהו סייבר א**, **לעיל** ה"ש 9.

מדינת ישראל, כמו מדינות מערביות רבות, פועלת לאסדרת ההגנה על מרחב הסייבר. כפי שעולה מהסקירה המשווה שהוצגה לעיל, הבסיס לאסדרה אפקטיבית טמון בהבנה שהאחריות צריכה להיות מוטלת על כלל השחקנים, והאסדרה של מרחב הסייבר אינה צריכה לחול על תשתיות קריטיות בלבד או להתמקד רק במגזר הציבורי. אולם היקף האחריות, סוג האסדרה המתאימה והכלי הרגולטורי הנבחר ייגזרו מרמת הסיכון הנשקף לאינטרס הציבורי ממתקפת סייבר מוצלחת על כל שחקן, בדומה לעקרון האחריות המשותפת אך השונה המקובל במשפט הבינלאומי בהקשר של שמירה על איכות הסביבה ומזעור הנזקים משינויי האקלים. לצד זאת ניכר שילוב מוגבר של המגזר הפרטי, התעשייה והאקדמיה בקביעת האסדרה המתאימה. בהתאם לניהול הסיכונים הנשקפים לאינטרס הציבור מתקיפת סייבר מוצלחת, מדינות שונות בחרו להחיל שילוב של כלים רגולטוריים שונים, החל ברגולציית ציווי ושליטה ריכוזית, עבור ברגולציית ציווי ושליטה רכה וביזורית וכלה ברגולציה שיתופית ורגולציה עצמית.

ביוני 2018 פורסם בישראל תזכיר חוק הסייבר, המבקש לכונן מסגרת פעולה נורמטיבית ומוסדית להגנת הסייבר במדינה. זהו צעד חיובי ונכון לאור הצורך לעגן בחוק את אופן פעולתו וסמכויותיו של מערך הסייבר הלאומי, הפועל להגנת מרחב הסייבר מכוח החלטות ממשלה זה כמה שנים.

במרץ 2021 נעשה ניסיון לחוקק הוראת שעה, אשר אינה עוסקת בשאלת האסדרה הרחבה אלא רק מבקשת להעניק למערך הסייבר באופן נקודתי ולזמן קצוב סמכויות אופרטיביות הנחוצות לשם התמודדות עם ארגונים המסרבים לשתף פעולה עם מערך הסייבר או לנקוט את רמת הגנת הסייבר הנדרשת לדעת המערך.

באשר לאסדרת הגנת הסייבר, התפיסה המגולמת בתזכיר חוק הסייבר היא כי על הרגולטורים המגזריים להחיל מנגנון אסדרה המשלב רגולציית ציווי ושליטה ריכוזית וביזורית, בפיקוח מערך הסייבר.

כפי שטענו במחקר זה, לתפיסתנו תזכיר חוק הסייבר אינו משקף את ההסתכלות הרחבה המתבקשת נוכח אתגרי היצירה והמימוש של אסדרת ההגנה על מרחב הסייבר. לפי המתווה המתואר בתזכיר חוק הסייבר, השיח בין מערך הסייבר

למגזר הפרטי ולאקדמיה בנוגע לקביעת סוג הרגולציה המתאים לכל מגזר מצומצם. עיקר שיתוף הפעולה בין המגזר הציבורי למגזר הפרטי מתמקד בשיתוף מידע בעל ערך אבטחתי. האסדרה המוצעת עוסקת בעיקר ברגולציית ציווי ושליטה תוך מתן סמכויות רחבות, ולעיתים מעורפלות, למערך הסייבר. תזכיר חוק הסייבר אינו משקף הגנה מספקת לזכות לפרטיות כזכות יסוד מרכזית בעולם הדיגיטלי, והשימוש שנעשה בזמן משבר הקורונה במידע הזמין לשב"כ מעורר חשש אמיתי כי סמכויות רחבות ומעורפלות עלולות לאפשר בעתיד שימוש ביכולותיו של מערך הסייבר למטרות נוספות שאי־אפשר לחזותן בנקודת הזמן הנוכחית. יתרה מכך, כפי שפרשת תקיפת הסייבר על חברת הביטוח שירביט חשפה, יש צורך דחוף בעיגון ברור, שקוף ומדויק של הסמכויות של כל אחת מהרשויות הרלוונטיות במקרה שבו נדרש לסייע לחברה פרטית בעת תקיפת סייבר – הרשות להגנת הפרטיות, הרשות הרגולטורית המגזרית ומערך הסייבר. זאת ועוד, הכרחי לקבוע בצורה ברורה ושקופה את יחסי הכוחות בין הרשויות הרלוונטיות, תחומי האחריות של כל אחת ואופן שיתוף הפעולה ביניהן.

לפיכך אנו ממליצות:

(**1**) להוסיף לחוק המוצע בתזכיר חוק הסייבר סעיף מטרה אשר יתחום את מרחב הפרשנות האפשרי של סמכויות מערך הסייבר על פי החוק. בסעיף יש להבהיר שמטרת החוק היא לעגן בחוק הוראות הנוגעות למבנה הארגוני של מערך הסייבר, לגופים המפקחים על פעילותו ולסמכויותיו בתחום הגנת מרחב הסייבר בישראל, תוך הגברת השקיפות ושיתוף התעשייה, האקדמיה, החברה האזרחית והציבור.

(**2**) לשנות את מודל ה"רגולציה על רגולטורים". יש למצב את מערך הסייבר **כרגולטור היחיד** הקובע את **התקינה וההנחיה** הנדרשות להגנת הסייבר; הכלי הרגולטורי שבו ייעשה שימוש ייקבע לפי המאפיינים הספציפיים של כל מגזר ספציפי ולפי רמת הסיכון הנשקפת לאינטרס הציבורי מתקיפת סייבר נגד ארגון במגזר זה.

(**3**) להבטיח שסמכויות הפיקוח והאכיפה יינתנו בידי רגולטורים מגזריים שדפוסי פעולתם אינם של ארגון ביטחוני, ואלו יפעלו בהתאם לכללי המשפט המינהלי הרגיל ובכלל זה מתוך חובת שקיפות שלטונית.

(**4**) לאזרח את מערך הסייבר או לכל הפחות להחיל עליו עקרונות מתחום המשפט הציבורי, ולא רק את הנורמות המשפטיות המקובלות בארגוני הביטחון. כיום המערך פועל כגוף ביטחוני המאמץ נורמות של חיסיון והיעדר שקיפות. אלו אינן מתאימות לגוף המנחה קשת ארגונים רחבה מהמגזר הפרטי, שאינה מצומצמת רק לתשתיות קריטיות, וקובע עבורם מסגרת לסטנדרטים טכנולוגיים להגנת סייבר.

(**5**) להעדיף ככל האפשר שקביעת התקינה להגנת הסייבר תיעשה תוך שיתוף התעשייה, האקדמיה והציבור כדי להתאימה למאפייני כל מגזר. אי־שיתוף הגורמים המאוסדרים יוצר מרמור ורתיעה משיתוף פעולה מרצון עם מערך הסייבר. בקביעת התקינה חשוב להתבסס גם על מידע מודיעיני, אולם יש להבטיח שבכל הנוגע לגופים שאינם תשתיות קריטיות או שתקיפת סייבר נגדם אינה צפויה לפגוע פגיעה חמורה באינטרס לאומי חשוב, קביעת התקינה תהיה שקופה ותיעשה ככל האפשר בדרך של שיתוף הציבור וקבלת הערותיו.

(**6**) לצמצם את סמכויותיו של מערך הסייבר:

(א) יש לצמצם את הגדרת "אינטרס חיוני" באמצעות הסרת ההתייחסות ל"ארגונים המספקים שירותים בהיקף משמעותי"; האחדת ההתייחסות לביטחון הציבור והימנעות מהכפילות הבאה לידי ביטוי במניית המונחים "ביטחון הציבור", "בטיחותו", "חיי אדם" ו"בריאות הציבור"; וקביעה כי כל אינטרס חיוני נוסף ייקבע בתקנות בידי ועדת הכנסת ולא בצו בידי ראש הממשלה.

באשר לתזכיר הוראת השעה, יש לצמצם את הגדרה "אינטרס ציבורי חיוני" באמצעות האחדת ההתייחסות לביטחון הציבור והימנעות מהכפילות הבאה לידי ביטוי במניית המונחים "ביטחון הציבור", "בטיחותו", "חיי אדם" ו"בריאות הציבור"; כן יש להסיר את ההתייחסות ל"תפקודו התקין והבטוח של מרחב הסייבר", שכן מדובר בהגדרת אינטרס רחבה מאוד ודי בהתייחסות הממוקדת יותר ל"תפקודם התקין של תשתיות, מערכות או שירותים חיוניים".

צמצום ההגדרה של "אינטרס החיוני" או של "אינטרס ציבורי חיוני" הוא בעל השלכות מהותיות, ויביא לצמצום הדרוש בסמכויות המערך וכן בסמכויות הקשורות להיקף רגולציית הציווי והשליטה הריכוזית הנתונה בידיו. כך, למשל, צמצום ההגדרה של "אינטרס חיוני" או של "אינטרס ציבורי חיוני" יוביל לצמצום מספר הארגונים שניתן יהיה להכפיפם באופן זמני לרגולציית ציווי ושליטה של מערך הסייבר,[543] או לצמצום מגוון המגזרים המשקיים שניתן יהיה להוסיף בהתאם להחלטת ראש הממשלה.[544]

(ב) יש לצמצם את הגדרת "מידע בעל ערך אבטחתי" בתזכיר חוק הסייבר למידע המשמש אינדיקציה לאיתור תקיפת סייבר, מידע על חולשות במערכת מחשב או מידע על נוזקות ואופני הפצתן בלבד.

(ג) יש להגדיר את המונח "עיבוד" בתזכיר חוק הסייבר ואת המונח "שימוש" בתזכיר הוראת השעה. בכל הקשור להעברת מידע לגופים ציבוריים ולגופים מיוחדים אין די בצמצום המוצע בתזכיר הוראת השעה: יש לקבוע את רשימת הגופים הציבוריים שמותר להעביר להם "מידע מוגן פרטיות" ולהכפיף את היקף המידע המועבר למבחן מידתיות. כן יש לקבוע כללים בנוגע להחזקת המידע, אבטחתו וביעורו. יש לצמצם את העברת "מידע מוגן פרטיות" לגוף מיוחד לסוגי מידע מסוימים בנסיבות ובתנאים ברורים הקבועים בחוק. יש להבטיח שהעברת מידע מארגון לרשות ציבורית, לארגון אחר או לגוף מיוחד תיעשה אך ורק לצורכי הגנת סייבר אצל מקבל המידע.

(ד) יש לקבוע אמות מידה ברורות לאפקטיביות הנדרשת מרשות מאסדרת בכל הקשור להגנת הסייבר, כדי להבטיח שקיפות מלאה ובחינה ציבורית של החלטת ראש הממשלה להוסיף מגזר משקי כלשהו לרגולציית ציווי ושליטה ריכוזית של מערך הסייבר עקב חוסר אפקטיביות של הרשות המאסדרת שלה הוא כפוף.[545]

(ה) יש לצמצם את סמכות הניטור בתזכיר חוק הסייבר באמצעות:

543 לפי סעיף 62 לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

544 **שם**, בסעיף 57 לחוק המוצע בתזכיר חוק הסייבר.

545 **שם**.

i הגדרה ברורה של ה"מידע" שהמערך מוסמך לאסוף ושל ה"עיבוד" שהוא מוסמך לבצע.

ii קביעה בגוף החוק הוראות בדבר שמירת המידע הנאסף במסגרת הניטור, השימוש בו, ביעורו ומחיקתו אם ארגון חוזר בו מהסכמתו לניטור.

(ו) יש לבטל את הסמכות השיוריות הנתונה למערך הסייבר "לבצע כל תפקיד אחר בתחום הגנת הסייבר שיקבע ראש הממשלה".[546] כפי שנוכחנו לדעת בתחילת משבר הקורונה, קיומה של סמכות שיורית עלול לאפשר שימוש בסמכויות המערך שלא למטרה שלשמה הוענקו מלכתחילה, בדומה לשימוש שנעשה ביכולות השב"כ באמצעות פרשנות מרחיבה שניתנה לסעיף 7(6)(ב) לחוק שירות הביטחון הכללי.[547]

(ז) יש לקבוע בחוק את תנאי הכשירות לתפקיד עובד במערך, לתפקיד ראש המערך ולתפקיד עובד בכיר וגורם אחראי, וכן לפרט בחוק את הסמכות הנתונה לראש המערך, לעובד בכיר ולגורמים הממנים את העובד הבכיר. תזכיר הוראת השעה משפר במעט היבט זה אך חסר הוראות רלוונטיות ל"עובד בכיר" ול"גורם אחראי".

(ח) באשר לסמכות לבצע פעולות במערכות מחשב של ארגון לשם טיפול בתקיפת סייבר:

i יש לשנות את ברירת המחדל לדיון בדלתיים פתוחות בכל דיון בצו לביצוע פעולות במערכות מחשב של ארגון המתבקש להסכים לכך על ידי מערך הסייבר, אלא אם בית המשפט מקבל את בקשת המערך לקיים דיון בדלתיים סגורות.

ii הסמכות לבצע בדיקה מדגמית אינה ברורה. מוצע להבהיר מי הם הארגונים או סוגי הארגונים שסמכות זו תחול עליהם. אין הצדקה להתיר סמכות לביצוע בדיקה מדגמית בכל ארגון, ללא קשר לתחום פעילותו ולסכנה הנשקפת לאינטרס הציבורי מתקיפתו.

546 **שם**, בסעיף 3(6) לחוק המוצע בתזכיר חוק הסייבר.

547 בג"ץ 2109/20 **בן מאיר נ' ראש הממשלה** (26.4.2020).

iii המנגנון של ביצוע פעולות בהסכמת הארגון הוא מנגנון בעייתי בעיקר נוכח פערי הכוחות בין המערך לארגון ובהתחשב בנסיבות מתן ההסכמה – כאשר הארגון נתון תחת תקיפת סייבר ובסכנה ליצירת "דלת אחורית". לפיכך, לדעתנו

א אין להסתפק רק בכך שההסכמה ניתנת לאחר קבלת הסבר מעובד בכיר בארגון, אלא יש לקבוע בחוק כי המערך רשאי להעדיף קבלת הסכמה מארגון על פני פנייה לקבלת צו בית משפט רק במקרים שבהם קוצר הזמן, חשש מפגיעה חמורה באינטרס חיוני או מידת שיתוף הפעולה של הארגון מצדיקים בחירה באפיק זה, ובלבד שהפגיעה בזכות לפרטיות של לקוחותיו היא מידתית.

ב יש לדווח אחת לשלושה חודשים לוועדה האחראית בכנסת על ביצוע פעולות בהסכמת הארגון ונסיבותיהן.

ג יש לפרסם לציבור אחת לחצי שנה את שמות הארגונים והנסיבות שבהן בוצעו פעולות בהסכמה.

ד יש להגביל את הסמכות לקבלת מידע מספק גישה לאינטרנט או מעובד השב"כ לפי תזכיר הוראת השעה. לא ברור מדוע מערך הסייבר זכאי להתייחסות מיוחדת לעומת רשויות חקירה אחרות, הנדרשות לפנות לקבלת צו מבית המשפט לפי חוק נתוני תקשורת גם במקרים של עבירות מסוג פשע. חוק נתוני תקשורת אף כולל מנגנון לקבלת הפרטים גם כאשר הזמן דוחק.[548] יש לאמץ מנגנון דומה גם בנוגע למערך הסייבר, ואין סיבה להתיר למערך הסייבר לפנות ללא צו לספק האינטרנט לשם קבלת מידע, או חמור מכך – לפנות לשב"כ.

(**7**) לעבות את מנגנוני הפיקוח על המערך:

(א) מפקח פרטיות פנימי:

i לבד מדרישות החיסיון הביטחוני, תנאי הכשירות לתפקיד ממונה על הגנת הפרטיות במערך צריכים להיקבע בידי רשם מאגרי המידע בלבד ללא התייעצות עם ראש המערך.

ii יש להבטיח את עצמאותו של מפקח הפרטיות הפנימי באמצעות הוספת הבהרה בחוק שלפיה הוא לא יהיה נתון לכל מרות זולת מרות החוק ויפעיל שיקול דעת עצמאי.

548 חוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת).

(ב) הוועדה המפקחת:

i יש להבהיר מהן דרישות הכשירות מהשופט הממונה ליו"ר הוועדה.

ii יש להגדיל את תדירות הגשת דוח מטעם הוועדה ולהעמידה על דיווח אחת ל־3 חודשים.

iii יש להטיל חובה על ראש המערך לפעול לתיקון הליקויים העולים מדוח הוועדה, אם הוועדה הצביעה על כאלו, עד להגשת הדוח הבא.

iv ההוראה שלפיה על הוועדה לחדול מטיפול בעניינו של אדם שהיא חוששת שהפר את הדין ולהעביר את הטיפול לגביו לגורם מוסמך אינה ברורה. יש להבהיר כי במקרה כזה על הוועדה לדווח על הפרת החוק ליועץ המשפטי של מערך הסייבר.

(ג) יש לתקן את חובת העיצוב לפרטיות ולהבטיח שתכלול גם חובה להטמיע אמצעים ארגוניים למזעור הפגיעה בזכות לפרטיות.

(ד) יש לצמצם את הנסיבות שבהן תותר הפרת חובת הסודיות המוטלת על ראש המערך ועובדיו לגבי מידע שהם אוספים מארגון.

(ה) חובת הסודיות המוטלת על ארגון בנוגע להוראות שמקבל מהמערך בעייתית. יש להתוות מנגנון אשר יבטיח שקיפות בפני הציבור, הוועדה המפקחת והוועדה האחראית בכנסת בכל הנוגע לפעולות המערך, להוראות שהוא נותן לארגונים ולזהות הארגונים המקבלים את הוראותיו, באופן שיבטיח שמירה על סודיות שיטות העבודה של הארגון לצד פיקוח אפקטיבי על פעולות המערך.

(ו) יש להוסיף הוראות מעודכנות בדבר מפקח פרטיות פנימי, ועדה מפקחת, חובת עיצוב לפרטיות וחובת סודיות גם לתזכיר הוראת השעה.

(**8**) להגביל את הפטור מאחריות:

(א) יש להכפיף את סעיפי הפטור מאחריות אזרחית או פלילית המוענק והפטור מאחריות בגין פגיעה בפרטיות[549] למבחן מידתיות במקום למבחן הסבירות המוצע. יש להוסיף את דרישת המידתיות גם לפטור המוענק לארגון עקב פעולה

549 סעיפים 8 ו־65(ב) לחוק המוצע בתזכיר חוק הסייבר, **לעיל** ה"ש 343.

המיועדת ל"הגנת סייבר". כמו כן, לתנאים למתן פטור מאחריות בגין פגיעה בפרטיות יש להוסיף את דרישת תום הלב.

(ב) יש להבהיר את תחולת פטור "נמל הביטחון" בתזכיר חוק הסייבר,[550] כך שיחול אך ורק על מידע שבעל תפקיד או עובד בארגון מסר למערך בהסכמה ולא על זה הנקלט באופן אוטומטי במערך הניטור.

(ג) יש להכפיף את הפטור הניתן לארגון לשם שיתוף מידע[551] לדרישה שטרם שיתוף המידע יסיר הארגון מידע אישי מזהה או ניתן לזיהוי, או יטמיע טכנולוגיה להסרת מידע כאמור.[552]

(**9**) יש לקבוע בחוק חלוקת סמכויות ברורה בין מערך הסייבר לרשויות ביטחון אחרות, ובעיקר בינו לבין השב"כ: תזכיר חוק הסייבר ואף תזכיר הוראת השעה מציגים מצב מטריד של כפילות סמכויות ושיתוף משימות בין השב"כ ומערך הסייבר. כפי שהסברנו לעיל בסעיף ה.5 בפרק 3, יש צורך אקוטי בהטמעת עקרונות של שיתוף ושל שקיפות כדי לייצר מערך פיקוח והנחיה מיטבי. לתפיסתנו, מערך כזה לא יוכל להתקיים במסגרת המתווה הנוכחי. לדעתנו חובה לבצע חלוקת סמכויות ברורה ולהגדיר את הנסיבות שבהן יוסמך גוף אחד על פני גוף אחר.

550 **שם**, בסעיף 41(א) לחוק המוצע בתזכיר חוק הסייבר.

551 **שם**, בסעיף 65(א) לחוק המוצע בתזכיר חוק הסייבר.

552 בדומה לדרישה המופיעה בחוק המסדיר את פעילותה של CISA, וראו Cybersecurity and Infrastructure Security Agency Act of 2018, **לעיל** ה"ש 41, בסעיפים 104(d)(2)(A), (B).

THE ISRAEL
DEMOCRACY
INSTITUTE

Policy Paper 173

WHAT IS CYBER SECURITY?

Part Two
The Challenges of Regulating Cyber Protection

Rachel Aridor Hershkovitz | Tehilla Shwartz Altshuler

January 2023

Text Editor [Hebrwe]: Hamutal Lerner
Series and Cover Design: Studio Alfabees
Typesetting: Ronit Gilad, Jerusalem
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-411-1

No portion of this book may be reproduced, copied, photographed, recorded, translated, stored in a database, broadcast, or transmitted in any form or by any means, electronic, optical, mechanical, or otherwise. Commercial use in any form of the material contained in this book without the express written permission of the publisher is strictly forbidden.

Copyright © 2023 by the Israel Democracy Institute (RA)
Printed in Israel

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-888
Website: en.idi.org.il

To order books:
Online Book Store: en.idi.org.il/publications
E-mail: orders@idi.org.il
Tel: (972)-2-5300-800

The views expressed in this policy paper do not necessarily reflect those of the Israel Democracy Institute.

All IDI publications may be downloaded for free, in full or in part, from our website.

Abstract

The unique features of cyberspace, especially hyperconnectivity and the speed of information transfer, are at the heart of both the great benefits it brings to society and the huge dangers it poses. The tremendous damage liable to be caused by cyberattacks, combined with the absence of adequate incentives for investment in cyber protection, has created a market failure that justifies government intervention in the regulation of cyber security.

Government intervention in the regulation of cyber protection faces several challenges, however. Some of these are technological challenges related to asymmetries between attackers and defenders, and to the inability to fully assess the effectiveness of actions taken for cyber protection and determine the proper sequence of such actions. Others stem from the complexity of the cyber protection world, which requires the involvement of experts from other fields, such as economics, psychology, law, and sociology, alongside experts in technology. Moreover, cyber protection plans must be cross-sectoral, because the dangers of cyberspace are not unique to any particular sector or industry, and thus they require an all-

encompassing regulatory policy as well as an understanding of the unique characteristics of each sector. Furthermore, cyber protection requires digital literacy among cyberspace users and policymakers so that they can make considered, balanced decisions.

Another major challenge is the issue of the “state of many hats.” The state plays multiple roles regarding cyberspace, wearing different hats that sometimes conflict with each other: it owns critical infrastructure; it is responsible for national security and is therefore supposed to protect critical infrastructure; it acts as a regulator for private-sector entities that possess cyberinfrastructure and are responsible for protecting it; it plays an active role in public and private cooperative efforts for cyber protection; it acts on the international level with and against other countries in an effort to protect cyberspace, whose geographical boundaries are blurred; it is a producer and disseminator of knowledge and information regarding cyber protection; and finally, it can itself serve as a cyber attacker that poses threats to other states or organizations.

Western countries, including Israel, have been engaged for several years in attempts to regulate cyber protection. What these various attempts have in common is the recognition that the vital importance of cyberspace to the national economy and daily life, combined with the weaknesses of cyberspace, poses many dangers to the public sector, the private sector, and the populace as a whole. This understanding has led to the adoption of the conceptual approach underlying effective regulation of cyber protection: that responsibility is shared by all actors, and that the regulation of cyberspace should not apply only to critical infrastructure or focus solely on the public sector. At the same time, the scope of this responsibility, the type of regulation that is appropriate, and the regulatory tools chosen should be determined based on the anticipated level of risk to the public interest from a successful cyberattack against each actor or sector. This approach is similar to the principle of “common but differentiated responsibilities” that has become standard in international

law in the context of environmental protection and mitigation of climate-change harms.

This study surveys cyber protection policy in several countries: the United States, Australia, England, the European Union and two of its member states (Denmark and France), and Israel. The different countries employ a variety of regulatory tools to protect cyberspace: hard/centralized command-and-control regulation; soft/decentralized command-and-control regulation; collaborative regulation; and self-regulation. The degree of responsibility of each actor in cyberspace, and consequently the regulatory tool selected to regulate cyber protection, are determined according to an assessment of the risk to important national interests posed by a cyberattack on a particular organization or on organizations in a particular sector. Therefore, the definition of these important national interests is the key to understanding the scope of state intervention in the market in order to protect cyberspace.

Unsurprisingly, there is a correlation between the anticipated risk level to these defined national interests and the degree of state intervention in the free market, as manifested in the regulatory tool used: the greater the risk, the more the state tends to apply more "interventionist" regulatory tools. The clearest outcome of the assessment of risk to important national interests is the distinction customarily made in all countries between organizations that belong to critical infrastructure sectors and those that do not. The regulation of cyberspace in critical infrastructure sectors is different from regulation in other sectors.

"Important national interests" are defined differently in Israel than in the other countries surveyed in this study. This difference, which influences the choice of regulatory tools applied to organizations in different sectors, is expressed mainly in the scope of either hard/centralized or soft/decentralized command-and-control regulation.

In June 2018, the Cyber Law Memorandum was published, based on the idea that the regulation of cyber protection should be carried out by sectoral regulators using a combination of centralized and decentralized command-and-control regulatory tools, under the supervision of the Israel National Cyber Directorate. The Cyber Law Memorandum is a positive and appropriate step, given the need to provide a formal legal basis for the activity and powers of the National Cyber Directorate, which has been operating under the aegis of government resolutions for several years now.

In our opinion, however, the memorandum does not reflect the broad perspective required in view of the challenges of developing and implementing regulation of cyber protection. The regulation of cyber protection proposed in the memorandum is not based on genuine, in-depth cooperation with the private sector and academia, which is essential given the characteristics of cyberspace. The definition of important national interests as "vital interests" is too broad; it does not distinguish between a vital interest and a security target that must function properly in order to protect an important national interest. Consequently, the proposed scope of state regulation and government intervention in the free market is not at all clear, and is liable to be extremely broad.

We therefore recommend the following:

(**1**) Add to the law proposed in the Cyber Law Memorandum an objects clause that defines the boundaries of possible interpretation of the powers granted by the law to the National Cyber Directorate.

(**2**) Change the current model of "regulating the different regulators," and position the National Cyber Directorate as the sole regulator in charge of setting the rules and required standards for cyber protection. The regulatory tools to be used should be determined according to the specific features of each individual sector and the perceived level of risk to the public interest from a cyberattack against an organization in this sector.

(**3**) Ensure that oversight and enforcement powers are given to sectoral regulators that do not function as security organizations. Rather, these regulators should operate according to the rules of ordinary administrative law, including the requirement of government transparency.

(**4**) Civilianize the National Cyber Directorate, or at least apply to it principles of public law, and not only the judicial norms that customarily apply to secret security services.

(**5**) As much as possible, ensure that standards for cyber protection are set in conjunction with industry, academia, and the public so that they suit the characteristics of each sector.

(**6**) Reduce the powers of the National Cyber Directorate, including by redefining the terms “vital interest” and “information with security value”; defining the term “information processing”; setting clear criteria for the effectiveness required of regulatory agencies with respect to cyber protection; reducing surveillance powers; eliminating the Directorate’s residual powers; setting minimum qualifications for office holders in the Directorate, and clarifying the powers held by each; limiting authorization to obtain information from an internet service provider or from an employee of the Israel Security Agency (ISA; the “Shin Bet”) under the temporary order memorandum; reinforcing the mechanisms for oversight of the Directorate; and restricting the Directorate’s exemption from civil and criminal liability.

(**7**) Stipulate in the law a clear division of powers between the National Cyber Directorate and other security authorities, particularly the ISA.

דומה שאין צורך להסביר היום את עוצמת הנזקים של מתקפות סייבר. החל בפגיעה במערכות מחשוב של בתי חולים ועצירת טיפולים מצילי חיים, עובר במניעת הזרמת דלק לתחנות דלק וכשלים במערכות החשמל והמים, וכלה בדלף של מידע רגיש ואינטימי או חסימת גישה למערכות מחשב בעסקים קטנים. התגברות מתקפות הסייבר נובעת מכשלי שוק היוצרים הגנת סייבר חסרה. כשלים אלה מצדיקים התערבות של המדינה לשם אסדרת ההגנה על מרחב הסייבר. אסדרה כזאת בישראל מחייבת למידה מניסיונן של מדינות אחרות וכן התמודדות עם אתגרים טכנולוגיים ועם הצורך באוריינות דיגיטלית בקרב מקבלי ההחלטות. אתגר נוסף שיש צורך להתמודד עימו הוא ריבוי הכובעים של המדינה בבואה לאסדר את הגנת הסייבר: כובע של רגולטור, כובע של בעלים על תשתיות, כובע של שחקן במרחב הבינלאומי ועוד.

מדינת ישראל ניצבת לפני צורך דחוף לאסדר את הגנת מרחב הסייבר. מטרת המחקר המובא לפניכם היא לסייע ביצירת מסגרת לאסדרה כזאת. המחקר מצביע על הצורך בהגדרת האינטרסים הציבוריים הרלוונטיים ובאיזונים בינם לבין ערכים אחרים כמו הזכות לפרטיות; כן הוא מצביע על ההכרח ביצירת מתווים לחלוקת האחריות להגנת מרחב הסייבר בין השחקנים – גורמי הפיקוח, האחראים על תשתיות קריטיות במשק ועסקים פרטיים בגדלים משתנים.

ד"ר רחל ארידור הרשקוביץ היא חוקרת בתוכנית "דמוקרטיה בעידן המידע" של המכון הישראלי לדמוקרטיה. עבודת הדוקטור שלה עסקה במסגרות לשיתופי פעולה בין הממשל לתעשייה לשם הגברת ההגנה על מרחב הסייבר. מומחית למשפט וטכנולוגיה, בדגש על הזכות לפרטיות.

ד"ר תהילה שוורץ אלטשולר היא עמיתה בכירה במכון הישראלי לדמוקרטיה וראשת התוכנית "דמוקרטיה בעידן המידע". חברת מועצת הארכיונים העליונה ולשעבר חברת נשיאות מועצת העיתונות. עמיתת מחקר בכירה במרכז פדרמן למשפט וסייבר באוניברסיטה העברית בירושלים. מומחית לאסדרת תקשורת ואתיקה עיתונאית ולממשק שבין טכנולוגיה, משפט ומדיניות.

מחיר מומלץ: 45₪
ינואר 2023

מסת"ב:
978–965–519–411–1

0 4500001269 1
דאנאקוד 450-1269

www.idi.org.il