רגולציה במרחב הסייבר

גבי סיבוני ועידו סיון־סביליה

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

מזכר
180

רגולציה במרחב הסייבר

גבי סיבוני ועידו סיון־סביליה

המכון למחקרי ביטחון לאומי

המכון למחקרי ביטחון לאומי, המשלב בתוכו את מרכז יפה למחקרים אסטרטגיים, הוקם בשנת 2006. למכון שתי מטרות מוצהרות: הראשונה היא לערוך מחקרים בסיסיים בנושאי הביטחון הלאומי של ישראל, המזרח התיכון והמערכת הבינלאומית, וזאת על פי אמות המידה האקדמיות הגבוהות ביותר, והשנייה – לתרום לדיון הציבורי ולעבודת הממשל בנושאים שנמצאים, או ראוי שיימצאו, בראש סדר היום הביטחוני של ישראל.

קהל המטרה של המכון הוא דרג מקבלי ההחלטות, מערכת הביטחון, מעצבי דעת הקהל בישראל, הקהילה האקדמית העוסקת בתחומי הביטחון בישראל ובעולם, והציבור המתעניין באשר הוא.

המכון מפרסם מחקרים שהוא מצא כראויים לתשומת הלב הציבורית, תוך שמירה על מדיניות נוקשה של אי משוא פנים. הדעות המובעות בפרסומים הן של המחברים בלבד, ואינן משקפות בהכרח את עמדות המכון, נאמניו או האישים והגופים התומכים בו.

רגולציה במרחב הסייבר

גבי סיבוני ועידו סיון־סביליה

מזכר 180 אוגוסט 2018

המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

Cyber Regulation

Gabi Siboni and Ido Sivan-Sevilla

המכון למחקרי ביטחון לאומי (חברה לתועלת הציבור - חל"ץ)

חיים לבנון 40
ת.ד. 39950
רמת־אביב
תל־אביב 6997556

דוא"ל: info@inss.org.il
אתר המכון: http://www.inss.org.il/he

ISBN: 978-965-92670-3-3

עורך עברית: אריה אידן
הביא לדפוס: משה גרונדמן

עיצוב גרפי: מיכל סמו קובץ ויעל ביבר, המשרד לעיצוב גרפי, אוניברסיטת תל אביב

תוכן העניינים

תודות

ראשית אנו מבקשים להודות לאלוף (מיל') עמוס ידלין, ראש המכון למחקרי ביטחון לאומי, על הערותיו המועילות. כמו כן, אנו מבקשים להודות לחוקרי המכון שהאירו והעירו לנו הערות בונות ומלמדות במהלך הכתיבה ותהליך הבקרה על חיבור זה: ד"ר ענת קורץ ותא"ל (מיל') שלמה ברום. תודה גם לחוקרים הדס קליין ודודי סימן־טוב על התייחסותם למגוון הנושאים בהם מטפל החיבור. תודות רבות גם לג'ודי רוזן ולמשה גרונדמן על הערותיהם ופעילותם להוצאתו לאור.

תודה למרואיינים הרבים שסייעו בהבנת המורכבות של מאמצי הרגולציה במרחב הסייבר. להלן רשימה חלקית של אלה מביניהם שניתן לזהותם בשמם: גדעון קונפינו, ראש היחידה להגנת הסייבר ברשות התקשוב הממשלתית (יה"ב), אבירם עצבה ויובל שגב ממערך הסייבר הלאומי, לימור שמרלינג מהרשות להגנת הפרטיות, ניר הלר מהממונה על הביטחון במשרד הביטחון (מלמ"ב), נתן הרשקוביץ, מנהל מחלקת מערכות מידע ברשות לניירות ערך, רחל יעקבי, הממונה על הטכנולוגיה והסייבר בפיקוח על הבנקים בבנק ישראל, ושלמה הר־נוי, מנכ"ל קבוצת "שדמה" העובדת עם משרד האנרגיה.

בנוסף, אנו מבקשים להודות למתמחים שסייעו בניתוח ובאיסוף המידע לחיבור זה: בנג'מין גו מאוניברסיטת הרוורד, דוד פוטשר מאוניברסיטת תל אביב ואוניברסיטת אוסטין בארה"ב וסנג'אנה ראטי מ־London School of Economics (LSE).

לבסוף נודה לחברי פורום הסייבר במכון למחקרי ביטחון לאומי על העצות במעלה הדרך, החיבור לשטח ושיתוף הידע.

גבי סיבוני, עידו סיון־סביליה
אוגוסט 2018

תקציר מנהלים

רגולציה במרחב הסייבר היא אתגר הנמצא בהתהוות. מדובר במרחב מורכב ודינמי הנשען ברובו על המגזר העיסקי־אזרחי והינו בעל פוטנציאל לגרימת נזק רב לביטחון הלאומי. חיבור זה סוקר את המאפיינים הייחודיים למרחב הסייבר, מתחקה אחר האסטרטגיות השונות בעולם לניהול סיכונים במרחב זה, ומציע מודל רגולטורי רב־שכבתי יחד עם המלצות קונקרטיות לאסדרה (רגולציה) של המגזר העיסקי־אזרחי במרחב הסייבר.

חוסנו של המגזר הפרטי במרחב הסייבר קשור ישירות לביטחון הלאומי. מגזר זה מהווה לרוב את החוליה החלשה דרכה מתפתחת מתקפה קיברנטית. אף על פי כן, סקירת הרגולציה במרחב הסייבר במדינות מערביות, ובכללן ישראל, מצביעה על היעדר מענה הולם לחולשה זו של המגזר העיסקי־אזרחי. החיבור הנוכחי שואף למלא חלל זה ונשען, לשם כך, על עקרונות רגולטוריים ממדינות שונות – ארצות הברית, בריטניה, צרפת, גרמניה וכן האיחוד האירופי – ועל למידה מתחומי רגולציה אחרים, העוסקים בהגנת הסביבה והאנרגיה הגרעינית. הגישה, הכלים הרגולטוריים ומערכות התמריצים בניסיונות האסדרה של מרחב הסייבר בעולם, יחד עם שיתופי הפעולה בין המגזר הציבורי למגזר הפרטי, בתוספת מגנוני פיצוי מדינתיים בתחומי הגנת הסביבה והאנרגיה הגרעינית, תורמים לפיתוחו של מודל רגולטורי חדש לאסדרת מרחב הסייבר במגזר העיסקי־אזרחי במדינת ישראל.

המודל המוצע במחקר זה מוצג יחד עם המלצות מעשיות ליישומו. המודל מתחלק לשלושה: רגולציה עצמית – בה ארגונים משיתים הסדרי פעולה על עצמם; רגולציה מחייבת – בה המדינה כופה הסדרים מלמעלה; ו – רגולציה מבוססת תמריצים – בה המדינה יוצרת תמריצים עבור ארגונים כדי שיאמצו רגולציה עצמית. אחד החידושים של המודל נוגע לשימוש בכלי הסטטוטורי הקיים של חוק רישוי עסקים לצורך מיפוי פוטנציאל הנזקים לביטחון הלאומי כתוצאה מפגיעות סייבר במגזר העיסקי. חידוש נוסף במודל הוא המיפוי וההתמקדות בצמתים מרכזיים במשק הסייבר הישראלי ובחינת האפשרות להתערבות מדינתית בה התועלת ממנה עולה עשרות מונים על העלות. חידוש שלישי הוא ההתבססות על מנגנוני תמריצים עבור המשק על ידי הקמת

שוק ביטוח סייבר, הסרת חסמי שקיפות על אירועי סייבר, הקלות מס למטמיעי הגנת סייבר ומתן תמריצים בצורת פטור מאחריות עבור שיתוף ידע פנים־מגזרי ובין־מגזרי.

תובנות מסקירת הספרות

התובנות העיקריות מסקירת הספרות העוסקת ברגולציה בסייבר מלמדות על השונות הגדולה באסדרת מרחב הסייבר במדינות השונות. העיסוק של מדינות במרחב הסייבר מתחיל בנקודות שונות בזמן ומתרכז סביב איומים על הביטחון הלאומי כמו פגיעה בתשתיות קריטיות, או בהתגוננות מפני פשיעת סייבר. כל המדינות משקיעות תקציבים משמעותיים בהגנת הסייבר, המיועדים לבניית יכולת מדינתית ומוסדות לפיקוח והשפעה על הנעשה במשק הסייבר המקומי, ובכלל זה על מרחבי האיום השונים שלו. זאת מתוך תפיסה כי הערכת הסיכון (Risk Assessment) בתחום הסייבר היא אחד התפקידים המאתגרים של הרגולטור, וכן מתוך שאיפה ליצור הבנה רחבה ככל שניתן על הנעשה במרחב זה. יחד עם זאת, ועל אף ההשקעה התקציבית ובניית היכולות המדינתיות להתמודד עם סיכונים בתחום הסייבר, בולט בהיעדרו הטיפול המדינתי בסיכונים אלו במגזר העיסקי־אזרחי. אין כיום מדינה המנחה באופן שיטתי את המגזר העיסקי־אזרחי ומתייחסת מבעוד מועד לאיומי ביטחון לאומי כתוצאה מנזקי סייבר פוטנציאליים במגזר זה.

הגישה הישראלית כלפי איומי הסייבר במגזר העיסקי־אזרחי חדשנית ומסועפת למדי. הנחיית המגזר נתונה בידי רגולטורים שונים ומפוקחת לעיתים ישירות על ידי המשרד הממשלתי האחראי (כמו בתחום הבריאות), הרשות המדינתית הרלוונטית (למשל, המפקח על הבנקים), או ארגון פרטי המועסק על ידי המדינה כמתווך רגולטורי בעל מומחיות בתחום (לדוגמה, בתחום האנרגיה). בשנתיים האחרונות נעשים ניסיונות למרכז את תהליך קבלת ההחלטות בתחום הסייבר בכלל המשק, כאשר חוק הסייבר, הנמצא עדיין בדיונים, שואף להיות מסגרת מנחה סדורה לארגונים נבחרים במשק. אף על פי כן, גם התפתחות זו טרם יצרה תהליך שיטתי וסדור לזיהוי מבעוד מועד של פוטנציאל הנזק שהתקפות סייבר עלולות לגרום לביטחון הלאומי.

היעדר מענה גורף עבור התמודדות המגזר העיסקי־אזרחי עם האיומים המתרבים בתחום הסייבר וההתמקדות הנוכחית במתן תמריצים נקודתיים בלבד, יוצרים פער משמעותי בתחום זה. ממעקב אחר הפעילות במשק בשנים האחרונות עולה כי השוק התחרותי מתגמל חברות על חדשנות בטכנולוגיה, הרבה יותר מתגמוליו על הגנת סייבר ראויה. משום כך, חברות עיסקיות אינן משקיעות דיו כדי ליצור הגנה מקיפה על עצמן. בהיעדר הנחייה מדינתית סדורה בנושא זה, נוצר חלל אותו יש למלא.

כדי ללמוד על האופן בו מדינות התמודדו בהצלחה עם אתגרי הסייבר במגזר העיסקי־אזרחי, פנו כותבי חיבור זה ללמוד מעולמות תוכן אחרים. ההנחה היא

שבחינה וניתוח של הנעשה בתחומי הגנת הסביבה והאנרגיה הגרעינית – תחומים בהם שחקנים פרטיים מהווים נתח משמעותי, וברוב המקרים מרכיבים את "קו ההגנה הקדמי" של המדינה מפני סיכונים – עשויים לסייע בפיתוח מודל משוכלל להגנת סייבר במגזר העיסקי־אזרחי גם בישראל. ניתוח המודלים השונים הוביל למסקנה כי מודל הרגולציה להגנת הסביבה בישראל מתאים לשמש כבסיס לפיתוח הרגולציה במרחב הסייבר הישראלי.

מודל רגולציה מוצע

האיומים המתקדמים יוצרים צורך מיידי בהתערבות מדינתית "חכמה" שתשלב כלים רגולטוריים מגוונים. זאת הן כדי לחייב נקיטת אמצעי הגנה ראויים ומידתיים, והן כדי לעודד את השוק להגן על עצמו באמצעות תמריצים, תוך זיהוי מקומות התערבות מרכזיים שהתועלת בהגנתם עולה על העלות.

המודל המוצע לרגולציה במרחב הסייבר הינו מודל המתבסס על הקיים, אך גם מחדש ומוסיף עליו. הוא עושה הבחנה בין רגולציה עצמית, הנחיות מדינתיות מחייבות ורגולציה וולונטרית מבוססת תמריצים, כמפורט להלן:

1. **רגולציה עצמית** – ארגוני ביטחון בעלי רגישות ביטחונית, כגון צה"ל, השב"כ, המוסד ומשטרת ישראל, יהיו כפופים להנחיות פנימיות בלבד, אשר יתוקפו באופן מחזורי על ידי מנגנוני ניהול הסיכונים של כל ארגון.
2. **רגולציה מחייבת** – המדינה תפעיל רגולציה מחייבת על גופים אשר פגיעה בתשתיות הסייבר שלהם משמעותה פגיעה חמורה בביטחון הלאומי של ישראל.
3. **רגולציה מבוססת תמריצים** – הבניית תמריצים מדינתיים שתפקידם יהיה לעודד הקמת מנגנונים להגנת סייבר בתוך ארגונים. רגולציה זו תהיה מבוססת, בין היתר, על עידוד עסקים לרכוש ביטוח לשיפוי במקרה של אירוע סייבר, על בסיס חובת דיווח על אירועים כאלה. בנוסף לכך, ייבחנו מודלים שונים למתן הקלות מס, בכפוף להשקעות הארגון בהגנת סייבר, וייעשו מאמצים לפתח מנגנוני שיתוף ידע לצורך הגנת סייבר במטרה להגביר את החוסן הכולל במרחב הקיברנטי.

הגופים עליהם תחול **הרגולציה המחייבת** יחולקו למגזרים על פי חמש הקטגוריות הבאות:

1. **תעשיות ביטחוניות ומתקנים רגישים** – אלה יפוקחו על ידי הממונה על הביטחון במשרד הביטחון (המלמ"ב). הנחיות המלמ"ב מיועדות לשמירת הסודיות בעבודתם של גופי הביטחון הכפופים להן. ראוי לציין בהקשר זה כי הרגולציה של המלמ"ב כוללת הן הנחיות ביטחוניות במרחב הסייבר עבור הגופים המפוקחים והן אסְדרה רגולטורית, כלומר הן דאגה לביטחון המדינה והן דאגה לרציפות התפקודית של הגוף המפוקח.

2. **גופים המוגדרים כתשתית קריטית** – הפיקוח עליהם יבוצע כפי שהוא נעשה היום – הן על ידי מערך הסייבר הלאומי והן על ידי שירות הביטחון הכללי. ועדת היגוי, אשר תורכב מנציגים של השב"כ, מערך הסייבר הלאומי, משרדי התשתיות הממשלתיים וחברות פרטיות העוסקות בהגנה על תשתיות קריטיות, תבחן ותגדיר מחדש לפי הצורך את התשתיות הקריטיות, ואלו יעמדו בתקנים מחמירים, כולל בדיקות חדירות תקופתיות בהתאם לתחום העיסוק. ועדת ההיגוי גם תבחן באופן תקופתי את האפשרות להכניס גופים חדשים למסגרת ההנחיות המחייבות או להסיר מהן גופים קיימים. מערך הסייבר הלאומי ייצר ידע ומומחיות, בשיתוף עם השב"כ, במטרה להגן על ארגוני תשתית קריטית.
3. **מגזרי משק החיוניים לרציפות התפקודית בישראל** – בנוסף על גופים המוגדרים כתשתית קריטית, קיימים מערכות וגופים רבים שחשיבותם לביטחון הלאומי היא עליונה, אך טרם הוגדרו כקריטיים על יד המדינה. כך, למשל, בתי חולים, מערכות רמזורים, מערכות בחירות, בנקים ותעשיות המזון אינם נכללים בהגדרה הקיימת של "תשתית קריטית." לפיכך, על הרגולטור המגזרי בכל אחד מהתחומים לגבש מומחיות ולהנחות את הגופים הנמצאים תחת אחריותו כיצד להתמודד עם איומי סייבר, וזאת כדי למנוע פגיעה בביטחון הלאומי של מדינת ישראל. המודל המוצע ממליץ להמשיך ולהסתמך על רגולטורים מגזריים הפועלים מול גופים בעלי פוטנציאל נזק לביטחון הלאומי. המודל גם מצדד בהישענות הרגולטור המגזרי על מומחי תוכן שיפעלו בהנחיית מערך הסייבר הלאומי. בדרך זו יאפשר המודל הנחייה מקצועית של הגופים המשמעותיים לביטחון הלאומי, ובמקביל לה הנחייה מחייבת של הרגולטור המגזרי בתחומם של הגופים המפוקחים הנמצאים תחת אחריותו.
4. **המגזר העיסקי־אזרחי** – המודל המוצע מחייב לדרוש מכל גוף עיסקי המבקש לקבל או לחדש את רישיון העסק שלו לבצע תסקיר ובדיקת היתכנות לפגיעה בביטחון הלאומי כתוצאה מפגיעת סייבר. כך ייווצר תהליך מובנה שיאפשר שיפור משמעותי של הגנה במיזמים פרטיים החשופים לפגיעת סייבר, שהשפעתה עלולה להיות רחבה ולהגיע לרמה הלאומית. הרגולטורים בתחום הסייבר במגזר זה יהיו הן מערך הסייבר הלאומי, שתפקידו לפתח ידע, כלים ושיטות לאופן בו ארגונים יכולים להעלות את רמת הגנת הסייבר שלהם, והן הרגולטורים המגזריים, המפתחים מומחיות בהתאם לצרכים של המגזר הספציפי ומבצעים את ההתאמות הנדרשות הנובעות מההנחיות הכלליות של מערך הסייבר הלאומי. התהליך המוצע כולל שימוש בכלים סטטוטוריים קיימים והכנסת תחום הגנת הסייבר כמרכיב מובנה למגזר העיסקי, תוך שימוש בתהליך הסטטוטורי הקיים. הרגולטור יקבע אמות מידה שיגדירו את המיזמים והפרויקטים שלגביהם תתקיים חובת הגשה של תסקיר עמידות קיברנטית. כל גוף שיוגדר כחייב בכך יידרש להגיש תסקיר כזה

לפני קבלת רשיון עסק. המודל גם מציע מספר קווים מנחים לתוכנו של תסקיר עמידות קיברנטית, כמו גם לגורמים שיוסמכו לערוך אותו ולהגישו, וכן לגורמים שיוסמכו לבדוק אותו.

5. **הגברת חוסנו של מרחב הסייבר דרך התערבות בצומתי מפתח** – רגולציה מחייבת על פי המודל המוצע תחול גם על צמתים חשובים שהתערבות מדינתית בהגנתם תביא תועלת רבה בעלות נמוכה. הרציונל מאחורי קביעת צמתים אלה הוא היותם נקודות מפתח קריטיות שהתועלת לביטחון הלאומי שתנבע מהפיקוח עליהן הינה גדולה. חשוב להדגיש כי המדינה לא תהיה זרוע ביצועית מול צמתים אלה וכי תפקידה יסתכם במיפוי הצמתים ובשיתוף פעולה עם הספקים הרלוונטיים במטרה לעודד את אבטחתם ולהגביר בכך את חוסנו של מרחב הסייבר הישראלי. דוגמאות לצמתים כאלה הם מארחי שרתי האינטרנט (ספקי Hosting), ספקי שירות רוחביים בשרשרת האספקה של ארגונים במשק, יישומים ומערכות מידע אחודות המנהלות סליקות של כרטיסי אשראי עליהם נשענים מרבית העסקים הפרטיים, וכן חברות אינטגרציה העוסקות בתמיכה במערכות מידע. לאחר זיהוי הצמתים, על המדינה יהיה להעסיק ספקי צד שלישי, שיהיו אחראים על בקרת האיכות של נותני שירותים קריטיים אלה.

המלצות ליישום

להלן סדרה של המלצות עיקריות שיסייעו למימוש המודל הרגולטורי המוצע:

1. בחינת הצורך להקים גוף ביקורת מקצועי ועצמאי במערך הסייבר הלאומי, שיפעל מול גופים, ארגונים ומוסדות המפעילים רגולציה עצמית (ארגוני הביטחון, צה"ל, משטרת ישראל וכדומה).
2. גיבוש פורום ביחידה להגנת הסייבר בממשלה (יה"ב), אשר יאפשר קבלת תמונה רוחבית על הטכניקות הרגולטוריות באמצעותן בוחרים משרדי הממשלה והרשויות להגן על המגזרים השונים הנמצאים בתחום אחריותם לצורך למידה והשתפרות.
3. הגברת האכיפה של משרד הכלכלה לצורך שיפור הציות לחוק רישוי עסקים.
4. הקמת זרוע ביצועית במערך הסייבר הלאומי לפיקוח על תסקירי העמידות הקיברנטית במשק.
5. קידום תקינת מקצועות הסייבר, בין השאר במטרה לקבוע תקנים עבור מבדקי איכות ההגנה בסייבר ועריכת תסקירים במשק.
6. הקמת פורום משותף למערך הסייבר הלאומי, ליחידה להגנת הסייבר בממשלה ולמובילים טכנולוגיים במשק לצורך זיהוי, ניתוח והגנה על צמתים חיוניים ומרכזיים במרחב הסייבר, מתוך רצון לחזק את החוסן הלאומי.

7. קידום חוק שיחייב את כלל הארגונים במשק לדווח על תקיפת סייבר ארגונית "משמעותית". זאת, כדי ליצור מוטיבציה להגנה מבעוד מועד, וכן כדי לאפשר הקמת מאגר מידע אקטוארי לחברות הביטוח, באופן שיעודד אותן לפתח שוק ביטוח לפוליסות הגנה בסייבר.
8. הקצאת תקציב ממשלתי ייעודי עבור הרשות לשוק ההון, ביטוח וחיסכון, במטרה ליצור ערבות מדינתית לחברות הביטוח במקרה של אירוע סייבר רחב היקף.
9. בחינת אפשרות שהממשלה תיתן הקלות מס עבור הטמעת הגנת סייבר ברמה ראויה.
10. הקמת יחידת סייבר ייעודית ברשות המיסים, שתשקול מתן הקלות מס במקרה של הטמעת הגנת סייבר ראויה.
11. קידום חקיקה שתיתן פטור מאחריות במקרה של פגיעת סייבר כתוצאה משיתוף ידע בין־ארגוני על איומים במרחב הסייבר.

בסיכום החיבור מובאות תובנות ממאמצי הרגולציה במרחב הסייבר ומוצגים האתגרים להמשך. התפתחות איום הייחוס מהתקנים מקושרים[1] ושימוש בבינה מלאכותית לצורכי תקיפה, מחדדים את הצורך במודל רגולטורי רב־שכבתי עבור המגזר העיסקי־אזרחי, באופן הצופה אתגרים עתידיים.

1 התקנים מקושרים הינם התקני חומרה ביתיים ותעשייתיים, כגון מצלמות אבטחה וטרמוסטטים, אשר השתדרגו ביכולת קישוריות דרך רשת האינטרנט. משמעות הדבר היא שמרחב הסייבר כולל לא רק מחשבים ומערכות מידע, אלא גם התקנים "פשוטים" יותר, אשר שולחים מידע וניתנים לשליטה מרחוק.

הקדמה

אתגר הגנת הסייבר חוצה תחומים, מגזרים וגישות. למידת האופן בו על המדינה להתערב כדי להבטיח את חוסנו של מרחב הסייבר ולמנוע פגיעה ברצף התפקודי ובביטחון הלאומי מורכבת מרבדים רבים וחושפת אינטרסים וכוחות הפועלים בכיוונים מנוגדים ומשלימים.

חיבור זה מציג את עמודי התווך של הבעיה, סוקר את הרקע וההתפתחות ההיסטורית של הרגולציה במרחב הסייבר במדינות מרכזיות בעולם המערבי, ומציע מודל משולב לחלופה רגולטורית מדינתית שתאפשר חיזוק הביטחון הלאומי במרחב הסייבר.

מדינות שונות ברחבי העולם משתמשות בכלים מגוונים להגנה בסייבר, המשלבים בין רגולציה מחייבת לרגולציה המעודדת שיתוף פעולה בין המגזרים הפרטי והציבורי. לעומת זאת, המגזר העיסקי־אזרחי נותר ברובו ללא מענה שיטתי במרחב זה ומגן על עצמו על פי שיקול הדעת והאינטרסים העיסקיים של כל ארגון. מצב זה מהווה סיכון ראשון במעלה לביטחון הלאומי. חולשתו של המגזר העיסקי־אזרחי כמרחב ללא גבולות טריטוריאליים מהווה כר פורה לתוקפים, המאפשר גישה למערכות ביטחוניות, לשירותים עיסקיים ולמידע אישי למכביר.

החיבור שלהלן בא לגשר על אתגר כבד זה הניצב בפני הביטחון הלאומי ועושה זאת על בסיס למידת המתרחש בעולם בתחום הגנת הסייבר ובתחומי רגולציה אחרים, כמו הגנת הסביבה והאנרגיה הגרעינית. החיבור מציע מסגרת מושגית ומודל רגולטורי חדש להגברת חוסנו של מרחב הסייבר בישראל, וכפועל יוצא מכך – של הביטחון הלאומי. המודל המוצע יכול להיות מאומץ גם על ידי מדינות נוספות המתמודדות עם אתגרים דומים לאלו של ישראל.

שאלות המחקר בהן עוסק חיבור זה הן:

1. מהם החוקים והמוסדות המאורגנים עליהם מבוססים מאמציה של מדינת ישראל בתחום הגנת הסייבר?
2. כיצד מבצעות מדינות בעולם המערבי רגולציה להגנת סייבר בכלל ובמגזר העיסקי־אזרחי בפרט?
3. מה ניתן ללמוד מהרגולציה של הגנת הסביבה והאנרגיה הגרעינית עבור הרגולציה של המגזר העיסקי־אזרחי בתחום הגנת הסייבר?

4. מהו המודל האפשרי לרגולציית הגנה בסייבר עבור המגזר העיסקי־אזרחי במדינת ישראל?

הדרכים לבחינת שאלות המחקר הינן, בראש ובראשונה, איסוף שיטתי של מסמכי מדיניות – חוקים, תקנות משנה, הנחיות רגולטוריות והוראות שעה – העוסקים בהגנת סייבר ובהגנת מידע, החל משנות התשעים של המאה העשרים ועד שנת 2017, וזאת בישראל, בארצות הברית, באיחוד האירופי, בבריטניה, בצרפת ובגרמניה. לאחר מיפוי המהלכים שננקטו בכל אחת מהמדינות, ממפה החיבור את הנעשה בתחום זה בישראל, וסוקר מודלים נוספים של רגולציה – בתחומי הגנת הסביבה והאנרגיה הגרעינית. זאת, מתוך ניסיון לאמץ, לפחות חלקית, מודלים רגולטוריים הפועלים באופן מוצלח במגזר העיסקי־אזרחי לצורך רגולציה בסייבר. פיתוח המודל המוצע בחיבור זה מתבסס על הידע שנצבר ועל ראיונות עם מקבלי החלטות בישראל, והוא נועד ליצור חלופה רגולטורית שתשרת נאמנה את הביטחון הלאומי של מדינת ישראל ואזרחיה.

קשיי המחקר נובעים בעיקרם מהצורך ללמוד מרחב שבו האיומים משתנים באופן תדיר וקצב ההתפתחויות בו גובר לרוב על מהירות התגובה של הליך המדיניות הציבורית. טכנולוגיות התקיפה וההגנה בסייבר מתפתחות בקצב מואץ, וגם המרחב עצמו מתרחב אל עבר שדה ההתקנים המקושרים. לעומת זאת, האסדרה המדינתית של מרחב הסייבר נשענת על מוסדות רגולטוריים ומקבלי החלטות שפועלים לרוב באופן שאינו עולה בקנה אחד עם ההתפתחות הטכנולוגית המואצת. קושי נוסף הוא האתגר שביצירת מודל רגולטורי חדש, המתבסס מצד אחד על למידה מהתמודדות של מדינות אחרות עם אתגרים מקבילים ועל תחומי רגולציה משדות אחרים, ומצד שני שואף להיות ישים עבור שחקנים רבים ככל האפשר במשק הישראלי. המעבר מהתיאוריה למעשה הינה אתגר בכל המלצה על מדיניות באשר היא, והדבר נכון שבעתיים בנושא הנדון בחיבור זה, שכן ישימות המודל צריכה להתבסס הן על הרגולטור והתכנות הביצוע אצל מקבלי ההחלטות והן על קבלה מצד נמעני הרגולציה – משוכה שלא תמיד ניתן לצפות את גובהה.

ההתמודדות עם קשיים אלה כרוכה בעדכון תדיר של סקירת המקורות והבאה בחשבון של כלל האתגרים עד לרגע האחרון. לפיכך, נוספו לסקירת הספרות גם תחומי ההתקנים המקושרים וסקירת שוק ביטוח הסייבר, בהם מתקיימת לאחרונה פעילות ענפה הן של המגזר העיסקי־אזרחי והן של רגולטורים שונים ברחבי העולם. בנוסף לכך, וכדי לגבש מודל ישים ברמה נאותה, נלקחו בחשבון הנחיות ותמריצים הקיימים במקומות אחרים, אשר יוצרים מודל שאינו מתמקד באכיפה נוקשה דרך פיקוד ושליטה של המדינה, אלא משלב שיח ומנגנונים לרגולציה עצמית של כלל המשק.

מכאן נובע גם חלק מחדשנותו של המחקר שמוצא את ביטויו בחיבור זה. עד היום לא נבנה מודל מקיף המשלב רגולציה מחייבת, רגולציה עצמית ויצירת תמריצים

למשק, תוך בחינה השוואתית של הנעשה בעולם ובתחומי רגולציה נוספים עם הנעשה במשק הישראלי. המחקר הנוכחי גם מספק סקירה מקיפה של התמודדות מדינות מרכזיות בעולם המערבי עם אתגר הסייבר ומאפשר בכך ללמוד על הדומה והשונה ביניהן בדרך בה מדינות בוחרות לבנות את משטריהן הרגולטוריים. חידוש נוסף הן ההמלצות למקבלי ההחלטות, הנובעות מההסתכלות הרחבה של מחקר זה וממיפוי נקודות מפתח במרחב הסייבר, וכוללות מגוון של תמריצים שנועדו ליצור רגולציה עצמית יעילה.

מבנה החיבור הינו כלהלן: בפרק הראשון – מבוא לרגולציה במרחב הסייבר – נסקרים האתגרים לחוסנו של המרחב, כשלי השוק האינהרנטיים שבו, היוצרים פערי הגנה משמעותיים עבור המשק, ופוטנציאל הנזק שפערים אלה טומנים בחובם לביטחון הלאומי. הסקירה מחדדת את התובנה, שבעוד שמדינות מערביות עוסקות בהרחבה בניהול סיכונים עבור החברה, סיכוני הסייבר מטופלים באופן צר ונקודתי, ללא תפיסה כוללת ותהליכים שיטתיים אל מול מרבית השחקנים במשק. בד בבד, מגדיר הפרק את המושג "רגולציה" כפי שהוא מעוגן בספרות האקדמית, מתאר את התפתחותו מבחינה היסטורית בארצות הברית ובאירופה, וסוקר את הספרות המחקרית המובילה בתחום זה, העוסקת בין השאר בטיעונים לרגולציה, בהסברים לאופן התפתחותה ובשינויים באופן בו היא מיושמת בעידן "הממשליות החדשה" ("from government to governance"). טענת המחקר היא כי רגולציה הינה הכלי המרכזי בידי מדינות מערביות להגברת הנוכחות המדינתית בתחומי חיים שונים; הרגולציה מתרחבת חרף התפשטות הניאו־ליברליזם ועקרונות השוק החופשי, ומשחקת תפקיד חשוב וקבוע בבניית שווקים ובשמירה על האינטרס הציבורי.

הפרק השני כולל סקירת ספרות על הנעשה בתחומי הרגולציה של הגנת הסייבר בארצות הברית (הן ברמה הפדרלית והן ברמה המדינתית), באיחוד האירופי, בבריטניה, בצרפת, בגרמניה ובישראל. הטבלה ההשוואתית בין המדינות, המובאת בסוף פרק זה, מלמדת על השונות הרבה בהתפתחות הרגולציה של מרחב הסייבר, וזאת מבחינת המבנה המוסדי, מידת הדומיננטיות של ארגוני הביטחון והתמריצים הניתנים לחיזוק ההגנה במשק. יחד עם זאת, ניתן לזהות דמיון רב באופן בו המדינות מטפלות במגזר העיסקי־אזרחי: טיפול נקודתי, הצהרתי לרוב, ללא תהליך סדור לניהול סיכוני סייבר.

פרק סקירת הספרות עוסק גם בשתי תופעות חדשות הניצבות לפתחם של מקבלי ההחלטות. הראשונה נוגעת להֶתקנים מקושרים, כלומר, למכשירים חדשים שאליהם מתווספת יכולת קישוריות, באופן המשנה את מרחב האיום המסורתי בסייבר; השנייה נוגעת לתחום המתפתח של ביטוח הסייבר ומציעה גישה חדשה של פיזור סיכונים בתחום הגנת הסייבר. שתי תופעות אלו חוצות מדינות ועדיין נמצאות בשלבי התהוות.

סקירת הספרות עומדת על שורשיהן של המחלוקות סביב אסדרת תחומים אלה ומעלה שאלות עקרוניות בפני מקבלי ההחלטות בראייה עתידית.

הפרק השלישי עוסק בלמידה מעולמות תוכן אחרים – הגנת הסביבה ואנרגיה גרעינית. הפרק סוקר ובהמשך מאמץ עקרונות רגולציה שפועלים בהצלחה בתחומים אלה, מתוך כוונה לחזק בעזרתם את הגנת הסייבר והביטחון הלאומי. הסקירה על רגולציית הגנת הסביבה כוללת תיאור האופן שבו היא התפתחה במדינת ישראל ומצביעה על קווי הדמיון בין תחום הסביבה ובין תחום הסייבר. במסגרת זו מנותח הכלי הרגולטורי של עריכת תסקיר השפעה על הסביבה ומשמעויותיו בהקשר של הרגולציה במגזר העיסקי־אזרחי.

כמה מעקרונותיה של הרגולציה בתחום הגנת הסביבה ניתנים לאימוץ עבור מרחב הסייבר. במסגרת זו ניתן לאמץ את הגישה הכוללנית להגנת הסביבה, שאינה מתמקדת בזיהום מסויים אלא פועלת להבנה כוללת של ההשלכות הישירות והעקיפות של כל מפגע סביבתי. בנוסף, מנגנוני התמריצים עבור התעשייה וההימנעות מריבוי מקבלי ההחלטות בתחום הגנת הסביבה (במקביל לתרבות הציות הבעייתית בישראל) הם עקרונות חשובים ורלוונטיים ליישום על כל מודל רגולטורי אפשרי להגנת הסייבר במשק. לבסוף, אימוץ תסקיר ההשפעה על הסביבה ככלי מדיניות למיפוי מראש של סיכוני סייבר אמור לסייע בשינוי האופן הצר והנקודתי בו מטופל המגזר העיסקי־אזרחי בכל הנוגע לסיכונים במרחב זה.

מתחום האנרגיה הגרעינית ניתן ללמוד על שיתופי הפעולה הנוצרים במגזר הפרטי, המובילים להתמקצעות ולפיתוח ידע איכותי, על יכולת הניטור והאכיפה של גוף בין־לאומי המכפיף מדינות רבות לנורמות אחידות ועל התערבות מדינתית לפיצויים במקרה של תאונה גרעינית. כל אלה מאפשרים לתעשייה להתפתח ולשוק הביטוח בתחום זה לשגשג.

הפרק הרביעי עוסק במודל הרגולטורי המוצע. מודל זה מתחלק לשלושה חלקים: רגולציה עצמית, רגולציה מחייבת ורגולציה מבוססת תמריצים. המודל מתבסס על הרגולציה הקיימת כבר כיום במדינת ישראל ושואף להרחיבה במטרה לתת מענה גם למגזר העיסקי־אזרחי. שיפורים ושדרוגים לרגולציה הקיימת מוצעים בכל אחד מחלקי המודל.

מודל הרגולציה העצמית, החָל על גופי ביטחון רגישים, כולל תוספות של יכולות בקרה ושל פיתוח הידע ההגנתי במערך הסייבר. **מודל הרגולציה המחייבת** עוסק במגוון מגזרים – מִתקני ביטחון, תשתיות קריטיות, ארגונים רגישים מהמגזר העיסקי המפוקחים באופן נקודתי, מיזמים ופרויקטים מתמשכים המובאים לאישור ורישוי, ונותני שירותים בעלי השפעה רבה על הנעשה במשק. מגוון מגזרים זה מוסדר ומפוקח כיום על ידי יישות מדינתית ייעודית, והחידושים המרכזיים במודל המוצע בהקשר

זה הם שניים: הראשון נוגע לשימוש בכלי הסטטוטורי של חוק רישוי עסקים למיפוי נזקי סייבר פוטנציאליים במגזר העיסקי־אזרחי, על ידי עריכת תסקיר השפעה על הביטחון הלאומי כתוצאה מפגיעת סייבר אפשרית בארגונים. כל ארגון המבקש רישוי ימלא שאלון פוטנציאל נזק שייערך בפיקוחו של מערך הסייבר הלאומי, האחראי על פיתוח הידע והמומחיות המגזרית. שאלון זה יגזור הנחיות לתסקיר וימפה סיכוני סייבר מבעוד מועד.

החידוש השני במודל הרגולציה המחייבת נוגע למיפוי צמתים מרכזיים שהינם בעלי השפעה על כלל המשק ולהתערבות מדינתית נקודתית שמטרתה לוודא הטמעת השירותים באופן ראוי ומאובטח בחברות השונות. דוגמאות אפשריות לכך הן ספקיות האינטרנט, ספקי שירותים מרכזיים בשרשראות האספקה של ארגונים, מארחי אתרים, מטמיעים של טכנולוגיות במגזרים רבים ונותני שירותים עיסקיים לכלל המשק. כל אלו הם בעלי השפעה מכרעת על פוטנציאל הנזק הנשקף מאיומי הסייבר השונים. שיפור האבטחה מפניהם, תוך פיקוח על אופן פעולתם, יבטיח את העלאת חוסנו של מרחב הסייבר הישראלי ושל הביטחון הלאומי בכללותו.

מודל **הרגולציה מבוססת התמריצים** עוסק בתחומים בהם ניתן לתמרץ את המגזר העיסקי כדי שיפעל לשיפור חוסנו של המרחב, ובכך יקרין על שיפור החוסן הלאומי. עידוד הקמתו של שוק ביטוח סייבר בישראל, תוך הסרת חסמי שקיפות באירועי סייבר בארגונים, יסייע לשלב שחקנים בעלי גב כלכלי, כמו חברות הביטוח, במאמצי הגנת הסייבר. תמריץ נוסף הוא מתן הקלות מס למטמיעי הגנת סייבר ברמה ראויה. תמריץ כזה עשוי לסייע לשינוי המשוואה הבעייתית, על פיה השוק מעדיף לקדם חדשנות וטכנולוגיה על פני ביטחון ופרטיות במרחב הסייבר. לבסוף, תמריצים לשיתופי ידע בין חברות מתחרות לצורך מיפוי קולקטיבי של האיומים ונקיטת צעדים פרו־אקטיביים למניעתם, יסייעו למניעת התקפות מבעוד מועד. תמריצים כאלו יכולים לכלול הסרת אחריות עיסקית במקרה של אירועי סייבר כתוצאה ממידע ששותף, ובכך ליצור בסיס לשיתופי פעולה ולראיית הגנת הסייבר כאתגר משותף וכטובין ציבורי.

הפרק החמישי עוסק בהמלצות ליישום המודל המוצע, על שלושת מרכיביו. הן עוסקות ראשית בארגונים רגישים הנתונים לרגולציה עצמית. הרחבת הפיקוח על ארגונים אלה צפוייה להיתקל בחסמים ארגוניים, וההמלצה היא לממשה באמצעות החלטת ממשלה ייעודית ובשיתוף פעולה הדוק עם מערך הסייבר הלאומי. בהמשך ההמלצות עוסקות בהרחבת הרגולציה המחייבת לחלקים ניכרים מהמגזר העיסקי־אזרחי דרך חוק רישוי עסקים, שאינו נאכף דיו במדינת ישראל. יש לפעול לחיזוק סמכויותיו של חוק זה ולשיפור תרבות הציות לו, תוך קביעת גורם־על אחד – משרד הכלכלה – שיהיה אחראי ליישומו ולאכיפתו. בנוסף מומלץ על פיתוח תמריצים להקמתו של שוק ביטוח לסייבר תוך קביעת נורמות לשקיפות באירועי סייבר, וזאת באמצעות

חקיקה ראשית, כפי שנעשה במקומות רבים בעולם. תמריצים נוספים, כגון הקלות מס ועידוד שיתופי מידע בין מתחרים, צריכים להיקבע בשיתוף עם רשות המיסים. לבסוף, תמריצים לעידוד שיתוף ידע בין־מגזרי יש לעגן בחקיקה ראשית.

בפרק הסיכום מנותחים תובנות ואתגרים הניצבים בפני מאמצי הרגולציה במרחב הסייבר. מערכות מדיניות ברחבי העולם עוסקות באופן תדיר בניהול סיכוני סייבר, ולמרות זאת, טרם נמצאה הנוסחה לפיקוח מיטבי על ניהול סיכונים אלו במגזר העיסקי־אזרחי. המודל המוצע מבקש להתמודד עם אתגר זה. מגוון כלים שיופעל על פני מגזרים שונים במשק יוכל לספק מענה רגולטורי רב־שכבתי לצורך לשמור על הביטחון הלאומי, וזאת על אף סיכוני הסייבר הגואים. ההתפתחות הטכנולוגית של עולם ההתקנים המקושרים והבינה המלאכותית הופכת את האתגרים של עולם הסייבר למהותיים עוד יותר. נדרש מודל סדור שיספק את התשתית הראויה להתמודדות עם אתגרים אלה.

פרק א׳: מבוא לרגולציה במרחב הסייבר

מרחב הסייבר מהווה אתגר עבור מקבלי ההחלטות. אתגר זה נובע, בראש ובראשונה, מתלות המדינה והחברה במרחב הסייבר, שהוא מיסודו מרחב פגיע. מרחב זה מאפשר, מצד אחד, זרימת מידע, המסייעת ברוב המקרים ליצירת פריחה כלכלית ורווחה חברתית, ומצד שני, הוא נתון לאיומים ביטחוניים, פליליים ומסחריים. האתגרים הניצבים בפני חוסנו של מרחב הסייבר[2] נובעים ממספר סיבות עיקריות:

1. ראשית, ישנה אסימטריה מובהקת בין חסמי הכניסה הנמוכים בפני תוקפים ובין עלויות ההגנה הגבוהות מפניהם. בעוד שתקיפה מוצלחת זקוקה לכיוון התקדמות יחיד, מאמצי ההגנה אמורים ומתיימרים לכסות את כלל הפגיעויות האפשריות.
2. שנית, מרחב הסייבר נשען על פרוטוקולי תקשורת מיושנים, המאפשרים אנונימיות רבה לתוקפים ומקשים על רשויות אכיפת החוק לזהות את מקור התקיפות.[3]
3. שלישית, מרחב הסייבר מאפשר הן ניצול חולשות חומרה או תוכנה הקיימות למכביר והן שימוש בכלי תקיפה קיימים שכבר פעלו בהצלחה בתקיפות קודמות. תופעות אלו גוררות מירוץ חימוש מואץ, המדרדר עוד יותר את רמת האבטחה. הראיה לכך היא קיומו של שוק משגשג לניצול חולשות zero-day.[4] בנוסף, לאחרונה נחשפה פעילות של חברות מסחריות הסוחרות עם ממשלות בחולשות תוכנה ובכלי תקיפה לצורך ריגול נגד אזרחים ו"מתנגדי משטר".[5]

---

2 חוסנו של מרחב הסייבר מתייחס לעמידותו בפני פגיעות אפשריות כתוצאה מחולשות תוכנה/חומרה, פרוטוקולים לא מאובטחים וגישה לא מורשית למידע.

3 פיתוחם של פרוטוקולים אלה תאם את הצרכים בראשית ימיה של רשת האינטרנט, בשנות השישים של המאה העשרים. באותם ימים, הצורך היה לאפשר קישוריות בין כמה עשרות מחשבים. אף אחד לא חזה אז כי על פרוטוקולים אלה תישען רשת של מיליארדי משתמשים.

4 חולשות zero-day הן חולשות חומרה או תוכנה שלרוב אינן ידועות ליצרן וטרם תוקנו. לעיתים אלו חולשות מוכרות שטרם הופץ להן תיקון בכל המערכות הרלוונטיות. על השוק המשגשג בתחום זה ראו: Andy Greenberg, "New Dark-Web Market is Selling Zero-Day Exploits to Hackers", *Wired*, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits

5 בחודשים האחרונים נחשפו מסמכים פנימיים של חברת Hacking Team האיטלקית, שעסקה בניצול חולשות ובפיתוח כלי תקיפה. המסמכים חשפו את היקף המסחר של החברה עם משטרים שונים בעולם. על התופעה הכוללת ראו: Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents", *The New York Times*, May 29, 2016, https://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html

4. רביעית, היעדר מכניזמים לשיתוף מידע על האיומים במרחב הסייבר ואמצעי ההגנה שבהם משתמשות חברות מסחריות, מקשים על גיבושו של מאמץ קולקטיבי ופרו־אקטיבי למניעת תקיפות במרחב זה. תופעה זו נובעת, בראש ובראשונה, משיתוף מידע חלקי ומשקיפות מוגבלת של חברות מסחריות הפועלות במגזר האזרחי.[6] גם המגזר הצבאי והמדינתי אינם תורמים את חלקם בנושא זה.
5. חמישית, יש מחסור בתמריצים כלכליים ובכלים טכנולוגיים לפיתוח הגנה נאותה. אמנם, נזקי הסייבר, המוערכים כיום במיליארדי דולרים, מתַמרצים את כוחות השוק להגן על עצמם, אך ברמה המדינתית, המגזר האזרחי ברובו אינו חייב בדיווח במקרה של פריצה ואיום סייבר שהתממש. אי לכך, עלויות הנזק כתוצאה מפריצה מוצלחת, וכן מוניטין החברה הנפרצת, אינם מונחים על הכף באופן שיתמרץ חברות להגן על עצמן מבעוד מועד.

על אף המודעות הגוברת של בעלי מניות וקהל הלקוחות במגזר הפרטי, אין, כאמור, הנחייה גורפת ומחייבת לפרסם אירועי סייבר ולדווח על הנזק שנגרם בעטיים. גם יכולותיה של מערכת הכלים הטכנולוגית הקיימת בשוק אינן מספיקות ליצירת הגנה הרמטית.[7] זאת ועוד, מרבית המשתמשים במרחב הסייבר אינם מודעים לסכנות שהוא טומן בחובו ומזינים אותו במידע רגיש וקריטי שאינו מוגן כראוי. בנוסף לכך, משתמשים רבים נופלים קורבן לניסיונות של הנדסה חברתית, בוחרים סיסמאות חלשות מדי, ובמרבית התקיפות מהוות את החוליה החלשה דרכה נפרצות מערכות.[8]

נוכח הנאמר לעיל, אין זה מפתיע כי חדשות לבקרים מתקבלים דיווחים מרחבי העולם על חולשות חדשות שנחשפות ועל פריצות למאגרי מידע, גניבת מידע רגיש והסבת נזק למערכות ממוחשבות.[9] הדבר נובע מחוסר הלימה בין הקלות בה חברות מסחריות ומדינות אוספות ומאחסנות מידע קריטי ובין יעילות המאמצים הנעשים כדי להגן על מרחב הסייבר. כך אנו מוצאים את עצמנו מול מרחב פגיע שבתפקודו התקין אנו תלויים לחלוטין.

המדינה מנסה להתערב ולמנוע התממשותם של סיכוני סייבר, או לפחות לצמצם בדיעבד, אך היא נתקלת בכשלי שוק מובנים המדרדרים את רמות ההגנה על פני המשק

---

6 Jason Mallinder and Peter Drabwell, "Cyber Security: A Critical Examination of Information Sharing versus Data Sensitivity Issues for Organizations at Risk of Cyber Attack", *Journal of Business Continuity & Emergency Planning*, Vol. 7, No. 2, 2014, pp. 103-11.

7 גבי סיבוני ועופר אסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, מזכר 149, תל אביב: המכון למחקרי ביטחון לאומי, 2015, עמ' 17–40.

8 Bruce Schneier, "Credential Stealing as Attack Vector", *Xconomy*, April 20, 2016, http://www.xconomy.com/boston/2016/04/20/credential-stealing-as-attack-vector/

9 Nate Lord, "The History of Data Breaches", *Digital Guardian*, September 28, 2015, https://digitalguardian.com/blog/history-data-breaches

כולו. הכשל המרכזי הינו ההחצנה השלילית של נזקי סייבר בארגונים: העלויות הנובעות מפגיעת סייבר בארגון אינן מושתות במלואן על הארגון עצמו, ולקוחות הארגון, או אפילו אינטרסים נעלים יותר כמו ביטחון הלאומי, נפגעים בדרך החורגת מגבולות הארגון. מאחר ומנהלי ארגונים אינם נושאים בכלל העלויות הנובעות מתוצאותיה של תקיפה מוצלחת, הם נוטים להשקיע בהגנת סייבר פחות מהנדרש. זה נובע גם מהעובדה שהתועלת שבהשקעה בהגנת סייבר איננה תמיד נהירה או ניתנת לכימות.

כשל שוק נוסף הוא היעדר אחריותיות על פגיעותם של מוצרי תוכנה וחומרה במרחב הסייבר. שוק הטכנולוגיה מתמרץ ומתגמל חברות המשכילות להיות הראשונות לפתח מוצר חדשני ואינו מעניק יתרון לחברות המייצרות מוצרים מאובטחים ומוגנים יותר מאחרים. על כן, השוק מוצף בתשתיות תוכנה וחומרה המכילות פגיעויות, ושלא כמו במוצרי צריכה אחרים, אין לחברות המייצרות חבות חוקית כלפי לקוחותיהן במקרה של נזק סייבר כתוצאה משימוש במוצריהן. היעדר אחריות מעמיק את הבעיה וגורם לכך שעוד מוצרים עם אבטחה לא ראויה יזכו לנתח שוק נכבד.

כשל שוק חשוב נוסף הוא קיומו של חוק הגבלים עיסקיים, המונע מחברות מתחרות לשתף מידע אודות איומי סייבר ומאמצי ההגנה שלהן. היעדר שיתוף מידע ראוי מפחית את היכולת להתגונן מבעוד מועד או בזמן אמת ויוצר אווירת אי־אמון בין שחקנים במשק שדווקא עשויים לסייע רבות האחד לשני בהעלאת חוסן הסייבר הכולל.[10] בנוסף לכשלי שוק מרכזיים אלה, מתמודדת המדינה עם העובדה כי מרחב הסייבר הוא מרכיב מרכזי בתוכנית ניהול הסיכונים הפנים ארגונית והתערבות בו נתפסת כהתערבות בוטה של המדינה במשק. על כן התערבות מדינתית שכזו, בגרעין פעילותו של ארגון פרטי, נתקלת בקשיים והתנגדויות רבות.

הסיכונים הנשקפים ממרחב סייבר, הכוללים פגיעה ברציפות התפקודית של הארגון, גניבת קניין רוחני, פגיעה בפרטיות, נזקי צד שלישי ופגיעה במהימנות מערכות המידע,[11] הינם המשך טבעי של סיכוני המדינה המודרנית, כפי שתיארם הסוציולוג אולריך בק בספרו *Risk Society*.[12] לדברי בק, החיים המודרניים, על פיתוחיהם הטכנולוגיים, טומנים בחובם הזדמנויות רבות, אך גם יוצרים סכנות חדשות לאדם ולסביבה. הכלכלן דיוויד מוס התייחס ב־2002[13] למורכבות של ניהול סיכונים על ידי הממשלה.

---

10 לסקירה ממצה של כשלי השוק בהגנת הסייבר ראו: Nathan Alexander Sales, "Regulating Cyber-Security", *Northwestern University Law Review,* Vol. 107, no. 4, 2013, pp. 1503-68.

11 לדיון על הסיכונים והאתגרים למקבלי החלטות במרחב הדיגיטלי ראו: OECD, *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document,* Paris, OECD Publication, 2015.

12 Ulrich Beck, *Risk Society: Towards a New Modernity,* California, Sage Publishing, 1986.

13 David Moss, *When All Else Fail: Government as the Ultimate Risk Manager*, Cambridge, Harvard University Press, 2002.

הוא הראה כיצד הממשל האמריקאי, המנהל סיכונים עבור כלל החברה האמריקאית, עבר שלושה שלבי התפתחות עוקבים באסטרטגיית ניהול הסיכונים שלו. ראשיתו של התהליך הייתה במאה ה־19, כאשר הממשל התערב באופן אגרסיבי בניהול סיכונים לצורך עידוד השקעות וצמיחת המשק (על ידי חוקים, כגון חוק החברות המגביל את הסיכון עבור המשקיעים בחברה, וחוק פשיטת רגל המגן על משקיע מפני ירידה מכל נכסיו). בהמשך עבר הממשל לניהול סיכונים עבור בטיחות העובדים ויציבות שוק העבודה (חוקי פיצויים לעובדים, ביטחון סוציאלי לעובדים – הולדתה של מדינת הרווחה האמריקאית). לבסוף, בשלב הנוכחי של העת המודרנית, הממשל האמריקאי עוסק בניהול סיכונים הנובעים מפיתוחים מודרניים, וכן בסיכונים הכרוכים בהם, הכוללים סיכוני סביבה, בטיחות במזון וכיום גם סיכוני סייבר, וזאת עבור כלל החברה בארצות הברית.

אסטרטגיות הסיכון שנוקטת המדינה נעות על הרצף שבין הפחתת סיכונים ובין חלוקתם מחדש בחברה. הפחתת סיכונים כוללת בעיקר מניעתם מבעוד מועד (למשל, רגולציה לבטיחות, שלטים המזהירים מפני מהירות מופרזת, ובשדה הסייבר – דרישות אבטחת מידע למניעת פריצה למערכות), וכן צעדים לצמצום נזקים (mitigation), שמטרתם היא להפחית את הנזק כתוצאה מסיכון שכבר התממש (למשל, רגולציית כיבוי אש, או בתחום הסייבר – צעדים לצמצום נזק מהתקפות סייבר[14] ודיווח לאזרחים ולגורמים מדינתיים על פריצה שקרתה כדי שיתגוננו מפניה מבעוד מועד).

חלוקה מחדש של סיכונים עוסקת בהעברת האחריות לסיכון בין היישויות השונות (למשל, חוקי בטיחות מוצרים המסיטים את האחריות מהצרכן ליצרן). דוגמה עכשווית משדה הסייבר הינם חוקי שיתוף מידע, המגבילים את האחריות של חברות מסחריות, הבוחרות לשתף מידע עם הממשלה, מפני פריצות סייבר. חלוקה מחדש של סיכונים יכולה לבוא לידי ביטוי גם בפיזור סיכונים על פני מבוטחים שונים – למשל, בחברות ביטוח. במקרה זה, כל מבוטח משלם פרמיה מסויימת כדי לכסות את הנזק מסיכון שיתממש אצל אחד המבוטחים. בעולם הסייבר כיום, פיזור הסיכונים על ידי המגזר הפרטי נעשה בעיקר עבור סיכוני צד שלישי,[15] ללא התערבות מדינתית.

למרות אסטרטגיות הסיכונים המגוונות, המדינה טרם השכילה למצוא את הדרך הראויה להתערב, בעיקר במגזר האזרחי, כדי להבטיח את רציפותו התפקודית של

14 על "מעגל ההגנה השלם" ראו: Gabi Siboni, "An Integrated Security Approach: The Key to Cyber Defense", *The Georgetown Journal of International Affairs*, May 7, 2015.

15 סיכוני "צד שלישי" בעולם הסייבר הינם סיכונים לפרטיות לקוחות של חברות מסחריות הנפגעים כתוצאה מפגיעת סייבר וגניבת מידע אישי. לעומת זאת, חברות הביטוח לא ששות לבטח סיכוני "צד ראשון" (כלומר, לחברות עצמן), מאחר וישנו מחסור במידע אקטוארי האמור לסייע בתמחור פרמיות ביטוח עבור סיכוני סייבר כאלה.

מרחב הסייבר, את חוסנו ואת יציבותו. החשיבות של המגזר האזרחי לחוסנו של מרחב זה היא עצומה. מגזר זה מהווה את החלק העיקרי במרחב הסייבר, ולכן הוא נחשף למרבית האיומים הקיימים בו. פגיעה במרחב זה היא בעלת השלכות כלכליות וביטחוניות על חוסנה של החברה, כפי שיפורט בהמשך.

כדי להבין כראוי את האתגר הרגולטורי, יש לתהות תחילה על קנקנו של מושג הרגולציה. ברמה הבסיסית ביותר, רגולציה היא פעולת ארגון, פיקוח ואכיפה המבוצעת על ידי המדינה או סוכנויות מדינתיות עצמאיות במטרה לכפות באופן חוקי כללי התנהגות מחייבים.[16] הרגולציה חלה על "נמעני רגולציה", שאותם הגוף הרגולטורי שואף להסדיר. ניתן לומר שרגולציה מסדירה את היחסים בין המדינה ובין המגזרים השונים הפועלים בה, כמו המגזר העיסקי, ארגונים ואף פרטים. הרגולציה שימשה בראשיתה בעיקר לתיאור הפיקוח של המדינה על ארגונים עיסקיים והתבססה על חוקים מפורשים שהכילו כללי התנהגות והסמיכו גופים כ"רגולטורים". הגדרה רחבה יותר לרגולציה עוסקת במטרות החברתיות שלה ולא רק במטרותיה הכלכליות. לפי הגדרה זו, רגולציה היא יותר מניטור ואכיפת החוק על עסקים פרטיים; היא עוסקת גם במסגרות ציבוריות ובהבטחת איכות החיים בשלל תחומים.

מושג הרגולציה נולד בארצות הברית בסוף המאה ה־19 כדרך פוליטית ומינהלית להסדיר את השוק. הרגולציה הפכה לכלי מרכזי בידי אנשי ממשל אמריקאים, שכן היא הייתה תגובה טבעית לכשלי שוק, להיעדר פיקוח ולהיווצרותם של "מונופולים טבעיים". לעומת זאת, באירופה נעשה הפיקוח בעיקר על ידי הלאמת השוק. הפיקוח באמצעות הלאמה עיכב את ההתפתחות הרגולטורית באירופה לעומת ארצות הברית.[17] יחד עם זאת, מסוף שנות השבעים ובמהלך שנות השמונים של המאה העשרים, התרחב השימוש ברגולציה גם באירופה והוקמו שם סוכנויות רגולטוריות עצמאיות, כחלק מהאצת האיחוד הכלכלי של היבשת.[18] עם עלייתם לשלטון של מרגרט תאצ'ר בבריטניה (1979) ורונלד רייגן בארצות הברית (1981), חלה התרחבות בפעילותן של סוכנויות רגולטוריות עצמאיות שפעלו לאסדרת השוק, במה שזכה לכינוי "המדינה הרגולטורית."[19]

16 דוד לוי־פאור, **רגולציה: רקע מושגי והיסטורי**, אוניברסיטת חיפה, 2010.

17 שם.

18 שם.

19 Giandomenico Majone, "The Rise of the Regulatory State in Europe", *West European Politic*s, Vol. 17, No. 3, 1994, pp. 77-101.

תפקיד המדינה עבר אז אט־אט מסבסוד שירותים ומסיוע לצמצום פערים, לייעול השוק באמצעות רגולציה (או דה־רגולציה[20]) מוגברת.

הרגולציה נתפסת לרוב כחקיקה או חקיקת משנה של המדינה, או של סוכנויות רגולטוריות עצמאיות. היא יכולה להתבטא גם בהוראות, צווים או הנחיות מחייבות. תפקידה הוא להסדיר את פעילות השוק על בסיס מדיניות שנקבעה על ידי הדרג המדיני. "המדינה הרגולטורית" מעניקה תפקיד מרכזי למומחים, והדרישה לרמת מומחיות גבוהה היא המוטיבציה הראשונית להקמת סוכנויות רגולטוריות עצמאיות.

את תרומת הרגולציה לציבור הרחב ניתן להסביר במספר אופנים: ראשית, הרגולציה שואפת להגן על ערכים וחירויות האזרח שעלולים להיפגע על ידי בעלי הכוח או כתוצאה מאיומים מבחוץ. הדבר מסביר את הצורך בכוחות צבא וביטחון, וכן ברשויות שיבלמו ויאזנו אותם במידת הצורך; שנית, מבחינה כלכלית, תפקיד הרגולציה הוא לתקן כשלי שוק הנובעים מהתנהלות השוק החופשי שאינה משרתת את האינטרס הציבורי.[21] לדוגמה, מונופול שמתמחר ומספק מוצרים כראות עיניו, ועל כן נדרש להטיל עליו פיקוח; שלישית, ניתן להצדיק רגולציה גם במצב של היעדר מידע או של א־סימטריה במידע, דבר הגורם לצרכנים, לחברות או למדינות להתנהג בצורה שלא משרתת את האינטרס הציבורי. במקרה זה, תפקידו של הרגולטור הוא לאפשר שקיפות וזרימת מידע; רביעית, רגולציה נובעת מהרצון להבטיח את קיומם של משאבים ציבוריים מִתכלים שאי אפשר למנוע את השימוש בהם, החל מאיכות האוויר וכלה במספר הדגים בים. במקרה זה, על הרגולטור לדאוג שמשאבים כאלה ימשיכו להתקיים, למרות שכוחות השוק נוטים לכלותם.

היווצרותה של רגולציה ואופן הפעילות של הרגולטור בהליך המדיניות הציבורית מוסברים בספרות באופנים שונים ומגוונים. תיאוריית האינטרס הציבורי (פונקציונליזם) גורסת כי רגולציה פועלת לקידום טובת הכלל ולהגדלת הרווחה החברתית.[22] לעומתה, תיאוריית האינטרס הפרטי מסתכלת על רמת הקבוצה ומניחה שסדר הכוח בחברה הוא תוצאה של עימותים בין קבוצות ושחקנים. במקרה זה, הרגולטור מונע על ידי אינטרסים פרטיים ומטרתו היא להגדיל את רווחתן של קבוצות אינטרסים המייצגות בדרך כלל פלח קטן באוכלוסייה. בהיבט זה, הרגולציה היא תוצר של יחסים בין קבוצות

---

20 פרופ' לוי־פאור מסביר מדוע דה־רגולציה לא רק מייתרת, אלא אף "מזמינה" עוד סוכנויות ופקידים לפיקוח על הפרטות ולשמירה על האינטרסים של המדינה.
ראו: David, Levi-Faur, "Regulation and Regulatory Governance", in David Levi-Faur (ed.), *Handbook on the Politics of Regulation*, Cheltenham, Edward Elgar Publishing, 2011.

21 שוריק דריישפיץ, "רגולציה – מה, איפה ומתי? מבט תאורטי ומשווה", **פרלמנט**, גיליון 64, מארס 2010, https://www.idi.org.il/parliaments/11097/11149

22 ראו, לדוגמה: Harold Demsetz, "Why Regulate Utilities?", *Journal of Law and Economics*, Vol. 11, 1968, pp. 55-65.

אינטרסים למדינה, ובינן לבין עצמן.[23] הקבוצה "המשפיעה" במקרה זה מִשתנָה ויכולה לנוע על פני הרצף שבין פלורליזם – קבוצות רבות המתחרות זו בזו באופן שווה, כשכל פעם ידה של קבוצה אחרת על העליונה – ובין אליטות – קבוצות מצומצמות של אנשי תעשייה, צבא ופוליטיקאים, שהאינטרסים שלהם מקודמים על ידי הרגולציה המדינתית. בתווך ניתן למצוא גישה ניאו־פלורליסטית, הגורסת כי העוצמה בחברה מבוזרת בצורה נזילה ובלתי שוויונית, כלומר, קבוצות אינטרסים עם כוח והשפעה רבים יותר משל קבוצות אחרות יכולות "לשבות" את הרגולטור ו"לִזכּות" במדיניות המיטיבה בעיקר עימן (Capture theory).

מול התיאוריות הבוחנות קבוצות בחברה ניתן למצוא תיאוריה מתחרה[24] – אֶטָטִיסְטית – שעל פיה המדינה היא אוטונומית, ניצבת במרכז ומהווה את הגורם החזק בעיצוב המדיניות, ולכן יש לה השפעה מכרעת על האופן בו מבוצעת הרגולציה בחברה. לפי תיאוריה זו, עוצמתה של המדינה התפתחה מתוך ביורוקרטיה חזקה, שניהלה את בניית התשתיות והביצורים בגבולות (למשל, ביפן שלאחר מלחמת העולם השנייה). לפיכך, המדינה אינה כלי שרת בידי קבוצות אינטרסים, אלא הגורם המכוון את הרגולציה בחברה ביד רמה. ניתן לתת למשטרים רגולטוריים גם הסבר מוסדי: העובדה שהרגולציה נוצרה במקרה זה על בסיס יכולותיהם של מוסדות,[25] או בהתאם למיקומם ההיסטורי בהליך המדיניות הציבורית.[26]

מאז אמצע שנות התשעים של המאה העשרים החלה להתפתח תיאוריה חדשה להסברת הרגולציה – התיאוריה הרעיונית. לפי אותה תיאוריה, לפרדיגמות יש תפקיד מרכזי בהליך עיצובה של המדיניות הציבורית:[27] רעיון מסויים נתפס כ"נכון" ב"חלון הזדמנות" מסויים וסוחף אחריו את מקבלי ההחלטות ליצירת רגולציה ברוח הפרדיגמה

---

23 למחקר אמפירי שבחן את הפעילות של קבוצות אינטרסים בארצות הברית ראו: F. R. Baumgartner and B. L. Leech, "Interest Niches and Policy Bandwagons: Patterns of Interest Group Involvement in National Politics", *Journal of Politics*, Vol. 63, 2001, pp. 1191-213.

24 ההתעצמות של התיאוריה המדינתית היא תוצאה של "הדילמה של מדיסון", הנשיא הרביעי של ארצות הברית, שאמר שמצד אחד אינך יכול להיות דמוקרט מבלי לתת לקבוצות להתארגן, אך מצד שני אין ביטחון שהתארגנות של קבוצות כוח תיתן ביטוי לאינטרס הציבורי ותפעל לטובת הציבור.

25 מחקר לדוגמה על האופן בו המדיניות להגנת הפרטיות באירופה יצרה מוסדות חזקים, שהעבירו חוקי פרטיות נוקשים אשר נגדו את רוח התקופה, ראו: A. L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *International Organization*, Vol. 62, No. 1, 2008, pp. 103-30.

26 מחקר העומד על העקביות של מדינת הרווחה המודרנית: Paul Pierson, "The New Politics of the Welfare State", *World Politics,* Vol. 48, No. 2, 1996, pp. 143-79.

27 ראו מחקר על שבירת הפרדיגמה הקיינסיאנית ומעבר לכלכלה מוניטרית בבריטניה: Peter Hall, "Policy Paradigms, Social Learning and the State: The Case of Economic Policymaking in Britain", *Comparative Politics*, Vol. 25, No. 3, 1993, pp. 275-96.

והאינטרסים הכרוכים בה.[28] פירוש הדבר הוא שרעיונות ואינטרסים שזורים במקרים רבים זה בזה, כאשר רעיון מסויים עוזר לתת לגיטימציה וביטוי לאינטרסים, ואלה מצידם יכולים לייצר רגולציה שתשרת את מטרותיהם.[29]

כל ההסברים הללו נבדלים ביניהם ברמת הרציונליות שלהם. למעשה, מלבד התיאוריות המדגישות פונקציונליזם ואינטרס ציבורי, שאר התיאוריות מסייעות להבין מדוע היווצרותה של רגולציה אינה בהכרח רציונלית כלפי מושא הרגולציה, אלא נובעת מאינטרסים אחרים.

האופן בו מיושמת רגולציה השתנה עם הזמן. הרגולציה החלה כקביעת כללים באופן חד־כיווני (top-down regulation) והייתה מבוססת בעיקר על הרתעה וענישה. יחד עם זאת, באמצע שנות התשעים של המאה העשרים צמח זרם "הממשליות החדשה" ("from government to governance"), שהתפתח מתוך הבנה כי לא ניתן עוד להסתפק ברגולציה של ציווי ושליטה כדי להשליט סדר בתחום מסויים לטובת האינטרס הציבורי, אלא יש לשלב גופים נוספים, בעלי ידע ומשאבים, ובאופן מבוזר, כדי להשיג שליטה והכוונה של המדינה.[30] על פי גישה זו, ניתן לגבש הליכים שיתופיים עם גורמי עניין בחברה כדי לפתח את הידע הנדרש ולפתור בעיות מורכבות. גישת "הממשליות החדשה" פועלת במקביל לגישה המסורתית ולא כתחליף לה. שתי הגישות משלימות זו את זו ומאפשרות לתת מענה אסדרתי לאתגרים מתפתחים וחוצי מגזרים. לעומת הגישה המסורתית והכופה, גישת "הממשליות החדשה" מביאה עימה שיתופיות וחלוקת כוח, אינטגרציה רב־שכבתית של כל השחקנים בתחום המפוקח, מתן שיקול דעת לשחקנים בשטח, יצירת ידע מתפתח ואפשרות לגמישות ושינוי בהתאם למציאות הדינמית.

פן נוסף של גישת "הממשליות החדשה" בא לידי ביטוי בהסדרי רגולציה עצמית מתקדמים, בהם התעשייה המפוקחת קובעת את כללי הפיקוח עבור עצמה במקום, ולעיתים לצד, פיקוח של רגולטור חיצוני. במסגרת הגישה החדשה ממונים בחברות "קציני ציות", שתפקידם הוא לוודא את קיומן התקין של הוראות הרגולציה בארגון ולדווח להנהלתו לפי הצורך.[31] רגולציה כזו מכונה בספרות management-based regulation, שכן היא מהווה פיקוח של הרגולטור באמצעות הטמעת תהליכים בארגון המפוקח, ולאו דווקא באמצעות כפייה של תקנים או יעדים רגולטוריים מסויימים.

---

28 מחקרו של Kingdon טבע מושגים כגון "חלון הזדמנויות" ו"יזם מדיניות", שמסבירים בצורה מדוייקת להפליא את הליך המדיניות הציבורית: John Kingdon, *Agendas, Alternatives and Public Policy,* 2nd edition, Boston, Little Brown, 1995.

29 Daniel Béland and Robert Cox, *Ideas and Politics in Social Science Research*, Oxford, Oxford University Press, 2010, Introduction.

30 שרון ידין, **מדיניות לאסדרה סביבתית אינטגרטיבית של מפעלי תעשייה בישראל – רקע, עקרונות יסוד והמלצות ליישום**, המשרד להגנת הסביבה, 2014.

31 שם.

רגולציה עצמית נשענת בעיקרה על משאבי הארגון וחוסכת השקעת משאבים וסנכרון עם השטח. כמו כן, היא מעניקה למפוקח שיקול דעת רחב ומאפשרת לו חופש פעולה מסויים. אחד המודלים של רגולציה עצמית הוא רגולציה עצמית כפויה (enforced self-regulation), במסגרתה המפוקח מסדיר בעצמו את הפיקוח על תחום מסויים, על פי הנחיית הרגולטור החיצוני ובפיקוחו.[32]

לסיכום, הרגולציה מקיפה כיום כמעט את כל תחומי החיים. היא התרחבה ועברה שינויים רבים עם הזמן, וממשיכה להתפתח על בסיס אינטרסים שונים ומגוונים. הרגולציה חורגת מעֵבר לפעולת אסְדרה בסיסית של פעילותם של עסקים פרטיים ומעֵבר לקידום מטרות ציבוריות־חברתיות; היא תופעת משילות ענפה המובילה להקמת מוסדות רבים, ויש לה השפעה ניכרת על החיים בעולם המודרני. על כן, הבנתן של מערכות רגולטוריות מאפשרת הבנה עמוקה יותר של אופן המשילות, הן ברמה הלאומית והן ברמה הבין־לאומית. התרחבות תופעת הרגולציה היא קרקע פוריה לכינון רגולציה גם בתחום הגנת הסייבר – תחום שטרם הוסדר בצורה מספקת ברחבי העולם, ובכלל זה במדינת ישראל.

32 כך נעשה, למשל, בחלק מהוראותיו של בנק ישראל, המורה לכל בנק לקבוע בעצמו נהלים פנימיים ליישום עקרונות כלליים שקבע הרגולטור.

פרק ב': סקירת ספרות

סקירת הספרות העוסקת ברגולציה במרחב הסייבר מתארת את הנעשה בתחום זה בארצות הברית, בישראל, באיחוד האירופי ובמספר מדינות נבחרות באירופה – גרמניה, צרפת ובריטניה. בנוסף לכך, היא עוסקת בנושאי רגולציה חוצי מדינות של התקנים מקושרים ומוצרי ביטוח בתחום הגנת הסייבר, בהם העשייה היא ראשונית וחלקית בלבד.

ארצות הברית

רגולציה פדרלית במרחב הסייבר

משטר הרגולציה בנושאי הגנת הסייבר בארצות הברית מורכב מאוסף של חוקים, הוראות נשיאותיות, פסיקות בתי משפט, תוכניות ממשלתיות, תקנים טכנולוגיים[33] וצווי ביטחון לאומי, שנבנו זה על גבי זה במהלך שלושים השנים האחרונות. נקודת הפתיחה להבנת תהליך הבנייתה של הרגולציה הפדרלית לאורך זמן הוא החוק משנת 1984 שעסק לראשונה בפשעי מחשב בארצות הברית.[34] מאז ועד היום נבנתה הרגולציה הפדרלית כטלאי על גבי טלאי, שיצר מערך המרכיב את סך כל מאמצי הממשל האמריקאי במניעה ובמזעור נזקים במרחב הסייבר בארצות הברית. מדובר במרחב הכולל את רשתות המידע הממשלתיות, תשתיות קריטיות, מערכות פיננסיות ורפואיות, מערכות ביטחוניות מסווגות,[35] וכן את המגזר העיסקי־אזרחי.

מקורות המידע באמצעותם ניתן ללמוד על הבניית משטר הרגולציה בארצות הברית לאורך השנים הינם רבים ומגוונים. מאחר והמשטר הרגולטורי בסייבר לא נבנה בצורה היררכית ובאסטרטגיה סדורה,[36] היו גורמים רבים מעורבים בעיצובו, חלקם באופן

---

33 באמצעות מסמכי הנחייה של מכון התקנים האמריקאי – National Institute of Standards and Technology (NIST).

34 The Comprehensive Crime Control Act, 1984.

35 מגזר זה קרוי בארצות הברית National Security Sector (NSS).

36 על האופן בו משטר הרגולציה נבנה טלאי על גבי טלאי ראו: Richard Harknett, James Stever, "The New Policy World of Cybersecurity", *Public Administration Review*, Vol. 71, No. 3, 2011, pp. 455-60; Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security", *Georgetown Journal of International Affairs*, International Engagement on Cyber IV, 2014, pp. 69-78.

שהגיב לאירועי סייבר שכבר התרחשו וחלקם באופן יזום, במטרה למנוע אירועי סייבר עתידיים. מקורות המידע כוללים דוחות של מרכז המחקר של הקונגרס האמריקאי; אתרים רשמיים של סוכנויות הרגולציה השונות בארצות הברית;[37] מסמכי אסטרטגיה שפורסמו על ידי הבית הלבן במהלך השנים;[38] דוחות של ועדות חקירה שהוקמו על ידי המדינה לאחר אירועים משמעותיים במרחב הסייבר;[39] מחקרים אמפיריים על משטרי הרגולציה לאורך השנים;[40] אתרים העוקבים אחר היסטוריית החקיקה בארצות הברית;[41] ארגוני חברה אזרחית, הבוחנים בעין ביקורתית את המרחב הדיגיטלי בארצות הברית ומדגישים את האינטרס הציבורי ברגולציה טכנולוגית;[42] מסמכים מסווגים שפורסמו או הודלפו במהלך השנים על האופן בו ארצות הברית "מסמנת מטרות" במרחב הסייבר ומשתמשת באסטרטגיות התקפה לצורכי הגנה; ניתוחים של חברות ייעוץ ומשרדי עריכת דין המפרשים פסיקות משפטיות במטרה לסייע לתעשייה בהבנת הדרישות המשתנות מצד המדינה;[43] בלוגים ואתרים מובילים המסייעים לעיצוב דעת הקהל בתחום זה, תוך ניתוח ביקורתי של הנעשה ברמת המדינה וסוכנויותיה.[44]

שלב א': ראשיתה של הרגולציה להגנת הסייבר בארצות הברית – התפתחות מרחב האיומים

נושא ביטחון הסייבר הגיע לפתחם של מקבלי ההחלטות בארצות הברית רק באמצע שנות השמונים של המאה העשרים. עם זאת, הבנת המניעים וההקשר שהביאו לעיצוב מדיניות הסייבר האמריקאית מאז ועד היום מחייבת לחזור אל שנות השישים והשבעים של המאה הקודמת, בהן נצברו ניסיון ותובנות במשרד ההגנה של ארצות הברית סביב מרחב הסייבר המתהווה והתנהלו מאבקי כוח סביב המנדט שיש למדינה לאסוף מידע

37 סוכנויות אלו כוללות את: FINRA, SEC, US Commodity Futures Trading Commission, FTC, FCC, FERC, NERC, Nuclear Regulatory Commission, DHS, NIST, SEC, וכן משרד ההגנה, משרד האנרגיה, מגזר הביטוח ומגזר הבריאות.

38 מסמכי אסטרטגיה אלה נבעו מרצונו של הממשל המכהן להביא לשינוי בתפיסה ולקדם את הגנת הסייבר של ארצות הברית. הם פורסמו חמש פעמים – בשנים 2003, 2006, 2008, 2009 ו־2011.

39 למשל, דוח הוועדה שתפקידה היה לבחון ולשנות את הרגלי המעקב של סוכנויות המודיעין אחרי חשיפות המדליף אדוארד סנודן. דוחות אלה מספקים סקירה היסטורית של הנעשה בארצות הברית בתחום הרגולציה על המרחב הדיגיטלי, כולל ההשלכות על ביטחון הסייבר.

40 למשל, מחקרה של פריסילה ריגן על חוקי הגנת המידע בארצות הברית בשנים 1965–1995: Priscilla Regan, *Legislating Privacy*: *Technology, Social Values and Public Policy*, Chapel Hill, University of North Carolina Press, 1995.

41 הבולטים שבהם הם: trackgov.us ו־Library of Congress

42 הארגונים הבולטים בתחום זה הם: Electronic Frontier Foundation (EFF), American Civil Liberties Unit (ACLU), Electronic Privacy Information Center (EPIC).

43 אחד המובילים שבהם הוא האתר של חברת הייעוץ המשפטי Skadden.

44 שניים מהמרכזיים שבהם: schneier.com והבלוג של חוקר אבטחת המידע Brian Krebs.

על אזרחיה. במסגרת זו חשוב להבין את התפיסות ההיסטוריות של משרד ההגנה, שהשפיעו על עיצוב תפיסותיהם של חברי הקונגרס ומקבלי ההחלטות בבית הלבן את נושא הגנת הסייבר. על פי ההיסטוריון של משרד ההגנה, מייקל וורנר,[45] אפשר לחלק את התפיסות שרווחו בשנות השבעים של המאה לארבע קבוצות עיקריות:

1. מידע רגיש במערכות המחשבים אינו בטוח.
2. מחשבים מכילים בתוכם פגיעויות שונות וקיימת אפשרות שאלו יהפכו לדרך נוספת לגניבת מידע.
3. יכולות תקיפה במרחב הסייבר הן חלק לגיטימי מהיכולות הצבאיות של המדינה.
4. מדינות אחרות יכולות לתקוף את ארצות הברית במרחב הסייבר, וכנראה כבר עושות זאת.

כל אחת מהתפיסות הללו עוצבה כבעיה, וזמן מה לאחר מכן הודגמה כבעיה בפועל. המדיניות שנקבעה להתמודד איתה הייתה תמיד תגובתית.

מחשבים החלו לתקשר האחד עם השני דרך רשתות בשנות השישים של המאה העשרים. ה"מכונות" עצמן, כפי שנקראו אז המחשבים, תפסו חדרים שלמים, היו יקרות מאוד ונזקקו למשאבים חשמליים רבים ולכוח אדם ייעודי כדי להפעילם. בעלי המחשבים נאלצו להתקינם בחדרים נפרדים ושמחו להשכיר את השימוש בהם לחברות, סוכנויות וחוקרים כדי למקסם את הרווח מתפעולם. מציאות זו העלתה את הדרישה לתוכנות מחשב שיהיו מסוגלות לעבוד במקביל לתוכנות אחרות, מבלי לחשוף מידע למשתמשים לא מורשים העובדים על אותה מכונה.

כבר בשנת 1966 ערך הקונגרס אמריקאי דיונים במטרה להבין את בעיית דליפת המידע ממחשבים. במקביל, מכון המחקר "ראנד" התבקש לערוך דוח בדיקה של דלף מידע ממחשבים. הדוח שהמכון פרסם בתחילת 1967 הזהיר כי כל עוד ישנם משתמשים לא ידועים, העובדים על אותן מכונות בו־זמנית, אין פתרון הנדסי לבעיית אבטחת המידע במערכות ממוחשבות.[46] כתוצאה מכך, פותחו פתרונות למצב הקיים, בצורת רמות הרשאה שונות על מערכות, הרשאות על קבצים, ערבול סיסמאות והצפנה. כאשר חברת IBM הציעה פתרון מסחרי לבעיה וביקשה להחיל אותו על הממשל הפדרלי, התעוררו חילוקי דעות סביב מידת מעורבותה של הסוכנות לביטחון לאומי של ארצות הברית (NSA) בנושא. היה זה בעקבות בקשתה של הסוכנות לאכוף תקן הצפנה נמוך יותר, כדי שתוכל לשבור הצפנה של מוצרים מסחריים במידת הצורך ולאסוף עליהם מידע.

---

45 Michael Warner, "Cybersecurity: A Pre-History", *Intelligence and National Security*, Vol. 27, No. 5, 2012, pp. 781-99.

46 Willis H. Ware, *Security and Privacy in Computer Systems*, California, Rand Corporation, 1967.

התרחבות רשתות המחשבים והפיכתן לגלובליות, בשנות השמונים של המאה העשרים, העלו לדיון את הסיכון הכרוך בקיומם של פגיעויות ונוזקות ואת יכולתם של פצחנים (האקרים) לחדור מרחוק ולשבש מערכות ממוחשבות. ב־1979 פרסם מפקד חיל האוויר האמריקאי דאז, רוג'ר שֶל, מסמך שסקר את האופנים השונים בהם ניתן לחדור למערכות ממוחשבות, וזאת על בסיס בדיקות חדירות שנעשו למערכות של חיל האוויר. שֶל הבדיל בין צירופי מקרים וטעויות ובין מערכות לא מאובטחות מיסודן, או מערכות שפותחו מחוץ לארצות הברית, וקבע כי בשני המקרים יש סיכון רב לחדירה מוצלחת.[47] בשנת 1983 פרסם העיתון "ניו יורק טיימס" כתבה על הלך הרוח במשרד ההגנה האמריקאי סביב נושא הסייבר וחשף את הדאגה הרבה ששררה שם נוכח אי־היכולת להגן על רשתות המחשבים כתוצאה מהגידול בהיקף המידע המסווג המאוחסן בהם, העלייה במספר הפצחנים הפוטנציאליים והתחכום הגובר של הפריצות.[48]

ממשל הנשיא רייגן התייחס לאתגר הסייבר בהוראה נשיאותית מ־1984,[49] שהייתה סודית בשעתה ועסקה בהגנה על מערכות המחשב הפדרליות. ההוראה הטילה על הסוכנות לביטחון לאומי את האחריות להגן על מערכות המחשבים, ובכלל זה לחקור את האיומים החדשים ולקבוע תקנים לטיפול בהם. בתגובה הביע הקונגרס דאגה וחשש שסוכנות מודיעין כמו NSA תהיה האחראית הבלעדית על ביטחון המידע הפדרלי־אזרחי, באופן שיסכן את פרטיותם של אזרחים ויפגע בזכויותיהם.[50] בשנים 1985־1987 נערכה בקונגרס שורה של דיונים על נושא הפרטיות והגנת הרשתות הפדרליות, ובמקביל קמו קואליציות של בנקים וארגוני החברה האזרחית שתמכו בנושאים אלה. מצב זה, שבא על רקע היחלשות כוחו של ממשל רייגן בעקבות משבר "איראן־קונטראס", אפשר לקונגרס להעביר חקיקה שחילקה את האחריות על הגנת הסייבר על מערכות פדרליות בין הסוכנות לביטחון לאומי ובין מכון התקנים האמריקאי

47 Roger R. Schell, "Computer Security: The Achilles' Heel of the Electronic Air Force?" *Air Force University Review*, (1979).

48 William J. Broad, "Computer Security Worries Military Experts", *The New York Times*, September 25, 1983, http://www.nytimes.com/1983/09/25/us/computer-security-worries-military-experts.html

49 National Security Directive #145.

50 חבר הקונגרס מטקסס ג'ק ברוקס כינה את ההוראה של הנשיא רייגן "הרחבה בלתי מתקבלת על הדעת של העוצמה הצבאית מול האזרחים" (ראה – Hearings to Consider H.R. 145, the Computer Security Act of 1987, to Amend the Federal Property and Administrative Services Act of 1949 Brooks Act to improve Federal Computer Systems Security Before the Subcomm. on Legislation and National Security of the H. Comm. on Oversight & Gov't Reform 100th Cong. 281 (1987))

(NIST). החקיקה יושמה, בסופו של דבר, על ידי הוראה נשיאותית של הנשיא ג'ורג' בוש האב ב־1990.[51]

בשנות השבעים של המאה העשרים התחדדה ההבנה בקרב הצבא האמריקאי כי מערכות הנשק המודרניות תלויות בזרימה יציבה ועקבית של מידע. על רקע זה נקבע מושג חדש – "לוחמת מידע". מושג זה נשען על התובנה שזרימת מידע במערכות נשק מתקדמות היא סבוכה ונתונה לאיומים רבים. בנוסף, קציני הצבא האמריקאי הגיעו למסקנה כי לוחמת המידע מאפשרת לפגוע בפיקוד ובשליטה של מערכות הנשק של היריב. אחד האירועים הראשונים בתחום זה היה הטיפול שביצעו האמריקאים בציוד בקרה קנדי שנרכש על ידי ברית המועצות לצינור הגז הטרנס סיבירי, שעל פי הערכות שלא אומתו, גרם לפיצוץ בצינור גז זה ב־1983. לפי אותן הערכות, מערכות התוכנה של חברת הגז הסובייטית, שתפקידן היה להפעיל את המשאבות ומערכות הבקרה, תוכנתו על ידי קוד עוין אמריקאי לשנות את מהירות המשאבות, באופן שיפעיל לחץ על הצינורות ויוביל לפיצוצם.[52]

המשך השימוש בלוחמת מידע היה במלחמת המפרץ הראשונה (1991), אשר אופיינה על ידי רבים כמלחמת המידע הראשונה. קולין פאואל, יו"ר המטות המשולבים של ארצות הברית במהלך המלחמה, סיפר ב־1993[53] על האופן בו התנהלה לוחמת המידע במהלך אותה מלחמה: הוקמו יחידות לוחמת מידע בחיל האוויר (1993), בחיל הים (1994) ובחיל הרגלים (1994). סין ורוסיה, שרצו להיות חלק ממהפכת המידע, אך נאלצו לקנות חומרה ותוכנה אמריקאיות עבור התשתיות שלהן, הבינו שהמערכות האמריקאיות מכילות "פצצות חכמות" שארצות הברית עשויה להפעיל ביום פקודה.[54]

באמצע שנות התשעים חלחלה תובנה נוספת בקרב מקבלי ההחלטות בארצות הברית: פגיעות במרחב הסייבר עשויה לבוא לידי ביטוי לא רק כתוצאה מאובדן מידע רגיש, אלא גם בעקבות פגיעה מכוונת במערכות התשתית הקריטיות של המדינה. מכון "ראנד" התבקש לבדוק את הסוגיה, ולאחר שערך מגוון סימולציות, הגיע למסקנה כי ביטחון הפנים בארצות הברית מעורער, וזאת כתוצאה מהתלות ההולכת וגוברת של המדינה

---

51 National Security Directive # 42: "National Policy for the Security of National Security Telecommunications and Information Systems".

52 החשיפה הראשונית של האירוע הייתה בספר: Thomas C. Reed, *At the Abbys: An Insider's History of the Cold War*, Casemate, Presidio Press, 2005.

53 Chairman of the Joint Chiefs of Staff, "Command and Control Warfare", Memorandum of Policy, No. 30, March 8, 1993, http://www.dtic.mil/dtic/tr/fulltext/u2/a389344.pdf

54 החששות הסיניות מתוארות במאמר –, Wang Pufeng, "The Challenge of Information Warfare" *China Military Science* (1995).

הרוסים הביעו את חששם בראיונות בספר – Adams James, *The Next World War: Computers are the Weapons and the Frontline is Everywhere* (Simon&Schuster Publishing, 1997).

והחברה במרחב הסייבר.[55] מוסדות המהווים חלק מהממשל האמריקאי, כמו משרד מבקר המדינה, בחנו גם הם את הסוגיה והגיעו למסקנות דומות. גם הפנטגון והבית הלבן הקימו ועדות לבחינת הנושא וועדות אלו הגיעו לאותה מסקנה – מרחב הסייבר יצר דרך זולה יחסית לתקיפה, העלולה לגרום לפגיעה אנושה בתשתיות המדינתיות.

שלב ב': המגזר הפרטי מעצים את כוחו

מגמה חשובה נוספת שהחלה באמצע שנות התשעים הייתה התחזקות כוחו של המגזר הפרטי בתהליכי קבלת ההחלטות סביב מרחב הסייבר בארצות הברית. התחזקות זו הגיעה על רקע רצונו של הממשל האמריקאי להתאים את התשתית החוקתית הקיימת לאיסוף מידע לפיתוחים הטכנולוגיים החדשים של התקופה. המשרד למחקר טכנולוגי[56] הגיע בשנת 1984 למסקנה כי המגבלות החוקיות על איסוף מידע ממשלתי אינן רלוונטיות כשמדובר בתשתיות התקשורת הדיגיטלית. בדיוני הקונגרס האמריקאי הושגה אז הסכמה כי יש לעדכן את החקיקה, ואכן ב־1986 חוקק, בתמיכתו של המגזר העיסקי,[57] החוק לשמירת הפרטיות בתקשורת האלקטרונית (Electronic Communication Privacy Act). החוק מרחיב את היריעה ומכליל גם תשתיות טלפוניה ותקשורת דיגיטליות במסגרת ההגבלות החלות על איסוף מידע על ידי הממשל.

תגובת הרשות המבצעת לחקיקת הקונגרס הגיעה בתחילת שנות התשעים. ב־1992 דחה הקונגרס הצעת חוק של ממשל ג'ורג' בוש האב, שדרשה מחברות המפעילות תשתיות דיגיטליות[58] לבנות ממשקים טכנולוגיים שיאפשרו למדינה לאסוף מידע מתשתיות אלו. הייתה זו הפעם ראשונה שבה ניתן היה לזהות הצעה לרגולציה, שיחד עם הלגיטימציה שהיא נתנה לעצם איסוף המידע, נועדה להחליש ביודעין תשתיות דיגיטליות במרחב הסייבר. מגמה זו נמשכה עם ההצעה לפתח חומרה להצפנה ("Clipper Chip"), אשר יחד עם הצפנת המידע מאפשרת לסוכנויות אכיפת החוק לפענח אותה ולגשת למידע. המגזר הפרטי בארצות הברית התנגד להצעה זו מחשש שלא יוכל להתחרות במוצרים של שווקים זרים, שבהם לא מתאפשרת גישה ממשלתית למידע. על רקע זה, הוחלט במכון התקנים האמריקאי כי אימוץ התקן הקריפטוגרפי יהיה על בסיס וולונטרי. השוק האמריקאי הגיב בהתאם, ונמנע כמעט לחלוטין מלאמץ את תקן ההצפנה השנוי

---

55 Roger C. Molander, Andrew S. Riddile and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, California, Rand Corporation, 1966.

56 The Office of Technology Assessment – משרד שנועד לסייע למחוקקים בנושאי ההתפתחות הטכנולוגית, אך נסגר עקב מחסור במשאבים בשנת 1995.

57 Priscilla Regan, *Legislating Privacy*: *Technology, Social Values and Public Policy*, Chapel Hill, University of North Carolina Press, 1995.

58 לדוגמה: חברות טלפוניה ותקשורת.

במחלוקת. בהמשך הוכיחו מדעני מחשב כי הטכנולוגיה שהוצעה הפכה את ההצפנה לפריצה לכל, והממשל האמריקאי החליט לוותר על תקן זה.[59]

ב־1994 כבר לא הצליח הקונגרס להתנגד ליוזמות הממשל, ואישר הצעת חוק שנועדה להקל על פעילותן של סוכנויות אכיפת החוק ודורשת מספקי תשתיות דיגיטליות לבנות במוצריהן ממשקים שיאפשרו גישה ממשלתית אליהן ואיסוף מידע באמצעותן (Communication Assistance to Law Enforcement Agencies – CALEA). בעקבות זאת פרסמו חברות שונות, ובהן Cisco, את הארכיטקטורה החדשה שלהן, שהתבררה כלא מאובטחת.[60] בלחץ מסיבי מצידם של בעלי עסקים ויצרני חומרה בארצות הברית, הסיר הממשל בשנת 2000 את הגבלות התקן בנושאי הצפנה, דבר שהביא לשינוי סדרי עדיפויות ולייחוס חשיבות עליונה לאינטרסים של המגזר הפרטי.

מאז אמצע שנות התשעים, כאשר יותר ויותר מוסדות וספקי שירותים מדינתיים עברו לעבודה דיגיטלית, הממשל הפדרלי החל להאציל סמכויות מוסדיות ואחריות לביטחון ברשתות השונות. ב־1995 קיבל משרד הניהול והתקציב (Office of Management and Budget – OMB) לראשונה סמכויות להגן על מידע הנמצא בידי הממשל הפדרלי. ב־1996 עודכנו סמכויות אלו בחוק קלינגר־כהן, שקבע שכל משרד ממשלתי ישמש כרגולטור המגזרי בתחום שיפוטו, כאשר משרד הניהול והתקציב יהיה זה שיפקח על כולם.

בנוסף לאסדרה המוסדית, החלה בשנים אלו קביעת תקנים לרגולציה לאבטחת מערכות ממוחשבות מחוץ לתחום הפדרלי. כך, למשל, התיקון השני לחוק ביטוח הבריאות (Health Insurance Portability and Accountability Act – HIPAA), שנחקק ב־1996, מטיל על משרד הבריאות האמריקאי לקבוע תקנים לאבטחת מידע ולשמירה על הפרטיות, שיחייבו את כל נותני שירותי הבריאות. לאחר שקיבל יותר מאלפיים התייחסויות מצד הציבור, השלים משרד הבריאות את תקנות החוק בשנת 2003 והחל לאכוף אותן ב־2005.

בשנת 1998 הייתה התייחסות ראשונה גם לתחום התשתיות הקריטיות. הנשיא קלינטון, בהוראה נשיאותית מספר 63, ניסה להסדיר את עבודת סוכנויות הממשל השונות במטרה לצמצם פגיעה אפשרית בתשתיות הקריטיות של המדינה. מטרתה העיקרית של ההוראה הייתה לשפר את יכולות ההגנה של סוכנויות פדרליות ואת יכולות

---

59 פירוט על התנהלות הממשל בנושא זה ניתן למצוא בספר: Diffie Whitfield and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge, MIT Press, 1998, pp. 212-23.

60 דוגמה בולטת לסיכונים שביישום ארכיטקטורה של טלפונים סלולריים המאפשרת איסוף מידע נחשפה ב־2007, לאחר שחברת Vodaphone ביוון הודתה כי בוצע ציתות לא חוקי למכשירי הטלפון של ראש הממשלה, ראש עיריית אתונה וכמאה בכירים נוספים בשירות הציבורי. לפרטים נוספים ראו: Vassilis Prevelakis and Diomidis Spinnelis, "The Athens Affair", *IEEE Spectrum*, June 29, 2007, http://spectrum.ieee.org/telecom/security/the-athens-affair

המדינה בכלל להגן על עצמה מפני מתקפות על תשתיות קריטיות, תוך שיתוף פעולה עם השחקנים במגזר הפרטי.[61] ההוראה מנתה עשרה מגזרים שהוגדרו כ"קריטיים"[62] ויצרה ארבעה מוסדות, במסגרת גופים שונים, כדי לשפר את יכולות ההגנה.[63]

מגזר נוסף שקיבל מענה רגולטורי בשנות התשעים של המאה העשרים הוא המגזר הפיננסי. ב־1999 התקבל חוק Gramm-Leach-Bliley, הדורש ממוסדות פיננסיים שקיפות כלפי לקוחותיהם בנושאים הנוגעים לשיתוף מידע ולהגנה נאותה על מידע אישי רגיש. החוק מגדיר את מוסדות המדינה הנדרשים ליישמו ותובע מהם לגבש תוכנית הגנת מידע מבוססת סיכון, בהתאם לאיומים המשתנים.

מתקפות הטרור ב־11 בספטמבר 2001 גררו עיסוק מוגבר ברגולציה של ערוצי איסוף מידע על ידי הממשל מתשתיות דיגיטליות, וכן תשומת לב מוגברת לתשתיות הקריטיות ולרשתות הממשלתיות. שני החוקים המרכזיים הנוגעים לחוסנו של מרחב הסייבר בתקופה זו היו Patriot Act משנת 2001 ו־Homeland Security Act משנת 2002. ה־Patriot Act אִפשר לממשל האמריקאי לפתוח ערוצים רבים ומגוונים לאיסוף מידע ממערכות דיגיטליות. חוק Homeland Security כלל, בנוסף להקמת משרד ייעודי לביטחון המולדת, חוק נוסף – ה־Cyber Security Enhancement Act, שמטרתו הייתה להפחית את ההגבלות על ספקיות אינטרנט בארצות הברית להעביר מידע לממשל ולהחמיר את הסנקציות על גישה לא מורשית למערכות מחשבים.

במקביל לשתי חקיקות מרכזיות אלו, הוציא הנשיא בוש הבן הוראות סודיות[64] שאפשרו לסוכנות לביטחון לאומי של ארצות הברית לאסוף מידע ללא צורך בצווים כדי להכיר טוב יותר את מפת איומי הסייבר ולנטר תקשורת בין־לאומית הקשורה לפעילות סייבר שהוגדרה כעוינת. התובע הכללי תרם את חלקו לנושא, כשהודיע שההגבלות על איסוף מידע ברשת האינטרנט אינן חלות על ה־FBI וכי הארגון יכול, אם יחפוץ בכך, לנטר את המתרחש בצ'אטים, במאגרי מידע פרטיים ובאתרים שונים.

ב־2002 חוזקה הגנת הרשתות הממשלתיות באמצעות Federal Information Security Management Act (FISMA). חוק זה מחייב כל סוכנות פדרלית לפתח תוכנית להגנת מידע עבור כל מערכות המחשבים המשרתות את הסוכנות, וזאת

61 רוב התשתיות הקריטיות בארצות הברית מופעלות על ידי המגזר הפרטי.

62 תקשורת, פיננסים, מים, תחבורה, שירותי חירום, כיבוי אש, בריאות, חשמל, נפט ואחסון.

63 המוסדות כוללים את המרכז לסנכרון הגנה על תשתיות ונגד טרור, הכפוף לנשיא; המשרד לתשתיות קריטיות, הכפוף למשרד המסחר; המשרד להגנה על תשתיות קריטיות, הכפוף ל־FBI ולגורמי אכיפת החוק השונים; המועצה המייעצת לתשתיות לאומיות (NIAC), הכפופה למשרד לביטחון המולדת ומטרתה היא לשפר את הקשר עם המגזר הפרטי.

64 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times,* December 16, 2005, http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html

בהתבסס על אסטרטגיה של תעדוף וניהול סיכונים של מכון התקנים האמריקאי ובפיקוחו של משרד הניהול והתקציב בבית הלבן. כל סוכנות פדרלית אימצה "תקני אבטחה מינימליים לרשתות פדרליות" (FIPS 200) בהתאם למסמך ההנחייה של מכון התקנים (NIST Special Publication 800-53), וכל סוכנות בנפרד קבעה את קטגוריית האבטחה הנדרשת עבורה, על בסיס התקן FIPS 199.

שלב ג': פעילותן של סוכנויות רגולטוריות עצמאיות

בנוסף לחקיקה, השתכללה בעשור האחרון פעילותן של סוכנויות רגולטוריות עצמאיות להגנת סייבר, כל אחת בתחום אחריותה. סוכנויות אלו מספקות את חקיקות המשנה למעטפת שיצרו החוקים הפדרליים, וכן עוסקות ביישום ובאכיפה.

הסוכנות הפעילה ביותר להגנת המידע בארצות הברית היא סוכנות הסחר הפדרלית (Federal Trade Commission – FTC). הסוכנות נכנסה הלכה למעשה לוואקום שנוצר כתוצאה מהיעדר רגולטור הגנת מידע מרכזי למגזר הפרטי ואכפה את הגנת המידע בעילה של הצורך לדאוג למסחר הוגן. יכולת הסוכנות לאכוף הגנת מידע בסייבר במגזר העיסקי קיבלה חיזוק משמעותי ב־2015, כאשר בית משפט פסק לטובת הסוכנות בתביעה שהוגשה נגד סמכותה לאכוף פרקטיקות הגנה בסייבר. השופט, בהחלטה תקדימית, פסק כי לסוכנות יש סמכות ואחריות לפעול מול המגזר העסקי, כאשר חברות אינן עושות מספיק על מנת להגן על המידע של לקוחותיהן.

לסוכנות הסחר הפדרלית היה תפקיד דומיננטי ביישום ואכיפה של חוקי הגנת מידע מגזריים של הממשל הפדרלי, הן בתחום הבריאות והן בתחום הפיננסים. הסוכנות גם הוציאה, יחד עם משרד המסחר של ארצות הברית, הנחיות לא מחייבות להגנת סייבר ופרטיות עבור ארגוני תשתית במגזר העיסקי שהוגדרו כלא קריטיים (non-critical infrastructure sectors), אך נחשבים לחיוניים לתפקודה של הכלכלה האמריקאית. ההנחיות עסקו בפיתוח משותף עם המגזר הפרטי של תקנים לאבטחת מידע, שאמורים היו להפוך לתקנים מחייבים עבור התעשייה האמריקאית. תקנים אלה כללו דרכים לצמצום פגיעויות במרחב הסייבר, מתן תמריצים עבור שקיפות באירועי סייבר, שיתוף מידע, וכן הסרת אחריות במקרה של פריצה. כאמור, מדובר בהנחיות לא מחייבות המאפשרות שיקול דעת נרחב לכל ארגון.

סוכנות רגולטורית נוספת בעלת תפקיד דומה אך משני יותר במרחב הסייבר הינה הרשות להגנת הצרכן (Consumer Financial Protection Bureau). ב־2016 קנסה הרשות לראשונה חברה שלא עמדה בתקנים הבסיסיים להגנה בסייבר. למעשה, עוד ב־2014 ניסתה הרשות לפעול לקידום שקיפות באירועי סייבר ברמה הפדרלית, אך ללא הצלחה.

סוכנות פדרלית הפעילה מאוד במרחב הסייבר היא הרשות לניירות ערך (Securities and Exchange Commission – SEC). לאורך השנים עסקה הרשות ביישום חוקים

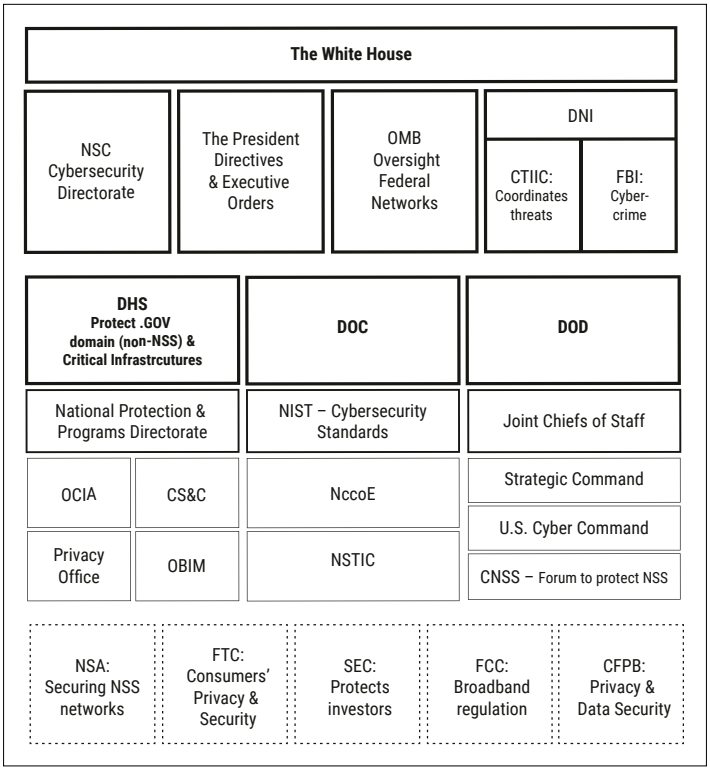
פדרליים הנוגעים להגנת סייבר במגזר הפיננסי ושמה דגש מיוחד על איומי גניבת זהות ועל מערכות פיננסיות שיציבותן חיונית ליציבות המשק כולו. לרשות לניירות ערך יש כוח רב, אך הוא מוגבל לגזרת האחריות שלה – התחום הפיננסי. בולטותה וחשיבותה של הרשות בהגנת הסייבר באו לידי ביטוי בפעילותה של הרשות לרגולציה פיננסית (Financial Industry Regulatory Authority – FINRA), המאגדת את כל החברות הכפופות לרגולציה של הרשות לניירות ערך ומנחה אותן כיצד ליישם הגנת מידע, כך שתעמוד בתנאיי הרגולציה המבוקשים. FINRA מהווה למעשה זרוע ביצועית של הממשל הפדרלי בתחום הפיננסי וגורם המתווך את הרגולציה לגופים הרלוונטיים מתוך מטרה להעלות את החוסן הפיננסי ברמה הלאומית. בנוסף לכך, מקיימת הרשות לניירות ערך תהליך דומה מול עסקים קטנים ובינוניים, הכולל מיפוי חולשות סייבר ותעדוף השקעות בהגנה בהתאם ליכולות הכלכליות המוגבלות שלהם. ב־2016 קנסה הרשות לראשונה חברה שלא עמדה בתנאי הסף להגנה בסייבר.

סוכנות פדרלית נוספת הפעילה בתחום הסייבר מאז 2015 היא רשות התקשורת הפדרלית (Federal Communications Commission – FCC), שעיסוקה העיקרי הוא בתשתיות תקשורת. הרשות מנחה ספקי תקשורת בנושאי הגנת סייבר, ובכלל זה כיצד ניתן ליישם את תפיסת ההגנה של מכון התקנים האמריקאי לרשתות פדרליות גם על רשתות של מפעילי תקשורת. ב־2016 פרסמה הרשות הנחיות מחייבות לספקי תקשורת בנושאי הגנת מידע ופרטיות הצרכנים. לפי אותן הנחיות, מפעילי תקשורת לא יוכלו עוד לסחור במידע אישי של לקוחותיהם ללא הסכמתם. בכך קבעה רשות התקשורת הפדרלית תקדים רגולטורי להגנה ולשמירה על פרטיותו של מידע אישי במרחב הסייבר.[65] כניסתו של הנשיא טראמפ לבית הלבן ב־2017 הביאה למינוי יושב ראש חדש לרשות, וזה החליט לבטל את תקנות הפרטיות אשר הותקנו על ידי קודמו.

הגוף המתכלל את הטיפול במרחב הסייבר בארצות הברית הוא המשרד לביטחון המולדת. מעֵבר להגנה על מתחם האתרים של הממשלה, מספק המשרד עזרים להגנה על התשתיות הקריטיות בארצות הברית ועוסק בשיתוף מידע שנועד לחזק את החוסן הכללי של מרחב הסייבר האמריקאי. המשרד לביטחון המולדת פועל כ"רגולטור־על", ומנחה את כל משרדי הממשלה בנושאים הקשורים להגנה על התשתיות הקריטיות שבתחום שיפוטם. בנוסף, לכל משרד פדרלי יש תוכנית הגנה ייעודית להתמודדות עם האתגרים הייחודיים הניצבים בפני התשתיות הקריטיות שבמסגרת אחריותו. יתר על כן, המשרד לביטחון המולדת נותן סיוע לניהול אירועי סייבר בזמן אמת,

65 להרחבה על המהלך התקדימי ראו: Ido Sivan-Sevilla, "The FCC's Latest Privacy Regulations: A New Stance on Private-Sector Protections?" *The Columbia Science and Technology Law Review*, December 12, 2016, http://stlr.org/2016/12/12/the-fccs-latest-privacy-regulations-a-new-stance-on-private-sector-protections/

מטפל בנושאי המודעות והחינוך של עתודת מובילי הסייבר של ארצות הברית ועורך מחקרים בתחום זה. לאחרונה החל המשרד לעסוק גם בפיתוח שוק ביטוח מפני נזקי סייבר עבור ארגוני המגזר הפרטי, במטרה לעודד צמיחה ולתת תמריצים לצורך הגנה נאותה על המידע. כמו כן, מסייע המשרד לביטחון המולדת לרשויות השונות העוסקות בהתמודדות עם פשיעת סייבר.



תרשים 1: סוכנויות ומוסדות העוסקים בנושא ביטחון הסייבר בארצות הברית

רגולציה מדינתית להגנה בסייבר בארצות הברית

אירועי סייבר משמעותיים אינם נחלתו של הממשל הפדרלי בלבד. יש התקפות משמעותיות על בנקים,[66] ניסיונות לפגוע בתשתיות קריטיות לאומיות[67] ופגיעה במערכות

66 על הפגיעה בבנק הגדול JP Morgan ראו: "What Lies behind the JPMorgan Chase Cyber-Attack", *The Economist*, November 12, 2005, http://www.economist.com/news/business-and-finance/21678214-criminal-economy-developing-faster-lawful-one-can-defend-itself-what-lies-behind

67 על הפגיעה בתשתיות החשמל באוקראינה ראו: Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

הסייבר בערים עצמן.[68] התקפות כופר על מחשבים ארגוניים ואישיים, וכן מידע אישי רגיש הנאסף מדי יום ממחשבים אישיים ומחברות קמעונאיות, לא תמיד דורשים התערבות ברמה הפדרלית. נושאים אלה נתפסים כ"רכים" יותר בהקשר של מאמצי ההגנה בסייבר. לתוך הוואקום הזה נכנסו המדינות השונות בארצות הברית, הפועלות לבניית מרחב דיגיטלי חסין ולשמירה על הפרטיות של אזרחיהן.[69]

המדינות השונות בארצות הברית משכילות לספק גמישות, מהירות תגובה וחדשנות, העולות בקנה אחד עם השינויים התכופים בעולם הטכנולוגי ורחוקות מ"גרירת הרגליים" האופיינית בנושאי חקיקה ברמה הפדרלית.[70] גם יכולת ההשפעה של "יזמי מדיניות"[71] כריזמטיים בכל אחת מהמדינות הינה גבוהה לאין שיעור מיכולות ההשפעה של מחוקקים ברמה הפדרלית. מדינות שנשרכו מאחור בנושאי הגנת הסייבר השכילו להתגבר במהירות על מכשולים ביורוקרטיים קודמים בזכות "יזמי מדיניות" שהיו במקום הנכון בזמן הנכון וידעו "לדחוף" מדיניות להגנת סייבר עד למימושה.

אחד החסרונות המהותיים ברמת המדינות בהשוואה לרמה הפדרלית הוא היעדר מודיעין סייבר מסַפק, ממנו נהנות לרוב סוכנויות פדרליות.[72] סוכנויות אלו נהנות מפירותיהם של ה־NSA וה־FBI בכל הקשור למודיעין על התקפות סייבר, בעוד שתחקור תקיפות ברמת המדינות מתבצע על בסיס יכולות מקומיות, והצעדים הננקטים שם הם על דעתו של המחוקק המדינתי בלבד.[73] היעדר מודיעין איכותי עשוי להסביר את אסטרטגיית הסיכון אותן נוקטות המדינות בארצות הברית, המתבססת על ביטוח

---

68 למשל, ראו הפגיעה במארס 2018 בעיר אטלנטה שבמדינת ג'ורג'יה בארה"ב על ידי התקפות כופר שדרשו מהמדינה השקעה של 2.6 מיליון דולר – Lilay Hay Newman, "Atlanta Spent $2.6M to Recover From A $52,000 Ransomware Scare", *Wired.com*, April 23th 2018. Available at https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

69 חובת הדיווח על אירועי סייבר הכוללים פגיעה בפרטיות חלה רק ברמת המדינות בארצות הברית. הממשל הפדרלי טרם השכיל להעביר חוק בנושא זה חרף ניסיונות רבים בשנים האחרונות לעשות זאת.

70 על ההבדלים בין הרמה הפדרלית לרמה המדינתית ראו: Paul Lipman, "4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective)", *Government Technology*, July 17, 2015, http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html

71 המושג "יזם מדיניות" שאול מהתיאוריה של ג'ון קינגדון (1988) על הליך עיצוב המדיניות הציבורית, בו יזם מדיניות מוכשר משכיל לחבר בין בעיית מדיניות ובין פתרונה, במידה והסביבה הפוליטית מאפשרת לקבוע מדיניות כזאת.

72 על הפער המודיעיני בין הרמה הפדרלית לרמת המדינות ראו: Amanda Ziadeh, "States vs. Feds: Who Does Cybersecurity Better?" *Government Cloud Insider*, November 4, 2015, https://gcn.com/articles/2015/11/04/fed-vs-sl-cybersecurity.aspx/

73 יש לסייג את הדברים כאשר מדובר בהתקפות רחבות היקף המחייבות את התערבות הרמה הפדרלית, כמו התקפות על מערכות פיננסיות, הונאות משמעותיות, חשיפת מידע רפואי וכדומה.

סייבר ופיזור סיכונים בין בעלי פוליסות ביטוח, וזאת בהשוואה למניעה ולצעדים פרו־אקטיביים על בסיס מודיעין איכותי, הננקטים ברמה הפדרלית.[74]

אחד האתגרים הבולטים איתם נדרשות המדינות בארצות הברית להתמודד הוא הגנה על התשתיות הקריטיות בתחומן. גבולות הגזרה של תשתיות אלו בעידן הדיגיטלי אינם ברורים דיים, וחלוקת האחריות בין המדינה ובין הממשל הפדרלי הינה נושא השנוי במחלוקת.[75] בלבול זה יוצר תרבות שבה ארגוני תשתיות קריטיות משתדלים לעמוד בדרישות הרגולציה הן ברמת המדינות והן ברמה הפדרלית, אך עסוקים פחות באפקטיביות ובמידת ההתאמה של דרישות אלו לצורכי הגנת הסייבר.

אתגר נוסף הוא הגנה על פרטיות הצרכנים ואכיפת תקנים ראויים לאבטחת מידע – מטרות המשלימות זו את זו. המדינות נוקטות דרכים שונות כדי להתוות תקני הגנה, ומיישמות מדיניות מחמירה בכל הנוגע לחובה לדווח על נזקי סייבר ולפצות אזרחים שפרטיותם נפגעה. יש מדינות בארצות הברית שהיעדר היכולת שלהן לשאת בעלויות גבוהות מדי הביא אותן להטיל את העלויות על החברות עצמן ולעודד את צמיחתו של שוק ביטוח בתחום הסייבר. העתקת האחריות על סיכוני הסייבר אל החברות ועידוד שוק לפיזור סיכונים מאפשרים למדינות לגלות אפקטיביות בהתגוננות מפני סיכונים אלה, על אף היעדר תקציבים מספיקים לכך.

תפקידן של המדינות השונות בארצות הברית בהקשר לביטחון הסייבר הוא רחב ומשלים את תפקידיו של הממשל הפדרלי בתחום זה. להלן ייסקרו צדדים שונים בתפקוד המדינות, ובכלל זה האופן בו הן משלימות את הרגולציה ברמה הפדרלית ונותנות מענה בתחומים בהם הממשל הפדרלי מתקשה לקבל החלטות.[76] כן תוסבר הדרך בה רגולציה להגנת הסייבר מאפשרת למדינות השונות לחזק את סמכותן מול ארגונים וחברות הפועלים בתחום שיפוטן. לבסוף ייסקר האופן בו המדינות יכולות, בזכות גמישותן היחסית, לקדם מיזמים ושיתופי פעולה מקומיים שמטרתם לתת מענה טוב יותר להגנת הסייבר.[77]

---

74 למשל, לרמת המדינה אין יכולת לבצע תקיפה בתגובה לפגיעה (hack back methodology).

75 ראו דוח של משרד מבקר המדינה אמריקאי בנושא זה: G. C. Wilshusen, "Cybersecurity: Challenges in Securing the Electricity Grid", Government Accountability Office, July 17, 2012.

76 התחום הבולט ביותר הוא פרטיות – הגנה על מידע אישי. מדינות רבות מספקות מעטפת חוקים ורגולציה נוקשה, ובכך לא רק תורמות לשמירה על הפרטיות, אלא מסייעות בעקיפין לבעיית ההגנה בסייבר. בפועל, מנהלי אבטחת מידע רבים מציינים רגולציה זו כאחד התמריצים ליישום הצפנה רחבה במערכות המידע של ארגונים.

77 לדוגמה, ראו היוזמה שמובילה מדינת ניו יורק עם רגולציית ביטחון סייבר נוקשה ומפורטת כלפי המגזר הפיננסי: Kevin Townsend, "New York State Imposes New Cybersecurity Regulation for Financial Services", *Security Week*, January 2, 2017, http://www.securityweek.com/new-york-state-imposes-new-cybersecurity-regulation-financial-services

המדינה כיישות רגולטורית משלימה לממשל הפדרלי

בדצמבר 2015 הוקם ערוץ סיוע "רשמי" בין הממשל הפדרלי ליישויות ממשלתיות, וביניהן המדינות בארצות הברית. ערוץ זה התבסס על החוק לשיתוף מידע על איומי סייבר (CISA) הנותן, בין השאר, למדינות השונות ממשק כמעט אוטומטי לשיתוף מידע על אירועי אבטחה ברשתות הממשלתיות. הממשל הפדרלי גם יוכל לסנכרן מידע זה עם מקורות מידע נוספים ולהזהיר את המדינות ברחבי ארצות הברית מבעוד מועד.[78] החוק תקף גם ליישויות בשוק הפרטי האמריקאי ונותן תמריצים רבים לשיתוף מידע, ובכלל זה הסרת אחריות במקרה של פריצה למערכות והבטחה לחיסיון המידע. אלה תמריצים משמעותיים עבור השוק הפרטי, האטרקטיביים גם ברמת המדינות, וזאת נוכח העובדה שאותן מדינות נהנות מסיוע הזרועות הפדרליות כדי לזהות איומים שמקורם בחברות הפועלות בתחומן.

החשיבות בשיתוף מידע כזה גדולה, בעיקר בהקשר של תשתיות קריטיות בתחום המדינה. כתשעים אחוזים מתשתיות אלו הינן בבעלות פרטית[79] ונמצאות בשטח השיפוט של המדינות השונות. אי לכך, חקיקה זאת מאפשרת למדינות לסייע בשיתוף מידע בין המגזר הפרטי למגזר הציבורי, מה עוד ולמשרד לביטחון המולדת יש מחלקה ייעודית להבטחת שיתוף הפעולה ברמת המדינות השונות. לכל מדינה יש גם אחריות להגן על הרשתות הממשלתיות שלה. לדוגמה, הממשל הפדרלי, בחסות המשרד לביטחון המולדת, מימן סריקת חולשות ברשתות ממשלתיות ומתן כלים לפתרונם במדינת ניו יורק.[80] לעומת זאת, בקליפורניה הוקם צוות מומחים ייעודי מקומי המגבש המלצות לקובעי המדיניות כיצד לנהוג בזמן חירום ומתווה תוכנית אסטרטגית להגנה על רשתות הממשלה המקומית בזמן תקיפה.[81]

צוותים ייעודיים לנושאי מזעור סיכונים ולגיבוש תגובות של מדינות לאירועי סייבר מקדמים, בנוסף לתפקידם בניהול אירועים, גם את מודעות הציבור הרחב לאירועים

78 על החוק החדשני וההנחיות כיצד לשתף מידע עם הממשל הפדרלי ראו: Daniel K. Alvarez and Naomi Parnes, "DHS, DOJ Release Final Cyber Threat Information Sharing Guidelines Under CISA", *Willkie Farr and Gallagher*, June 24, 2016, http://www.willkie.com/~/media/Files/Publications/2016/06/DHS_DOJ_Release_Final_Cyber_Threat.pdf

79 Diffie Whitfield and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, Cambridge, MIT Press, 1998, pp. 212-23.

80 עוד על הפרויקט ראו באתר המשרד לשירותי מידע וטכנולוגיה של מדינת ניו יורק: New York State Division of Homeland Security and Emergency Service – Office of Cyber Security, "NYS Local Government Vulnerability Scanning Project, September 22, 2011, https://www.its.ny.gov/document/nys-local-government-vulnerability-scanning-project

81 ראו הדוח הסוקר באופן השוואתי את המדיניות במדינות מפתח ומפרט על יוזמה זו בקליפורניה: Francesca Spidalieri, "State of the States on Cybersecurity", Pell Center, November 2015, http://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf

אלה. קליפורניה היא מקרה פרטי מעניין. הצוות הייעודי בה נתון לסמכות המשרד לשירותי חירום (California Office of Emergency Services) ואחראי הן על איומי סייבר והן על איומים פיזיים על תשתיות דיגיטליות בכלל ותשתיות קריטיות בפרט.

המדינות השונות בארצות הברית משתמשות בתקני הגנה קיימים להגנת המידע, כגון Payment Card Industry Data Security Standards (PCI DSS) – דרישות אבטחה עבור חברות המספקות שירותי תשלום מקוונים – כדי לעודד חברות שונות לאמצם. מדינת וושינגטון, למשל, אימצה בשנת 2010 חוק המסיר אחריות מחברות תשלום שחוו פריצה אך עמדו בתקני PCI, וזאת כדי לתמרץ חברות אחרות לאמץ תקנים אלה.[82] בעקבות מדינת וושינגטון, אימצו מינסוטה ונבדה חוקים דומים. מסצ'וסטס ונבדה אף הרחיקו לכת ואימצו "רגולציה מרשמית",[83] שבמסגרתה קבעו לחברות שונות את התקנים שבהן עליהן לעמוד. מדינות אלו בחרו לאמץ את התקן של חברות התשלומים המקוונים כתקן מחייב, ומסצ'וסטס אף דרשה לקבל בכתב את תוכנית הגנת המידע של כל חברה, שלפי הנחייתה אמורה לכלול פיקוח על ספקי צד שלישי, הערכות סיכונים והטלת סנקציות במקרה של הפרת דרישות הגנת המידע בתוך החברה.[84] מדינת ניו יורק חוקקה בשנת 2015 את ה־Data Security Act, הקובע כי ארגונים וחברות בניו יורק חייבים להגן על כל שירות שאוסף ומעבד מידע אישי. לצורך זה הורחבה ההגדרה של מידע אישי והיא כוללת מספר רשיון נהיגה, מספר חשבון בנק, מידע רפואי, כתובת הדואר האלקטרוני וסיסמה. עם זאת, ניו יורק מסתפקת בתעודה מסַפק צד שלישי המבטיחה את רמת ההגנה של הארגון המדובר, כדי שניתן יהיה להגדירו כ"מאובטח ברמה ראויה".

החוקים שנחקקו במדינות השונות כרוכים בעלויות לא מעטות עבור חברות מסחריות, וזאת בנוסף לצורך של ארגונים, הנובע מחוקים אלה, לבחון מחדש את מדיניות הגנת המידע שלהם. במסגרת זו מקבלים תשומת לב מיוחדת סיווג מידע אישי והאופן בו הוא מוחזק: חברות שוקלות מחדש את האופן בו הן מגיבות לאירועים ואת החוזים

---

82 Tom Kemp, "Buckle Up with Cybersecurity … it's the Law", *Forbes*, February 1, 2012, http://www.forbes.com/sites/tomkemp/2012/02/01/buckle-up-with-cybersecurity-its-the-law/#5fa6b50b933f

83 בניגוד ל"רגולציה תהליכית", "רגולציה מרשמית" היא הצורה הקשיחה והמסורתית של רגולציה, הקובעת מבעוד מועד באילו תנאי סף יש לעמוד. לסקירה תיאורטית של התחום ראו: Gilad Sharon, "It Runs in the Family: Meta-Regulation and its Siblings", *Regulation & Governance*, Vol. 4, No. 4, 2010, pp. 485-506.

84 לדרישה המדינתית הרשמית ראו: Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, "A Small Business Guide: Formulating A Comprehensive Written Information Security Program", 2016, http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf

עם ספקי צד שלישי, כדי לוודא שהמידע שלהן מוגן לכל אורך תהליך העבודה.[85] ההבדלים במדיניות הגנת הסייבר במדינות השונות יוצרים גם הם אתגרים לחברות ולארגונים הפועלים באותן מדינות, ואלה נאלצים להתמודד עם שורה של תקנים ועם היכולת לעמוד בהם (כמו בפלורידה וקליפורניה), וגם לקבל על עצמם את הדרישות הטכניות שמציבה הרגולציה (כמו במסצ'וסטס).

האופן בו מדינות בוחרות להכיל רגולציה של הגנת מידע כדי לשמור על עסקים וארגונים מפני התקפות סייבר בתחום שיפוטן, משתית את העלויות כמעט לחלוטין על הארגון עצמו. בקליפורניה, למשל, הדרישות המחמירות עשויות להיות קשות מדי עבור בעלי עסקים קטנים ובינוניים, שלא יצליחו לעמוד בעלויות ועשויים להתעלם מבעיות אבטחה, או לחילופין להיסגר, ובדרך זו לצמצם את התחרות במשק. מדיניות ביטוח ראויה עשויה להיות פתרון ביניים הולם במקרה כזה.

המדינות השונות בארצות הברית מכתיבות למעשה את ההתפתחויות בתחום הדיווח על אירועי סייבר. קליפורניה הייתה החלוצה בתחום זה, כאשר חקקה ב־2003 חוק המחייב חברות לדווח על גניבת מידע אישי של לקוחותיהן,[86] ובכך סללה את הדרך ל־46 מדינות נוספות בארצות הברית לחוקק חוקים דומים.[87] קליפורניה דורשת מחברות ומסוכנויות מדינתיות לדווח ולפצות את לקוחותיהן במקרה של פריצת סייבר וגניבת מידע ממערכות ארגוניות, כולל דיווח לתובע הכללי של המדינה. מאחר וחברות אינן ששות לשאת בהוצאות הקבועות בחוק במקרה של פריצה ושל הדיווח בעקבותיה, החקיקה היוותה, הלכה למעשה, תמריץ לחברות להתגונן מבעוד מועד.

עדכון שנעשה לחקיקה בקליפורניה בשנת 2016 מחייב חברות לאמץ עשרים דרישת אבטחה שונות, וקובע כי אלו שיעשו זאת יזכו, במקרה של פריצה, לסיוע מהמדינה. בכך הטילה קליפורניה את עלויות ההגנה והדיווח על החברות, תוך איום בסנקציות במקרה של אי־ציות לחוק. מדינות אחרות, כמו פלורידה, ארקנסו ומרילנד, אף הרחיקו לכת והרחיבו את היריעה לנושאים כמו חובת הדיווח על פריצה ולוח הזמנים שבמסגרתו יש להודיע ללקוחות על פגיעה בפרטיותם. כך, למשל, פלורידה קיבלה ב־2014 את חוק

---

85 Jim Halpert, "State Breach Notification Laws – Updates from 2015 Legislative Sessions, 6 Action Steps for Companies", *DLA PIPER,* July 20, 2015, https://www.dlapiper.com/en/us/insights/publications/2015/07/state-breach-notification-laws/

86 תופעה זו שכיחה בתחום הרגולציה בארצות הברית ונקראת California Effect - רגולציה שהתחילה בקליפורניה, חלחלה למדינות אחרות והשפיעה על מבנה השוק האמריקאי. לפרטים נוספים ראו: David Vogel, "Environmental Regulation and Economic Integration", Yale Center for Environmental Law and Policy, 1999, http://www.iatp.org/files/Environmental_Regulation_and_Economic_Integrat.pdf

87 מעקב אחר החקיקה במדינות השונות בארצות הברית בוצע על ידי ה־National Conference of State Legislatures.

הגנת המידע (The Information Protection Act), המחייב דיווח על איסוף מידע אישי באופן לא מורשה כתוצאה מפריצה, כמו גם על גישה למידע אישי על ידי עובדים מתוך הארגון הפועלים ללא הרשאה. לפי אותו חוק, הודעה ללקוחות על הפרת פרטיותם צריכה להינתן תוך שלושים יום במקום 45 יום, כפי שנהוג במדינות אחרות.[88]

חיזוק סמכות המדינות ברגולציית הסייבר

לא כל המהלכים המדינתיים בתחום הגנת הסייבר נגזרים משיתוף פעולה עם הרמה הפדרלית בארצות הברית. קיימים נושאים בהם המדינות השונות שומרות על סמכויותיהן, כמו, למשל, בתחומי התשתיות המדינתיות ופרטיות האזרחים – נושא אותו הממשל הפדרלי זנח במידה רבה. המדינות השונות מנצלות את העובדה כי הן מכירות מקרוב את התשתיות בשטחן ופועלות להגביר את מאמצי הגנת הסייבר על תשתיות אלו. לדוגמה, חברות תשתית בפנסילבניה נדרשות לדווח על כל מתקפה הגורמת לנזק של יותר מ־50,000 דולר. בטקסס נדרשות מערכות תשתית פחות "מסורתיות", כגון מערכות מונים, לעמוד בתקני אבטחת מידע שקבע ארגון עצמאי, בשיתוף הרשות לתשתיות ציבוריות של המדינה (Texas PUC).

על פי מכון המדיניות Bipartisan, הסמכות של המדינות השונות בארצות הברית להתגונן מפני התקפות סייבר אינה מוגבלת לרשות לתשתיות ציבוריות של כל מדינה (PUC), אלא כוללת גם את משרדי המושל, משרדי האנרגיה, וראש תחום מערכות המידע (CIO) של כל מדינה. כחלק מתפקידו המרכזי של המושל בתיאום אבטחת הסייבר, הקים איגוד מושלי המדינות (National Governors Association) מרכז משאבים חדש לאבטחת הסייבר במדינות השונות. מרכז זה אמור לבחון את הצורך של כל מדינה לגבש מדיניות הולמת לאבטחת סייבר לתשתיות הנמצאות בגבולותיה ובבעלותה.[89]

המאבק בין המדינות השונות בארצות הברית ובין הממשל הפדרלי בתחום פרטיות המידע והגנתו בא לידי ביטוי בולט במגזר הבנקאות, כאשר לבנק מסויים יש לקוחות במספר מדינות, אך עליו לעמוד ברגולציית דיווח אירועים של המדינה בה הוא מתארח. במסצ'וסטס, לדוגמה, קיים חוק הדורש מחברות פיננסיות לדווח בכתב על האופן בו

88 לסקירה על החוק בפלורידה ראו: George Grachis, "Florida Privacy Law Adds Breach Notification and Strengthens Compliance", *CSO*, September 2, 2016, http://www.csoonline.com/article/3112741/leadership-management/florida-privacy-law-adds-breach-notification-and-strengthens-compliance.html

89 Michael Hayden, Curt Herbert, Susan Tierney, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat", Bipartisan Policy Center, February 28, 2014, http://bipartisanpolicy.org/library/cybersecurity-electric-grid/

הן מגנות על מידע אישי וכיצד הן משתמשות בו.[90] במדינות אחרות, דוגמת קליפורניה, המדינה דורשת ואוכפת תקנים מחמירים לשמירה על הפרטיות, על פיהם חברות שלא יעמדו בדרישות יוגדרו כ"נעדרות אבטחה סבירה", ייאלצו לעמוד למשפט ויחויבו לתת את הדין במקרה של פריצה למערכותיהן.[91]

אכיפת תקן הפרטיות על ידי המדינות השונות בארצות הברית החלה בקליפורניה ב־2002, עם קבלת חוקים המחייבים חברות לדווח על פריצות סייבר. חשיפותיו של אדוארד סנודן על תוכניות המעקב הפדרליות הביאו אותן מדינות לגבש גישה פרו־אקטיבית יותר כלפי סוגיות של הפרת פרטיות. כך, למשל, בינואר 2016 נכנס לתוקף חוק פרטיות במדינת דלאוור (המצטרף לחוק דומה הקיים במדינת קליפורניה), היוצר הגנה קשוחה בהרבה על הפרטיות ומרחיב את יריעת ההגדרה מהו מידע אישי שיש להגן עליו.[92]

קידום מיזמים ושיתופי פעולה בין הרמה המדינתית לרמה הפדרלית

מעבר לפעילות הנפרדת של הממשל הפדרלי ושל המדינות השונות בארצות הברית בסוגיות של רגולציה, מתקיימת לעיתים הפרייה הדדית בין שני הצדדים המביאה לשיפור רמות ההגנה הקיימות בסייבר. כך, למשל, המשרד לשירותים פיננסיים במדינת ניו יורק פרסם ב־2015 המלצות לחיזוק ההגנה בסייבר ודרש במקביל מהמחוקקים הפדרליים לפתח תשתית רגולטורית רחבה יותר להתמודדות עם סוגיה זו, מבלי שהדבר יפגע בעצמאותן של המדינות השנות. לפי המשרד לשירותים פיננסיים, התוכנית הפדרלית צריכה לכסות את נושאי הרציפות התפקודית של בעלי עסקים, אבטחה בשרשרת האספקה מול ספקים חיצוניים ואבטחה של המערכות והרשתות עצמן.[93]

אין דוגמאות רבות למקרים שבהם המדינות דורשות מהרגולטור הפדרלי הנחיות נוספות לאכיפת הרגולציה בסייבר, אך מודל שיתוף פעולה זה כבר נוסה בהצלחה

---

90 על הנחיות רשמיות של המשרד לרגולציית עסקים ועניינים צרכניים של מדינת מסצ'וסטס ראו: http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf

91 Paul Otto and Brian Kennedy, "Reasonable Security becomes Reasonably Clear to the California Attorney General", Hogan Lovells Chronicle of Data Protection, March 1, 2016, http://www.hldataprotection.com/2016/03/articles/cybersecurity-data-breaches/reasonable-security-becomes-reasonably-clear/ על סיכום אירועי פריצה בקליפורניה ראו דוח של התובע הכללי: K. D. Harris, *California Data Breach Report 2012-2015,* California Department of Justice, February 2016, https://oag.ca.gov/breachreport2016

92 בנוסף להגנה על המספר האישי בביטוח הלאומי (social security number), דורשת מדינת דלאוור להגן על כל מידע שעשוי לאכן ולזהות אנשים פרטיים.

93 Sarah V. Riddell and Melissa R. Hall, "NYDFS Issues letter to Federal Financial Regulators Seeking Collaboration on Cybersecurity Efforts", *Morgan Lewis,* November 11, 2015, https://www.morganlewis.com/blogs/finreg/2015/11/nydfs-issues-letter-to-federal-financial-regulators-seeking-collaboration-on-cybersecurity-efforts

ב־2003, כאשר המרכז להגנת האינטרנט (Center for Internet Security), מרכז ללא מטרות רווח הפועל למיגור איומי סייבר,[94] הקים את המרכז לשיתוף מידע (MS-ISAC) להגברת שיתוף המידע בין מדינות לממשל הפדרלי בתחום זה. מוסד זה התבסס עם השנים, וכיום הוא נחשב לאחד הגורמים החשובים במאמצי הגנת הסייבר של ארצות הברית. מה שהחל כקבוצה קטנה של מדינות בצפון־מזרח ארצות הברית, שהתאגדו כדי לחלוק מידע, הפך למשאב לאומי הפועל יחד עם הממשל האמריקאי והמשרד לביטחון המולדת כדי לסייע בניטור, במעקב אחרי איומים ובתגובות לאירועים. המרכז לשיתוף מידע אינו גובה דמי חברות, כולל נציגים מחמישים המדינות של ארצות הברית ומספק מגוון שירותים, ובכללם ניטור תקני אבטחה וייעוץ. בכך הוא הצליח לאחד באופן לא שגרתי את הממשל הפדרלי עם מאמצי המדינות השונות בהתגוננות מפני איומי סייבר.

האיחוד האירופי

האיחוד האירופי הוא מסגרת של מדינות דמוקרטיות באירופה, שראשיתה ברעיון להקים שוק אירופי משותף. האיחוד לא נועד להחליף את המדינות הקיימות ואינו פדרציה כמו הממשל הפדרלי בארצות הברית. יחד עם זאת, ניתן להתייחס אליו כאל ארגון־על שאליו העבירו מדינות אירופיות חלק מתהליכי קבלת ההחלטות הריבוניות שלהן, ובכלל זה בתחום הסייבר.

האיחוד האירופי מונה שלושה מוסדות פוליטיים עיקריים, שתחתם מתרכזים מאמצי הרגולציה שלו: מועצת השרים (EU Council) מייצגת לרוב את האינטרס הפוליטי של המדינות החברות, ותפקידה הוא לאשר או לתקן חקיקה המוצעת על ידי הנציבות האירופית (EU Commission), לאמץ את תקציבי האיחוד ולחתום על הסכמים בין־לאומיים; הפרלמנט האירופי מייצג את אזרחי המדינות החברות באיחוד ונבחר ישירות על ידם. חבריו רשאים להציג שאילתות למועצת השרים ולנציבות האירופית ולדרוש מהם דיווחים על פעילותם; הנציבות האירופית היא הגוף המייצג את האינטרס האירופי המשותף. היא יוזמת ומתאמת את מדיניות האיחוד ואת החקיקה הנעשית במסגרתו, תוך פיקוח על יישומן ואכיפתן, וכן אמורה לפקח על יישום חקיקת האיחוד במדינות החברות, להכין ולנהל את תקציבו ולערוך משא ומתן עם מדינות שמחוץ לאיחוד ועם גורמים בין־לאומיים אחרים. הנציבות מורכבת מ־25 נציבים המנהלים את שגרת הפעילות של האיחוד במספר רב של תחומים – חקלאות, סביבה, אנרגיה, מיסוי, תקצוב, בריאות, תקשורת, המרחב הדיגיטלי, ביטחון פנים ומשפט.

94 ראו עוד על מרכז זה כאן – https://www.cisecurity.org/about-us/

הנציבות האירופית מהווה את הכוח המניע העיקרי סביב מרחב הסייבר באיחוד האירופי. רגולציית הגנת הסייבר של האיחוד שונה משיטת הטלאי על גבי טלאי של ארצות הברית, על אף המבנה המוסדי המסועף שלה. הגנת הסייבר של האיחוד מבוססת על אסטרטגיה סדורה, היררכית, השמה דגש על הגנת מידע אישי ועל שמירת הזכות לפרטיות. עיקר כוחה של אסטרטגיה זו הוא בקביעת הרגולציה במרחב הסייבר עבור המדינות החברות באיחוד, כאשר כל מדינה מממשת את הרגולציה באמצעות חוקים והנחיות פנימיים. הרגולציה, החוקים וההנחיות המדינתיות נוגעים למרבית המגזרים במשק, ובכלל זה התעשייה, התשתיות הקריטיות ושחקני השוק המרכזיים בכלכלת האינטרנט.

משטר הרגולציה של האיחוד האירופי בנושא הגנת הסייבר כולל אסטרטגיות מדיניות של הנציבות, הנחיות מחייבות למדינות החברות (דירקטיבות) ויצירה של שיתופי פעולה בין הסוכנויות השונות. מעורבות האיחוד האירופי בנושא הגנת הסייבר הלכה והתרחבה עם השנים: כבר ב־1995 הוחלט במועצת השרים על הצורך לגבש תבחינים משותפים להערכת סיכוני סייבר למדינות החברות באיחוד,[95] אך רק ב־2004 הפכה הרגולציה לגורם פעיל, עם כינונה של European Network and Information Security Agency (ENISA).

הסוכנות לביטחון מידע של האיחוד החלה את דרכה עם קבלת אחריות על תרגולי חירום בכל הקשור לפגיעות סייבר. היא עוסקת בקידום אסטרטגיות לניהול סיכונים בקרב המדינות החברות ובסיוע למוסדותיהן על ידי יצירת מנגנונים לשיתוף מידע כדי התמודד עם התקפות סייבר בזמן אמת. תחומי האחריות של הסוכנות הלכו והתרחבו עם השנים, ובהחלטות של נציבות האיחוד מ־2008 ומ־2017 הוגדלו תקציבה וכוחה באופן המבטא את החשיבות הגוברת שמוסדות האיחוד מייחסים לטיפול בסיכוני סייבר.

בנוסף לפעילות הרגולטורית המתבצעת דרך ENISA, הקים האיחוד האירופי ב־2012 את EU Computer Emergency Response Team (CERT-EU) במטרה להגן על רשתות האיחוד מפני מתקפות סייבר. מוסד נוסף של האיחוד, האחראי על שיתופי פעולה בין המדינות סביב פשיעת סייבר, הוקם גם הוא באותה שנה – Europol's Cyber Crime Center (EC3).

בנוסף לפעילות המוסדית, מפרסמת הנציבות האירופית מדי מספר שנים אסטרטגיות לאסדרת מרחב הסייבר. ב־2001 פרסמה הנציבות הצעה להגנה על רשתות ומערכות מידע, וב־2006 עוגנה הצעה זו באסטרטגיה חדשה – A Strategy for a Secure Information Society – הכוללת צעדים לשיפור הגנת המידע של מערכות. ב־2010 פורסמה תוכנית

95 Council Recommendation 95/144/EC, April 7, 1995, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995H0144&from=EN

שטוקהולם ו־ Digital Agenda for Europe, אשר כללו המלצות וצעדים לאבטחת הגנת המידע של מערכות אירופיות, ובכלל זה הקמת צוותי תגובה לאירועים, וכן צעדי מנע נגד תקיפות סייבר.

נקודת מפנה בהגנת הסייבר הייתה ב־2013, כאשר האיחוד האירופי אימץ אסטרטגיה מקיפה בתחום זה. האסטרטגיה החדשה איגדה בתוכה אסטרטגיות ותוכניות במרחב הסייבר שקדמו לה והדגישה ערכים אירופיים בסיסיים, כמו חופש הביטוי, פרטיות, ממשל דמוקרטי ואחריות משותפת לביטחון. מטרתה העיקרית של האסטרטגיה החדשה הייתה הגברת החוסן של מרחב הסייבר, כחלק מתפקידו של האיחוד האירופי כאחראי על השוק האירופי המשותף ועל הביטחון במדינות המרכיבות אותו. במסגרת זו קבעה האסטרטגיה דרישות מינימליות להגנה על מרחב הסייבר, ובכלל זה דיווח על אירועי סייבר. האסטרטגיה גם עוסקת במאמצים להפחית את פשיעת הסייבר, תוך הגברת היכולות של המדינות החברות למגר פשיעה זו.

האסטרטגיה להגנת הסייבר באיחוד האירופי היא חלק מהמדיניות האירופית המשותפת להגנה וביטחון (Common Security and Defence Policy), עליה הסכימו מדינות האיחוד באמנת ניס מ־2001, המעודדת שיתוף פעולה ביניהן בנושאי ביטחון והגנה. בד בבד עוסקת האסטרטגיה בפיתוח משאבים טכנולוגיים לקידום הגנת הסייבר במטרה להפחית את התלות בגורמים חיצוניים וליצור תקנים מחמירים למוצרי אבטחה. כפועל יוצא מכך הוגדלו תקציבי האיחוד והוגברו המאמצים לקידום הנושא. מאז 2013 הושקעו יותר מ־600 מיליון אירו במחקר ופיתוח בתחומים אלה.[96] האסטרטגיה האירופית עוסקת, בנוסף לכך, בקידום הגנת הסייבר ברמה הגלובלית, וזאת כחלק ממדיניות החוץ של האיחוד האירופי.

ב־2016 הקים האיחוד את ה־(Contractual Public-Private Partnership (CPPP, כביטוי לשיתוף פעולה עם המגזר העיסקי בהגנת הסייבר, כשהמטרה היא לקדם פיתוח של מוצרים חדשים להגנת סייבר עבור המדינות החברות.

ניתן לחלק באופן גס את מוסדות האיחוד האירופי העוסקים בהגנת הסייבר לארבעה:

1. ההגנה על המגזר האזרחי והעיסקי ועל מוסדות האיחוד מבוצעת באמצעות ENISA, אשר מתווה את התקנים למדינות החברות ומאגדת את המרכזים לדיווחים על אירועי סייבר בכלל היבשת. הסוכנות לביטחון מידע מבצעת איסוף וניתוח של מידע על אירועי סייבר, מקדמת הערכות וניהול סיכונים למיצוי היכולות להתמודד עם אירועי סייבר בארגונים, עורכת תרגילים לבדיקת חוסנו של האיחוד במרחב הסייבר, תומכת בארגוני CERT במדינות החברות, אחראית על תוכניות לשיתוף

96 "Cybersecurity Initiatives", European Commissioner, January 2017, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

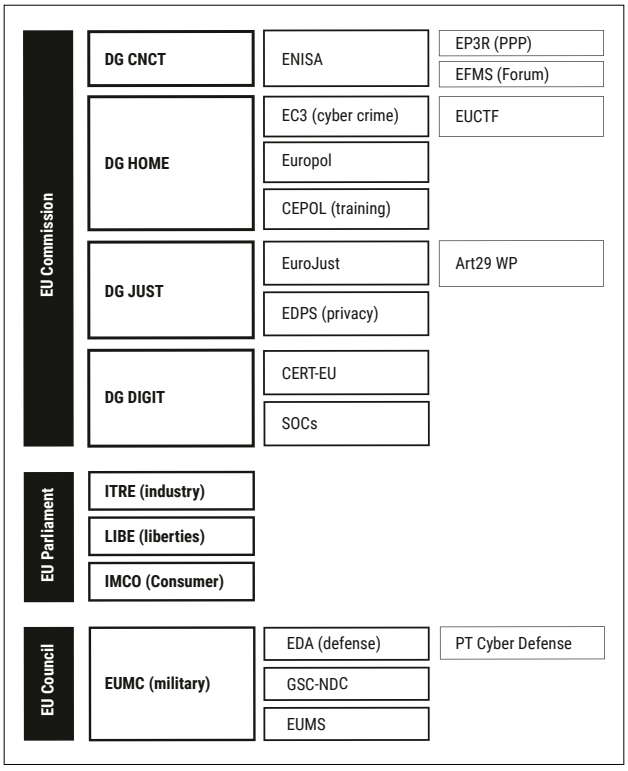
מידע להגנה על תשתיות קריטיות ועוסקת בהעלאת המודעות בקרב ארגונים לנושאי אבטחה והגנה בסייבר. חודש אוקטובר מדי שנה מוכרז כחודש המודעות הייעודי.

2. EU Computer Emergency Response Team (CERT-EU) הוקם, כאמור, ב־2012 במטרה לנהל באופן יעיל ואפקטיבי את ההתמודדות עם תקיפות סייבר על מוסדות האיחוד. שיתוף הפעולה בנושא זה כולל מומחי הגנת סייבר מכל מוסדות האיחוד, המדינות החברות וארגוני הגנה עיסקיים.
3. פשיעת סייבר מרוכזת תחת אחריותו של Europol's Cybercrime Center (EC3), שהוקם ב־2012 כחלק מ־Europol במטרה לרכז את הלחימה בפשיעת הסייבר ברמת האיחוד. המרכז תומך במדינות החברות באיחוד ובמאמצי החקירה שלהן, מבצע ניתוח אסטרטגי של הנעשה בתחום הפשיעה בסייבר, מתווה שיתוף פעולה בין השחקנים הרלוונטיים השונים, ביניהם סוכנויות אכיפת חוק, המגזר העיסקי, האקדמיה וחברות אבטחה רלוונטיות, תומך בתרגולי מיגור פשיעה בקרב המדינות החברות, מבצע תחקור אירועי פשיעה בסייבר ותומך במאמצי המדינות החברות בנושא זה.
4. הגנה על מערכות ביטחון לאומי נעשית על ידי הסוכנות האירופית להגנה – The European Defence Agency (EDA).

מוסדות האיחוד מטפלים גם בהגנת הפרטיות. זו מתבצעת באמצעות שני גופים – הרשות להגנת מידע האירופאית (European Data Protection Supervisor (EDPS)) הגוף המרכז את הממונים על הגנת המידע במדינות החברות השונות (Article 29 Working Party) – מנחים את המדינות החברות באיחוד בנושאי הגנת מידע אישי השנויים במחלוקת (למשל, שימוש בכלי טיס בלתי מאויישים לצורכי צילום). חלק נכבד מפעילותם של גופים אלה עוסק באבטחת מידע בתחום הסייבר.

אף שלאיחוד האירופי כגוף אין מנדט מוצהר בתחום החקיקה הקשורה בהגנת סייבר, רגולציה של האיחוד באמצעות חקיקה התפתחה החל מ־2005. באותה שנה הוקמה התשתית החוקתית של הנציבות האירופית להגנה נגד התקפות סייבר. מטרתה של התשתית הייתה, בראש ובראשונה, להגביר את שיתוף הפעולה בין רשויות החוק בכל מדינה חברה באיחוד. ב־2013 הפכה תשתית זו להנחייה – The directive on attacks against information systems – שהבסיס החוקתי לה היא האמנה העוסקת בתפקוד האיחוד, המחייבת שיתוף פעולה בין המדינות החברות בנושאי פשיעה. ב־2013 הניחה הנציבות האירופית גם את הבסיס להגנה מבעוד מועד על מערכות ממוחשבות, תוך התבססות על נימוקים כלכליים של הרצון להסדיר את פעילות השוק המשותף בדרך של אבטחת תשתיות המחשוב המאפשרות את תפקודו.

ב־2016 אושרו שתי הנחיות מחייבות של האיחוד האירופי הנוגעות לביטחון סייבר ולהגנה על מידע – The Network and Information Security Directive (NIS),



תרשים 2: סוכנויות ומוסדות העוסקים בנושא ביטחון הסייבר באיחוד האירופי

ו־The General Data Protection Regulation Directive (GDPR). ההנחייה הראשונה, הצפויה להיכנס לתוקף לקראת סוף 2018, היא הניסיון הראשון לגבש תקנים אחודים ומינימליים עבור כל מדינות האיחוד בכל הנוגע להגנת סייבר. לפי הנחייה זו, על כל המדינות החברות לגבש אסטרטגיית הגנת סייבר המתאימה להן, ובמקביל על האיחוד להקים סוכנות ייעודית שתוודא את יישום ההנחייה במדינות השונות. במסגרת זו גם ניתנו לכל מדינה חברה הסמכות וההנחיות להטלת סנקציות בתחומה במקרה של הפרת תנאי האסטרטגיה של האיחוד האירופי להתגוננות בסייבר. ההנחייה עוסקת לא רק במגזר העיסקי בכל מדינה, אלא גם ברשתות המדינתיות עצמן.

ההנחייה להגנת המידע מ־2016, שנכנסה לתוקפה במאי 2018, מעדכנת את הנחיית הגנת הפרטיות הקודמת של האיחוד, שהייתה במשך 21 שנה רגולציית הפרטיות והגנת המידע המשמעותית ביותר. מטרת ההנחייה החדשה היא לאפשר למשתמשים לקבל החלטה על האופן בו מידע אישי על אודותיהם יעובד וישותף עם אחרים. ההנחייה כוללת התייחסות ל"זכות להישכח", על פיה ניתן לבקש הסרה של מידע לא מהימן, הסכמה מפורשת של יחידים לעיבוד מידע אישי עליהם, דיווח על גניבות מידע והפרות

של פרטיות כתוצאה מתקיפת סייבר תוך 72 שעות, והזכות של יחידים להעביר מידע בין ספקי שירות שונים.

ההנחייה בדבר ביטחון הרשתות והמידע גם קוראת ליצירת מנגונים לשיתוף פעולה אסטרטגי בין המדינות החברות, ושמה דגש מיוחד על המגזרים הפיננסי, האנרגיה, המים, התחבורה, הבנקים, הבריאות וספקי התשתיות הדיגיטליות. החידוש העיקרי בהנחייה בהקשר זה הינו שמנועי חיפוש, ספקי תשתיות ענן וחנויות מקוונות יהיו כפופים להנחיות הגנה מחייבות ויצטרכו להעביר דיווחים במקרה של התקפת סייבר וגניבת מידע. הנחיות דומות כבר חלות ברמת האיחוד האירופי על מפעילי תשתיות תקשורת ואינטרנט במסגרת EU Telecoms Regulatory Framework משנת 2009.

למעשה, כבר ב־2001 נוסדה תשתית חוקתית להגנת סייבר ברמת האיחוד, כאשר מוסדות האיחוד יצאו בחקיקה נגד פשיעת סייבר, פרסמו הנחיות למיגור הונאות בשירותים מקוונים ופנו למדינות החברות בבקשה להרחיב את ההגדרות של המושג "פשיעת סייבר". במסגרת זו פרסם האיחוד ב־2011 הנחיות להתמודדות עם פגיעה בילדים במרחב המקוון, וב־2013 – הנחייה להגנה על מערכות ממוחשבות מפני פשיעה. בנוסף לדרישה מהמדינות החברות לחדד את ההגדרות של פשיעת סייבר, תבע מהן האיחוד להטיל סנקציות משמעותיות יותר על פושעי סייבר.

מתברר כי המדינות החברות באיחוד העדיפו הנחיות פחות מחייבות, בעוד שמוסדות האיחוד התעקשו לגבש תקנים ברורים ומחייבים להגנת מידע וביקשו ליצור אחידות בין המדינות החברות בנושאי הגנת סייבר. כיום, רק ל־17 מחברות האיחוד האירופי יש אסטרטגיית הגנה כלשהי בסייבר, וכל אחת מהאסטרטגיות שונה מהשנייה. האיחוד רואה, לפיכך, צורך לתמרץ סטנדרטיזציה של הגנת הסייבר בכל המדינות החברות ומעוניין לצורך זה לקבוע תקן מחייב ואחיד לכולן.

ההיסטוריה של הגנת הפרטיות באיחוד האירופי נסקרת בצורה מקיפה במאמר של אברהם ניומן מ־2008.[97] המאמר עוסק במדיניות שקדמה לחקיקה המכוננת של האיחוד בנושא הפרטיות מ־1995. עד אז לא ניכר כל רצון של המדינות החברות לקדם חקיקה ברמת האיחוד להגנת המידע והפרטיות. היו אלה דווקא מוסדות הגנת המידע ברמת המדינות הספציפיות אשר קידמו את השיח בנושא זה ועיצבו את החקיקה בהמשך. יחד עם זאת, הצורך בהגנת הפרטיות, נוכח מאמצים של מדינות זרות לחדור לתחום זה, היה נהיר לעורכי הדין ולאנשי האקדמיה שעסקו בנושא כבר בשנות השישים של המאה העשרים. צורך זה חלחל אט־אט גם לתודעת המדינות והביא, בסוף שנות השבעים של המאה, את צרפת, גרמניה ולוקסמבורג להנהיג רפורמות בצורת מתן

97 Abraham Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", *International Organization*, Vol. 62, No. 1, 2008, pp. 103-30.

סמכות למוסדות הגנת המידע המדינתיים לאכוף את חוקי הפרטיות המקומיים. סמכות זו גם הִקנתה לאותם מוסדות עצמאות מפני פוליטיקאים ושרי ממשלה, דבר שהיה קריטי בגיבוש החקיקה בהמשך. מדינות אחרות, כמו שווייץ, אימצו חקיקה פחות מחייבת, שהתייחסה למגזרים רגישים בלבד, כגון מגזרי הבריאות והבנקאות. חקיקה זו הסתמכה ברובה על כוחות השוק ועל רגולציה עצמית. איטליה, יוון, ספרד, פורטוגל ובלגיה נעדרו כל סוג של חקיקה בנושא של הגנה על הפרטיות, ורק בשנת 1995 הצטרפו למגמה הכללית באיחוד ואימצו חקיקה לאומית בנושא זה.

קהילת תומכי הפרטיות השכילה להפעיל שדולה במוסדות האיחוד, ובסופו של דבר הצליחה להביא את הפרלמנט האירופי לאמץ שורה של החלטות בנושא הפרטיות. לעומת זאת, הנציבות האירופית לא הראתה עניין בקידום הנושא וחששה בעיקר מהעלויות הצפויות למגזר העיסקי בגינו. מגמה זו של הנציבות האירופית נמשכה עד שנות התשעים של המאה. מועצת אירופה, מצידה, הקימה קבוצת לימוד בנושא, אך לא הייתה לה, למעשה, השפעה ממשית על התפתחות הטיפול בהגנת הפרטיות בסייבר.

השינוי בהבנה כי הגנה על הפרטיות צריכה להיות מטופלת לא רק ברמת המדינות וכי על האיחוד האירופי לגבש תקן אחיד ומחמיר לכלל החברות בו התחולל, כאמור, בעיקר על רקע התבססות מעמדם של מוסדות הגנת המידע העצמאיים בכל אחת מהמדינות החברות באיחוד. ב־1988 כבר היו 11 מוסדות כאלה, אשר שיתפו פעולה ביניהם לקידום הטיפול בשאלת הפרטיות באיחוד. שיתוף פעולה זה נמשך עד לגיבושה של טיוטה לרפורמה בנושא ההגנה על הפרטיות ברמת האיחוד האירופי.

ההבדלים בין מדינות האיחוד בשיטות ההגנה על הפרטיות העמידו בספק את היכולת לגבש נורמות אחידות בנושאי הפרטיות באירופה. מצב זה, יחד עם ההשפעות הכלכליות שיצרו ההבדלים בין המדינות השונות, חיזקו את הצורך המיידי בחוקי פרטיות אחודים ביבשת. בשלב זה, כוחם של מוסדות הגנת הפרטיות המדינתיים היה כה חזק, עד שהם איימו שאם לא תהיה חקיקה של האיחוד בנושא הפרטיות עד שנת 1992, הם יחסמו זרימת מידע המגיע מחוץ לאיחוד ובתוכו. על רקע זה, ועל אף התנגדות התעשייה, השתכנעה לבסוף הנציבות האירופית לתמוך בחקיקת חוקי פרטיות נוקשים ברמת האיחוד. המגזר העיסקי לא היה שחקן מרכזי בתהליך, אך שיתף פעולה מתוך רצון להקטין את עלויות הרגולציה העתידיות. בסופו של דבר, מוסדות הגנת הפרטיות המדינתיים הצליחו לשנות את סדרי העדיפות של האיחוד האירופי בסוגיה זאת.

אמנת אמסטרדם מ־1997, אשר עדכנה את הסכמי שיתופי הפעולה בין המדינות החברות באיחוד ושיקפה את הסכמת המדינות לקדם חקיקה בתחום שונים דרך הפרלמנט האירופי, החילה את הנחיות הגנת המידע והפרטיות גם על מוסדות האיחוד

האירופי והקימה במסגרת זו את European Data Protection Supervisor (EDPS) – גוף שנועד לנטר את רמת הציות של מוסדות האיחוד לחוקי הפרטיות.

תרומה חשובה נוספת של חקיקת הגנת מידע אישי באיחוד האירופי היא בהשלכות של הגנת המידע האישי על קידום ההגנה בסייבר. זאת, מאחר וארגונים וגופים במדינות האיחוד יצטרכו להוכיח כי אימצו את כל אמצעי ההגנה האפשריים כדי להימנע מחשיפת מידע אישי בידי גורמים לא מורשים. זאת ועוד, ההנחייה מרחיבה את ההגדרה של מידע אישי ומתייחסת גם למידע גנטי, פסיכולוגי, כלכלי, תרבותי וחברתי כאל מידע עליו יש להגן, ובתוך כך מגבילה את משך הזמן בו ניתן לאחסן מידע כזה. בנוסף לכך, כוללת ההנחייה קנסות וסנקציות משמעותיים במקרים של הפרת הפרטיות והיעדר הגנה מספקת על מידע אישי. קנסות כאלה יכולים להגיע עד ארבעה אחוזים מהמחזור של כל עסק, או עד עשרים מיליון אירו (הגבוה מביניהם).

מאמצי האיחוד האירופי בתחום הגנת הסייבר, ובמיוחד ההתקדמות המשמעותית שחלה בהם מאז האסטרטגיה שגובשה בשנת 2013, משקפים את רצון האיחוד להפוך הן לשחקן גלובלי משפיע והן לשחקן המכוונן את מאמצי ההגנה במדינות החברות. תפיסה זו מדגישה את החשיבות של המגזר העיסקי והציבורי כאחד, ויש לה השפעה ברמות שונות.[98] אף על פי כן, הגנת הסייבר אינה מוזכרת במפורש באמנות האיחוד השונות, ולכאורה אין למוסדות האיחוד גם כיום מנדט חוקתי ברור בתחום הסייבר. לפיכך, פועל האיחוד האירופי בסוגיה זו על ידי גיבוש אסטרטגיה המחברת בין צורכי הגנת הסייבר ובין שיתופי פעולה בתחומים אחרים, בין השאר באמצעות מתן תמריצים למדינות החברות.

בריטניה

ממשלת בריטניה החלה לעסוק בהגנת סייבר כבר בשנת 1997, עם גיבושה של התוכנית להגנת משרדי הממשלה – Government Secure Intranet (Gsi). מטרת התוכנית הייתה לאפשר שיתוף מידע בין משרדי הממשלה השונים באופן מאובטח. ב־1999 הרחיבה הממשלה את היריעה והקימה את National Infrastructure Security Coordination Centre (NISCC), שמטרתו הייתה למזער איומים על תשתיות קריטיות ולהגן עליהן מפני מתקפות אלקטרוניות.[99] התקפות הסייבר על אסטוניה ב־2007, אשר פגעו במרבית השירותים המקוונים במדינה, היו קריאת השכמה נוספת לממשל הבריטי והביאו להקמת מרכז הגנת סייבר ייעודי – The Centre for the Protection of National

98 Ramses A. Wessel, "Towards EU cybersecurity Law: Regulating a New Policy Field", in N. Tsagourias, R. Buchan (eds.) *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar, 2016, chapter 19.

99 "The Launch of the National Cyber Security Center", *NCSC*, February 2017, p. 8.

Infrastructure – המאחד את NISCC ומרכז נוסף בשם The National Security Advice Centre (NSAC), שהיה יחידה של סוכנות מודיעין הפנים הבריטית MI5. מטרתו של המרכז החדש הייתה להבטיח את חסינות התשתיות הלאומיות במדינה ולהגן עליהן מפני איומי סייבר.

החוק הבריטי העיקרי העוסק בתשתיות קריטיות הוא Civil Contingencies Act משנת 2004, המעניק סמכות רחבה למדינה במגזרים מרכזיים, כגון תקשורת, תחבורה ותשתיות מים וחשמל. סמכות זו כוללת מתן רשיונות והקפאת היתרי פעולה למגזר העיסקי כאשר מתעוררים איומים על הביטחון הלאומי כתוצאה מהיעדר הגנה על תשתיות קריטיות. עם זאת, הגישה הבסיסית כלפי המגזר הפרטי בבריטניה היא ברובה גישה של שיתוף פעולה וולונטרי.

בשנת 2009 פורסמה האסטרטגיה הלאומית הבריטית הראשונה במרחב הסייבר, ובמסגרתה הוגדרו פשיעת סייבר והתקפות סייבר כאחד מחמשת האיומים המרכזיים על בריטניה, כשאיום הסייבר נתפס הן כאיום על הביטחון הלאומי והן כאיום על כלכלת המדינה.[100] האסטרטגיה עודכנה ב־2011 והפכה לתוכנית חומש של בריטניה לשנים 2011־2016 להגנת הסייבר במדינה, שתוקצבה בסכום של 860 מיליון לירות שטרלינג. מטרותיה של האסטרטגיה המעודכנת היו מיגור פשיעת הסייבר, הגנה על האינטרסים הכלכליים והלאומיים של בריטניה במרחב הסייבר, עיצוב מרחב סייבר יציב שיאפשר ביטוי ראוי לכל האזרחים, ופיתוח הידע והיכולות הבריטיות בתחום הסייבר.[101]

בנובמבר 2016 עודכנה אסטרטגיה זו לחמש שנים נוספות, הפעם עם תקציב כפול של כ־1.9 מיליארד ליש"ט.[102] האסטרטגיה החדשה מתריעה, כי לצד ההזדמנויות שנוצרו במרחב הסייבר, ישנם איומים חדשים וגורמים עוינים המעוניינים לגנוב מידע ולהסב נזק לאומה הבריטית.[103] האסטרטגיה גם קובעת כי שילוב הכוחות בין הממשלה ובין המגזר העיסקי בנושאי הגנת הסייבר אינו יוצר הגנה מספקת מפני האיומים במרחב זה, וכי לא מעט תשתיות קריטיות אינן מאובטחות כראוי. ספציפית, ממשלת בריטניה טוענת במסמך האסטרטגיה כי המגזר העיסקי אינו מגן על עצמו בקצב משביע רצון, ולכן על המדינה לפעול ולהיות נוכחת באופן נחרץ ומחייב יותר בפעילותו של המגזר הפרטי בתחום הסייבר.[104] האסטרטגיה החדשה גם מזהה מספר

100 Melissa Hathaway et al., "The United Kingdom Cyber Readiness at Glance", Potomac Institute for Policy Studies, 2016, p. 5.

101 The Final Annual Report on the 2011-2016 UK Cyber Security Strategy", UK Parliament, April 2016, p. 7.

102 "National Cyber Security Strategy 2016 to 2021", HM Government, November 2016.

103 "National Risk Register of Civil Emergencies", Cabinet Office, 2015.

104 "National Cyber Security Strategy 2016 to 2021", HM Government, November 2016.

כשלי שוק: ראשית, עשייה בלתי מספקת של הגופים השונים כדי להגן על האינטרס הציבורי בתחום הגנת המידע וההגנה על הפרטיות; שנית, המגזר העיסקי אינו מכיר דיו את האיומים השונים ואת צורת ההתגוננות מפניהם, ויש משבר אמון בין ספקי ההגנה ובין ארגונים וחברות שונים.

המבנה המוסדי

ניתן להבחין בשלושה מאפיינים עיקריים בתפיסה הבריטית להגנת הסייבר: סוכנויות המודיעין הן הגורם המוביל והמרכז את מאמצי ההגנה וההתקפה במרחב; לשחקני השוק ולחברות השונות יש השפעה רבה על קבלת ההחלטות של המדינה בנושא; הממשלה, כגוף הנדרש להגן על הציבור, מובילה ומשמשת דוגמה לשחקנים אחרים כיצד להתגונן במרחב הסייבר.

המאפיין הראשון – דומיננטיות קהילת המודיעין במאמצי ההגנה וההתקפה במרחב הסייבר – הלך והתעצם עם הזמן. ג'ורג' אוסבורן, שר האוצר של בריטניה (Chancellor of the Exchequer) צוטט כאומר שלארגון המודיעין האלקטרוני של בריטניה (GCHQ) יש תפקיד ייחודי ומשפיע בהגנת הסייבר במדינה לעומת סוכנויות אחרות. לדבריו, גופים נוספים, כגון משרד ההגנה, גורמי אכיפת החוק והמגזר העיסקי־אזרחי, חשובים בפני עצמם, אך חשיבותו והשפעתו של GCHQ עולות על כולם.[105]

שני המאפיינים הנוספים – תפקידיהם של שחקני השוק ושל הממשלה – באים לידי ביטוי, בין היתר, בהשתת רגולציה בלתי מחייבת על המגזר העיסקי־אזרחי, במקביל לאימוץ המלצות המדינה להגנה בסייבר על ידי משרדי הממשלה השונים. בנוסף לכך, המדינה מנסה לתמרץ ארגונים במגזר העיסקי בבריטניה לאמץ את המלצותיה בתחום זה על ידי הפיכתן לתנאי סף לזכאות להגשת מועמדות למכרזים העוסקים בפרויקטים של המדינה. הדוח המסכם של הפרלמנט הבריטי על פעילות הממשלה בנושא הסייבר בשנים 2011־2016 מטיל את האחריות להגנת התשתיות הלאומיות על המגזר העיסקי, תוך ציון העובדה שהממשלה פועלת בשיתוף פעולה מלא עם התעשייה הבריטית ומספקת לה מומחיות וייעוץ כשהדבר מתבקש.[106]

הגישה הרכה כלפי המגזר העיסקי באה לידי ביטוי גם באופן שהמדינה בוחרת להגן על פרטיות המידע. הגישה שממשלת בריטניה מאמצת כלפי המגזר העיסקי הינה ידידותית וכוללת מעט מאוד הנחיות מחייבות, מה עוד ורוב מוחלט של ההנחיות

---

105 גו'רג' אוסבורן, "שיחה עם קהילת המודיעין על מאמצי הסייבר של בריטניה", 17 בנובמבר, 2015. לטקסט המלא מהנאום ראו כאן – https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

106 "The Final Annual Report on the 2011-2016 UK Cyber Security Strategy", UK Parliament, April 2016.

מלוות בתמריצים. תמריצים אלה כוללים הקלות מס על הוצאות הגנה בסייבר וקבלת מענקים ממשלתיים עבור הגנת סייבר נאותה (שכאמור, היא גם תנאי סף להשתתפות במכרזי ממשלה). הממשלה גם נרתעת מניסוח הנחיות מחייבות שייצרו תרבות של ציות מצד החברות, אך לא יתנו מענה מלא לאיומים המשתנים במרחב הסייבר.[107]

כדי לעקוב אחר התפתחות הרגולציה בנושאי הגנת הסייבר בבריטניה ייסקרו להלן השחקנים העיקריים והמשימות שהוטלו עליהם, ובכלל זה ההחלטה משנת 2017 שאיגדה את סוכנויות המדינה השונות העוסקות בהגנת סייבר תחת מעטפת מוסדית אחת. כאמור, השחקן העיקרי בתחום זה הוא GCHQ, הכפוף למזכיר המדינה לענייני חוץ וחבר העמים הבריטי (שאינו חלק ממשרד החוץ הבריטי). סוכנות מודיעין זו הוקמה ב־1916 בשם Government Code & Cypher School וקיבלה את שמה הנוכחי ב־1946. היא מעסיקה יותר מ־6,000 עובדים ומשתפת פעולה עם ארגוני המודיעין הבריטיים MI5 ו־MI6. משימתה המוצהרת בתחום הסייבר היא להגן על מערכות הממשלה מפני איומי סייבר, לתמוך בכוחות הצבא במרחב הפיזי והקיברנטי ולהגן על הציבור בתחומים אלה. הסוכנות אחראית על אבטחת תשתיות קריטיות, תמיכה בתעשייה בתחום הסייבר, הגנת מרחב הסייבר בכללותו וקידום המודעות לנושא הסייבר.

ב־2017 הקימה בריטניה מערך ארגוני חדש להתמודדות עם אתגר הסייבר – The National Cyber Security Center (NCSC) – שבראשו הועמד GCHQ. הסוכנויות העיקריות המאוגדות ופועלות במסגרת המערך החדש הן:

1. Communications-Electronic Security Group (CESG) (שפעלה עד אז במסגרת GCHQ).
2. Center for Cyber Assessment (CCA).
3. Computer Emergency Response Team UK (CERT UK).
4. Center for the Protection of National Infrastructure (CPNI).
5. Cybersecurity Information Sharing Partnership (CiSP).

NCSC אמור לטפל בכל המגזרים הפועלים במרחב הסייבר, תוך מתן עדיפות למגזרים לאומיים־ביטחוניים בעלי חשיבות אסטרטגית וכלכלית לבריטניה.[108] הגישה שגובשה לפעילותו של המערך החדש מאפשרת למגזר העיסקי להיות מעורב בניסוח ההנחיות להגנה בסייבר. לצורך זה הוקם פורום ייעודי של רגולטורים בתחום הסייבר, שנועד לשתף ידע ומידע לטובת הכלל. NCSC פועל באופן צמוד עם משרד ההגנה הבריטי, התעשייה והאקדמיה במטרה לוודא שההגנה המסופקת על ידיו בתחום הסייבר הינה ברמה איכותית מספקת.

---

107 "Cyber Security Regulation and Incentives Review", HM Government, December 2016, p. 3.

108 Conor Ward, "The UK's Cybersecurity Regulatory Landscape: An Overview", Hogan Lovells Chronicle of Data Protection, December 2016.

מטרותיו המוגדרות של המערך המוסדי החדש העוסק בהגנת סייבר הן איסוף ושיתוף מידע, פיתוח יכולות במרחב הסייבר, מתן תגובה לאירועי סייבר ותמיכה בתשתיות קריטיות בבעלות פרטית או ציבורית. אחת הסיבות לאיחוד הסוכנויות הבריטיות השונות העוסקות בסייבר הייתה הרצון לאפשר הבנה טובה יותר של תפקידי המדינה במרחב זה וגישה נוחה יותר אל הגורמים הממשלתיים המטפלים בו. זאת, בין השאר, לאחר שמחקר על מצב הגנת הסייבר בבריטניה מצא כי מודעות המגזרים השונים לתוכניות הסייבר של המדינה אינה מספקת.[109]

כדי להבין את תפקידו של הגוף החדש, ייסקרו להלן כל אחת מהסוכנויות המרכיבות אותו, תוך תיאור התפתחותן לאורך זמן. CESG הייתה הזרוע הטכנולוגית של GCHQ בכל הקשור לאבטחת מידע. זרוע זו קיימת מאז מלחמת העולם הראשונה, ופעילותה העיקרית מתמקדת בזרועות הצבא ובאבטחת רשתות ממשלתיות. הפעילויות המשמעותיות של זרוע זו כוללות, בין היתר, תוכנית העוסקת בהגנת המגזר הציבורי והממשלתי (Certified Cyber Security Consultancy Scheme), המעניקה תעודת הסמכה לאיכות אבטחת המידע ומאשרת לחברות שהוסמכו לכך לספק הגנה למגזר הציבורי.[110] תוכנית משמעותית נוספת של CESG היא Cyber Essentials (בשיתוף תעשיית הביטוח), שמטרתה היא להנחות את הארגונים בצעדים להגנה בסייבר. חמישה מאפיינים עיקריים לתוכנית זו: הגדרה מאובטחת של השירותים; הפרדה ראויה בין אזורים שונים ברשתות ארגוניות; בקרת גישה והרשאות; ניהול עדכוני תוכנה; הגנה מפני פוגענים (Malwares).[111] מאז אוקטובר 2014 הפכה תוכנית זו למחייבת ספקים ונותני שירותים בשירות הממשלה. אלה הבוחרים לאמץ אותה זוכים למעין חותמת איכות ונהנים מפרמיות ביטוח זולות יותר. מאז היווסדותה של התוכנית ב־2014 היא סיפקה יותר מאלפיים אישורים על רמת הגנה ראויה בארגונים שונים.

החברות הגדולות במשק הבריטי – BAE Systems, Lockheed Martin, Barclays, Hewlett-Packard – עובדות לפי התקנים המוצעים בתוכנית זו. למרות זאת, סקר שנערך ב־2017 הצביע על שיעורי אימוץ לא מספקים של התוכנית בקרב כלל המגזר העיסקי בבריטניה, כאשר רק עשרה אחוזים מהחברות הקטנות ועשרים אחוזים מהחברות הגדולות אימצו אותה. אחת המסקנות של הסקר הייתה להפוך את התוכנית

109 Rebecca Klahr et al., "Cyber Security Breaches Survey 2017", University of Portsmouth Research Portal, April 2017.

110 Melissa Hathaway et al., "The United Kingdom Cyber Readiness at Glance", Potomac Institute for Policy Studies, 2016.

111 "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk", HM Government and MARSH, 2015.

למחייבת. הסקר גם מצא כי התוכנית גוררת עימה עלויות רבות וכי ניתוחי עלות־תועלת הנעשים על בסיסה לא תמיד מדוייקים.[112]

הארגון החשוב השני במסגרת NCSC הוא CERT-UK, שנוסד ב־2014. לפני כן פעלו בבריטניה כעשרים גופים פרטיים־ציבוריים לשיתוף פעולה בתחום ההגנה בסייבר, שהשניים המרכזיים בהם היו The Computer Security Incident Response Team (CSIRT-UK), שפעל במסגרת הארגון להגנה על תשתיות קריטיות, ו־GovCertUk, שפעל במסגרת CESG. בשנתיים שעברו מאז שהוקם ועד שהוכפף ל־NCSC, פעל CERT-UK עם התעשייה, המדינה והאקדמיה בבריטניה במטרה לשפר את יכולות התגובה וההתאוששות מפגיעות במרחב הסייבר. לצורך זה נהג הארגון לערוך שלושה תרגילים בשנה, שנועדו לבחון את מוכנות המערכות ואת עומק שיתוף הפעולה ביניהן. תפקידיו של CERT-UK הם להגיב לאירועים בזמן אמת, להעלות את המודעות לסיכוני סייבר, לתמוך בתשתיות קריטיות ולהוות כתובת גישה אחידה לארגוני ה־CERT השונים ברחבי העולם.

ארגון נוסף בתוך NCSC הוא Center for the Protection of National Infrastructure (CPNI), הפועל במסגרת ארגון מודיעין הפנים של בריטניה. הוא הוקם ב־2007 כמיזוג בין שני מוסדות: NISCC להגנה על תשתיות קריטיות ו־NSAC, שפעל במסגרת 5MI ויעץ לגופים שונים של ממשלת בריטניה. מטרת המיזוג הייתה לסייע לממשלה בהגנה על תשתיות לאומיות ובהתמודדות עם איומי טרור. בריטניה הגדירה 13 מגזרים כקריטיים – כימיקלים, המגזר האזרחי־גרעיני, תקשורת, ביטחון, תשתיות חירום, אנרגיה, פיננסים, מזון, שירותים ממשלתיים, בריאות, חלל, תחבורה, תשתיות מים.[113] תשתית קריטית, לפי הגדרת הממשלה הבריטית, היא כל מה שחיוני לתפקודה התקין של המדינה.

במהלך השנים הפיץ CPNI מספר הנחיות, הן לארגונים גדולים והן לעסקים קטנים ובינוניים, אשר כללו תקני הגנה בסייבר. הארגון גם מספק תשתית למיגור אירועי סייבר ולתגובה עליהם ונותן הדרכה לעובדים ולבעלי עסקים בדבר האיומים במרחב הסייבר ודרכי ההתגוננות מפניהם. כל זאת, על בסיס החזון של הקניית הרגלי עבודה נכונים והעלאת המודעות להגנה על רשתות ארגוניות.

מוסד חשוב נוסף הינו Center for Cyber Assessment (CCA), שהוקם באפריל 2013. גוף זה עוסק בהערכת מידע מודיעיני, ויש לו, בין השאר, גישה למידע מודיעיני מסווג הנמצא באחריותו של GCHQ. המרכז להערכת סייבר מתדרך את פקידי הממשלה הרלוונטיים ומגבש הערכות על סיכוני סייבר לתשתיות הקריטיות של המדינה.

112 Chad Heitzenrater and Andrew Simpson, "Policy, Statistics and Questions: Reflections on UK Cyber Security Disclosures", *Journal of Cybersecurity*, Vol. 2, No. 1, 2016, pp. 43-56.

113 "Summary of the 2015-16 Sector Resilience Plans", Cabinet Office, May 2016.

מאמצי שיתוף המידע על איומי סייבר בבריטניה מרוכזים ברובם ב־Cybersecurity Information Sharing Partnership (CiSP). זוהי תוכנית המשלבת בין התעשייה, הממשלה וגורמי אכיפת החוק ומאפשרת לשתף מידע על איומי סייבר באופן חסוי ומאובטח. נכון למאי 2016, שותפים כ־2,220 ארגונים בבריטניה לתוכנית שיתוף המידע והיא הפכה לדוגמה עבור מדינות אחרות. יחד עם זאת, סקרים שבוצעו בקרב משתתפי התוכנית מראים כי 58 אחוזים מהנשאלים חושבים שפריצות הסייבר שהם חווים אינן מצריכות דיווח, וכי הם גם אינם יודעים למי עליהם לדווח.[114] שיתוף המידע באמצעות CiSP מהווה אינדיקציה עבור חברות הביטוח השונות לתמחור פוליסות הגנה במרחב הסייבר. למעשה, השוק הבריטי עדיין לא מציע פוליסות ביטוח תחרותיות שיאפשרו הגנה אמיתית בסייבר במחיר סביר.

בנוסף לפעילות הענפה במסגרת NCSC, גם משרד ההגנה הבריטי נושא בסמכות ובאחריות לפיתוח יכולות תקיפה והגנה במרחב הסייבר, שמטרתן היא לספק הגנה מפני האיומים השונים בתחום זה. הפעילות הצבאית הבריטית במרחב הסייבר מרוכזת תחת Joint Cyber and Electromagnetic Activities Group (JCG), שבמסגרתה פועלת Joint Force Cyber Group, שתפקידה הוא לפתח יכולות בתחום הסייבר. בנוסף לכך פועל Defence Assurance and Information Security (DAIS), האחראי על אבטחת המידע במערכת הביטחונית הבריטית.

פיתוח יכולות התקפיות במרחב הסייבר נמצא באחריות GCHQ, הפועל בשיתוף עם משרד ההגנה הבריטי. לאחרונה הקצתה הממשלה ארבעים מיליון ליש"ט לפתיחתו של מרכז מבצעי להגנת סייבר במסגרת משרד ההגנה הבריטי – Cyber Security Operations Centre (CSOC) – שגם הוא אמור לפעול בהנחיית GCHQ. מטרתו של גוף זה היא לבצע ניתוח ומחקר מודיעיניים יחד עם סוכנויות אחרות, במטרה לספק הגנה על רשתות לאומיות בכלל ועל אלו של משרד ההגנה בפרט.

זרוע מוסדית חשובה נוספת היא National Crime Agency, העוסקת בפשיעת סייבר. במסמך האסטרטגיה שפורסם ב־2016 מפורטת הפעילות הבריטית נגד פשיעת סייבר הן ברמה הלאומית והן ברמה הבין־לאומית. ההתמקדות ברמה הלאומית היא בפשעים נגד אזרחים בריטיים ובתמיכה בקורבנות של פשיעת סייבר, כמו גם בטיפול בפושעי סייבר בריטיים. ההתמקדות ברמה הבין־לאומית היא בפשע מאורגן ובפגיעה ברווחיות הפשיעה בסייבר. בתוך הסוכנות הלאומית ללחימה בפשיעה פועלת יחידת

114 Rebecca Klahr, Shah Jayesh, Sheriffs Paul, Rossington Tom, Pestell Gemma, Button Mark, Wang Victoria, "Cyber Security Breaches Survey 2017", April 2017, Portsmouth Research Portal, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

תיאום – The National Cyber Crime Unit (NCCU) – המתאמת את המענה לפשעי סייבר, ובעת אירוע פשע כזה מתאמת את פעילותם של גורמי אכיפת החוק – NCSC ו־ GCHQ. בכל אחד מהאזורים בבריטניה קיימת יחידה ללחימה בפשיעה אזורית, שבתוכה פועלת גם יחידה ייעודית ללחימה בפשיעת סייבר.

חקיקה

החקיקה הבריטית בנושאי הגנת סייבר מתמקדת בתחומי הגנת הפרטיות והגנה על מידע, וזאת באמצעות שתי חקיקות מרכזיות: Data Protection Act משנת 1998 ו־ Electronic Communications Regulations משנת 2003, העוסקות באיסוף ובעיבוד מידע. תהליך החקיקה החל כבר ב־1984 על ידי The Information Commissioner's Office (ICO) – סוכנות עצמאית שתפקידה היה לדאוג לאינטרס הציבורי בשמירה על הפרטיות – שקבעה שמונה עקרונות לניהול תקין של מידע אישי. תפקידה המקורי של סוכנות זו היה רישום בעלי מאגרי מידע חדשים, אך ב־1987 הוקמה בה מחלקת חקירות, ועם כניסתו לתוקף של חוק הפרטיות מ־1998, היא צברה כוח רב והפכה לגוף האחראי לכך שמידע אישי יטופל באופן חוקי ולמטרות מוגדרות בלבד. במסגרת זו נקבע כי יוטלו סנקציות על כל מי שלא יגן כראוי על פרטיות המידע האישי.

ב־2011 הוטלה על הסוכנות גם האחראיות על יישום חוק חופש המידע – Freedom of Information Act, שבמסגרתו היא הוסמכה להטיל קנסות כספיים של עד חצי מיליון ליש"ט על פגיעה בפרטיות. ב־2015 הסירה הממשלה את התנאי של הוכחת נזק לצורך הטלת קנסות, וכוחה של הסוכנות המשיך להתחזק. כיום היא יכולה לדרוש מארגונים מידע על האופן בו הם מגנים על הפרטיות של לקוחותיהם, לדרוש מהם נקיטת צעדים מחייבים נוספים, לבצע ביקורות, להטיל קנסות ולתבוע בבית משפט כל מי שאינו ממלא את חובת ההגנה על הפרטיות. כך, למשל, ב־2015־2016 הטילה הסוכנות קנסות בשיעור של 2.6 מיליון ליש"ט, וקצב הטלת הקנסות הולך וגובר מאז. הקנסות הוכחו כמהלך אפקטיבי בשתי רמות: הן כגורם המשפיע על שינוי פרקטיקות ארגוניות בקרב הנקנסים, והן כגורם מרתיע עבור ארגונים אחרים.[115]

על אף שאין חוק גורף[116] המחייב דיווח בעת תקיפת סייבר ופגיעה אפשרית במידע אישי, קיימת הסכמה בבריטניה ש־ICO הוא הכתובת לקבלת דיווח על כך והגורם המחליט על אופן התגובה הראוי – אם על ידי הטלת סנקציות ואם על ידי בדיקה של הסטטוס הארגוני בשאלת הגנת הסייבר.

---

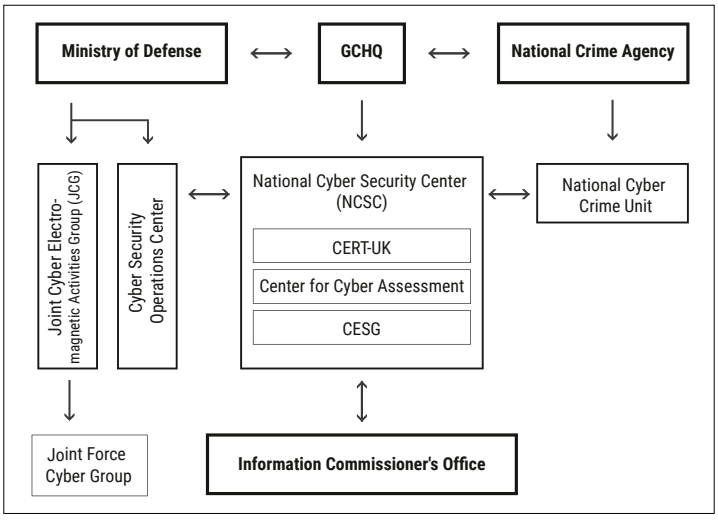
115 "Information Commissioner's Annual Report and Financial Statements 2013/2014", *Information Commissioner's Office*.

116 למעט תחום התקשורת, הכפוף לרגולציה ייעודית מ־2003 – Privacy and Electronic Communications (EC Directive).

החוק הבריטי המרכזי העוסק באיסוף מידע בסייבר ובמעקב אחריו על ידי המדינה חוקק בשנת 2000 – Regulation of Investigatory Powers Act (RIPA). חוק נוסף בתחום זה הוא Data Retention and Investigatory Powers (DRIP) משנת 2014, המאפשר למזכיר המדינה לענייני חוץ וחבר העמים הבריטי לדרוש מחברות תקשורת להעביר אליו מידע עד שנה אחורה. בנובמבר 2016 התקבל בבריטניה חוק חדש – The Investigatory Powers Bill – המאחד את שני החוקים ומרכז את הסמכויות והאחריות בנושא הסייבר הכלולות בשניהם.

תחומי הפרטיות והמעקב אחרי מידע בסייבר נמצאים בליבת העיסוק של הסוכנויות הבריטיות השונות, כאשר אסטרטגיית הביטחון הלאומית מ־2015 מבטאת את רצון הממשלה להביא לאיזון בין קידום הביטחון הלאומי ובין שמירה על פרטיות האזרחים.[117]

תרשים 3 מתאר את המבנה המוסדי של הגופים שתוארו לעיל ומסייע להבנה טובה יותר של תפקידי השחקנים השונים ושל קשרי הגומלין ביניהם.



תרשים 3: סוכנויות ומוסדות העוסקים בנושא הגנת הסייבר בבריטניה

צרפת

שלושה אירועי סייבר משמעותיים הדגישו את החשיבות והדחיפות של ההגנה על מרחב הסייבר בעיני שלטונות צרפת: התקפות הסייבר על אסטוניה בשנת 2007, וכתוצאה

117 UK Prime Minister Office, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015, p. 19, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

מכך הפגיעה האנושה באספקת שירותים מדינתיים, היוו את הרקע למסמך הנחייה של ממשלת צרפת משנת 2008, שהעלה את הגנת הסייבר לרמה של עדיפות לאומית עליונה; בתחילת 2009 הפך משרד ההגנה הצרפתי לקורבן של התולעת Conficker,[118] מה שחידד את ההבנה בקרב מקבלי ההחלטות בצרפת כי נדרשת התערבות מדינתית אגרסיבית יותר כדי להתמודד עם האיומים במרחב הסייבר; חשיפת מתקפת Stuxnet ב־2013 הביאה להוראה ישירה של נשיא צרפת, ובעקבותיה להחלטת ממשלה, המדגישה את חשיבות ההגנה בסייבר.

התפתחות נוספת בעמדת ממשלת צרפת בתחום הגנת הסייבר הייתה ב־2015, כאשר צרפת חוותה שתי התקפות סייבר משמעותיות: בינואר אותה שנה לִוו מתקפות הטרור של ארגון המדינה האסלאמית על מערכת העיתון "שרלי הבדו" במאמץ של טרוריסטים לפעול במרחב הסייבר נגד אתרי אינטרנט צרפתיים פרטיים וציבוריים; באפריל 2015 בוצעה השתלטות דיגיטלית של ארגון המדינה האסלאמית על ערוץ הטלויזיה TV5 והופצו הודעות תמיכה באסלאם הקיצוני והתבטאויות נגד הממשל הצרפתי.

מחקרים בודדים בלבד עוסקים במאמצי ההגנה של צרפת במרחב הסייבר. ב־2014 פורסם מחקר על פעילות הסוכנויות השונות בצרפת בתחום זה,[119] וב־2016 פורסמה הערכה על יכולות ההגנה בסייבר של צרפת בזירות שונות.[120] להלן יובאו תובנות מרכזיות ממחקרים אלה, מתוך כוונה לשרטט תמונה רחבה ומקיפה ככל האפשר על הנעשה בצרפת בתחום הגנת הסייבר.

ההבחנה המרכזית של משטר הרגולציה הצרפתי היא בין Cyber Defense, הנוגע ליכולות מבצעיות־אקטיביות לשמירת ההגנה במרחב הסייבר, ובין Cyber Protection, הנוגע למניעת התקפות במרחב זה. מדובר בשתי מטרות הקשורות זו בזו, ולעיתים משלימות האחת את השנייה, המקודמות ומטופלות על ידי החוקים השונים והסוכנויות השונות בצרפת.

המבנה המוסדי

ניתן לזהות ארבעה שחקנים עיקריים ברגולציה הצרפתית במרחב הסייבר: השחקן המרכזי הראשון הוא הסוכנות הלאומית לביטחון מערכות מידע (ANSSI) – הגוף העיקרי

---

118 תולעת מחשבים שהדביקה על פי ההערכות כ־12 מיליון מחשבים בעלי מערכות הפעלה Windows. לתיאור מפורט של פעולת התולעת ראו: הרצל לוי ואפיק קסטיאל, "ניתוח תולעת ה־Conficker", *Digital Whisper*, גיליון 6, מארס 2010, https://www.digitalwhisper.co.il/files/Zines/0x06/DW6-3-Conficker.pdf

119 Philippe Vitel, Henrik Bliddal, "French Cyber Security and Defence: An Overview", *Information & Security: An International Journal,* Vol. 32, 2014, pp. 3209-1-13.

120 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, "France Cyber Readiness at a Glance", Potomac Institute for Policy Studies, 2016.

העוסק בהגנת הסייבר בצרפת. הסוכנות הוקמה ב־2009 וכפופה ישירות למשרד ראש הממשלה. עיקר עיסוקה הוא בהגנה על תשתיות קריטיות ובמניעת התקפות סייבר. תקציבה גדל משמעותית בין 2010 ל־2014 – מ־43 מיליון אירו ל־83.8 מיליון אירו.[121] הסוכנות הלאומית לביטחון מערכות מידע אינה גוף מודיעיני האוסף מידע לצורכי הגנה ואפשר להתייחס אליה כמקבילה של המשרד לביטחון המולדת בארצות הברית.

האסטרטגיה הצרפתית במרחב הסייבר מ־2013 עוסקת בסמכותה של סוכנות זאת להגן על מפעילי תשתיות חיוניות – גופים ציבוריים או פרטיים המפעילים תשתיות, שפגיעה בתפקודן תפגע משמעותית ביכולות הכלכליות של המדינה או ביכולותיה להגן על עצמה. רשימת המפעילים החיוניים הינה חסויה מנימוקים של ביטחון לאומי. תהליך ההגנה על תשתיות חיוניות החל למעשה הרבה לפני שנת 2013, וזכה לדחיפה בעיקר לאחר התקפות טרור משמעותיות שהתרחשו בארצות הברית, במדריד ובלונדון.[122] מסמך פנימי של משרד ההגנה הצרפתי עסק בתשתיות חיוניות כבר ב־2005 וב־2006, וכלל במסגרתן 12 מגזרים בארבעה תחומים: תשתיות לאזרחים (בריאות, מזון, מים); תשתיות לתפקוד המדינה (צבאיות ואזרחיות, כולל בתי משפט); תשתיות כלכליות (אנרגיה, תחבורה, מגזר פיננסי); תשתיות טכנולוגיות (תעשייה, חלל, מידע). ב־2013 הוגדרו המפעילים בכל אחד מהמגזרים הללו כ"מפעילי תשתיות חיוניות".

תפקידה המרכזי של הסוכנות הלאומית לביטחון מערכות מידע הוא להתוות את התקנים הרצויים להגנת סייבר, לקבל דיווחים על אירועי סייבר אצל מפעילי תשתיות חיוניות, לבצע אצלם ביקורות פתע לצורך בדיקת ההגנה בסייבר ולהחליט על האופן בו הרשתות השונות יסווגו. למעשה, אלו ההנחיות המחייבות היחידות הקיימות בצרפת להגנה בסייבר. תפקיד נוסף של הסוכנות הוא לעודד את תעשיית הסייבר בצרפת ולהעלות את המודעות לסיכוני סייבר בקרב האזרחים. גופים שאינם נמצאים תחת ההגדרה של מפעילי תשתיות חיוניות אינם כפופים להנחיות מחייבות להגנת סייבר מצד המדינה.

ב־2017 פרסמה הסוכנות הלאומית לביטחון מערכות מידע מסמך הכולל 42 המלצות להתגוננות בסייבר, וכן הנחיות ייעודיות לבעלי עסקים קטנים ובינוניים. כמו כן, היא יצרה "חותמת" ייחודית של המדינה – France Cybersecurity Label – המוענקת לפתרונות אבטחת מידע צרפתיים. הסוכנות גם עוסקת ברישוי מוצרים ונותני שירותים על פי שלוש רמות מומחיות. מוצרים ובעלי מקצוע אשר סווגו על ידי המדינה ברמה הגבוהה ביותר מורשים לעבוד עם מפעילי תשתיות חיוניות. בנוסף

121 French Prime Minister Office, "Politics of France Cybersecurity," February 20, 2014, https://www.ssi.gouv.fr/uploads/IMG/pdf/dossier_de_presse_web_20140220.pdf

122 ראו מסמך רשמי של הסוכנות הלאומית לביטחון מידע המתאר תהליך זה: https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/

לכך, עוסקת הסוכנות לביטחון מערכות מידע בקמפיינים ובעריכת כנסים להעלאת המודעות לסיכוני סייבר.

שחקן חשוב נוסף בהגנת הסייבר בצרפת הוא משרד ההגנה. בשנת 2011 הונהג במשרד ההגנה תפקיד חדש – ראש תחום הגנה בסייבר, שאחריותו היא לקדם את ביטחון הסייבר במשרד וכן לקדם מבצעי סייבר לחיזוק ההגנה באופן כללי. במשרד ההגנה הצרפתי גם קיים צוות משימה ייעודי, שתפקידו הוא לקדם את היכולות הטכנולוגיות להגנה בסייבר, וכן זרוע התקפית לזיהוי ולתגובה מהירה במקרה של תקיפות סייבר ברחבי צרפת. בדצמבר 2016 הודיע שר ההגנה הצרפתי על שינויים בתחום הגנת הסייבר במשרד והורה על הקמת יחידת סייבר ייעודית – פיקוד הסייבר (The Cyber Command).

פיקוד הסייבר הצרפתי מרכז בתוכו את כל יכולות הסייבר של משרד ההגנה והוא כפוף ישירות לראש המטות המשולבים של צבא צרפת. בתחילה נשקלה האפשרות לפתח מומחיות לסייבר בתוך כל אחת מזרועות הים, האוויר והיבשה של הצבא הצרפתי, אך לבסוף הוחלט להקים יחידת ייעודית שתרכז את כל הפעילות בתחום הסייבר. ייעוד היחידה הוא איסוף מידע ומודיעין, הגנה ומניעת תקיפות סייבר, וכן תגובה לאירועי סייבר במקרה הצורך. תחומי אחריותה כוללים גם תשתיות קריטיות והיא פועלת בתיאום עם ANSSI, שעליה מוטלת האחריות הכוללת בנושא הסייבר בצרפת. אחד הנושאים המרכזיים שבהם עוסק פיקוד הסייבר הצרפתי הוא פיתוח תגובות אוטומטיות לתקיפות סייבר. למעשה, האחריות על הגנת הסייבר בצרפת מחולקת בין שלוש סוכנויות: ANSSI העוסקת בהגנה על תשתיות חיוניות ופועלת במסגרת משרד ראש הממשלה; פיקוד הסייבר של משרד ההגנה האחראי על מבצעים צבאיים במרחב הסייבר; סוכנות המודיעין הצרפתית המספקת את היכולות הטכנולוגיות לתמיכה בתהליכים אלה.

משרד ההגנה הצרפתי פועל גם במגזר האזרחי. ב־2014 הודיע המשרד על פיתוח יכולות הגנה בסייבר עבור כלל החברות הצרפתיות במטרה לתמוך בתעשייה המקומית. במסגרת זו נקט המשרד שתי פעולות משמעותיות: הקמת יחידת מצוינות להגנה בסייבר והקמת גוף אזרחי להעלאת המודעות ולחיבור בין האקדמיה, התעשייה והחברה לצורך גיבוש פתרונות הגנה במרחב הסייבר.

שחקן מוסדי שלישי חשוב במרחב הסייבר הצרפתי הוא משרד הפנים, העוסק בעיקר בפשיעת סייבר. ב־2014 שדרג המשרד את יכולותיו לטפל בפשיעה בסייבר כשמינה אדם מיוחד לטפל באופן ייעודי בבעיה. הפונקציה החדשה נשענת על חקיקה המקנה סמכויות לטיפול בפשיעת סייבר ומרחיבה את ההגדרה של פשע סייבר. משרד הפנים גם מגבש סטטיסטיקות ייעודיות של פשעי סייבר לצורך שיפור הטיפול בבעיה, וכן מפרסם דוח שנתי על פשיעת סייבר. בנוסף לכך, המשרד פועל בשיתוף פעולה עם הגופים

הנוספים בצרפת העוסקים בהגנה על מרחב הסייבר, במטרה להעלות את המודעות בקרב קטינים לבעייה ולעודד את התעשייה להשקיע במחקר ופיתוח במרחב הסייבר.

גורם רביעי הממלא תפקיד מרכזי וכבד משקל בתחום הגנת הסייבר בצרפת הוא הרגולטור להגנת הפרטיות – המועצה למידע חופשי (CNIL). זהו מוסד רגולטורי שהיה ממובילי המאבק להגנת המידע לא רק בצרפת, אלא באירופה בכלל. תקציבו כיום הינו 16 מיליון אירו והוא מונה 192 עובדים. סמכויותיו כוללות חקירה ושליטה על פרקטיקות השימוש במאגרי המידע השונים בצרפת ויכולת להטיל סנקציות על ארגונים שאינם פועלים בהתאם להנחיות האבטחה. המועצה גם בודקת פניות של אזרחים הטוענים לפגיעה בפרטיותם על ידי ארגונים ומוסדות המחזיקים במידע אישי. היא גם זו המאשרת בפועל עיבוד אוטומטי של מידע, מביעה את דעתה על ההתנהלות הממשלתית כלפי מידע אישי, מייעצת בכל הנוגע לתשתית חוקתית להגנת הפרטיות ומסייעת לחברות פרטיות להבין מצבים של פגיעה אפשרית במידע. ההנחיות האירופיות להגנת המידע מחייבות כל ארגון שיש לו מאגר מידע גדול ליידע את המועצה למידע חופשי במקרה של גניבת מידע או פריצה למערכותיו.

יש מי שמותחים ביקורת על המועצה, ובכלל זה על שהיא מחמירה מדי וסובלת מעודף רגולציה, בעוד שאחרים טוענים כי היא אינה אפקטיבית מספיק מול מונופולים טכנולוגיים גדולים, כמו "גוגל" ו"פייסבוק". למרות זאת, החקיקה הצרפתית מ־2016 הרחיבה גם את סמכויותיה של המועצה למידע חופשי, ובכלל זה מאפשרת לה להטיל סנקציות על פגיעות בפרטיות אפילו על ארגונים גדולים. הדבר הקנה למועצה את היכולת לתבוע גם מחברת "פייסבוק" הקפדה רבה יותר מבעבר על פרטיות המשתמשים.[123]

חקיקה

תשתית החקיקה הצרפתית העוסקת באיסוף מידע לצורכי ביטחון, ובכלל זה בהגנת הסייבר, החלה להיווצר כבר בשנת 1978, כאשר נחקק חוק לאומי להגנה על מידע אישי ושמירה על הפרטיות. צרפת הינה מחלוצות השמירה על הפרטיות וההגנה על המידע הן באירופה והן בעולם בכלל. החוק מ־1978 הקים את סוכנות הגנת המידע הצרפתית רבת ההשפעה. בהמשך חקקה צרפת חוק למניעת פשעים במרחב הסייבר (1988), שכָּלל הטלת סנקציות, וב־1991 נחקק החוק המאפשר לסוכנות המודיעין הצרפתית לבצע איסוף מידע באופן נרחב. חוק זה מהווה את התשתית הרגולטורית לתוכניות המעקב של צרפת החל מ־2008.

פשיעת הסייבר חזרה להעסיק את המחוקקים בצרפת ב־2001 וב־2004, עם שורה של חוקים שעדכנו את סמכויות הענישה בהתאם להתפתחויות הטכנולוגיות. ב־2006

123 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, "France Cyber Readiness at a Glance", Potomac Institute for Policy Studies, 2016, p. 10.

נחקק חוק המקנה עדיפות לביטחון המדינה על פני פרטיות האזרחים ומורה לארגונים האוספים מידע על לקוחותיהם לאפשר לסוכני אכיפת החוק גישה למידע זה ללא צו ייעודי מבית המשפט. העדיפות לביטחון המדינה קיבלה דחיפה נוספת בשנת 2011 בדמות חוק המאפשר איסוף מסיבי של מידע ממערכות מחשב בזמן אירוע ביטחוני "חמור", כגון אירוע טרור.

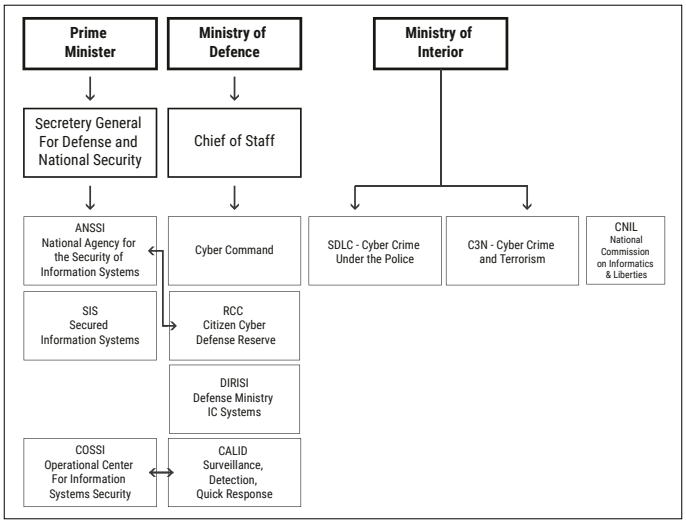
ב־2015 קיבלו מאמצי הביטחון של המדינה במרחב הסייבר דחיפה חוקתית נוספת: חקיקה חדשה בנושאי מודיעין קבעה את הכלים בהם יוכלו רשויות הביטחון לעשות שימוש, וכן הרחיבה את תחומי איסוף המידע במרחב הסייבר מעֵבר לנושאי טרור, מודיעין כלכלי, פשע מאורגן וריגול נגדי, כך שהמדינה תוכל לאסוף מידע גם עבור מטרה כללית כמו "קידום אינטרסים של מדיניות החוץ הצרפתית" או מניעת אלימות ונזקים במקומות ציבוריים. החוק גם מאפשר מעקב ואיסוף פולשניים יותר, ובכלל זה על אזרחים בעלי קשר כלשהו לאיום על ביטחון המדינה. התקפות הטרור בניס ביולי 2016 הפכו חוק זה לחודרני אף יותר.[124]

באוקטובר 2016 הציגה צרפת חקיקה מאזנת בדמות חוק הרפובליקה הדיגיטלית. חוק זה מאפשר הגנה על הפרטיות ושמירה על מידע אישי במרחב הסייבר, תוך שהוא מעלה את המודעות לסכנות ומדגיש את חשיבות ההגנה על האינטרסים של האזרחים במרחב זה, למשל על ידי מתן זכות לקבל את כל המידע שנאסף עליהם או "להישכח" בחיפושי "גוגל". בנוסף לכך, החוק מורה על גישה חופשית למרחב הסייבר לכל. יחד עם זאת, אירועי טרור שונים שקרו בצרפת מאז נחקק החוק גרמו לכך שהוא לא נאכף במלואו.

הרגולציה בצרפת הייתה ערוכה טוב יחסית לאימוץ ההנחייה של האיחוד האירופי להגנה על מרחב הסייבר (Network Security and Information Directive – NIS). גוף הרגולציה הצרפתי האחראי לכך היא הסוכנות הלאומית לביטחון מערכות המידע.

תרשים 4 מתאר את ההיררכיה והקשרים בין הסוכנויות והגופים השונים בצרפת העוסקים בהגנת סייבר. בראש התרשים מופיעים ארגונים ברמת המשרדים הממשלתיים; תחתיהם נמצאת רמה הבאה בהיררכיה במסגרת כל משרד; ולבסוף ברמה התחתונה נמצאים השחקנים המעורבים באופן ישיר בהתוויית הרגולציה בתחום הסייבר.

124 Felix Treguer, "Intelligence Reform and the Snowden Paradox: The Case of France", *Media and Communication*, Vol. 5, No. 1, 2017, pp. 17-28.



תרשים 4: סוכנויות ומוסדות העוסקים בנושא ביטחון הסייבר בצרפת

גרמניה

הגישה הגרמנית לרגולציית הגנה בסייבר נשענת הן על שחקנים מדינתיים והן על שחקנים בין־לאומיים. מסמך האסטרטגיה הגרמנית הראשון בנושא זה פורסם ב־2011 על ידי משרד הפנים של גרמניה, וכבר בפתיחתו ניתן ביטוי לגישה של "אחריות משותפת למדינה, לתעשייה ולחברה לקידום הגנת הסייבר בגרמניה".[125] המסמך האסטרטגי האחרון שפורסם על ידי משרד הפנים הגרמני ב־2016 מחזק גישה זו ואף מרחיב אותה לתחום המדעי ולמגזר העיסקי.

המבנה המוסדי

הגורמים העיקריים הממלאים תפקיד בהגנת הסייבר בגרמניה הם משרד הפנים הגרמני (Bundesministerium des Innern – BMI), הנציבות הלאומית להגנה בסייבר (National Cyber Security Council), הצבא הגרמני (Bundeswehr), שירות המודיעין הפדרלי (BND) ויוזמות נוספות של גורמים ממשלתיים, וכן ארגוני הגנת המידע וארגוני חברה אזרחית.

משרד הפנים הגרמני

משרד הפנים הינו היישות המרכזית בתחום הרגולציה של הגנת הסייבר בגרמניה. למעשה, המשרד מאגד בתוכו את רוב מאמצי המדינה להבטחת ההגנה בסייבר, על

125 ראו מסמך האסטרטגיה *Cyber Security Strategy for Germany 2011* באתר משרד הפנים הגרמני: http://www.bmi.bund.de

שלל רבדיה – טכנולוגיה, מודיעין, פשיעת סייבר ותשתיות קריטיות. מספר סוכנויות מרכזיות העוסקות בהגנת סייבר פועלות תחת אחריותו של משרד הפנים: המשרד הפדרלי לאבטחת מידע (BSI), העוסק בעיקר בנושאים טכנולוגיים; המשרד הפדרלי להגנת החוקה (BfV), העוסק בעיקר בנושאי מודיעין פנים; סוכנות המשטרה הפדרלית לפשיעה (BKA), העוסקת בפשיעת סייבר; המשרד הפדרלי להתגוננות אזרחית ולסיוע במצבי אסון (BBK), העוסק בתשתיות קריטיות.

המשרד הפדרלי לאבטחת מידע הוקם ב־1991 והיה אחראי מתחילת דרכו על עיצוב ומימוש הגנת הסייבר בגרמניה, תוך קידום תחומי המניעה, הגילוי והתגובה לאירועים. כיום הוא אחראי על מימוש אסטרטגיות הסייבר של גרמניה ונושא באחריות להגנת הסייבר בכל המגזרים – המדינתי, העיסקי והאזרחי. כמו כן, הוא עורך מחקרים ומפיק דוחות סטטוס שנתיים על מצב הגנת הסייבר במדינה. בתחילת 2017 מנה המשרד יותר מ־650 עובדים בחמש מחלקות – אחת כללית וארבע ייעודיות – העוסקות בייעוץ, תיאום, הצפנה, פיתוח תקנים והסמכה בנושאי הגנת הסייבר והמידע.

ב־1994 פרסם המשרד הפדרלי לאבטחת מידע לראשונה מסמך תקנים לניהול הגנת מערכות המידע בגרמניה, וב־2001 הוא קיבע את מעמדו כאחראי על אספקת שירותי הגנת מידע עבור כלל המדינה. בעשור הראשון של המאה הנוכחית, עם התפתחות הדרכון וכרטיס הבריאות האלקטרוני, פיתח המשרד את הפרוטוקולים וההוראות הטכנולוגיות לתמיכה במיזמים אלה. עד מהרה הוא הפך גם לגוף המרכזי לקבלת דיווחים על אירועי סייבר ולזיהוי פערים בהגנת הסייבר בגרמניה, הן עבור מוסדות המדינה והן עבור הציבור הרחב. המשרד לביטחון המידע אמון גם על מרכזי ה־CERT בגרמניה. ה־CERT הראשון בגרמניה הוקם על ידי המשרד הפדרלי לאבטחת מידע ב־1994, וב־2001 הוא הוכרז למרכז ה־CERT הרשמי של גרמניה. ב־2006 הוקם מרכז CERT ייעודי עבור אזרחי גרמניה, במטרה להעלות את המודעות ולספק להם מידע מהימן ועדכני על הסכנות הטמונות בסייבר.

אסטרטגיית הסייבר של גרמניה מ־2011 הנחתה את המשרד הפדרלי לאבטחת מידע להקים מרכז תגובה ייעודי לאירועי סייבר מדינתיים – Cyber AZ – המשתף פעולה עם משרדי המודיעין וביטחון הפנים ועם המשטרה בגרמניה. גם התעשייה והאקדמיה נטלו חלק בעיצוב המרכז ומעורבות מאז בקבלת ההחלטות סביב אירועי סייבר. מרכז התגובה מסייע למועצה לביטחון לאומי של גרמניה לקבל החלטות בנושאי סייבר, הן באופן שוטף והן באירועים ספציפיים. למעשה, המרכז הביא למיסוד שיתופי מידע וידע בין הרשויות השונות האחראיות להגנת הסייבר בגרמניה.

משרד הפנים הגרמני מקיים פעילות ענפה גם בתחום התשתיות הקריטיות. ב־2003 הגדירה גרמניה מהי תשתית קריטית ברמה הפדרלית: "הארגונים והמוסדות בעלי חשיבות עליונה למדינה, אשר פגיעה בהם תוביל להפרה בוטה של ביטחון הציבור

ולמחסור בצרכים בסיסים של המדינה".[126] ב־2005 הציגה המדינה את התוכנית הלאומית להגנה על תשתיות מערכות מידע, שנועדה הן עבור מוסדות המדינה והן עבור התעשייה. המגזרים שהוגדרו בתוכנית זו כתשתית קריטית הם: אנרגיה, תקשורת ותשתיות מידע, תחבורה, בריאות, מים, מזון, פיננסים וביטוח, תקשורת המונים, מדיה ותרבות (ובכלל זה טלוויזיה, רדיו, עיתונות אלקטרונית וכתובה, מבני מדינה סמליים ומוסדות מדינתיים.[127] בנוסף, הממשלה דאז יצאה בתוכנית ייעודית לשיתוף פעולה בין התעשייה ובין המדינה בכל הקשור לתשתיות קריטיות. התוכנית עסקה בכל המגזרים הרלוונטיים שהוגדרו כתשתית קריטית וטיפלה בנושאים הקשורים הן להגנה פיזית והן להגנת סייבר בתשתיות אלו. בנוסף לכך, התוכנית התוותה סימולציות לניהול אירועי סייבר בתשתיות קריטיות, קידמה פעולות הכשרה והדרכה בתחום זה, פרסמה מחקרים והגדירה אלו תשתיות קריטיות אמורות לעמוד בדרישות להגנת מערכות המידע שלהן.

ב־2007 פרסמה הממשלה הפדרלית תוכנית ליישום ההגנה על תשתיות קריטיות בגרמניה (KRITIS). התוכנית עסקה בניהול משברים ובתגובה לאירועים, כמו גם ברציפות התפקודית של תשתיות אלו. ספציפית, התוכנית הציגה את עקרונות מערכת היחסים ושיתופי הפעולה בין הממשל ובין מפעילים פרטיים של תשתיות קריטיות וסקרה את האופן בו יש להגיב לאירועי סייבר. ב־2011 החלו ניסיונות למסד עקרונות אלה בחקיקה, שהובילו בסופו של דבר לחקיקתו של חוק ביטחון המידע IT Security) (Act משנת 2015, המהווה את התשתית החוקתית הנוכחית להגנת מערכות המידע של מפעילי תשתיות הסייבר בגרמניה. החוק קובע כי המפעילים הפרטיים צריכים להגן לא רק על האתרים שלהם, אלא גם על מערכות הקצה האחורי (backend). תקני ההגנה אינם מעוגנים בחקיקה אלא מבוססים על התקינה הבין־לאומית של ISO או DIN. ההימנעות מקביעת תקנים גרמניים בחקיקה נועדה לאפשר למערכות ההגנה להתעדכן עם הזמן. כתוצאה מכך, התעשייה הגרמנית יכולה לקבוע את התקנים עבור עצמה, כל עוד הם מאפשרים לשמור על תקינות התשתיות. החקיקה מ־2015 משמשת כיום הנחייה תקפה גם לתעשיות שאינן כפופות לה באופן פורמלי. חקיקת חוק ביטחון המידע קיבעה את מעמדו של המשרד הפדרלי לאבטחת מידע כגוף המרכזי העוסק באיסוף מידע על אירועי סייבר בתשתיות קריטיות.

ב־2016 נכנסה לתוקפה הרגולציה של KRITIS, המפרטת את הקריטריונים על פיהם מפעילים פרטיים יוגדרו ככפופים לרגולציה של תשתיות קריטיות. רגולציה זו מאפשרת למשרד הפדרלי לאבטחת מידע להטיל קנסות על מפעילי תשתיות קריטיות

126 ראו ההגדרה באתר של המשרד הפדרלי להתגוננות אזרחית ולסיוע במצבי אסון: http://www.bbk.bund.de

127 ראו אתר ייעודי שהוקם בנושא זה: http://www.kritis.bund.de

שאינם עומדים בתקינה הנדרשת, עד לסכום מרבי של 100,000 אירו. החידוש האחרון בשיתוף הפעולה בין המדינה לתעשייה הוא הקריאה לביצוע "Security By Design" שמטרתה היא להכניס שיקולים של הגנת סייבר בפיתוחים עתידיים.

הרשויות בגרמניה הגדירו את תשתית האינטרנט במדינה כתשתית קריטית עבור החברה הגרמנית. למרות זאת, יש מומחים הטוענים כי הממשלה הפדרלית אינה עושה מספיק בתחום זה. הם מדגימים את טענתם באמצעות הצבעה על ההשקעות המעטות בהגנת הסייבר במסגרת התוכניות הלאומיות לעידוד מעבר לתעשייה מבוססת תשתיות דיגיטליות.[128] למעשה, האסטרטגיה הגרמנית להגנת הסייבר שפורסמה בשנת 2016 מאשרת מצב זה, כשהיא מצביעה על היעדר מוסדות וגופים מדינתיים שיכולים לסייע לציבור הרחב להתמודד עם אירועי סייבר ומתייחסת אל הצוותים המוקמים אד־הוק במוסדות שונים בעקבות אירועי סייבר – Mobile Incident Response Teams (MIRTs) – כגופים העוסקים בכך.

המשרד הפדרלי לאבטחת מידע אחראי גם על הגנת המידע של הרשתות הפדרליות עצמן. הוא עושה זאת על ידי קביעת ארכיטקטורה בעלת יתירות ואימוץ מדיניות של הצפנה רחבת היקף. בנוסף לכך, מבצע המשרד הערכות מצב לגבי הגנת סייבר עבור המדינה באופן כללי וממליץ במסגרת זו על פרקטיקות לשיפורה. כמו כן, הוא מבצע הערכה של מוצרי ההגנה השונים הקיימים בשוק ומאשר את איכותם. כך, למשל, מספטמבר 2015 ועד יוני 2016 אישר המשרד 47 מוצרי הגנה שונים, ש־27 מתוכם נפסלו בהמשך בשל אי־עמידה בתקינה.

בשונה ממדינות אחרות, למשרד הפדרלי לאבטחת מידע יש גם אחריות על העלאת מודעות הציבור הרחב להגנה בסייבר. לשם כך, יש לו אתר אינטרנט ייעודי[129] העוסק בנושאים טכנולוגיים הקשורים להגנה בסייבר: אספקת מידע והמלצות בנושאים "בוערים", כמו, למשל, הצפנת דואר אלקטרוני, אבטחת טלפונים ניידים ועבודה מאובטחת ברשתות חברתיות. דוגמה לפופולריות של האתר ניתן לראות בעובדה שמיולי 2015 ועד יוני 2016 ביקרו בו כ־173,000 מבקרים.

משרד הפנים הגרמני פועל בתחום הגנת הסייבר גם מעבר לפעילותו האינטנסיבית של המשרד הפדרלי לאבטחת מידע. כך, למשל, משרד הפנים יצא ביוזמה לשיתוף מידע בין הגופים השונים בגרמניה (במסגרת Alliance for Cyber Security). היוזמה נשאה פרי והביאה לשיתוף פעולה בין המשרד הפדרלי לאבטחת מידע ובין ההתאחדות הפדרלית לניהול מידע (Bitkom).

---

128 Melissa Hathaway, Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, "Germany Cyber Readiness at a Glance", Potomac Institute for Policy Studies, October 2016, http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf

129 האתר הוא ברובו בשפה הגרמנית: http://www.bsi-fuer-buerger.de

מרכז ה – Alliance for Cybersecurity מאגד בתוכו את כל שחקני המפתח בגרמניה מהמגזרים הפרטי והציבורי, הקים ספריה לביטחון סייבר ועורך אירועי "שולחנות עגולים" בנושא זה. מטרתו היא לתמוך בגופים המוסדיים להגנת הסייבר ולחזק אותם. כל יישות באשר היא – סוכנות, חברה מסחרית, מכון מחקר אקדמי – רשאית להשתתף ולהשתמש במידע של המרכז, בהתאם לרמות הסיווג ולמידת הדחיפות.

תחום פעולה נוסף של משרד הפנים הגרמני הוא פיתוח יכולות טכנולוגיות לצורך מאבק בפשיעה ובטרור. במסגרת זו הקים משרד הפנים את יחידת ZITis, שתפקידה הוא לייצר יכולות טכנולוגיות בנושאי ניטור רשתות תקשורת, חקירת רשתות, שבירת צפנים, עבודה עם ביג דאטה, ונושאי ריגול ופשיעה בסייבר. היחידה מונה כיום כ־120 איש ותקציבה מגיע לעשרה מיליון אירו.

במסגרת משרד הפנים נמצא גם המשרד הפדרלי להגנת החוקה, המרַכז את נושאי מודיעין הפנים בגרמניה. מטרתו העיקרית של המשרד הפדרלי להגנת החוקה הוא לאסוף מידע ולנתח פעילויות שאינן עולות בקנה אחד עם החוקה הגרמנית. הוא אמון על ניתוח מודיעיני של פעילות גורמים לאומניים קיצוניים וזרים בגרמניה, וכן של פעילות ריגול בשטח המדינה. המשרד הפדרלי להגנת החוקה מונה כ־3,000 עובדים ופועל גם במרחב הסייבר, בכלל זה לניטור תכנים אסלאמיים קיצוניים ברשת האינטרנט. בנוסף לכך פועלים במסגרתו צוותים ייעודיים, המתכנסים במקרה של אירוע סייבר הקשור בגורמים קיצוניים או בגורמי טרור. המשרד הפדרלי להגנת החוקה גם החל להפעיל לאחרונה קמפיינים של השפעה במרחב הסייבר ולקיים פיקוח על מקורות חדשותיים.

משרד הפנים הגרמני כולל בתוכו גם את המשרד הפדרלי להתגוננות אזרחית ולסיוע במצבי אסון, המהווה את זרוע הביצוע שלו בעניינים הקשורים להגנה אזרחית ולהתמודדות עם אסונות. משרד זה הוקם בשנת 2004 בעקבות אירועי 11 בספטמבר 2001 בארצות הברית ושטפונות שפקדו את גרמניה ב־2002. עיסוקו בענייני סייבר נעשה דרך פעילותו סביב תשתיות קריטיות וכולל פיתוח הנחיות עבודה ותרגילים בנושא.

תחת משרד הפנים נמצאת גם סוכנות המשטרה הפדרלית לפשיעה, המובילה את מאמצי הלחימה של גרמניה בפשיעת סייבר. קיימים חוקים שונים העוסקים בהרתעה ובהטלת סנקציות על פשיעת סייבר בגרמניה, הכוללת, בין היתר, הונאות מחשב, גניבת מידע, גרימת נזק, ריגול עיסקי, ניסיונות דיוג ועוד. סוכנות המשטרה הפדרלית החלה לעסוק בנושאי סייבר כבר בשנת 1998, ובכלל זה בחיפושים ברשת האינטרנט אחר תכנים לא חוקיים. היא משתפת פעולה עם הרשויות השונות ברמה המקומית, עורכת מחקרים בנושאי פשיעת סייבר ומתמודדת עם מצבים של דיווחים חסרים על פשיעות סייבר שחווים אזרחים.

גורמים מדינתיים נוספים

לצד התשתית המוסדית הקיימת במשרד הפנים הגרמני, המהווה, כאמור, את עיקר הפעילות להגנת הסייבר במדינה, קיימים גופים נוספים המעורבים בתחום זה, שראוי להתעכב על פעילותם. הנציבות הלאומית להגנה בסייבר הוקמה כחלק מהאסטרטגיה הלאומית של 2011 ונועדה לאפשר עיסוק חוצה זירות בנושאי הגנת הסייבר. משרדי הפנים, ההגנה, המסחר, הטכנולוגיה, המשפטים, החינוך והכלכלה פועלים במסגרת זו יחד עם התעשייה והאקדמיה במטרה לגבש גישות משותפות להגנת הסייבר. תפקיד הנציבות הוא להמליץ על שינויים באסטרטגיה בעת הצורך, על קידום חקיקה בתחום הסייבר, וכן לקדם מחקר וסיוע בסוגיות הגנת הסייבר, בשיתוף פעולה עם גורמים בין־לאומיים.

שחקן חשוב נוסף בהגנת הסייבר בגרמניה הוא הצבא הגרמני, שהגנת סייבר מהווה חלק מתפיסת התפקיד שלו. על פי מסמך האסטרטגיה מ־2011, הצבא הגרמני היה אמור להגן בעיקר על עצמו, אך על פי האסטרטגיה מ־2016 נועד לו תפקיד בהגנת הסייבר בכל מוסדות המדינה. מסמך האסטרטגיה האחרון חידד את התפקיד הכפול של הצבא: התגוננות מפני איומי סייבר בכל מה שנוגע לנכסיו שלו, במקביל לניצול מרחב הסייבר לקידום מטרותיו. משרד ההגנה הגרמני גם נתן במסמך אסטרטגי זה ביטוי לרצונו לאפשר לצבא יכולות לתקיפה חוזרת (hack-back) במקרה שהוא מותקף.

סוכנות חשובה נוספת העוסקת בהגנת הסייבר בגרמניה היא שירות המודיעין הפדרלי, שהוקם אחרי מלחמת העולם השנייה ועוסק באיסוף מודיעין חוץ. ל־BND יש יכולות טכנולוגיות לאיסוף וניטור מידע מחוץ לגבולות גרמניה, בנוסף לעיסוקו בגילוי ריגול ובתקיפות סייבר נגד גרמניה ותשתיות קריטיות במדינה. במסגרת זו מפעיל שירות המודיעין הפדרלי מערכת סיגינט כסיוע להתגוננות נגד איומי סייבר ובכלל זה מערכות להתרעה על איומים כאלה על בסיס המידע שהוא עצמו אוסף.

בנוסף לפעילות השוטפת של המשרדים השונים בתחום הגנת הסייבר, ישנן בגרמניה גם יוזמות ספציפיות בתחום זה המקודמות באמצעות שרים או הממשלה באופן כללי. ניתן לחלק יוזמות אלו לשתי קטגוריות עיקריות: יוזמות לחיזוק הריבונות הגרמנית במרחב הסייבר ויוזמות לעידוד ופיתוח החינוך והעלאת המודעות בקרב הציבור לאיומי הסייבר ולצורך להתגונן מפניהם.

היוזמות לחיזוק הריבונות הגרמנית במרחב הסייבר מוצאות ביטוי באסטרטגיית הסייבר הגרמנית משנת 2011. במסגרת זו בולטת ההשקעה של המדינה בחדשנות ובמחקר בתחום הסייבר מתוך כוונה לחזק את יכולותיה של גרמניה לשלוט על הנעשה בשטחה בתחום זה. מסמך האסטרטגיה מ־2016 מקדם מוצרים שיוצרו בגרמניה כדי לחזק את הכלכלה הגרמנית, וזאת באמצעות עידוד הגנת סייבר של חברות.

הגברת מודעות הציבור לאיומי הסייבר מוצאת גם ביטוי באסטרטגיה של 2011, שם מודגשת הכוונה לספק תמריצים ליצירת מנגנונים לרישוי מוצרים מאובטחים לשימוש הציבור. ב־2015 יצאה ממשלת הגרמניה בתוכנית לקידום מחקר ופיתוח בתחום הגנת הסייבר והקצתה לכך סכום של כמאתיים מיליון דולר עד שנת 2020. זאת ועוד, מסמך האסטרטגיה של שנת 2016 נותן ביטוי לכוונת הממשלה לקדם שימוש במוצרי הצפנה מקומיים כסטנדרט הרצוי. המטרה במקרה זה הייתה לקדם את התעשייה הגרמנית בנושא ולהפוך את השימוש במוצרי אבטחה ברמה גבוהה לנחלת כלל הציבור. האסטרטגיה מ־2016 גם מבקשת לכלול "חינוך דיגיטלי" בכל רמות מערכת החינוך הגרמנית, תוך שיתוף פעולה בין הממשלה לאוניברסיטאות השונות. בפועל, שיתוף פעולה זה הוביל להקמתם של שלושה מרכזי מחקר גרמניים בנושאי הגנת סייבר, שמטרתם היא לגשר על המחסור הקיים במומחי הגנת סייבר גרמנים שישרתו את התעשייה והמדינה. תוכניות המחקר והפיתוח מסייעות, בין השאר, לשופטים ואנשי אכיפת החוק להתמקצע בעולם תוכן חדש הנדרש לפעילותם.

משרד החינוך והמחקר הגרמני מוביל גם פרויקט לדיגיטליזציה של התעשייה. הפרויקט עוסק ברובו בהגנת סייבר במגזר התעשייתי־יצרני וכולל התאגדות של 14 חברות שונות ושבעה מכוני מחקר לפיתוח פתרונות הגנת סייבר עבור התעשייה. תוכנית זאת מסייעת לבעלי עסקים קטנים ובינוניים לפתח ולהשתמש בפתרונות שאין ביכולתם לממן מתקציבם.

כאמור, גרמניה גם נשענת ועושה שימוש נרחב ביוזמות ובשיתופי פעולה ברמה הבין־לאומית, הן במסגרת האיחוד האירופי והן בזירה הגלובלית שמחוץ לאיחוד. שיתופי הפעולה הללו כוללים את האו"ם, נאט"ו, מדינות ה – G-7 והנציבות האירופית. האסטרטגיה הגרמנית משנת 2016 נותנת ביטוי למגמה זו כשהיא מדגישה את החשיבות שבמיצוב גרמניה ככוח עולה בתחום הגנת הסייבר הן במסגרת האיחוד האירופי והן ברמה הבין־לאומית. למעשה, עוד ב־2011 מינה שר החוץ הגרמני דאז צוות לתיאום וסנכרון הפעילות בתחום הסייבר ברמה הבין־לאומית, מתוך ראייתו כמרכיב חשוב במדיניות החוץ של גרמניה.

פרטיות והגנת המידע

תפיסת הפרטיות הגרמנית הינה תפיסה מורחבת, אשר שמה במרכז את זכויות האזרח. ככזו, יש לה תפקיד מרכזי באסדרת הגנת הסייבר ובאבטחת המידע במדינה. היא נשענת על התפיסה החוקתית כי כל אזרח חופשי לפתח את אישיותו ורצונותיו ולהגדיר בעצמו את השימוש במידע אישי על אודותיו ואת הפצתו. על פי החוק הגרמני, מידע אישי הוא כל מידע המכיל פרטים אישיים על היחיד ברמות שונות. המידע האישי מחולק לשלוש רמות של רגישות:

1. רמה פנימית/אישית – מידע על אישיותו של האדם, שחייב להישאר חסוי בכל מחיר.
2. רמה פרטית – העוסקת בנתונים אישיים של אדם, שעבורם צריך לבקש את רשותו.
3. רמה אינדיבידואלית – האדם כאזרח בקולקטיב גדול, שיש עליו מידע אישי פומבי שאותו ניתן לאסוף.

נציבות הגנת המידע הגרמנית נוסדה בחוק הפדרלי להגנת המידע משנת 1977, אשר עודכן מספר פעמים מאז. בשנת 1990 עודכן חוק הגנת המידע בהתאם לפיתוחים הטכנולוגיים של אותה תקופה. החוק עודכן שוב בשנת 2001 במטרה לעמוד בהנחיית הגנת המידע האירופית מ־1995 וכדי לעמוד בתקן אירופי אחוד להגנה על מידע אישי.

ב־2005 נחקק בגרמניה חוק חופש המידע, העוסק בחובותיה של נציבות הגנת המידע לאפשר גישה למידע ציבורי. החוק עודכן בשנת 2009 כדי לאפשר שקיפות ושליטה על מושאי המידע ושימוש במידע על אודותיהם לצורכי פרסום. החקיקה בנושאי פרטיות בגרמניה כוללת חוקים נוספים, העוסקים בשאלת הפרטיות בתחומים מוגדרים, למשל מידע תקשורתי או פעילות של גופי הביטחון.

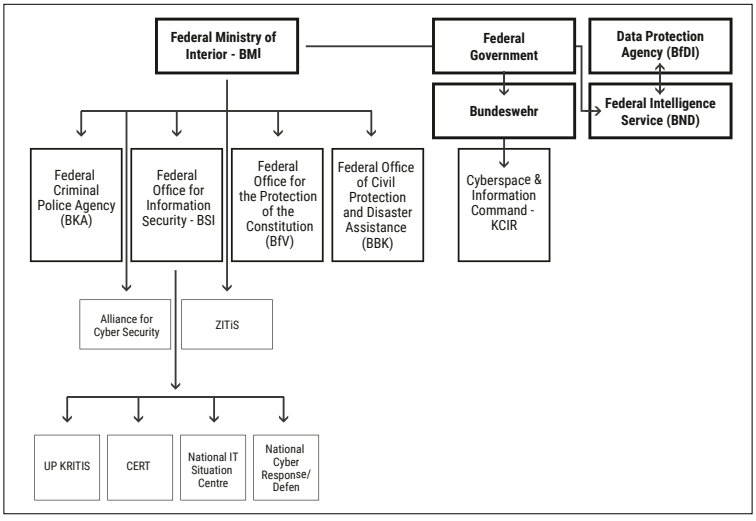
נציבות הגנת המידע הפכה בשנת 2016 לסוכנות עצמאית שאינה כפופה לגופים אחרים. חיזוק עצמאותה בא בעקבות חקיקה מ־2014 בנושא הגנת הפרטיות, שהושפעה מחשיפות המידע של אדוארד סנודן ומהשערוריות שנחשפו בארצות הברית סביב שאלת הזכות לפרטיות. כיום כפופה נציבות הגנת המידע רק לפרלמנט ולבתי המשפט בגרמניה ומעמדה עולה בקנה אחד עם הדרישות האירופיות להגנת מידע, המורות על אי־תלות מוחלטת בכל גוף של הרשות המבצעת במדינת הלאום. הנציבות משרתת גופים ציבוריים וכן גופים פרטיים בגרמניה, כגון ספקי תקשורת ושירותי דואר. בנוסף, היא מהווה כתובת לאזרחים להגשת תלונות על הפרות פרטיות מצד גופים פרטיים וציבוריים. היא גם עוסקת בגישה של אזרחים למידע ציבורי ומעודדת שקיפות שלטונית. מבחינת כוח האכיפה, נציבות הגנת המידע אינה יכול להטיל קנסות ונשענת בנושא זה על סוכנויות הגנת המידע ברמת המדינות בגרמניה (שהטילו כבר בעבר קנס בגובה של 1.1 מיליון אירו על חברת רכבות).

חשיפותיו של המדליף אדוארד סנודן היכו גלים בגרמניה וגררו ביקורת פומבית חסרת תקדים מצידם של חברי פרלמנט וקבינט גרמנים כלפי ארצות הברית. הקנצלרית מרקל אף הגדילה לעשות והביאה, יחד עם נשיאת ברזיל דאז, לקבלת החלטה בעצרת הכללית של האו"ם ב־2013 (החלטה 68/167) השוללת מעקב ואיסוף מידע באופן לא חוקי, כפי שנחשף על ידי סנודן, וקובעת שהדבר נוגד ערכים של מדינה דמוקרטית.

חשיפותיו של סנודן גם הובילו לבדק בית בשירותי המודיעין הגרמניים ולרפורמה בהם, לאחר שהתברר כי הם פועלים ללא תשתית חוקתית ברורה וללא פיקוח מתאים.[130]

ב־2016, אחרי שנה של משא ומתן עם חברי הפרלמנט, הציעה ממשלת גרמניה תשתית חוקתית חדשה לאיסוף מודיעין זר. במסגרת הרפורמה, נדרשים אישורים לפני איסוף מודיעין ובקרות לאחר האיסוף, וניתן לערער על חוקיות האיסוף במקרה הצורך. בנוסף, הרפורמה אמורה להגביר את רמת השקיפות של שיתופי הפעולה המודיעיניים בין מדינות המערב, שהיו גורם מרכזי בהפרות הפרטיות על ידי מדינות שונות. הרפורמה החדשה מטילה הגבלות על איסוף מידע על ידי סוכנויות המודיעין הגרמניות, ועושה זאת תוך הבחנה בין אזרחים גרמנים לאזרחי האיחוד האירופי ובינם לבין אזרחי יתר מדינות העולם. יתרונות הרפורמה הם בהקמת תשתית חוקתית ברורה ומוצהרת לפעילות המודיעין הגרמני. יחד עם זאת, מבקרי הרפורמה טוענים כי פרוצדורות נוספות יוצרת קושי בפיקוח על ענייני המודיעין בגרמניה, ואינן מטילות מגבלות על איסוף של מטא־נתונים.

תרשים 5 סוקר את ההיררכיה והקשרים בין סוכנויות המדינה השונות בגרמניה העוסקות בהגנת סייבר, כפי שנסקרו לעיל:



תרשים 5: הסוכנויות והמוסדות העוסקים בנושא הגנת הסייבר בגרמניה

130 Thorsten Wetzlin, "Germany Intelligence Reform: More Surveillance, Modest Restrains and Inefficient Controls: Policy Brief", Stiftung Neue Verantwortung, June 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf

ישראל

אסְדרת הגנת הסייבר במדינת ישראל נפרסת על פני שני עשורים, החל מ־1998, כשנקבעו דרישות מחייבות לגופים ציבוריים, ועד איחוד מטה הסייבר ומערך הסייבר הלאומי למערך הסייבר תחת משרד ראש הממשלה בסוף 2017. הגישה הישראלית בכל הנוגע למתן הנחיות מחייבות למגזר העיסקי בתחום הגנת הסייבר היא מעֵין ייצור כלאיים בין הגישה האמריקאית לגישה האירופית. מצד אחד, רוב המגזר הפרטי בישראל אינו נתון תחת רגולציה מחייבת כלשהי, והמדינה, כמו ארצות הברית ומדינות רבות באירופה, מסתמכת על כוחות השוק ועל יצירת שיתופי פעולה כדי למצוא את האיזון הנכון בין הגנה ראויה להשקעה הכלכלית הכרוכה בכך. מצד שני, הגישה של התערבות מדינתית באה לידי ביטוי ברגולציה המושתת על חברות פרטיות במגזרים מסויימים, כגון בנקים, שוק ההון, תחום האנרגיה ומוסדות בריאות, שמדינת ישראל מעניקה להם חשיבות אסטרטגית, אף שלא כולם עונים להגדרה של "תשתיות קריטיות". עם השנים עברה ישראל מרגולציה נקודתית על גופים קריטיים לביטחון המדינה לרגולציה שהייתה ברובה מגזרית, בה כל משרד ביצע פיקוח על פי דרישותיו. בהמשך התפתחה רגולציה מרכזית תחת גוף מרכזי אחד שהוסמך לתת הנחיות להגנת הסייבר, גיבש מתודולוגיה ושפה משותפות בתחום זה והקים יחידות ייעודיות שהורכבו מאנשי מערך ההגנה בכל משרד ממשלתי ונועדו להנחיל תפיסה אחידה להגנת הסייבר.[131]

ההתערבות המדינתית בהגנת הסייבר במגזר הפרטי בישראל מתבטאת בשני אופנים עיקריים. ראשית, תשתיות המוגדרות כקריטיות, כגון מים, חשמל ותחבורה, נתונות להנחייה מדינתית מקיפה ומחייבת על ידי שירות הביטחון הכללי ומערך הסייבר הלאומי. הנחייה זאת נעשית בהתבסס על סמכויות הרגולציה והאכיפה של כל רשות או משרד ממשלתי בתחום שיפוטו. כך, למשל, משרד האנרגיה מפקח באמצעות חברה פרטית על תשתיות מים וחשמל הנמצאות בבעלות פרטית. דוגמה נוספת היא משרד הבריאות המפקח על בתי חולים, או הרשות לניירות ערך המפקחת על המערכות המרכזיות למסחר פיננסי. צורת ההתערבות המדינתית השנייה היא בתשתיות שאינן מוגדרות כקריטיות. אלו נתונות להנחיית המדינה דרך רגולטורים מגזריים, המפקחים על הנמצא תחת אחריותם.

ברקע של שני אופני ההתערבות הללו ניצב חוק הגנת הפרטיות, הכולל בתוכו היבטים של הגנת מידע, ומוחל על כל המגזרים שבהם מוחזקים מאגרי מידע אישיים המכילים יותר מ־10,000 רשומות. ב־2017 עודכנו, לראשונה מאז 1981, תקנות אבטחת

131 נכון לאפריל 2018, כבר הוקמו יחידות ייעודיות ב־15 מתוך 18 משרדי ממשלה, שבהן מוצבים אנשי מערך הסייבר, המופקדים על פיקוח והתמודדות עם האתגרים המגזריים של כל משרד.

המידע הנובעות מחוק זה, והן מהוות את התשתית החוקתית המתקדמת להגנת המידע והפרטיות במרחב הסייבר.

תהליך התגבשותה של הרגולציה במרחב הסייבר בישראל החל בסוף שנות התשעים של המאה העשרים יחד עם יוזמת "ממשל זמין" שהובילה לכינונה ב־1997 של "תהילה" – הגוף שנועד לספק למשרדי הממשלה ולרשויות השונות מענה מאובטח להתחברות לאינטרנט, לפעילות מקוונת בין־משרדית ולפעילות מקוונת אל מול האזרחים.[132] יחד עם זאת, ועל אף הניסיונות לספק מענה אחוד למשרדי הממשלה, הוסיפו אלה לפעול באופן עצמאי, ללא גורם מקצועי שינחה אותם.[133]

המשך תהליך התגבשותה של רגולציית הסייבר בישראל כולל שני שלבים עיקריים, שגם הם נעשו ללא תפיסה אסטרטגית לאומית החלה על כלל המגזרים במשק.[134] ראשיתה של רגולציה להגנת סייבר בישראל מול המגזר הפרטי היא בחוק להסדרת הביטחון בגופים ציבוריים (1998), שפירט את הדרישות להגנה על מערכות המידע של גופים שהוגדרו כ"חיוניים" למדינה, כלומר, גופים שפגיעה בהם תסב נזק למדינה (למשל, לתל"ג). גופים אלה כללו את מגזרי התעופה, תשתיות המים, החשמל והתקשורת. ב־2002 נקבע כי המנחה המקצועי שלהם תהיה הרשות הלאומית לאבטחת מידע (רא"ם), הכפופה לשירות הביטחון הכללי. ראוי לציין כי הגופים המונחים הינם פרטיים וציבוריים כאחד (בתי הזיקוק, חברת אל־על, חברת החשמל, רכבת ישראל וכדומה). כמו כן נקבע כי גופים חיוניים נוספים ייבחרו בקפידה על ידי ועדת היגוי ייעודית. עם השנים הלכה רשימת הגופים החיוניים והתרחבה. גופים רבים, שלא הוגדרו כבעלי פוטנציאל נזק גבוה, נותרו ללא הנחייה והגנתם נגזרה בעיקר משיקולים כלכליים של כוחות השוק.

ב־2011 נכנסה ישראל לשלב ב' בפיתוח הרגולציה במרחב הסייבר, כאשר הממשלה שינתה את גישתה והחלה לתת את הדעת לצורך לפעול גם מול המגזר האזרחי, תוך העברת סמכויות מסוכנויות המודיעין אל מערך הסייבר שהוקם לראשונה במשרד ראש הממשלה. ההחלטה לעדכן את האופן בו המדינה פועלת במרחב הסייבר לא נבעה מאירוע מכונן או ממשבר שהצריך חשיבה מחודשת, אלא מתובנה כי ההסדרים הקיימים אינם מתאימים להתמודדות עם אתגרי הסייבר המתעדכנים.[135]

---

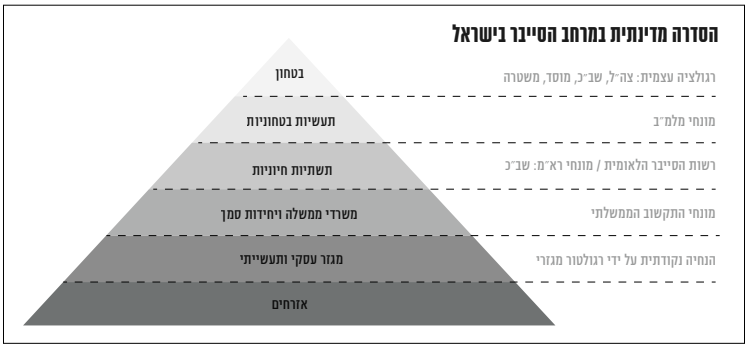
132 Deborah Housen-Couriel, "Israel", NATO CCD COE Series Reports on National Organizational Models for Cyber Security, 2017.

133 Dmitry (Dima) Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy", *The Washington Quarterly*, Vol. 40, No. 2, 2017, pp. 113-27.

134 סיבוני ואסף, **קווים מנחים לאסטרטגיה לאומית במרחב הסייבר**, עמ' 22.

135 Dmitry (Dima) Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy".

צוות משימה, שכלל מומחים מהמגזרים השונים, המליץ על הקמת מטה הסייבר הלאומי במסגרת משרד ראש הממשלה. הקמת המטה נעשתה מתוך רצון ליצור אינטגרציה מוצלחת יותר עם חברות במשק ולאמץ תפיסה הוליסטית רחבה לעיסוק במרחב הסייבר בישראל. ב־2015 החליטה הממשלה (בהחלטה מספר 2444)[136] על הקמת הרשות הלאומית להגנת הסייבר כיחידת סמך במשרד ראש הממשלה, שייעודה הוא הגנת מרחב הסייבר האזרחי. תפקיד הרשות הוא להגן על נכסים קריטיים במטרה לשמור על רציפות תפקודית של תשתיות המדינה הקריטיות, והיא פועלת כגוף מנחה מול כלל המשק באמצעות הרגולטורים השונים.[137] בתחילת 2018 אוחדה הרשות הלאומית להגנת הסייבר עם מטה הסייבר הלאומי והוקם מערך הסייבר הלאומי.



תרשים 6: תחומי אחריות בפיקוח על הגנת הסייבר בישראל, 2018

בראש הפירמידה נמצאים גופים הנתונים לפיקוח עצמי. אלה הם בעיקר גופי ביטחון רגישים, כגון השב"כ, המוסד וצה"ל, המגנים על עצמם ואינם מחוייבים בדיווח או בפיקוח חיצוני על אופן התנהלותם. אין תקינת אבטחת מידע מחייבת על פיה גופים רגישים אלה צריכים לפעול.

ברמה הבאה נמצאים מתקנים רגישים והתעשיות הביטחונית, דוגמת התעשייה האווירית, רפא"ל ואחרים, הנתונים לפיקוח של הממונה על הביטחון במשרד הביטחון (המלמ"ב). ההנחיות הניתנות על ידי המלמ"ב מיועדות לשמירת הסודיות וכן למניעת פגיעה בביטחון הלאומי כתוצאה מפגיעה קיברנטית בגופים רגישים אלה.

בהמשך הפירמידה נמצאות התשתיות שהוגדרו כחיוניות וקריטיות על ידי ועדת ההיגוי. אלו נתונות, כאמור, לפיקוח מקיף הן על ידי מערך הסייבר הלאומי (מרבית

136 לנוסח ההחלטה המלא ראו: "קידום ההערכות הלאומית להגנת הסייבר", משרד ראש הממשלה, http://www.pmo.gov.il/Secretary/GovDecisions/2015/Pages/des2444.aspx

137 "סיכום שנות הקמת הרשות הלאומית להגנת הסייבר, 2016–2017", מערך הסייבר הלאומי, 31 בדצמבר 2017.

המגזרים)[138] והן על ידי שירות הביטחון הכללי (תשתיות תקשורת). התשתיות החיוניות כוללות, כאמור, את הגז, האנרגיה, החשמל, המים, התחבורה, הבריאות, תשתיות תקשורת, שדות תעופה, המוסד לביטוח לאומי ועוד, שפגיעה בהם עלולה לפגוע משמעותית במהלך החיים התקין במדינת ישראל ולהסב נזק לביטחון הלאומי.

ועדת החוץ והביטחון של הכנסת קבעה ב־2016 כי מערך הסייבר הלאומי צריך להיות הגורם האחראי על הגנת הסייבר בישראל וכי תפקידו הוא לחזק את החוסן המדינתי, להכווין את צורכי ההגנה הרלוונטיים בסייבר ולהתמודד עם אירועי תקיפת סייבר על יעדים ישראליים.[139] הוועדה הכירה בכך שהקמת מערך הסייבר הלאומי תפגע באחריותו ובסמכויותיו של השב"כ בנושא זה וקראה, לפיכך, לשיתוף פעולה בין הגוף שעיסוקו הבלעדי הוא הגנת סייבר, הלוקח בחשבון שיקולים אזרחיים־מדינתיים, לבין גופי הביטחון בעלי מומחיות בהיבטים הביטחוניים והמודיעיניים במרחב זה. על פי הוועדה, הרשות להגנת הסייבר אינה צריכה להפוך לגוף מודיעין נוסף, אלא להתבסס על יכולות האיסוף של גופי המודיעין הקיימים. החשיבות שבהסדרת האחריות בין הגופים השונים העוסקים בסייבר באה לידי ביטוי גם בדוח השנתי של מבקר המדינה מ־2016, המעיד על קיומם של פערים בין החלטות הממשלה על הקמת מערך הסייבר הלאומי ובין מימושן בפועל.

ברמה הבאה בתרשים נמצאים משרדי הממשלה, המונחים על ידי מערך התקשוב הממשלתי, שתפקידו הוא לדאוג להגנת הסייבר של כל משרד, כולל יחידות הסמך שלו. מערך התקשוב הוא למעשה התפתחות של הגוף הראשוני – "תהילה" – שהוקם כאמור ב־1997 כחלק מבניית מערך "ממשל זמין" של משרדי הממשלה.

ברמה הבאה בפירמידה נמצא המגזר העיסקי, שברובו אינו נתון לרגולציה, מלבד פיקוח נקודתי על הבנקים, שוק ההון, ניירות ערך, מפעלי אנרגיה ומוסדות בריאות המונחים על ידי הרגולטור המגזרי. רובו ככולו של המגזר העיסקי־אזרחי אינו נתון להנחייה מדינתית, לוקה בשיתוף ידע ועוסק בצמצום נזקים בלבד מול הלקוחות, תוך דיווח להם על אירועי סייבר כראות עיניו.

ראוי להתעכב על פעילותם של הרגולטורים המגזריים, החורגת מתחומי אחריותם של משרדי הממשלה השונים וזולגת, כאמור, במספר מקומות למגזר העיסקי. שתי דוגמאות כאלו הן בנק ישראל והאגף לשוק ההון באוצר. במארס 2015 הפיץ בנק

138 ביולי 2017 הושלם מהלך של העברת הסמכויות מהרשות הלאומית להגנת הסייבר לשב"כ לגבי 26 גופי תשתיות קריטיות במדינה.

139 ועדת החוץ והביטחון, "דין וחשבון בנושא בחינת חלוקת האחריות והסמכות בנושא הגנת הסייבר בישראל", הכנסת, אוגוסט 2016.

ישראל הוראה מספר 361 – "ניהול הגנת הסייבר" בקרב הבנקים.[140] הוראה זו כוללת הנחיות לבניית תוכנית ניהול סיכוני סייבר בכל בנק, כאשר בנק ישראל משאיר לרוב את ההחלטה על שיטת הביצוע בידי הבנקים עצמם. מרכיב חשוב בהוראה הוא ההתבססות על קצין אבטחת מידע ייעודי להגנת הסייבר של הבנק המפוקח, הנושא באחריות מול בנק ישראל. המפקח על הבנקים קובע בהוראה כי השינויים הטכנולוגיים והקישוריות של מערכות המידע יוצרים קרקע פוריה לסיכוני סייבר משמעותיים עבור הבנקים. סיכונים אלה כוללים: שיבוש פעילות תקינה ומאובטחת, מניעת שירות מלקוחות הבנקים, חשיפת מידע פרטי, מחיקה ושיבוש של נתונים, ירידה באמון הציבור, פגיעה בתדמית התאגיד הבנקאי ופגיעה ביכולת לנהל נכסים ולקוחות. ההוראה מפרטת את בעלי התפקידים השונים ואת האופן בו עליהם לתרום לקידום הגנת הסייבר בבנקים: דירקטוריון הבנק אמון על התוויית האסטרטגיה ואישור המסגרת לניהול סיכוני סייבר, תוך קביעת אופן הפיקוח וקבלת דיווחים על אירועי סייבר משמעותיים. תפקיד ההנהלה הבכירה הוא לגבש את מדיניות הגנת הסייבר של הבנק וליישמה, להקצות את המשאבים הנאותים ולקבל תמונת מצב עיתית על הנעשה בתחום זה. כמו כן, ימונה "מנָהל הגנת סייבר" ייעודי, שתפקידו להשפיע על האופן בו הבנק נחשף לסיכוני סייבר, לגבש מתודולוגיה ולתכלל את מאמצי הבנק בתחום הגנת הסייבר, תוך שיתוף פעולה עם כל הגופים הרלוונטיים בארגון, כולל ייזום תרגילים למוכנות סייבר.

ההוראה של בנק ישראל דורשת מכל בנק לגבש תוכנית עבודה רב־שנתית להתמודדות עם איומי סייבר, שתתבסס על האסטרטגיה שלו ועל ניתוח סיכונים וחשיפות לאיומי סייבר ותתעדף יישום בקרות לצמצום סיכוני הסייבר של הבנק. הערכת סיכוני הסייבר תבוצע על ידי כל בנק אחת לשנה לכל הפחות, ותכלול מיפוי תהליכים עיסקיים ושימוש במדדים לצורך כימות החשיפה לסיכונים. תהליך זה יבוצע באופן השוואתי שיאפשר יצירת תעדוף, ויתועד ויאושר על ידי ההנהלה הבכירה.

הוראת בנק ישראל גם מפרטת כיצד ליצור מערך בקרות אפקטיבי להפחתת סיכוני סייבר, וזאת על ידי שימוש בטכנולוגיות, בתהליכים, בנהלים ובאנשי מקצוע חוצי ארגון. לשם כך תיבחן כל שרשרת האספקה של הבנק, הכוללת ספקים, תאגידים קשורים, לקוחות, ספקי תקשורת ותשתיות מחשוב, מיקור חוץ, ספקי שירותים וגורמים בחו"ל. כל גורם שזוהה כרלוונטי יעבור "בדיקת נאותות וניטור" כדי לוודא שהוא לא מחולל סיכון סייבר עבור הבנק. בנוסף, הבנקים יבצעו מחקר איומים עצמאי, תוך שיתוף מידע וניתוח תרחישים אשר יסייעו לחיזוק מערך הגנת הסייבר והסביבה התפעולית

140 ניהול בנקאי תקין, "הוראה 361 – ניהול הגנת סייבר", המפקח על הבנקים, מארס 2015, https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf

כנגד מתקפה פוטנציאלית. זאת, במקביל לניתוח תמונת מצב עדכנית של חוזק אבטחת הבנק על סמך הסביבה הפנימית והחיצונית שלו.

בקרות הסייבר בכל בנק אמורות לסייע למהלכי תגובה ראויים לאירועים, להסטה ולעיכוב של תוקפים פוטנציאליים, ליכולות עמידות ושיקום הפעילות העיסקית, ליכולת תחקור לאחור, לצמצום החשיפה לאיומים על ידי הקשחת מערכות וצמצום הרשאות, ליישום אבטחה רב־שכבתית בנקודות שונות בארגון, ולניהול תהליכי סייבר רלוונטיים לניטור זהויות, נכסים ושרשרת האספקה.

על פי ההוראה, הבנקים אמורים להגדיר את הנדרש מהגורם האנושי, ועיסוקם בהיבטי מיון, גיוס וקליטת כוח אדם צריך להיעשות תוך הגברת המודעות לנושא הסייבר. איוש מערכי הניטור והבקרה שהוקמו יהיה רציף, ויעשה שימוש בזיהוי אנומליות, תוך שילוב עם מערכות אחרות. דיווח על אירועי סייבר יבוצע באופן פנימי ללא חשיפה לציבור. הערכת הבקרות על הגנת הסייבר בבנק תיעשה בשילוב עם מנגנוני הערכה קיימים, סקרי פגיעויות ומבדקי חדירה מבוקרים. דוחות סיכוני הסייבר של הבנק יכללו מצב עדכני ומנומק של מדדי הסיכון, פירוט של נזקים משמעותיים ואירועים חיצוניים רלוונטיים העלולים להשפיע על הבנק בתחום הסייבר.

דוגמה נוספת לפיקוח נקודתי במגזר הפרטי ניתן לראות בחוזר לניהול סיכוני סייבר של האגף לשוק ההון במשרד האוצר מאוגוסט 2016. כמו הפיקוח על הבנקים, גם אגף הפיקוח על שוק ההון הגיע למסקנה כי האיומים הטכנולוגיים המתעצמים עלולים לשבש את פעילותם התקינה של הגופים המפוקחים. על כן, האגף החליט לקבוע עקרונות להגנה ולשמירה על סודיות, שלמות וזמינות המידע, תוך אבטחת מערכות מידע והתהליכים העיסקיים.[141] הציפיה היא שכל גוף מוסדי בשוק ההון הישראלי יאמץ את התקנים המובאים בחוזר האגף לשוק ההון. החוזר גם מפרט את תפקידם של הדירקטוריון, המנכ"ל, ועדת היגוי שתוקם ומנהל הגנת סייבר ייעודי בארגון. בנוסף לתהליך ניהול סיכונים מפורט, מתאר החוזר בפירוט רב את אמצעי הגנת הסייבר שכל ארגון מפוקח צריך לאמץ. מדובר באיסוף מודיעין, בניטור ובקרת מידע, במוכנות לאירועים, בביצוע סקרים ומבחני חדירות, באבטחת מערכות תקשורת ותפעול (כולל בתהליכי רכש ופיתוח של מערכות חדשות), בניהול משתמשים והרשאות, במיקור חוץ, באבטחה פיזית, בתהליכי גיוס עובדים ובאבטחת ערוצי התקשרות עם גורמים פנימיים וחיצוניים.

גורם נוסף הנמצא בבעלות פרטית ונתון להנחייה נקודתית הם מפעלי תשתיות חשמל ואנרגיה פרטיים. משרד האנרגיה והתשתיות הלאומיות מבצע פיקוח על הגנת הסייבר של מפעילי תשתיות פרטיים באמצעות מנהל הביטחון למגזר העיסקי באגף

141 דורית סלינגר, משרד האוצר – אגף שוק ההון, ביטוח וחיסכון, אוגוסט 2016.

הביטחון במשרד, האחראי על הרציפות התפקודית, ומתוקף כך גם על אבטחת המידע והאבטחה הפיזית של התשתיות השונות. ההנחייה מבוצעת באופן הבא: על כל יזם הפועל בתחום האנרגיה ומפיק חשמל מעל כמות מסויימת לקבל רשיון ממשרד האנרגיה. קבלת הרשיון מותנית במילוי הנחיות המשרד השונות בתהליך שאורך בדרך כלל מספר שנים. המשרד מנחה את היזמים הפרטיים באמצעות מיקור חוץ, שתפקידו לדאוג שיבוצע סקר סיכונים ראוי וימונו יועצי אבטחת מידע, שיבטיחו את הרציפות התפקודית של כל יזם תשתיתי.

התשתיות האופרטיביות של כל יזם נמצאות תחת פיקוח משרד האנרגיה, והחיבורים לחברת החשמל מפוקחים על ידי הגורם המפקח על חברת החשמל בתוקף היותה תשתית קריטית מדינתית – במקרה זה השב"כ או מערך הסייבר הלאומי. העלויות המושתות על כל יזם פרטי אינן מבוטלות, אך הגורם המנחה פועל מול ספקי האבטחה השונים להוזלתן וגם אינו גובה דמי שירות בעבור הייעוץ הניתן, שכן הוא נעשה ביוזמת המדינה. כך מתמרצת המדינה את היזמים הפרטיים בתחום החשמל להתגונן באופן ראוי. המדינה גם הקימה מרכז לניהול אירועי סייבר עבור המגזר הייחודי של משק האנרגיה הפרטי, ומצליחה לגרום לחברות מתחרות לשתף ביניהן מידע על אירועי סייבר.

בנוסף לפיקוח הסלקטיבי על המגזרים השונים, מדינת ישראל פרסמה שש הנחיות ויוזמות רגולטוריות משמעותיות הנוגעות למגזר העיסקי־אזרחי. ההנחייה הראשונה, שמטרתה להגביר את הפיקוח שכבר מבוצע על ידי האגף לפיקוח על ייצוא ביטחוני במשרד הביטחון, עסקה בהגדלת מספר המוצרים שיהיו תחת פיקוח מדינתי[142] מתוך רצון לפקח על מירוץ החימוש בסייבר ולשמור על היתרון היחסי של מדינת ישראל בתחום זה.

לאחר תהליך היוועצות ארוך עם תעשיות הסייבר השונות, החליטה המדינה לסגת מפיקוח הדוק ולהמשיך להיצמד להסדרי פיקוח בין־לאומיים בלבד. הסיבה לכך נעוצה בהתנגדות התעשייה, שחששה כי לא תוכל להתחרות בתעשיות ממדינות שאינן מפוקחות.[143] הרצון לשמור על מעמדה של ישראל כיצואנית סייבר מובילה ביחס לגודל האוכלוסייה[144] הוביל, בין היתר, לשמירת הסטטוס קוו בנושא הפיקוח. הדבר מצביע על עומק ההבנה ההדדית ושיתוף הפעולה הנרחב בין התעשיות השונות

142 ההרחבה כוללת בעיקר מוצרי חדירה, ניתוח פריצות וידע על קיומן של חולשות חומרה/תוכנה.

143 לפרטים נוספים ראו כתבה של כתב אורח, "מאחורי הקלעים של ביטול צו הסייבר החדש", גיק־טיים, אפריל 2016, http://www.geektime.co.il/the-decline-of-the-israeli-cyber-law/

144 על המהפכה שאירעה בבאר שבע, שהמדינה שמה לה למטרה להפוך אותה לבירת הסייבר האזורית, ראו: Warwick Ashford, "Israel's Cyber Security Frontier", *ComputerWeekly*, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier

למשרד הביטחון.[145] המשרד הלך לקראת התעשייה בשאלת הפיקוח על הסייבר, אך עדיין שומר על דריסת רגל בתחום זה וגם נמצא במעגל קבלת ההחלטות עבור כל מוצר סייבר בעל אפיון התקפי מובהק.

היוזמה השנייה שמה לה למטרה לטפח את ההון האנושי וליצור סטנדרטים לעוסקים בהגנת הסייבר, תוך קביעת רף מקצועי עבורם. בדצמבר 2015 פרסם מטה הסייבר הלאומי מסמך השואף להסדיר את מקצועות הגנת הסייבר בישראל. מדובר בהמלצה רשמית המהווה מעין רגולציה, שבמסגרתה מפרטת המדינה את רמת המקצועיות הנדרשת לעוסקים בהגנת סייבר על רבדיה השונים.[146] למעשה זוהי הנחייה שאין לה דוגמה בעולם, העשויה מצד אחד להעלות את רמת המקצועיות על ידי קביעת מסלולי הכשרה שונים שיפותחו במיוחד עבור הרגולציה, אך מצד שני עלולה לייתר את האופן האוטודידקטי בו מרבית המומחים בתחום דינמי זה צוברים את הידע שלהם.[147]

מהתבוננות בנעשה בעולם ניתן ללמוד כי יש מדינות המשקיעות בניסוח הנחייה אחודה עבור מכלול הידע שצריכים לרכוש העוסקים בתחום. כן ניכרת מגמה במדינות שונות להכיר בתעודות מקצועיות ואקדמיות קיימות המעידות על כישורים ויכולות במרחב הסייבר. בבריטניה נעשה ניסיון לבצע הסמכה ציבורית לאנשי מקצוע שונים בתחום זה. בנוסף, ממשלת בריטניה מאפשרת התקשרות חוזית רק עם אלה שעברו הסמכה מוכרת.

מערך הסייבר הלאומי בישראל בחר להעניק תעודות הסמכה לסייבר, שידרשו בחינת הסמכה כל שלוש שנים, ובכך קבע המלצה בדבר הידע והכישורים הנדרשים בתחום זה, תוך הנהגת סטנדרט מדינתי מקובל. בנוסף, עשתה המדינה הבחנה בין מקצועות ותפקידים בתחום הגנת הסייבר, בין השאר בין "בעל מקצוע" ל"בעל תפקיד". הראשון אובחן כאדם המוסמך לתחום ידע מסויים הדורש מיומנות ייחודית, בעוד שהשני הוא מי נמצא בתפקידו מתוקף מינוי ארגוני, המשלב תחומי התמחות המוכרים

145 Matthew Waxman and David Hindin, "How Does Israel Regulate Encryption?" November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption

146 משרד ראש הממשלה – מטה הסייבר הלאומי, **מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל**, משרד ראש הממשלה, 2015, http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf

147 ראו דו"ח בנושא זה: National Research Council, *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*, Washington, DC, The National Academic Press, 2013, http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making

כמקצוע. בשלב ראשון בחרה ישראל להסדיר את הגדרת "בעל המקצוע" ולא את "בעל התפקיד".[148] "בעלי המקצוע" חולקו לחמש קבוצות עיקריות:

1. מיישם הגנת סייבר – אדם המיישם את הגנת הסייבר של הארגון.
2. מוסמך מבדקי חדירה, בעל יכולת באיתור חולשות ובדיקות חדירות למערכות.
3. מוסמך תחקור סייבר, בעל יכולות לתחקור אירועי סייבר.
4. מוסמך מתודולוגיות סייבר
5. מוסמך טכנולוגיות סייבר.

לכל אחד ממקצועות אלה יש שתי רמות הסמכה – בסיסית ומתקדמת. למימוש הרגולציה הוחלט להקים במערך הסייבר הלאומי יחידה ייעודית שתהווה סמכות מקצועית ותטפל בכלל ההיבטים הנדרשים לרגולציה – תיקוף מקצועות ותחומי הידע, הכנת מבחנים לבדיקת הידע הנדרש, הגדרת תנאים ותבחינים לפטור חלקי מבחינות, הגדרת תהליכים לחידוש תעודה, הגדרת רמות הסמכה לכל מקצוע, הגדרת תבחינים לעמידה בכשירות מקצועית, קידום חקיקה ראשית/משנית בנושא. מטרת הרגולציה היא להבטיח את האינטרס הציבורי ולהגן מפני בעלי מקצוע לא מיומנים העשויים להסב נזק, וכן לוודא שבעלי מקצוע שהשלכות פעילותם עשויות לחרוג מעבר למעסיקים עצמם יהיו בעלי רמת מקצועית מספקת.

ההנחייה השלישית הינה עדכון לתקנות אבטחת המידע להגנת הפרטיות במאגרי מידע, כפי שאושרו במארס 2017 על ידי שרת המשפטים. העדכון כולל את הרחבת הסמכויות של ראש הרשות למשפט וטכנולוגיה (רמו"ט), וכן רשימה ארוכה של דרישות להגנת מידע מבעלי מאגרי מידע. התקנות החדשות כוללות חובת דיווח לרמו"ט (ולעיתים גם לבעלי המידע עצמם) במקרה של פריצה למאגרי מידע, הפחתה של כמות המידע האישי המוחזקת בידי אחרים, דרישה למינוי אחראי הגנת מידע והכשרה של עובדי הארגון בנושאי ביטחון ופרטיות מידע.

התקנות החדשות עוסקות גם במיקור חוץ, בהצפנה, בניטור, במבדקי חדירות, בתיעוד ובגיבוי המידע. מדובר בתקנות מודולריות, המכילות דרישות מחייבות על פי רגישות מאגרי המידע. ככל שמדובר במידע רגיש יותר וביותר אנשים החשופים אליו, כך התקנות מחמירות יותר. התקנות מדרגות מאגרי מידע על פי מִדרג – מאגרי מידע "רגילים" מאגרים בעלי רגישות "בינונית" ומאגרים שרגישות המידע בהם "גבוהה".[149] מאגרי מידע "רגילים" (עד 100,000 רשומות ועשרה מנהלים) מחוייבים ברמת אבטחה

148 משרד ראש הממשלה – מטה הסייבר הלאומי, **מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל**, משרד ראש הממשלה, 2015, http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf

149 Omer Tene, "Israel Enacts Landmark Data Security Notification Regulations", May 2017, https://iapp.org/news/a/israel-enacts-landmark-data-security-notification-regulations

בסיסית. מאגרים עם כמאה בעלי גישה ועד 100,000 רשומות יוגדרו כ"בינוניים" ויחויבו ברמת אבטחה גבוהה יותר. מאגרי מידע עם יותר מ־100,000 רשומות ויותר ממאה בעלי גישה מחוייבים ברמת אבטחה "גבוהה". בנק ישראל ואגף שוק ההון באוצר מעוניינים שחלק מתקנות אלו לא יחולו עליהם מחשש לכפילות בפיקוח כתוצאה מההנחיות שהם עצמם הוציאו בנושא זה.

ההחלטה לקדם את התקנות החדשות של שרת המשפטים נבעה משני מניעים עיקריים. ראשית, האיחוד האירופי איים להפסיק להכיר בישראל כמדינה השומרת על פרטיות על פי תקני האיחוד, דבר שהיה גורם להשלכות מרחיקות לכת על כלכלת ישראל, שכן חברות ישראליות לא היו יכולות לאסוף ולנתח מידע על אזרחים של האיחוד האירופי. הסיבה השנייה הייתה הרצון של חברות קטנות ובינוניות ליצור תקן ברור להגנה על מידע. הרף של התקנות החדשות נתפס כנמוך ביותר האפשרי, והן נכנסו לתוקף ב־8 במאי 2018.[150]

יוזמה רביעית היא "תורת ההגנה בסייבר לארגון"[151] שפרסם מערך הסייבר הלאומי באפריל 2017. המסמך תקף לארגוני המגזר העיסקי־אזרחי ומספק כלים לניהול וטיוב ההגנה בארגונים, תוך בניית תוכנית עבודה סדורה. התורה רואה בארגונים במשק מרכיבים חשובים בהעלאת החוסן הלאומי של מדינת ישראל ומחלקת אותם לשתי קטגוריות: ארגונים שפוטנציאל הנזק שלהם כתוצאה מאירוע סייבר אינו מהותי, וארגונים שעוצמת הנזק מאירוע סייבר בהם עשויה להיות משמעותית.[152] המסמך של מערך הסייבר הלאומי אינו מחייב, והוא למעשה תוכנית עבודה להפחתת סיכוני הסייבר עבור ארגונים שאין להם הנחייה ייעודית של מערך הסייבר הלאומי. המסמך מתמקד בהגנה רב־שכבתית על הארגון ועוסק ב"אנשים, טכנולוגיה ותהליכים" לצורך העלאת החוסן הארגוני. הוא מתבסס על הנחיות מכון התקנים האמריקאי (NIST), הכוללות תורת הגנה על ארגונים מפני תקיפה, לצד חיזוק יכולות לגילוי והתאוששות אחריה. מערך הסייבר הלאומי אימץ תורה זו והתאים אותה למאפייני המשק הישראלי על פי חמישה שלבים עיקריים: זיהוי פוטנציאל הנזק; הגנה מפני סיכונים; איתור אירוע; תגובה; התאוששות. כל ארגון עובר שלב של מיפוי נכסים ופירוט של דרישות ההגנה ממנו, וזאת על סמך הבקרות המרכזיות שלו: הצפנה, הגנה על מידע, אבטחת רשת, מחשוב ענן וכדומה. ארגונים בעלי פוטנציאל נזק גבוה צריכים לבצע הערכה של רמת

---

150 אילן שחר, "אחרי עיכוב של שבע שנים: גם עסקים קטנים יחויבו בתקנות אבטחת מידע", **כלכליסט**, 13 במארס 2017.

151 משרד ראש הממשלה – מערך הסייבר הלאומי, **תורת ההגנה בסייבר לארגון – גרסה 1.0**, משרד ראש הממשלה, אפריל 2018, https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_418_A4.pdf

152 הקריטריון להבחנה בין קטגוריה א' לקטגוריה ב' הוא האם עלות הטיפול באירוע סייבר עולה על 100,000 ₪. אם התשובה היא חיובית, פוטנציאל הנזק מאירוע סייבר נחשב למשמעותי.

ההגנה הנדרשת מכל נכס שמופה וכן לקבוע את ההסתברות של מימוש הסיכון, וזאת על פי מענה לשאלות הנוגעות לנוהלי אבטחת המידע בארגון.

פעילות מערך הסייבר הלאומי באה לידי ביטוי גם ביוזמה חמישית לגיבוש האסטרטגיה הישראלית הראשונה להגנה בסייבר.[153] האסטרטגיה מתארת את תפיסת הפעולה של מערך הסייבר הלאומי, הכוללת התייחסות לעמידות משקית, חוסן מערכתי והגנה לאומית. חדשנותה היא בכך שהיא מייחדת מקום מרכזי לפיתוח ועידוד חדשנות טכנולוגית בישראל במגזר העיסקי, באוניברסיטאות ובחינוך טרום אוניברסיטאי ומתייחסת לחדשנות כמכפיל כוח במאמצי הגנת הסייבר. המאמצים ליצור עמידות משקית נוגעים ישירות למגזר העיסקי־אזרחי ומתבטאים בהנחייה ישירה ועקיפה לארגונים במשק, לרוב דרך רגולטורים מגזריים קיימים, וכן בפיתוח מומחיות בתחום זה. האסטרטגיה מורכבת מבעוד מועד (מניעה), הכוללת בחינה של תהליכי ניהול הסיכונים, תכנון הארכיטקטורות בארגונים ונוהלי השימוש במערכות, כולל סיכונים הנובעים מהגורם האנושי והאופן בו ניתן ליישם פתרונות טכנולוגיים. מרכיב נוסף באסטרטגיה הוא הגנה בזמן אמת באמצעות מעורבות מדינתית וסיוע בהכלת התקיפות. מקצועיות המדינה בתחום, הכוללת סיוע של צוותים טכנולוגיים וניסיון בעבודה עם מגזרים קריטיים, רלוונטית למשק כולו ויכולה לסייע רבות בהתמודדות עם תקיפות נקודתיות.

יוזמה שישית ואחרונה היא טיוטת "חוק הסייבר" הנמצאת בסבבי דיונים במערך הסייבר הלאומי ואצל גורמים נוספים. החוק המוצע מעגן את סמכויות מערך הסייבר הממשלתי החדש ומכפיף אליו את כל בנושאי הגנת הסייבר במשק. החוק קובע מסגרת משפטית לטיפול באירועי סייבר בזמן אמת ומאפשר מתן תמריצים למשק בתחום זה, וביניהם פטור מאחריות לפעילות הגנה פנים ארגונית ואישור מהממונה על ההגבלים העיסקיים לשיתוף מידע בנושאי סייבר בין מתחרים במשק. החוק גם קובע כי יש ריבון אחד להגנת הסייבר במדינת ישראל והוא מערך הסייבר הלאומי ומנסה לשרטט גבולות גזרה ברורים בין הגופים הרגולטוריים השונים העוסקים בסייבר. ההחלטה מיהו הרגולטור המרכזי שאחראי באופן ישיר על הגנת הסייבר בכל מקרה ואירוע דורשת מיפוי מדוקדק והערכה מקיפה. כך, למשל, בבתי חולים יש מעורבות של רגולטורים רבים, והיבטי סייבר קיימים גם בתחומי ההגנה הסביבתית של בית החולים וגם בפעילותו הרציפה. הכוונה העומדת בבסיס החוק היא להסדיר את הנושא ולפתור את הקשיים עבור כלל המשק.

153 משרד ראש הממשלה – מערך הסייבר הלאומי, **האסטרטגיה הישראלית להגנה בסייבר**, משרד ראש הממשלה, 2017.

הסוגייה המרכזית אליה נדרש חוק הסייבר היא מי במשק יהיה נתון תחת רגולציה מחייבת. לשם כך מחלק החוק את המשק לשלוש קבוצות. מתוך כ־600,000 ארגונים במשק, כאלף יוגדרו ברמה A – ארגונים קריטיים המחויבים להגנה על ידי המדינה. שאר הארגונים יתחלקו בין רמה B, לגביהם יישמרו הנחיות הרגולציה הקיימות היום, ויתווסף פיקוח מלמעלה, ורמה C – ארגונים שפוטנציאל הנזק שלהם אינו מצדיק הנחייה מחייבת והם יפעלו על בסיס תמריצים בלבד. החוק מציע שמערך הסייבר הלאומי יהיה הרגולטור הבלעדי והמרכזי של גופים בעלי סיכון גבוה, בעוד שלגבי גופים אחרים יישמר הביזור הקיים על בסיס תקינה בין־לאומית.

כדי לעמוד באתגר של הסדרת נושא הסייבר באופן כולל, מסמיך מערך הסייבר הלאומי את אנשיו לשרת בכל אחד ממשרדי הממשלה כדי לספק תמיכה ומענה מקצועיים לאתגרים של כל משרד. בכך מאפשר מערך הסייבר הלאומי לרגולטור המגזרי לפעול בנושא הגנת הסייבר בתחום אחריותו, תוך שהוא שומר על בקרה ודריסת רגל לגבי הקורה בנושא זה בכל משרד. הערכת התועלת של החוק החדש מצביעה על צמצום נזקים לארגונים ולאינטרס הציבורי מצד אחד, ועל צמיחת שוק הסייבר הישראלי והגדלת האמון במרחב הדיגיטלי מצד שני.

יש להבחין בין אסדרת ההגנה בסייבר במצבי חירום, קרי בעת אירועי סייבר בזמן אמת, ובין אסדרתה בשגרה, כלומר התמודדות עם סיכונים מבעוד מועד. ישראל מציגה תפיסה מתקדמת של הגנה בסייבר בזמן אירוע, יצרה מעגלים של שיתופי פעולה בין גופים בעלי אינטרסים מתחרים ופועלת למען המטרה המשותפת גם בזירה הבין־לאומית.[154] לעומת זאת, ההנחיות שהמדינה נתנה למשק כיצד לפעול בשגרה הן מורכבות יותר והבנייתן גוררת מאבקי כוח רבים בין רגולטורים ובין בעלי אינטרסים פרטיים וביניהם אלה האמונים על האינטרס הציבורי.

לסיכום, הסתכלות רוחבית על האסטרטגיה של מדינת ישראל בתחום הסייבר מראה כי על אף החדשנות והייחודיות של שילוב המדינה בהגנה על המשק, עדיין חסרה התייחסות מדינתית כוללנית לטיפול במגזר העיסקי־אזרחי. חוק הסייבר אכן הולך כברת דרך ניכרת במטרה לתת מענה לפער זה, אך המשק בכללותו חסר מענה שיטתי שיקיף את כלל המגזרים ויטפל בכל פרויקט קיים וחדש שיש בו פוטנציאל נזק לביטחון הלאומי כתוצאה מפגיעת סייבר. על אף המיפוי המדוקדק של השוק, כפי שתואר לעיל, עדיין נותרו בו גופים מרכזיים שאינם נמצאים תחת פיקוח, למרות שהשפעתם על החוסן הלאומי של מדינת ישראל במרחב הסייבר הינה גדולה. חברות כמו "מטריקס"

154 למשל, הקמת ה־CERT הלאומי בבאר שבע, הפעיל מאז אוקטובר 2016, או הקמת מרכז CERT, לתחום הפיננסי שנועד ליצור מנגנון מוסדי לשיתוף פעולה בין כל השחקנים הרלוונטיים למיגור אירוע סייבר במערכת הפיננסית. גם במגזר האנרגיה הוקם מרכז ייעודי לניהול אירועים, שיוצר מומחיות מגזרית בנושא.

ומל"ם, למשל, מספקות שירותים דיגיטליים לחברות רבות במשק, אך פועלות ללא רגולטור שיוודא את איכות עבודתן או אבטחתן. הרגולציה המדינתית כלפי המגזר העיסקי־אזרחי במרחב הסייבר אמנם התפתחה משמעותית בשנתיים האחרונות, אך כאמור, עדיין חסרה תפיסה כוללת לפיקוח על המגזר הפרטי, שבמסגרתה כל ארגון יהיה מפוקח באופן בלתי תלוי על ידי הרגולטור המגזרי האמון עליו, וזאת בהתאם לתחום עיסוקו, ולגודל מאגרי המידע שברשותו.

נושאי אסדרה נוספים

שני נושאי אסדרה נוספים הם הֶתקנים מקושרים וביטוח סייבר. לשני אלה פוטנציאל להשפיע על מבנה המשטר הרגולטורי סביב הגנת הסייבר, אך הם עדיין עומדים לפתחם של מקבלי ההחלטות, ואלה טרם החליטו על אופן הסדרתם. הסקירה שלהלן מחדדת את הפערים הקיימים סביב שני הנושאים ואת הסוגיות לדיון. המודל הרגולטורי המוצע בהמשך לוקח בחשבון חלק מההתפתחויות האחרונות בכל אחד משני נושאים אלה.

הֶתקנים מקושרים

העשור השני של המאה הנוכחית הוא עידן החיבור ההמוני לרשת האינטרנט של מכשירים וחיישנים "חכמים". בעבר חוברו לאינטרנט מחשבים מסחריים, בהמשך פרטיים, ומאוחר יותר גם טלפונים ניידים. כיום מתבצע חיבור של סוגי מכשירים רבים במטרה לשתף מידע וליצור דרכי התקשרות שישפרו את תפקודו של המכשיר. דוגמאות לכך הן מצלמות המאפשרות שליטה ושימוש מרחוק, פרטי לבוש לספורטאים המודדים דופק וסימני מאמץ, מכוניות "חכמות", בקרי טמפרטורה, מקררים, מייבשי כביסה ונורות. מכשירים פשוטים ובעלי יכולת השפעה נקודתית הפכו למכשירים "חכמים" ובכך ליעילים יותר וכאלה שחוסכים כסף לצרכן. עם זאת, מכשירים אלה גם נעשו פגיעים למתקפות ברשת האינטרנט ועלולים להפוך בעצמם לכלי בידי תוקפים.

לאחרונה התבטא השר לביטחון המולדת בארצות הברית כי "הגנה על מכשירים חכמים בעידן האינטרנט של הדברים הפכה לצורך ביטחוני לאומי אמריקאי".[155] מדינת אילינוי מנסה להפוך למדינה ה"חכמה" הראשונה בארצות הברית המשקיעה בשירותים מקוונים ובניצול יתרונותיהם של מכשירים מחוברים להגברת יעילותם. על פי גרטנר, מכון המחקר לנושאים טכנולוגיים, מספרם של המכשירים ה"חכמים" צפוי לעלות ל־20 מיליארד לקראת שנת 2020.[156] שוק המכשירים ה"חכמים" נאמד באחרונה על

155 Eliza Chapman and Tom Uren, *The Internet of Insecure Things,* Issues Paper, ASPI International Cyber Policy Center, 2018, https://www.aspi.org.au/report/InternetOfInsecureThings

156 "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", Egham, U.K., February 7, 2017, https://www.gartner.com/newsroom/id/3598917

ידי חברת "סיסקו" בכ־19 טריליון דולר. חברת "סימנס" – אחת המתמחות במכשירים "חכמים" – מכנה תופעה זו "המהפכה התעשייתית הרביעית", אחרי מהפכת הקיטור, החשמל והמחשב. לפי המשרד לביטחון המולדת, התרחבות שוק המכשירים ה"חכמים" גורמת לכך שחלון ההזדמנות לאבטחתם הולך ומתקצר.

אין הגדרה חד־משמעית למושג "האינטרנט של הדברים", והוא נתון לפרשנויות רבות. כהגדרה מכלילה מדובר במושג העוסק בקישוריות של עצמים פיזיים לרשת האינטרנט לצורך זיהוי בפני עצמים אחרים וניהול מבני נתונים ומידע ללא התערבות אדם. סוכנות הסחר הפדרלית האמריקאית פרסמה ב־2015 את ההגדרה שלה ל"אינטרנט של הדברים": "התקנים וחיישנים שאינם מחשבים, טלפונים ניידים או טאבלטים, המתחברים, מאחסנים ומעבירים מידע אחד לשני דרך רשת האינטרנט".[157]

על אף היתרונות המובנים הגלומים בקישוריות ובמסדי נתונים עבור עצמים פיזיים, יש בהם גם סיכונים לאובייקטים עצמם, כמו גם לרשת בה הם פועלים ולבתים ולמבנים בסביבתם הם שוהים. היו מספר מקרים בהם בוצעו פריצות להתקנים "חכמים", שהדגישו את פוטנציאל הנזק בהם. חברת האבטחה McAfee הדגימה בשנת 2012 כיצד היא מסוגלת לגרום לטלפון אנדרואיד להתחמם עד כדי השמדה עצמית. באותה שנה גם בוצעה פריצה מוצלחת למערכות של מכונית מדגם "קרייזלר". ב־2014 זיהתה חברת האבטחה Proofpoint מתקפת סייבר שבוצעה באמצעות התקנים "חכמים", כגון טלוויזיות, רמקולים, מקררים ונתבי תקשורת, אשר שלחו דואר אלקטרוני נגוע למטרות התפשטות. ב־2015 וב־2016 התגלו בכנסי ההאקרים הגדולים בעולם (DefCon) 113 חולשות בהתקנים "חכמים" במכשירים שונים, כולל דלתות, טרמוסטטים, מקררים, כסאות גלגלים ופנלים סולריים. באוקטובר 2016 גילו חוקרים דרך לתקוף נורות "חכמות" וליצור תגובות שרשרת מהאחת לשנייה.

ההתקפה המפורסמת ביותר עד כה נערכה באוקטובר 2016, כאשר חולשה במצלמות אבטחה "חכמות" נוצלה לצורך הפיכתן למערכת של תוכנות זדוניות (Botnet).[158] החולשה נבעה מסיסמאות חלשות של היצרן ופגעה בחברת Dyn, המספקת שירותי פרוטוקול שמות תחום (Domaine Name System – DNS) רבים ברשת האינטרנט. כתוצאה מהתקיפה הפכו 85 אתרים ללא זמינים למשך יום אחד, ובהם אתרים פופולריים כמו "נטפליקס", "טוויטר", "פיי־פאל" ו"סוני". בעלי ההתקנים ה"חכמים" לא ידעו כי

157 FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World", January 2015, Available here: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

158 ראו הבלוג הרשמי של חברת Dyn, המנתח את התקיפה שבוצעה במערכות החברה: Scott Hilton, "Dyn Analysis Summary of Friday October 21 Attack", October 26, 2016, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

מוצריהם מעורבים במתקפה כלשהי, מאחר ואותם התקנים חכמים המשיכו לפעול כרגיל גם במהלך התקיפות על Dyn.

האירועים הללו חידדו את ההבנה כי התקנים חכמים חסרים אבטחה ברמה הבסיסית ביותר. המוצרים הפגיעים אינם רק התקנים בשימוש אישי, אלא גם בקרים תעשייתיים העוסקים בתחבורה, חשמל, נפט, גז וייצור מזון. מצב זה עלול ליצור סיכונים רבים הן לביטחון הלאומי והן לארגונים המשלבים התקנים "חכמים" בשירות שלהם. התקנים רפואיים אף מהווים סכנת חיים, כתוצאה מהגנת סייבר לא מספקת לקישוריות שהם מאפשרים.

הממשל הפדרלי בארצות הברית מכיר בחשיבותם של התקנים "חכמים" לכלכלה ולחברה ומנסה לקדם את אבטחתם, אך עד כה ללא הצלחה רבה. בתחילת 2015 פרסם הסנאט האמריקאי הצהרה המצדדת בגיבוש מדיניות לאומית עבור התקנים "חכמים". הסנאט ראה בהמשך פיתוח התקנים כאלה חשיבות עליונה לקידום חדשנות כלכלית, אך גם הכיר בצורך למנוע הונאות ושימוש לא ראוי בהתקנים אלה.[159] הצהרת הסנאט הייתה יריית הפתיחה במהלכים של הקונגרס האמריקאי שנועדו להבין טוב יותר את האתגרים בתחום זה באמצעות כינוס ועדות מומחים וקידום חקיקה, אלא שהפעילות הפרלמנטרית בנושא לא הייתה משמעותית.

הרשות המבצעת בארצות הברית ניסתה גם היא לקדם את השימוש בהתקנים "חכמים", תוך שמירה על אבטחתם. כך, מינהל התקשורת והמידע (National Telecommunications and Information Administration – NTIA) פרסם בתחילת 2017 נייר עמדה המזהה את הצורך בהתערבות של סוכנויות ממשלתיות בקידום התקנתם של עדכוני אבטחה.[160] גם מכון התקנים האמריקאי, המעורב מאוד בתחום הגנת הסייבר בארצות הברית, עורך כנסים ומקים צוותי חשיבה בנושא זה. ככלל, ההשקעה הכספית של הממשל האמריקאי בנושא ההתקנים המקושרים היא משמעותית מאוד: 250 מיליון דולר במחקר על ערים "חכמות" בנוסף לערים המקבלות סיוע כספי גם מסוכנויות מגזריות כמו תחבורה וסביבה, וכן מהקרן הלאומית למדע. יחד עם זאת, קידום הטיפול מתעכב נוכח עמדת הקונגרס, שטרם קידם חקיקה או מדיניות משמעותית בנושא בשל החשש הקבוע מפני פגיעה בתעשייה, בצמיחה ובחדשנות, המונע גיבוש רגולציה מחייבת.

---

159 U.S. Senate Resolution #110, "A Resolution Expressing the Sense of the Senate about a Strategy for the Internet of Things to Promote Economic Growth and Consumer Empowerment", U.S. Senate 114th Congress, March 2015.

160 The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, "Fostering the Advancement of the Internet of Things", The Department of Commerce, January 2017.

סוכנות הסחר הפדרלית, בהיותה הרגולטור המרכזי העוסק בהגנת מידע, מנסה לקדם את הטיפול בנושא, בין השאר דרך תביעות בבתי משפט נגד ארגונים המספקים התקנים "חכמים" מבלי לעמוד בדרישות האבטחה הבסיסיות. ב־2014 הגישה הסוכנות תביעה נגד חברת TRENDnet המוכרת מצלמות וידאו, אך אינה מאבטחת אותן כראוי למרות התחייבותה לעשות זאת, ומאפשרת לכל המחזיק בכתובת האינטרנט של המצלמה לצפות ולהאזין לתכנים שהיא מצלמת. בעקבות תביעה הגיעה החברה להבנות עם סוכנות הסחר הפדרלית בדבר גיבוש תוכנית להעלאת רמות האבטחה במוצריה ויידוע הצרכנים על פגיעויות אפשריות בהם.

במקרה אחר תבעה סוכנות הסחר הפדרלית את חברת ASUSTek, המייצרת נתבי תקשורת לרשתות ביתיות. החברה סיפקה נתבים עם חולשות אבטחה מהותיות אשר איפשרו בתחילת 2014 לתוקפים גישה לא מורשית לכ־13,000 מחשבים. בנוסף, החברה לא עשתה די כדי לקדם התקנת עדכוני אבטחה בנתבים והשאירה את לקוחותיה חשופים לפריצות. כתוצאה מהתביעה שילמה חברת ASUSTek קנסות, שִדרגה את תוכניות האבטחה שלה והודיעה למשתמשים כיצד עליהם להגן על עצמם.

תביעה נוספת של סוכנות הסחר הפדרלית הוגשה בינואר 2017 נגד חברת D-Link. הייתה זו תביעה מעט יוצאת דופן, שכן היא לא באה בעקבות פריצה או נזק ברורים, אלא בעקבות אבחנה של סוכנות הסחר כי החברה, המייצרת בעיקר מצלמות "חכמות" ונתבי תקשורת, לא עשתה מספיק כדי להגן על מוצריה. מחדלי החברה כללו היעדר בדיקות תוכנה מספקות, אבטחה לא מספקת עבור בקרת גישה והגדרות המוצרים ואי־שימוש בהצפנה במקומות רגישים. גם במקרה זה המחדלים נחשפו למרות הבטחות החברה שמוצריה מאובטחים בצורה המעודכנת ביותר.

סוכנות ממשל אמריקאית נוספת ההופכת למשמעותית במאמצי ההגנה על התקנים "חכמים" היא רשות התקשורת הפדרלית. אמנם, אין לרשות זאת מנדט מובהק על אבטחת מוצרים "חכמים", אך האישור שהיא מעניקה למוצרים להשתמש במרחב תדרים מוסכם מנוצל על ידיה כדי להתערב ולהעלות את רמת האבטחה של אותם מוצרים "חכמים". ראש שדולת הגנת הסייבר בקונגרס האמריקאי אף המליץ בהקשר זה לערוך בחינה מחדש של הליך האישור של התקני תקשורת על ידי רשות התקשורת הפדרלית במטרה להתאימו לצורך בפיקוח על אבטחת התקנים "חכמים". תהליך זה נעצר לאחר הבחירות לנשיאות ארצות הברית ב־2016 וחילופי השלטון שבאו בעקבותיהן, וכיום אין לרשות התקשורת הפדרלית מענה מעודכן להתקנים "חכמים".

לוואקום שנוצר בהיעדר התערבות מדינתית משמעותית נכנסו ארגוני צד שלישי פרטיים, המתַפקדים כרגולטורים. הארגון העיקרי המטפל בתחום ההתקנים החכמים בארצות הברית הוא Underwriters Laboratories (UL), אשר פועל לקידום "מדע בטוח" ובנה באפריל 2016 תוכנית ייעודית לבדיקה ואשרור רמות אבטחה בהתקנים "חכמים".

הארגון גורס כי התעשייה בתחום זה זקוקה למדדים בסיסיים ולתהליכים שיאפשרו הערכה ומדידה נאותות של רמות האבטחה בהתקנים "חכמים". התקנים ש־UL הציע פותחו בשיתוף סוכנויות ממשלתיות, כגון המשרד לביטחון המולדת, סוכנות הביטחון הלאומית ורשות התקשורת הפדרלית, יחד עם אנשי תעשייה ואקדמיה. גם UL הצהיר שהוא פועל בכל נושאי ההתקנים ה"חכמים" על בסיס פרסומי מכון התקנים האמריקאי. הרציונל מאחורי התוכנית של UL הוא לספק ליצרנים ולמשקיעים ביטחון ואמון בנושאי הגנת הסייבר של המוצר ה"חכם" עימו הם עובדים.

ביקורות רבות נשמעות בארצות הברית על מאמצי רגולציה אלה, וגורמים לא מעטים מטילים ספק בבקיאות הטכנולוגית של UL. בנוסף, העובדה שגורם פרטי אמור להנחות את התעשייה ליישם תקנים מסויימים מעוררת שאלות של ניגוד אינטרסים. חשש נוסף נוגע להיעדר הליך ניטור ובקרה לאחר שניתן אישור אבטחה להתקן ה"חכם", למרות שהגנת הסייבר, בהיותה דינמית, מחייבת היזון חוזר ובדיקות התואמות את השינויים בתחום זה.

לסיכום, הליך האבטחה של התקנים "חכמים" הוא סבוך. הטכנולוגיות משתנות, הרכיבים הקריטיים מגיעים מכל רחבי העולם, והאיומים הם דינמיים. פיתוח תקנים ראויים הוא שלב חשוב, אך ראשון בלבד. בהמשך יש לערוך חשיבה על האופן בו ימומשו התקנים ועל הדרך בה יש לתמרץ את השוק לאמצם. פירוט נוסף בנושא זה – במסגרת המודל המוצע לרגולציה המובא בהמשך.

ביטוח סייבר

הסיכונים הגוברים בעולם הסייבר מחדדים את הצורך בנקיטת אסטרטגיות שונות לניהול סיכונים על ידי המדינה. ישראל עוסקת כיום במניעת סיכונים (Risk Prevention), דרך הנחיות מחייבות להגנה בסייבר הניתנות למגזרים שהוגדרו כתשתית קריטית או למגזרים פרטיים מפוקחים. מדינות אחרות פועלות לסייע בצמצום נזקים (Risk Mitigation), דרך מרכזי Cert לאומיים ומגזריים. מה שחסר הוא אסטרטגיה לפיזור סיכונים (Risk Spreading). פיזור סיכונים הוא תהליך שבו מנגנון ביטוח ותשלומי פרמיה מפזרים את סיכוני הסייבר של שחקן מסויים על פני כל בעלי הפוליסה האחרים. השוק החופשי לא הצליח עד כה לפתח מנגנוני פיזור סיכונים יעילים במרחב הסייבר, ושני האתגרים העיקריים שנותרו הם יצירת סטנדרטיזציה ושפה משותפת לכימות וכיסוי נזקי סייבר מצד ראשון או מצד שלישי, ובניית מאגר מידע אקטוארי לחישוב עלויות הפרמיה.

שוק ביטוח הסייבר בארצות הברית קיים מאז שנת 2005 ובשנת 2014 בלבד "גלגל" סכום של 2.5 מיליארד דולר. אף על פי כן המדינה צופה מהצד בשוק זה ואינה מתערבת בו. שוק ביטוח הסייבר מתמקד בנזקי צד שלישי בלבד, ויש מקום רב לייעל

את אופן פעולתו משלוש סיבות עיקריות: כל פוליסה דורשת כיום משאבים רבים ונקבעת עבור כל ארגון מבוטח בנפרד; פוליסות הביטוח אינן מעלות את רמת החוסן של הארגונים המבוטחים; הפוליסות משאירות מקום לפרשנות רבה ובתי המשפט תופסים מקום מרכזי מדי בפיצוי לקוחות על ידי חברות הביטוח במקרה של פגיעה.

מרחב האיומים הדינמי והעלויות הגבוהות במקרה של פריצה מוצלחת גורמים לחברות רבות לגלות עניין ברכישת פוליסות ביטוח מפני נזקי סייבר. חברות אלו רוצות לבטח את עצמן מפני הוצאות בלתי צפויות הן מול לקוחות שפרטיותם נפגעה והן כתוצאה מנזקי סייבר בתוך הארגון. חברות מתגוננות גם מפני נזקי רציפות תפקודית, אובדן מידע עיסקי ממערכות, אובדן הכנסה ופגיעה ביציבות הרשת הארגונית. כאמור, מרחב האיומים ופוטנציאל הנזק, יחד עם השונות הגדולה בין החברות, מובילים לרכישת פוליסות ביטוח ייעודיות המותאמות ספציפית לכל חברה. חברות הביטוח Marsh ו־AIG מדווחות על עלייה משמעותית של עשרות אחוזים ברכישת פוליסות ביטוח לשיפוי בגין פגיעות בסייבר מדי שנה.

שוק ביטוח הסייבר מוצף בצד הדרישה, אך אין עליו פיקוח רגולטורי מתאים, ועסקים קטנים ובינוניים מתקשים לשאת בהוצאות הפוליסה היקרות. ב־2015 פרסמו מדינת ניו יורק והמחלקה לשירותים פיננסיים שלה דוח על מצב האבטחה במגזר הפיננסי והודיעו על חיפוש דרכים לפיתוח שוק הביטוח בתחום זה.[161] ב־2016 העיד נציג של מדינת דרום דקוטה בפני הקונגרס האמריקאי על הדרכים בהם המדינה מנסה לעודד שוק זה.[162]

מספר מקרים שנדונו בפני בתי המשפט בארצות הברית הבליטו את הצורך בהתערבות רגולטורית בהבניית שוק ביטוח הסייבר. ביוני 2016 פסקו השופטים לטובת חברת הביטוח Federal, שממנה רכשה חברת P.F. Chang פוליסה להתגוננות מפני נזקי סייבר. חברת הביטוח לא נשאה בנזק שנגרם מפריצה מוצלחת למערכות של חברת Chang, שכן הפריצה אירעה כתוצאה מהתנהלות מול ספקי צד שלישי – סוגייה שלא הייתה מכוסה במפורש בפוליסה שנרכשה. הפרשנות המשפטית של מקרה זה הבליטה, כאמור, את החשיבות של קביעת תקנים והנחיות מדינתיים לשוק ביטוח הסייבר.

פיתוח שוק ביטוח הסייבר תלוי, בראש ובראשונה, באופן ההתערבות של המדינה, דבר המעורר את השאלה כיצד בדיוק על המדינה להתערב? האם על ידי הנחיות מחייבות לרכישת פוליסה? האם על ידי דרישת פוליסת ביטוח מכל חברה המעוניינת לעבוד עם המדינה? סוגייה נוספת בהקשר זה היא עידוד שקיפות וחובת דיווח על גניבות

161 ראו דיווח רשמי של המשרד לשירותים פיננסיים במדינת ניו יורק: https://www.dfs.ny.gov/reportpub/cyber/dfs_cyber_insurance_report_022015.pdf

162 עדותו של Adam W. Hamm בקונגרס האמריקאי, מארס 2016, http://www.naic.org/documents/government_relations_160322_testimony_hamm_cyber_insurancer_risk_managment.pdf

מידע ופריצות לחברות מסחריות, וזאת כתמריץ לרכישת פוליסת ביטוח (כפי שקורה בארצות הברית ברמת המדינות). במסגרת זו נשאלת השאלה מה צריכה לכלול חובת הדיווח על אירועי סייבר כדי שיהיה בה תמריץ אפקטיבי לרכישת פוליסות ביטוח – על מה מדווחים (למשל, אירועים משמעותיים עם פגיעות מעֵבר לסף מסויים)? למי מדווחים? כמה מהר מדווחים? עם מי מתייעצים לפני שמדווחים? מהם הפיצויים שיש לקבוע לבעלי הנזק כדי לעודד רכישת פוליסות והגנות מבעוד מועד? מה דינו של מידע מוצפן? האם כל הארגונים זהים? אלו מדרגי סיכון בתחום הגנת הסייבר יש לקבוע?

תפקיד נוסף של המדינה הינו, כאמור, סיוע במידע אקטוארי לחברות הביטוח לצורך גיבוש מחירי הפרמיה. בארצות הברית, למשל, המשרד לביטחון המולדת עוקב אחר כל התביעות שהוגשו לחברות הביטוח בהקשר של נזקי סייבר ומעודד, באמצעות חוק שהתקבל בסוף 2015, בעלי עסקים לשתף מידע על האיומים הקיימים על הרשתות שלהם. תחום קלאסי נוסף להתערבות המדינה הוא על ידי הגבלת האחריות (liability) של חברות הביטוח במקרה של "אסון סייבר" כדי שלא יפשטו את הרגל, וזאת על ידי יצירת אפשרויות מימון למקרי חירום.

שאלה נוספת היא מהו סוג הפוליסה שיש לקדם? האם פוליסות לנזקי צד ראשון (הרשתות והחברות עצמן) או פוליסות לנזקי צד שלישי (הלקוחות שמידע אישי עליהם נגנב)? בנוסף לכך, יש לתת את הדעת איך מגבשים פוליסת ביטוח אפקטיבית ומהם העקרונות המנחים בסוגייה זאת. האם על ידי דרישה למוצרי הגנה מסוג מסויים, או על ידי אימוץ עקרונות הגנה המופיעים במסמכי מכון התקנים האמריקאי, ואיזה מקום תופסת הקונפיגורציה בשטח?[163] שאלות נוספות הניצבות לפתחה של המדינה הן מהם המגזרים הפופולריים שעתידים לעשות שימוש בשוק הביטוח – קמעונאות, פיננסים, שיווק, חברות ייעוץ, חברות ייצור? ומהי מידת ההיכרות הנדרשת בין סוכן הביטוח למבקש הפוליסה? האם פיתוח פוליסה חייב להיעשות באופן ספציפי לצרכים ולנוהלי העבודה של כל ארגון, או שניתן לפתח מודל כללי ולהתאימו לארגונים השונים בעלות שולית פחותה? במסגרת זו יש לקחת בחשבון סוגיות כמו היערכות הארגון לתרחישי סייבר, מוצרי ההגנה בהם הוא משתמש, רמת המודעות של העובדים, תדירות עדכוני האבטחה וכדומה.

שוק ביטוח הסייבר בישראל מוכוון לעסקים הקטנים והבינוניים. לעומת זאת, עסקים גדולים הם לקוחות של שוק הביטוח העולמי. כך, למשל, חברת "מנורה" מכרה בשנים 2014-2016 כאלף פוליסות עבור סיכוני צד א' וצד ג' במרחב הסייבר. החברה מציעה שלושה סוגי כיסויים: ביטוח סייבר כחלק מפרק צד ג' בפוליסת בית העסק;

163 לקונפיגורציות יש משקל בקביעת פוליסת ביטוח. למשל, גם את מערכת ההפעלה "לינוקס", הנתפסת כמאובטחת יותר מהמערכת הרווחת של חברת "מיקרוסופט", ניתן להגדיר כלא מאובטחת.

ביטוח סייבר כחלק מביטוח אחריות מקצועית; ביטוח סייבר stand alone לחברות הדורשות פתרון ייעודי. חברות הביטוח המוכרות פוליסות ללקוחות מנהלות את האירוע כולו, ולא רק מפצות על נזק. יחד עם זאת, רמת המודעות של לקוחות לגובה הסיכון היא נמוכה. תשתית סייבר שנפגעת ואינה נמנית על ספקי השירות בארצות הברית, כלומר אינה משרתת הרבה מאוד לקוחות במרחב הדיגיטלי, נחשבת לסיכון סייבר בינוני/נמוך.

תובנות מסקר הספרות

סקירת הספרות על הנעשה בתחום רגולציית הסייבר במדינות השונות מלמדת על הדומה והשונה באסדרת מרחב הסייבר בעולם. מדינות שונות החלו לעסוק במרחב הסייבר בנקודות זמן שונות והתרכזו באיומים על תשתיות קריטיות ועל הביטחון הלאומי או בהתגוננות מפני פשיעת סייבר. כל המדינות משקיעות תקציבים משמעותיים בהגנת הסייבר לצורך בניית יכולת מדינתית ומוסדית לפיקוח והשפעה על הנעשה במשק ובמרחבי האיום השונים. ברוב המדינות (פרט לארצות הברית וגרמניה) ישנו יש גוף מרכזי בצורת סוכנות או מוסד, המרכז את הטיפול באיומי סייבר, קובע את התקנים להתמודדות איתם ומאפשר קבלת החלטות סדורה בתחום זה, על אף המורכבות והרב־שכבתיות של בעיית הסייבר.

יחד עם זאת, ועל אף ההשקעה התקציבית ובניית היכולות המדינתיות בתחום זה, בולט בהיעדרו הטיפול של המדינות השונות במגזר העיסקי־אזרחי. אין ולו מדינה אחת המנחה באופן שיטתי את המגזר העיסקי־אזרחי ומתייחסת מבעוד מועד לאיומי ביטחון לאומי כתוצאה מנזקי סייבר במגזר זה. האיחוד האירופי קבע לאחרונה כי החקיקה המחייבת הגנה בסייבר תכסה גם ספקי שירותים דיגיטליים, כמו מנועי חיפוש ושירותי ענן, שבאופן מסורתי לא נכללו במעטפת הרגולציה המדינתית. עם זאת, גם האיחוד האירופי אינו מספק מענה כולל לאיומי הסייבר. בארצות הברית, רוב המגזר העיסקי־אזרחי אינו כפוף להנחיות מחייבות, למעט מספר תחומים יוצאי דופן, כמו פיננסים, בריאות ואנרגיה. גם בבריטניה ובצרפת המגזר העיסקי־אזרחי אינו כפוף כמעט בכלל לרגולציה. בגרמניה ישנם ניסיונות ליצור שיתופי פעולה בין המדינה ובין המגזר העיסקי־אזרחי לצורך גיבוש תקנים להגנה במרחב הסייבר, אך הדבר אינו מתבצע באופן שיטתי ומתייחס למגזרים ספציפיים בלבד.

הגישה הישראלית כלפי המגזר העיסקי־אזרחי מורכבת. הנחיית מגזר זה בהתגוננות נגד איומי סייבר מפוצלת בין רגולטורים למגזרים שונים, ומפוקחת לעיתים ישירות על ידי המשרד הממשלתי האחראי (כמו בתחום הבריאות), הרשות המדינתית הרלוונטית (למשל, המפקח על הבנקים), או ארגון פרטי המועסק על ידי המדינה כמתווך רגולטורי בעל מומחיות בתחום (לדוגמה, בתחום האנרגיה). על אף הניסיונות להכפיף את כלל

המשק להנחיות מחייבות להתגוננות בסייבר באמצעות מערך הסייבר הלאומי, חסר עדיין תהליך שיטתי וסדור לזיהוי מבעוד מועד של פוטנציאל הנזק לביטחון הלאומי כתוצאה מנזקי סייבר. פער זה בולט עוד יותר בעקבות התפתחות שוק ההתקנים המקושרים, המזמנים סיכוני סייבר חדשים ממגזרים שטרם הוגדרו כאיום פוטנציאלי על מרחב הסייבר והביטחון הלאומי.

בנוסף להיעדר רגולציה מחייבת, גם התמריצים הניתנים למגזר העיסקי־אזרחי במדינות השונות לוקים בחסר. בארצות הברית, תמריצים אלו מתמקדים בשיתוף מידע ובמתן פטור מאחריות במקרה הצורך. לעומת זאת, האיחוד האירופי מפתח תשתית רגולטורית למתן תעודות עבור מוצרים מאובטחים באופן שיתמרץ את השוק להחיל על עצמו מרצון תקנים מחייבים. נושא התקינה נוכח מאוד גם במדינות אירופה השונות. בבריטניה, למשל, הונהגה קבלת תו תקן עבור רמת הגנה על מוצרים וארגונים, וניתנות הקלות מס לגופים המטמיעים אמצעי הגנת סייבר; צרפת משתמשת בכוחה של המדינה כמעסיק מרכזי וקובעת תנאי סף להגנה בסייבר עבור נותני שירותים המעוניינים לעבוד עם הממשלה ולהשתתף במכרזיה; גרמניה קובעת תנאי סף להצפנה לארגונים המעוניינים לעבוד עם המדינה, ובנוסף לכך מתקיימת בה פעילות לפיתוח תקנים ותקנות בתחום הסייבר.

היעדר מענה הולם למגזר העיסקי־אזרחי בולט במיוחד על רקע התפתחותם של התקנים מקושרים והפעילות של שוק ביטוח הסייבר. היסטוריית האבטחה הרעועה של התקנים מקושרים ברחבי העולם מלמדת על היקפו של איום הייחוס החדש המגיע מהמגזר הפרטי, שאינו מקבל מענה מדינתי הולם. איום זה גובר על רקע הקשיים בפיתוחו של שוק ביטוח הסייבר, באופן שיעודד רכישת פוליסות על ידי כלל המשק. קיימים פערים משמעותיים ושאלות קונקרטיות עליהם המדינה תצטרך לתת את הדעת בבואה לפתח את שוק ביטוח הסייבר לטובת כלל המשק.

לסיכום, סקירת הספרות מלמדת על השקעות רבות ובניית יכולות מדינתיות משמעותיות בהתגוננות מפני איומי הסייבר. עם זאת, מתן תמריצים נקודתיים בלבד למשק והיעדר מענה גורף למגזר העיסקי־אזרחי נוכח האיומים המתרבים, יוצרים פער משמעותי בתחום זה. חברות שאינן כפופות להנחיות ואינן עורכות ניהול סיכונים סדור לפעילותן במרחב הסייבר עלולות להסב נזק לביטחון הלאומי. בנוסף, הפעילות במשק בשנים האחרונות מראה כי שוק תחרותי מתגמל חברות על מוצרים טכנולוגיים מתקדמים, אך לא עבור אבטחה ראויה. כתוצאה מכך, סביר להניח שחברות עיסקיות לא ישקיעו די כדי להגן על עצמן. בהיעדר הנחייה מדינתית סדורה, נוצר חלל אותו יש למלא.

כדי ללמוד על האופן בו ניתן להתמודד בהצלחה עם איומי סייבר במגזר העיסקי־אזרחי, יש צורך לבחון עולמות תוכן אחרים. בחינה וניתוח של הנעשה בתחומי הגנת

הסביבה והאנרגיה הגרעינית, בהם שחקנים פרטיים מהווים נתח משמעותי, וברוב המקרים מרכיבים את "קו ההגנה הקדמי" של המדינה מפני סיכונים, עשויים לסייע בפיתוח מודל משוכלל להגנת סייבר גם במגזר העיסקי־אזרחי.

התפתחות הרגולציה במדינות מערביות – סיכום השוואתי

בטבלה שלהלן מובא סיכום השוואתי של התפתחות הרגולציה במרחב הסייבר במדינות המערביות שנסקרו לעיל. ניתן לראות את המועדים השונים בהם החל העיסוק ברגולציה בסייבר בכל מדינה, את ההבדלים בתקציבים המושקעים, ריכוזיות מול ביזור המשטר, מקומו של המגזר העיסקי, השפעתם של גופי המודיעין, המגזרים הנתונים תחת הנחיות והתמריצים הניתנים למגזר העיסקי־אזרחי.

	תחילת התפתחות משטרי הרגולציה בסייבר	גובה התקציב השנתי של הסוכנויות המרכזיות	מבנה מרוכז/ מבוזר	מקומו של המגזר העיסקי־אזרחי	השפעתם של גופי המודיעין	המגזרים הנתונים תחת הנחיות מחייבות	התמריצים הניתנים למגזר העיסקי־אזרחי
ארצות הברית	1965 – חקיקת Brooks Act שעסקה בסיווג מידע ברשתות פדרליות והסמיכה את מכון התקנים הפדרלי (NIST) להגן על מידע ממשלתי.	תקציב הסייבר האמריקאי מפוזר על פני מספר רב של סוכנויות. התקציב המוצע ל־2018 עבור ה־DHS הוא 1.5 מיליארד דולר, אך תקציב זה כולל תחומים נוספים.	מבנה מבוזר – מרובה סוכנויות וללא סוכנות מרכזית אחת, אם כי בתחום התשתיות הקריטיות, DHS פועל כ"מטא־רגולטור."	ברובו לא נתון תחת הנחיות מחייבות, למעט יוצאי דופן בתחום התשתיות, הבריאות והפיננסים.	גדולה – גופי המודיעין שומרים על מקומם כמשפיעים, לעיתים נגד הלך הרוח של המחוקקים בקונגרס.	תשתיות קריטיות, בריאות ופיננסים.	שיתוף מידע על איומי סייבר עם המדינה מאפשר הסרת אחריות במקרה של נזק כתוצאה מהמידע המשותף (CISA)
האיחוד האירופי	2001 – הנחייה ראשונה להגנת סייבר ומערכות מידע.	תקציב ENISA – הסוכנות המרכזת את רוב המאמצים לאסדרת הגנת הסייבר באיחוד האירופי – היה ב־2016 11.1 מיליון אירו.	הגנת הסייבר מבוצעת בנציבות האירופית מעל ארבעה Directorate Generals. מבנה המוסדי כולל ארבעה מוסדות עיקריים החולקים ביניהם את הסמכויות.	המגזר העיסקי מפוקח באמצעות הנחיות מחייבות להגנת מידע אישי ורשתות תקשורת. הן כוללות תחומים של מנועי חיפוש ושירותי ענן, הנכללים לראשונה ברגולציית הגנת מידע.	השפעת גופי המודיעין ברמת האיחוד היא קטנה. האיחוד מדגיש בעיקר פרטיות ואינטרסים צרכניים. יחד עם זאת, השפעתם של גופי המודיעין גדולה ברמת המדינות באירופה.	מגזרים רגישים וספקי שירותים במרחב הסייבר, הכוללים את מגזר הפיננסים, אנרגיה, מים, תחבורה, בנקים, בריאות וספקי תשתיות דיגיטליות, בדגש על מנועי חיפוש, שירותי ענן וחנויות מקוונות.	האיחוד פועל בעיקר בהרתעה ובהטלת קנסות. בסוף 2017 נכנסה ENISA למהלך של תקינה מול התעשייה באמצעות פיקוח על מתן תעודות למוצרים ולארגונים העוסקים בהגנת הסייבר.
בריטניה	1997 – גיבוש תוכנית להגנה על משרדי ממשלה.	400 מיליון ליש"ט	מבנה מרוכז בראשות NCSC ובהובלת סוכנות המודיעין GCHQ.	המגזר העיסקי נתון ברובו תחת רגולציה שאינה מחייבת.	השפעה משמעותית. סוכנות המודיעין GCHQ מובילה את מאמצי ההגנה על כלל המגזרים.	משרדי ממשלה ותשתיות קריטיות.	הקלות מס, תנאי סף למכרזים ממשלתיים, תוכנית הגנה מדינתית המספקת תו תקן לרמת ההגנה של מוצרים וארגונים.

	תחילת התפתחות משטרי הרגולציה בסייבר	גובה התקציב השנתי של הסוכנויות המרכזיות	מבנה מרוכז/ מבוזר	מקומו של המגזר העיסקי־אזרחי	השפעתם של גופי המודיעין	המגזרים הנתונים תחת הנחיות מחייבות	התמריצים הניתנים למגזר העיסקי־אזרחי
צרפת	1988 – חוק למניעת פשעי מחשב וסייבר.	84 מיליון אירו.	מבנה מרוכז ברמת הסוכנויות על ידי ANSSI.	ברובו אינו נתון תחת פיקוח ורגולציה מחייבים.	גופי המודיעין לא מובילים את מאמצי ההגנה, אך נותנים את הטון ומקבלים עדיפות על פני כל גוף אחר במדיניות הסייבר של המדינה, באמצעות החוק לשמירת הביטחון הלאומי.	מי שמופיע תחת ההגדרה "מפעילי תשתיות חיוניות".	רישוי מוצרים להוכחת רמת אבטחה ראויה ולקביעת סף התגוננות של ספקי שירותים המעוניינים לעבוד עם המדינה.
גרמניה	1991 – הקמת המשרד הפדרלי לאבטחת מידע (BSI).	תקציב BSI ב־2014 היה 88 מיליון אירו. התוכנית הממשלתית לקידום הגנת סייבר מתוקצבת בארבעים מיליון אירו בשנה.[164]	מבנה מבוזר ברובו, אך למשרד ל־BSI יש סמכויות רבות לפעול במגזרים שונים במשק.	מסמכי אסטרטגיה מורים על שיתוף פעולה עם המגזר הפרטי. יישום תקני /ISO DIN נעשה באופן דינמי.	השפעה חלקית. סוכנויות המודיעין הן חלק ממכלול הסוכנויות במדינה. גם לסוכנויות הגנת המידע והפרטיות יש דריסת רגל משמעותית בתחום ההגנה בסייבר.	תשתיות קריטיות בתחומים שונים. קנסות מוטלים אם תשתיות אלו לא עמדו בתקנים.	תקינה לאיכות ההגנה של מוצרים בשוק, תקן הצפנה מחייב לגופים המבקשים לעבוד עם המדינה.
ישראל	1998 – הקמת ועדת ההיגוי למיפוי תשתיות קריטיות.	מערך הסייבר הלאומי מתוקצב בכמאתיים מיליון שקלים בשנה.[165]	בראשיתו מבוזר – כל רגולטור מגזרי היה אחרי על הגנת סייבר בתחום שיפוטו. בשנתיים האחרונות מתמרכז לריבון אחד.	נתון להנחיות הרגולטורים מגזריים. לרוב מפוקח על ידי רשות מדינתית.	השפעה גדולה וניכרת. מאבקי כוח בין מערך הסייבר הלאומי ובין גופי המודיעין המסורתיים.	תשתיות קריטיות, בנקים, מוסדות מסויימים בשוק ההון, גופים פרטיים עם מאגרי מידע גדולים. לאחרונה נעשה ניסיון להכפיף גופים רבים יותר.	פרסום תורת הגנה והעברת ידע מקצועי במידת הצורך ממערך הסייבר הלאומי. שיתוף פעולה עם המדינה סביב ניהול אירועים בזמן אמת.

164 ISACA, "A Guide for the Implementation of Cyber Security Checks in Companies and Government Agencies", 2014, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/Materialien/leitfaden_EN.pdf

165 מאיר אורבך, "הממשלה אישרה את הקמת מערך הסייבר הלאומי", **כלכליסט**, 15 בפברואר 2015, https://www.calcalist.co.il/internet/articles/0,7340,L-3652448,00.html

פרק ג׳: מודלים של רגולציה מעולמות תוכן אחרים

כדי לבחון ולזהות את המודל המיטבי לפיתוח רגולציה עבור מרחב הסייבר, ראוי ללמוד כיצד התפתחה רגולציה מול המשק בתחומים נוספים. לצורך הניתוח נבחרו תחום הגנת הסביבה ותחום האנרגיה הגרעינית – שני תחומים הטומנים בחובם סיכונים משמעותיים עבור המדינה והחברה: כל מפעל הוא בעל פוטנציאל זיהום ונזק לסביבה וכל ייצור ושימוש באנרגיה גרעינית עלול להפוך לסיכון מהותי. מדובר בשני תחומים "ותיקים" יותר מתחום הסייבר מבחינת משך אסדרתם על ידי מדינות.

מטרתו של פרק זה היא לתאר את הרגולציה בתחומי הגנת הסביבה והאנרגיה הגרעינית וללמוד על העקרונות אותם ניתן לאמץ מאסדרת תחומים אלה עבור המודל הרגולטורי המוצע בתחום הסייבר.

מודל הרגולציה מתחום הגנת הסביבה

דמיון רב ניתן למצוא בין אתגרי הגנת הסביבה לאתגרי הגנת הסייבר. האתגרים בתחום הגנת הסביבה נגזרים לא רק מריבוי האיומים וממורכבותם, אלא גם מחסמי רגולציה וממערכת היחסים בין המדינה לתעשייה, נוכח הרצון לנהל סיכוני סביבה על פני כלל המגזרים במשק. הקְבלה בין אתגרי הרגולציה בתחום הגנת הסביבה ובין אלה של תחום הסייבר מאפשרת לזקק תובנות אשר ינחו את המודל המוצע בפרק הבא.

מספר נקודות השקה קיימות בין שני התחומים. ראשית, שניהם תחומים מתפתחים ודינמיים שצמחו ביתר שאת בארבעים השנים האחרונות. ניהול סיכוני הגנת הסביבה מכיל בתוכו היבטים מתחומים שונים, כגון מדע, הנדסה, כלכלה, משפט, פוליטיקה, בריאות ותקשורת. גם תחום הגנת הסייבר מסועף מאוד וכולל אתגרים מתחומי הטכנולוגיה, המשפט, הביטחון, אכיפת החוק, זכויות הפרט והתפתחות כלכלית. בנוסף, שני התחומים חסרי גבולות טריטוריאליים ברורים ונתונים לאיומים מצד מגוון רחב של מקורות. בשני התחומים גם קיים פער בין צורכי החברות הפועלות במדינה מתועשת ובין הרצון לשמור על האינטרס הציבורי ועל מרחב נקי. הרגולציה בשני בתחום הגנת הסביבה ובמרחב הסייבר נתפסת כמפגרת אחר התפתחויות טכנולוגיות ומוצגת על ידי בעלי אינטרסים עיסקיים כנוקשה ומנותקת מצורכיהם. שני התחומים טומנים

בחובם אתגרי רגולציה חוצי מגזרים ויוצרים עימותים בין המגזר העיסקי מצד אחד ובין רצון המדינה להגן על האינטרס הציבורי ולשמור על הביטחון הלאומי מצד שני.

רגולציה סביבתית בישראל

פיתוח הכלכלה והתעשייה המודרניות מביא עמו תופעות לוואי סביבתיות לא רצויות של זיהומים, כילוי אנרגיה וייצור פסולת. המדינות המתפתחות בעולם מנסות להתמודד עם התופעות אלו על ידי רגולציה "מסורתית" של מכסות פליטה, הטלת קנסות, ניהול מערכת רשיונות והטלת איסורים למניעת זיהומים. כמו כן, יש תוכניות אסדרה מבוססות תמריצים, כמו עידוד מפעלים לפיתוח והתקנה של טכנולוגיות ירוקות, הקמת מנגנוני סחר בפליטות וכינון תוכניות רגולציה וולונטריות המקנות יתרון תחרותי בשוק.

הגישה הרווחת בקרב המדינות המתקדמות היא גישה "אינטגרטיבית" להגנת הסביבה, המסתכלת עליה כמכלול ואינה עוסקת בזיהום פרטני או במפגע ספציפי. בישראל, לעומת זאת, הרגולציה הסביבתית טרם אימצה השקפה אינטגרטיבית כזאת בכל הקשור לזיהומים שמייצרים מפעלים תעשייתיים.[166] העיקרון המנחה את מאמצי הרגולציה הסביבתית בישראל הוא שכל סוג של זיהום מטופל על ידי רגולציה נפרדת, באמצעות חקיקה ראשית או משנית ותחת סמכותם של רגולטורים שונים. יש מספר רב של מקורות חקיקה, ואלה דורשים מבעלי עסקים מספר רב של היתרים בגין הזיהומים השונים הכרוכים בפעילותם. בישראל קיימים יותר מ־350 פריטי חקיקה ורגולציה, ובהם חוקים, פקודות, תקנות, וצווים, הקשורים בצורה ישירה או עקיפה להגנת הסביבה.[167]

כל מי שהוגדר כאחראי להפעלתו של מקור זיהום נאלץ להצטייד בהיתרים ורשיונות, כגון היתר פליטה לאוויר, היתר להטלת פסולת לים, היתר רעלים ורשיון עסק. אישורים רגולטוריים אלה כפופים לתהליכים ממושכים ויקרים שעל המפעל לקיים מול מספר רשויות רגולטוריות בו־זמנית: המשרד להגנת הסביבה (היתרי פליטות, פסולת, רעלים), הרשויות המקומיות (רישוי עסק, מניעת מפגעים), משרד הכלכלה (בטיחות וגהות), הרשות למים וביוב (הזרמת שפכים), רשות המים ומשרד התשתיות (זיהום מקור מים), המפקח על התעבורה במשרד התחבורה (הובלת חומרים מסוכנים) וועדות לתכנון ובנייה.[168]

---

166 שרון ידין, "מדיניות לאסדרה סביבתית אינטגרטיבית של מפעלי תעשייה בישראל – רקע, עקרונות יסוד והמלצות ליישום", המשרד להגנת הסביבה, 2014.

167 על פי נתוני המשרד להגנת הסביבה: http://www.sviva.gov.il/InfoServices/ReservoirInfo/Legislation

168 שרון ידין.

משרדי ממשלה רבים הם בעלי דריסת רגל בנושאי הגנת הסביבה: משרד האנרגיה והמים אחראי על חקיקה מקיפה העוסקת בנושאים של חיסכון באנרגיה וניהול מערך המים והביוב; משרד הבריאות אחראי על בריאות הציבור במי השתייה, איכות השפכים, ייצור מזון ומכירתו; משרד החקלאות אחראי על הגנת החי והצומח; משרד הכלכלה אחראי על נושאי בטיחות וגהות בעבודה; משרד התחבורה עוסק בהובלת חומרים מסוכנים. ראוי לציין כי כל המשרדים הללו נעדרי סמכות אכיפה, וזו נותרה נחלתו הבלעדית של המשרד להגנת הסביבה, כאוכף היחידי בתחום.[169] על אף ריבוי הסמכויות וביזורן, האכיפה בתחום ההגנה על הסביבה לוקה בחסר ומצטרפת לתרבות השלטונית הקלוקלת של אי־יישום החלטות הממשלה. לדוגמה, החלטת הממשלה משנת 2002 על ייצור חשמל מאנרגיות מתחדשות וצמצום פליטת גזי החממה, לא השיגה אף אחד מיעדי הביניים שלה ואיש לא שילם את המחיר על כך.

תסקיר ההשפעה על הסביבה

אחת מאבני היסוד של הרגולציה הסביבתית בישראל, וגם בעולם, היא מערכת תסקירי ההשפעה על הסביבה. מעבר לבליל החוקים וההיתרים שתוארו לעיל, תסקירי ההשפעה על הסביבה מאפשרים לשיקולים של הגנת הסביבה להיות גורם מכריע בתהליך קבלת ההחלטות על פיתוחם של פרויקטים חדשים במדינת ישראל.[170] להלן פירוט מטרתו ואופן פעולתו של תסקיר ההשפעה על הסביבה בתוך תהליך קבלת ההחלטות, תוך השוואת הנעשה בישראל בתחום זה לנעשה בארצות הברית, בריטניה והולנד.

תהליך הערכת ההשפעה על הסביבה הינו אמצעי לבדיקת ההשפעות הצפויות של צעדי פיתוח על הסביבה, באופן המאפשר נקיטה מראש של האמצעים הדרושים למניעת השפעות סביבתיות שליליות או להפחתתן. מטרתו של התסקיר היא לשלב בין צורכי הגנת הסביבה ובין הפיתוח הכלכלי ולהבטיח כי פרויקטים יתחשבו גם בשיקולים סביבתיים עוד בשלב התכנון. הרציונל העומד מאחורי התהליך הוא שהרבה יותר אפקטיבי לשלב פתרונות בשלב התכנון מאשר לחפש פתרונות לאחר הקמת הפרויקט והפעלתו.

בישראל נוהגת מערכת של תסקירי השפעה על הסביבה כחלק ממערכות התכנון והבנייה, מתוך תפיסה שיש לחייב שילוב של היבטים סביבתיים בתוך תהליך קבלת ההחלטות של מערכת התכנון וכחלק אינטגרלי משיקולי מוסדות התכנון והבנייה. עיגונה של מערכת תסקירי ההשפעה בחקיקה הישראלית נעשה ב־1982, כאשר התקנות שנקבעו הסדירו את אופן הטיפול במסמכים הסוקרים את ההשפעה של תוכניות

169 צבי לוינסון וגיל דרור, "רגולציה סביבתית מתקדמת... לאחור", **מים והשקיה**, 3 ביולי 2016.
170 ולרי ברכיה ואורי מרינוב, "תסקיר השפעה על הסביבה – קובץ מאמרים", המשרד להגנת הסביבה – אגף התכנון, ירושלים, 1997.

הפיתוח על הסביבה הנדונה בתוכנית. היו מקרים בהם התסקיר הצביע על סיכונים כה גבוהים, עד כי לא הייתה ברירה אלא להמליץ על דחיית התוכניות המוצעות.

בארצות הברית החלו להפעיל מערכת של תסקירי השפעה על הסביבה על פי חוק כבר בשנת 1970. בעקבותיה הלכו מדינות אחרות, כמו קנדה, יפן, אוסטרליה, אוסטריה, שוויץ והולנד. בשנת 1985 אימצה מועצת אירופה את רעיון תסקירי ההשפעה, ומשנת 1988 מיושם רעיון התסקיר במדינות החברות באיחוד האירופי הלכה למעשה.

תסקיר ההשפעה על הסביבה נועד במהותו להבטיח מסירה של כל המידע הדרוש לצורך הכרה ובחינה של הפרויקט המוצע וההשפעות הצפויות עקב הקמתו והפעלתו, וכן להציע את האמצעים הדרושים כדי למנוע פגיעה בסביבה או להקטינה. חשיבותו של התסקיר היא בארבעה מישורים עיקריים: ככלי עזר בידי מוסדות התכנון לקבלת החלטות בדבר ביצוע פרויקטים; כמדריך למוסדות אלה מה עליהם לדרוש מהיזם כדי להגן על האינטרס הציבורי; כאמצעי להבהיר ליזם את ההשלכות של הפרויקט מבחינת איכות הסביבה ולהביא בפני הציבור מידע הקשור להשפעות הפרויקט על הסביבה, שבו הוא יכול להשתמש לצורך הגשת התנגדויות; כמסגרת המשלבת מומחי הגנת סביבה בתהליכי קבלת ההחלטות בנושאי תכנון ובנייה.

שלב מקדים לעריכת תסקיר השפעה על הסביבה הן ההנחיות לתסקיר, הנכתבות על ידי המשרד לאיכות הסביבה על פי דרישת מוסד התכנון. ההנחיות לתסקיר כוללות תיאור הסביבה המתוכננת של הפרויקט; המצב הקיים לפני ההשפעות הסביבתיות הצפויות; הצגת חלופות ופירוט הסיבות למיקום התוכנית, תוך הצגת השיקולים שהנחו את היזם בבחירת החלופה המוצעת; תיאור התוכנית עצמה והפעילות הנובעת מביצועה, כולל ההשלכות הסביבתיות; הערכה של ההשפעות הסביבתיות הצפויות והאמצעים שיש לנקוט כדי למנוע או לצמצם השפעות שליליות (עיקר התסקיר); לבסוף, מסקנות והמלצות במתכונת של צעדים יישומיים למילוי הוראות התוכנית.

הגשת התסקיר נדרשת במקרים שבהם יש לפרויקטים המוצעים השלכות משמעותיות על הגנת הסביבה. בחלק מן המקרים, הגשת התסקיר היא חובה המעוגנת בחקיקה ובמקרים אחרים היא נתונה לשיקול דעתם של מוסדות התכנון. התקנות המחייבות הגשת תסקיר כוללות תוכניות להקמת שדות תעופה, תחנות כוח, נמלים ואתרים לסילוק פסולת רעילה. מוסדות התכנון מחליטים במקרים רבים להגיש תסקיר השפעה על הסביבה גם לגבי תוכניות שאין חובה חוקית להחיל תסקיר זה עליהן. מדובר בתוכניות העוסקות בהקמת מנחתים, מעגנים, עורקי אספקת מים, סכרים ואגמי אגירה, מפעלים לטיהור שפכים, אתרי כרייה וחציבה, אתרים לסילוק פסולת מוצקה ותוכניות להקמת מפעלי תעשייה לא באזורי תעשייה. ההנחייה לביצוע תסקיר חלה גם על מספר רב של תוכניות מתאר ארציות, מחוזיות ומקומיות, וכן על כל תוכנית הנראית למוסדות התכנון או לשר הממונה כבעייתית מבחינת הסביבה.

הגורמים העיקריים המעורבים במערכת תסקירי השפעה על הסביבה הם:

1. **היזם** – פרטי או ציבורי. היזם אחראי על הגשת התסקיר למוסד התכנון בו נדונה התוכנית. הוא יכול להיעזר במומחים המספקים שירותי ייעוץ בתחומי ההשפעות על הסביבה.
2. **מוסד התכנון** – באחריותו לספק הנחיות להכנת התסקיר עבור היזם, וכן לבדוק את התסקיר המוגש ולפרסם חוות דעת עליו, בסיוע המשרד להגנת הסביבה.
3. **אגף התכנון במשרד להגנת הסביבה** – אחראי על תסקירי ההשפעה. מכין את ההנחיות ובודק את התסקירים המוגשים, וזאת בעזרת מומחים מכל תחום סביבתי.
4. **יועץ סביבתי** – איש מקצוע המייעץ בבדיקת התסקיר המוגש למשרד להגנת הסביבה, וכן ליזם האחראי על הגשת התסקיר. היועץ הסביבתי עשוי לבוא ממגוון משרדי ממשלה עם נגיעה לתחום הסביבה, או להיות גורם חיצוני הפועל מטעמם.

התהליך לגיבושו ולמימושו של תסקיר השפעה על הסביבה מורכב משמונה שלבים:

1. שלב א' – היזם מגיש תוכנית למוסד התכנון, וזה מחליט האם קיים צורך בהכנת התסקיר.
2. שלב ב' – באם עלה הצורך בתסקיר, מוסד התכנון פונה אל היועץ הסביבתי כדי שיכין את הצעת ההנחיות להגשת התסקיר.
3. שלב ג' – היועץ הסביבתי מגיש את ההנחיות למשרד הגנת הסביבה, ואלו נמסרות, לאחר אישור מנכ"ל המשרד להגנת הסביבה, למוסד התכנון.
4. שלב ד' – מוסד התכנון דן בהנחיות ומוסר אותן ליזם.
5. שלב ה' – היזם מכין את התסקיר (בעזרת יועצים חיצוניים, אם הוא מוצא לנכון), ומגיש אותו למוסד התכנון.
6. שלב ו' – מוסד התכנון בודק את התסקיר בעזרת המשרד להגנת הסביבה ומוודא, בתוך שלושה חודשים לכל היותר, שכל ההשלכות הסביבתיות שנכללו בהנחיות לתסקיר אכן קיבלו מענה.
7. שלב ז' – המשרד להגנת הסביבה מעביר למוסד התכנון את חוות דעתו על התסקיר שהוגש.
8. שלב ח' – מוסד התכנון מחליט האם להפקיד את התוכנית או לדחותה. אם הוחלט לאשר את התוכנית, התסקיר וחוות הדעת עומדים לעיון הציבור לצורך הגשת התנגדויות.

מערכת תסקירי ההשפעה על הסביבה במדינת ישראל הוקמה על בסיס המודל האמריקאי, הגורס כי הציבור זכאי לדעת מהן ההשפעות הסביבתיות של הפרויקטים המוצעים. המערכת האמריקאית מניחה שחשיפת היזם לביקורת ציבורית ולתביעות משפטיות תוביל אותו לנקוט צעדים למניעת מִפגעים. הכנת התסקיר בארצות הברית היא תנאי לקבלת תקציבים פדרליים, ועם זאת, המוסד האמריקאי המחליט על אישורם

של פרויקטים אינו חייב להתחשב בממצאי התסקיר. בישראל המצב שונה, כאשר קיימת מלכתחילה האפשרות לשלב את מערכת התסקירים בתהליך קבלת ההחלטות בנושאי תכנון.

השוואה של תסקירי ההשפעה על הסביבה בארצות הברית, בבריטניה ובהולנד מלמדת על גישה שונה לביצועם בכל אחת מהמדינות. ב**ארצות הברית**, עריכת התסקירים נקבעה בחוק החל על כל הפעילויות הפדרלית שיש להן השלכות על הגנת הסביבה (לא רק פעולות פיזיות של בנייה או שימוש בקרקע). כאמור, החוק האמריקאי אינו מחייב התייחסות לממצאיו של התסקיר בעת קבלת ההחלטות, ואין בו הגדרה ספציפית של סוגי הפרויקטים המחייבים הגשת תסקיר. האחריות הפורמלית להכנת תסקיר השפעה על הסביבה בארצות הברית מוטלת על הסוכנות הפדרלית להגנת הסביבה, כאשר היזם אחראי על הכנתו והמוסד המדינתי אחראי על תוכנו.

אחד הנושאים החשובים בתסקירי השפעה על הסביבה בארצות הברית הוא ההתייחסות לחלופות אפשריות. במסגרת זו חייב התסקיר להתייחס לכל החלופות הסבירות, ובכלל זה לחלופה של אי־ביצוע הפרויקט. כל התסקירים עוברים בדיקה של הסוכנות הממשלתית להגנת הסביבה (EPA), הבוחנת את שלמותם ורמתם המקצועית. השפעת חוות הדעת של הסוכנות על קבלת ההחלטות ביחס לפרויקט מסוים תלויה ביחסי העבודה בינה ובין המשרד הממשלתי האחראי על התסקיר.

חלק חשוב בתהליך האמריקאי הוא מסירת מידע לציבור. "שימוע ציבורי" הינו הליך ממוסד ומוסדר בתהליך הערכת התסקיר. עם זאת, כאשר הסוכנות להגנת הסביבה מחליטה שאין לפרויקט מסוים השפעה משמעותית על הסביבה, התסקיר אינו מובא לשימוע ציבורי ולציבור אין הזדמנות להביע את עמדתו לגביו.

מערכת תסקירי ההשפעה על הסביבה ב**בריטניה** מהווה חלק מתהליך התכנון הפיזי. מוסדות התכנון שם מחוייבים להשתמש בממצאי התסקיר בעת קבלת ההחלטות, למעט החלטות בתחומי החקלאות, הייעור, הביטחון, הניקוז והגנת החופים. למרות זאת, גם בבריטניה מעמדו של התסקיר בקבלת ההחלטות הוא מוגבל: תסקיר שאינו שלם אינו מהווה סיבה מוצדקת לעיכוב קבלת החלטה על תוכנית המוגשת לדיון. ליזם יש זכות לערער על הדרישה לתסקיר, וסמכות ההכרעה ניתנת בידי השר להגנת הסביבה. יזם המגיש תזכיר השפעה על הסביבה אינו נדרש להציג במסגרתו חלופות, אלא רק הסברים על מיגור הסיכונים שעלו בפרויקט המוצע. אין בבריטניה שלב שבו גורם ממשלתי נותן הנחיות לתסקיר, וגם אין מערכת מקצועית לבדיקת תסקירים.

ההתייחסות לתסקירי השפעה על הסביבה ב**הולנד** מחייבת הרבה יותר ומהווה חלק מחקיקה סביבתית כללית, המאפשרת לדרוש תסקיר לכל פעילות שחייבת לקבל אישור או רשיון כלשהו. גם יש חובה להשתמש בממצאי התסקירים בעת אישור תוכניות או מתן רשיונות. החקיקה ההולנדית כוללת פירוט רב של סוגי הפרויקטים

והאזורים הרגישים לסיכוני סביבה, כמו גם אמות מידה לבחינת השפעתם ודרישה לעריכת תסקירים. יזם המבקש לקים פרויקט מחוייב להתייחס בתסקיר ההשפעה על הסביבה לחלופות השונות, תוך הצבעה על היתרונות והחסרונות של כל חלופה, כולל חלופה של אי־ביצוע הפרויקט. כל תסקיר מוגש לגוף בלתי תלוי של מומחים לאיכות הסביבה, הממונים על ידי הממשלה. גוף זה מוסר את חוות דעתו למוסד המחליט, לרבות המלצות לאישור או דחיית הפרויקט. שימוע ציבורי הוא חלק מוסדר בתהליך, והציבור רשאי לפנות לבית המשפט כאשר הוא סבור שההליך היה לקוי.

לסיכום, תסקיר ההשפעה על הסביבה לא נועד לפתור בעיות סביבתיות קיימות. הוא גם אינו יעיל כאשר ההשלכות הסביבתיות ידועות היטב ואין צורך בבדיקות כדי לאשר אותן, או כאשר רמת התכנון אינה מפורטת דיה כדי שניתן יהיה להבחין בהשפעות סביבתיות. התסקיר משמש כלי יעיל בתהליך קבלת החלטות על פרויקטים מוצעים, ומיקומו הייחודי בתהליך זה מאפשר להכניס שיקולי הגנת סביבה בפרויקטים של מגזרים רבים במשק. בדרך זו ניתן למפות ולנהל סיכונים מבעוד מועד. ממצאי התסקיר מאפשרים למקבלי ההחלטות לאשר הקמה של פרויקטים, להתנות את יישומם במגבלות וסייגים, לערוך בהם שינויים, לעכב את ביצועם, או אפילו לבטלם כליל.[171]

בין הגנת הסביבה להגנת סייבר

בהסתכלות רחבה על ציר הזמן ניתן למצוא נקודות השקה רבות בהתפתחות הרגולציה בתחום הסביבה ובמרחב הסייבר. מבחינת ציר הזמן, הרגולציה הסביבתית הקדימה במספר עשורים את הרגולציה במרחב הסייבר. מבחינת התפתחות הרגולציה, בשני התחומים היא החלה בהטלת סנקציות: הסנקציות הראשונות בתחום הגנת הסביבה הוטלו על מזהמי סביבה שלא עמדו בדרישות המדינתיות. הסנקציות הראשונות במרחב הסייבר הוטלו על פשעי מחשב, כפי שאלה הוגדרו בחקיקה ראשית במדינות השונות. בהמשך, הרגולציה השתיתה פיקוח והנחיות על מי שהוגדרו כשחקני המפתח הן בתחום הגנת הסביבה והן במרחב הסייבר. בתחום הראשון היו אלה מקורות הזיהום המרכזיים, בעוד שבמרחב הסייבר הפיקוח וההנחיות הוטלו על תשתיות של מערכות מידע שהוגדרו כקריטיות לביטחון הלאומי. כיום, הרגולציה בשני התחומים הולכת ומתרחבת, חלה על מספר גדל והולך של מגזרים ואט־אט נתפסת כתקן מחייב עבור מספר רב יותר של בעלי עסקים וארגונים.

בשני התחומים, האתוס הראשוני לא עמד במבחן המציאות. הרצון לשמור על האתוס של טבע או מרחב דיגיטלי חופשי מהתערבות, ממנו כולם יכולים להנות במידה שווה, לא עלה בקנה אחד עם התפתחות התעשייה והטכנולוגיה ותופעות הלוואי השליליות

171 שם.

שבאו עימן. עד מהרה התמלאה הסביבה במשאבי מים מזוהמים, בצריכה לא שוויונית של משאבי הטבע ובזיהום האוויר והים. מרחב הסייבר עבר מסלול דומה, כאשר היה נתון לאיומים מצד שחקנים מדינתיים ותת־מדינתיים ששאפו לנצל את חולשותיו, לגנוב מידע רגיש ולהסב נזק.

במדינת ישראל, הסנקציות הראשונות בתחום הסביבה הוטלו על הפוגעים בחיות הבר, בצומח ובניקיון המים. הסנקציות הראשונות בתחום הסייבר שהוטלו בישראל היו על פושעי המחשב – ההאקרים הקלאסיים – אותם שאפה המדינה להרתיע. הגלגול הבא של הרגולציה בשני התחומים כבר יצא מתוך נקודת הנחה שונה: ההבנה כי לפגיעות בסביבה או במרחב הסייבר יש השלכות על תחומים אחרים, הקשורים בכלכלה, בביטחון ובתפקוד הציבור. איומים חדשים הפכו לחלק מהשיח והתחדדה התפיסה כי תחומי הסביבה והסייבר הם מרחבים שהשפעתם עלולה להיות מרחיקת לכת, ועל כן הם דורשים טיפול רוחבי ולא נקודתי מצד המדינה.

כתוצאה מכך, הוקמו בישראל יישויות רגולטוריות שתפקידן היה לפקח על מה שבתחילת הדרך הוגדר כ"קריטי". הבעיות הבוערות בתחום הסביבה הביאו להקמתן של עמותות כגון "אדם, טבע ודין" וארגוני סביבה נוספים, שצמחו בהמשך לתנועת חברה אזרחית גדולה למען הסביבה.[172] השינוי בשיח הביא אחריו מבול של חוקים ותקנות, כגון חוק מניעת מִפגעים (שהוביל להקמתו של גוף אכיפה בדמות המועצה הציבורית לרעש וזיהום אוויר), חוק העוסק באיכות מי השתייה, פקודת זיהום הים בשמן, חוק מניעת זיהום הים, חוק שמירת הניקיון, חוק זיהום מים ממקורות יבשתיים, חוק החומרים המסוכנים וחוק איסוף ופינוי פסולת למיחזור. החוקים הללו היוו רגולציה שבעקבותיה נקבעו תקנים ונורמות ליישום צעדים מבעוד מועד שתפקידם היה למנוע זיהום, מִפגעים ושימוש לא נאות במשאבי טבע. גם במרחב הסייבר, ההסתכלות על הנזקים הינה מגזרית, כאשר כל רגולטור מגן על מרחב הסייבר הנמצא בתחום אחריותו.

על אף נקודות ההשקה הרבות, הרגולציה בתחום הגנת הסביבה מקדימה את מרגולציה במרחב הסייבר במידת מעורבותם של מנגנונים חזקים ושל ארגוני חברה אזרחית בטיפול באתגרים. המנגנונים המוסדיים החזקים לפיקוח וניהול הגנת הסביבה כוללים את חוק הרשויות המקומיות, המטיל את האחריות על הביוב העירוני על הרשויות; חוק גנים לאומיים ושמורות טבע, שהקים את רשות הגנים הלאומיים ושמורות הטבע העוסקת בהגנה על אתרים בעלי ערך היסטורי ולאומי ואת רשות הנחלים לשימור נחלי הארץ; חוק התכנון והבנייה שכּוֹנן את מוסדות הבנייה; חוק רישוי עסקים, שמטרתו

172 למעלה ממאה ארגונים רשומים כחברים בארגון הגג "חיים וסביבה". פירוט נוסף קיים בדו"ח שנערך באוניברסיטת בן גוריון: אלון טל, שירה ליאון זכות, ליאת פרנקל אשורי, איתי גרינשפן, שירה עקוב, "התנועה הסביבתית בישראל – מגמות, צרכים ופוטנציאל", אוניברסיטת בן גוריון בנגב, יוני 2011.

למנוע מִפגעים ועוד. הגברת ההשפעה של תהליכי הגלובליזציה וההפרטה של הטיפול בסיכוני הסביבה במאה ה־21 העלו את המודעות לארגוני סביבה אזרחיים וחיזקו את מעמדם הציבורי. ארגונים אלה ניצלו את המומנטום שנוצר וקידמו חוקים נוספים, כגון חוק הפיקדון על מיחזור בקבוקים, חוק שמירת הסביבה החופית, חוק אוויר נקי וחוק הסדרת הטיפול באריזות. גם בית המשפט העליון גילה בפסיקותיו יחס אוהד להגנת הסביבה ולתפקידם של ארגוני הסביבה.

עם הצטרפותה של ישראל ל־OECD, החלה המדינה לאמץ כלים כלכליים לקידום מטרות סביבתיות, כמו אגרות והיטלי פליטה בחוק אוויר נקי, מנגנון הפיקדון בחוק הפיקדון על מכלי משקה, היטל הזרמת שפכים לים, מנגנוני אכיפה כלכליים ועיגון חובת דיווח ומרשם לצורך שקיפות במידע על סיכונים סביבתיים. במקביל התעצמו בתקופה זו מנגוני רגולציה עצמית המושתתים על רצונם של גופים מסחריים להגן על הסביבה, וזאת על בסיס תקנים קיימים, כגון ISO 14001, התו הירוק ומדד מעל"ה. מנגנונים אלה מפוקחים על ידי הגופים עצמם או על ידי גורמי צד שלישי בלתי תלויים.

מרחב הסייבר טרם עבר התפתחות דומה. מלבד ההגנה על תשתיות קריטיות וההנחייה של גופים פרטניים, כגון בנק ישראל והרשות לשוק ההון, אין פיקוח על הגנת הסייבר באמצעות מנגנונים של רגולציה עצמית ואין הגנה על כלל המגזר העיסקי־אזרחי. מודל הרגולציה המוצע בהמשך שואף לגשר על פער זה.

אימוץ מודלים רגולטוריים מתחום הגנת הסביבה למרחב הסייבר

מסקירת המודלים הרגולטוריים בתחום הסביבה ניתן להפיק מספר תובנות לצורך פיתוח מודל לרגולציה במרחב הסייבר. ראשית, מוצע לאמץ גישה כוללנית לרגולציה במרחב זה. כשם שלמִפגע סביבתי עשויות להיות השלכות חוצות מגזרים, כך גם פגיעה במערכות מידע עשויה לגרור תגובת שרשרת שתסכן את הביטחון הלאומי של מדינת ישראל. רגולציה כוללנית בתחום הסביבה אינה בוחנת זיהומים בראייה חד־ממדית, אלא מתיימרת להתייחס להשפעות חוצות מגזרים. מניעת זיהום אוויר ממפעל המזהם את מקורות המים באגם הסמוך לו תשפר הן את איכות האוויר והן את איכות המים.[173] הרגולטור בתחום הסביבה אמור לקחת בחשבון שתי השפעות אלו בבואו לבחון את העלות מול התועלת של הרגולציה המוצעת. בהתאם לכך, המודל המוצע למרחב הסייבר יצטרך להתייחס אל מנעד ההשלכות הרחבות של תקיפת סייבר כתוצאה מפערים ברמת ההגנה.

שנית, כפי שבתחום הגנת הסביבה אנו עדים למעבר מרגולציה "מסורתית" של היטלים ותקנים קשיחים לרגולציה מבוססת תמריצים ומנגנוני שוק, כך גם במרחב

173 שרון ידין.

הסייבר יש ליצור מנגנונים שיתמרצו את התעשייה להגן על עצמה, במיוחד כשמודל השוק הנוכחי בתחום הסייבר אינו מתמרץ דיו פיתוח של מוצרים מאובטחים ומעדיף חדשנות ויזמות על פני אבטחה והגנה. החשיבות הרבה שיש לאופן בו נוהגת התעשייה גרמה למקבלי ההחלטות בתחום הסביבה ליצור תמריצים עבור המגזר הפרטי. עידוד מפעלים לפיתוח והתקנה של טכנולוגיות לצמצום זיהומים בתמורה להטבות, מנגנוני סחר בפליטות, ואף בנייה בחסות המדינה של מפעלים "ירוקים" הם רק חלק מהדוגמאות לאופן בו המדינה מעודדת שמירה על הסביבה במגזרים הפרטיים. העבודה מול התעשייה במרחב הסייבר תצטרך להיעשות על ידי מנגנונים דומים, אשר ישנו את שיווי המשקל במודל השוק הנוכחי, באופן שיקנה הטבות על רמות הגנה ראויות ולאו דווקא על יזמות וחדשנות בלבד.

עיקרון נוסף שחשוב לאמץ הוא הימנעות מריבוי סמכויות ומקבלי החלטות בתחום הגנת הסייבר. מלימוד הנעשה בתחום הסביבה וממעקב אחר מעורבותם של יותר מחמישה משרדי ממשלה ללא סמכויות אכיפה מתאימות, ניתן להסיק כי המגזר העיסקי־אזרחי ייצא נשכר מעבודה מול גוף מטה אחוד שינחה את הרגולטורים המגזריים על פי הצורך. התשתית המוסדית לגוף אחוד כזה במרחב הסייבר הונחה עם הקמת המטה ומערך הסייבר הלאומי בשנים האחרונות. יחד עם זאת, מאבקי הכוחות סביב סמכויות, כפי שהשתקפו בדוחות מבקר המדינה ובדיוני ועדות הכנסת, מעידים כי שינוי המבנה המוסדי נתקל בקשיים. מהנעשה בתחום הסביבה אנו למדים שהאחדה כזאת היא חשובה כדי להגיע לרגולציה יעילה. ואכן, מאז מסוף 2017 מתקבל הרושם שהאסדרה במרחב הסייבר מתקדמת בכיוון הנכון בחסות מערך הסייבר הלאומי.

תחום הסביבה מהווה מקרה בוחן חשוב לתרבות הציות הבעייתית של המפוקחים ולתופעה של אי־קבלת אחריות על ידי הגורמים המפקחים במדינת ישראל. העובדה שלא מתבצעת אכיפה מספקת של חוק רישוי העסקים, עליו מתבססת, בין היתר, הגנת הסביבה בארגונים פרטיים והעובדה שהחלטות ממשלה בנושאי הגנת הסביבה אינן מבוצעות ואינן כוללות התייחסות לגורם האחראי למימושן, הן נורות אזהרה עבור פיתוח הרגולציה במרחב הסייבר. המודל המוצע לרגולציה במרחב זה יצטרך לקחת בחשבון את תרבות אי־הציות של המפוקחים ולקבוע מדרג של הטלת סנקציות שיהפוך את תופעת אי־הציות ללא כדאית עבורם. כמו כן, יש לגבש מנגנוני בקרה חיצוניים על יישום החלטות ממשלה בתחומי הגנת הסייבר, שגם יוודאו את ביצוען.

לבסוף, אימוץ העקרונות של תהליך תסקיר ההשפעה על הסביבה בקבלת החלטות על פעילותם של ארגונים וחברות במרחב הסייבר ושילובם במודל המוצע, ייתן מענה למגוון רחב של מגזרים ברמת הכלי הרגולטורי. כשם שתסקיר ההשפעה על הסביבה נועד לספק תמונה מצב על אופן הניצול של משאבי הטבע (קרקע, אוויר, מים) או על עוצמת חשיפתה של האוכלוסייה למִפגעים (זיהום אוויר, רעש) ולקבוע את סבירותם

ביחס לתרומתו של כל פרויקט, כך תסקיר פגיעות סייבר של כל פרויקט יאפשר מניעה או צמצום של פגיעה בביטחון הלאומי של מדינת ישראל על ידי פגיעה במרחב הסייבר. בד בבד, אימוצו של מודל התסקיר הסביבתי יסייע להפיג חששות מפני איומי סייבר הנשקפים מפרויקטים חדשים, וכתוצאה מכך יעודד את פיתוח התעשייה והכלכלה.

מודל רגולציה מתחום האנרגיה הגרעינית

הרגולציה בתחום האנרגיה הגרעינית, כמו זו שבתחום הגנת הסביבה, מהווה מקור שממנו ניתן ללמוד רבות על פעולות אסדרה שיש לנקוט גם במרחב הסייבר. ראשיתו של תחום האנרגיה הגרעינית הוא בתגליות מדעיות גרמניות בשנת 1938, אשר אפשרו לראשונה את פיתוחה התיאורטי של פצצה גרעינית.[174] בתגובה לכך, האיצה ארצות הברית את המחקר בתחומה בנושא זה והעשירה את מצבור האורניום שלה במטרה להקדים את הגרמנים בפיתוח יכולות גרעיניות.[175] נשיא ארצות הברית דאז, רוזוולט, חתם בשנת 1941 על הוראה נשיאותית להקמת המשרד למחקר ופיתוח מדעיים (Office of Scientific Research and Development), וכן לפיתוח פרויקטים ישומיים במקביל למחקר הקיים. בה בעת, הצליחו חוקרים באוניברסיטת בירמינגהאם בבריטניה להגיע לגילויים משמעותיים בתחומי המחקר הגרעיני, שהביאו אותם להקדים את בעלי הברית האמריקאים עימם הם נהגו לשתף ידע בתחום זה. שיתוף הפעולה בין שתי המדינות הביא את הנשיא רוזוולט לאשר את פיתוחה של פצצה גרעינית, תוך שהוא מסמיך את הצבא האמריקאי להוביל את הפרויקט,[176] שנודע כ"תוכנית מנהטן".

במהלך שנות הארבעים של המאה העשרים חדלה ארצות הברית לשתף ידע עם בעלות בריתה ונוצרה בה תרבות של הסתרת הפיתוח של יכולותיה הגרעיניות. אסטרטגיה זו האיצה את מירוץ החימוש הגרעיני. ב־1952 יצרה בריטניה פצצה גרעינית משלה. נשיא ארצות הברית דאז, אייזנהאואר, החליט לשנות את מדיניות ההסתרה, ובנאום באו"ם הכריז על תוכנית "Atoms for Peace" בין בעלות הברית המערביות במסגרת הסוכנות הבין־לאומית לאנרגיה אטומית. הדבר הוביל להסכמי שיתוף ידע בין המדינות, תוך ניצול יתרון הידע האמריקאי למטרות כלכליות ופוליטיות.[177] במסגרת זו הסכימה ארצות הברית לספק ידע על אורניום מועשר, מים כבדים ופיתוח

174 Tom Sharpe, "Explore the Making of the Atomic Bomb: Guide Details Manhattan Project Sites in N.M.", *McClatchy - Tribune Business News*, June 15, 2010.

175 L.R. Walton, W.A. Orenstein and L.K. Pickering, "The History of the United States Advisory Committee on Immunization Practices (ACIP)", *Vaccine,* Vol. 33, No. 3, 2015, pp. 405-14.

176 William Lanouette, "Book Review – Nuclear Rivals: Anglo-American Atomic Relations 1941-1952 by Septimus H. Paul", *Isis*, Vol. 93, No. 1, 2002, pp. 128-9.

177 Yateen R. Pargaonkar, "Leveraging Patent Landscape Analysis and IP Competitive Intelligence for Competitive Advantage", *World Patent Information,* Vol. 45, 2016, pp. 10-20.

פצצות גרעיניות, כל עוד המדינות השותפות הבטיחו להשתמש באנרגיה הגרעינית למטרות שלום. האכיפה של מטרות השימוש באנרגיה הגרעינית בוצעה על ידי פקחים אמריקאים במדינות השונות.

שנות החמישים של המאה העשרים סימלו את תקופת ההפרטה של יכולות פיתוח האנרגיה הגרעינית של ארצות הברית. חברות אמריקאיות הפכו לדומיננטיות בזירה הבין־לאומית בכל הקשור לאנרגיה גרעינית, והוועדה לפיקוח גרעיני (Nuclear Regulatory Commission) הפכה לרגולטור של התעשייה הפרטית האמריקאית בתחום הגרעין והתמודדה עם אתגרי פיקוח ואכיפה של בטיחות מפעלים שעסקו בתחום זה. גם כיום, רוב תשתיות האנרגיה הגרעינית בארצות הברית הן בבעלות חברות פרטיות, אך המדינה מעורבת באופן עמוק ומפורט בפעילותן של חברות אלו ובמימון המחקר בתחום עיסוקן. מעורבות זאת אינה מתקבלת באהדה בקרב המגזר הפרטי, בין השאר בשל הסרבול שהיא יוצרת. כך, למשל, תהליך הבחינה של המדינה להקמת מפעל גרעיני חדש אורך בין שלוש לחמש שנים, והמימון למדענים העוסקים בנושא מגיע בעיקר דרך מעבדות לאומיות ואוניברסיטאות הפועלות במשותף עם התעשייה.

הסיכון המרכזי בפיתוחה של אנרגיה גרעינית הוא השימוש בה לפיתוח נשק להשמדה המונית בלוח זמנים קצר. חשש זה היה הדלק המניע של תקופת המלחמה הקרה בין ארצות הברית לברית המועצות. כיום, הסיכון העיקרי נובע מהאפשרות של נפילת נשק להשמדה המונית ויכולות גרעיניות לידי שחקנים לא מדינתיים, כמו ארגון המדינה האסלאמית. סיכון שנוטה להתממש באופן תדיר הרבה יותר הוא סיכון הבטיחות האישית והסביבתית שבפעילותם של מתקנים גרעיניים.

שני סיכונים מרכזיים מנוהלים על ידי הרגולציה המדינתית בתחום האנרגיה הגרעינית: הראשון הוא סיכוני בטיחות בעבודה במתקנים גרעיניים. הרגולציה בתחום זה עוסקת בתפעול מתקנים גרעיניים ובתקני הבטיחות בהם, כולל מניעת חשיפה לקרינה ונזק סביבתי. הסיכון השני קשור בהפקת נשק להשמדה המונית. הרגולציה בתחום זה עוסקת במניעת השימוש באנרגיה גרעינית לצרכים מלחמתיים ועושה זאת באמצעות רישוי, הגבלות ייצוא ומעקב אחר השימוש בחומרים במתקנים גרעיניים. לצד החשיבות שהרגולציה הגרעינית מייחסת לנושא הפקתו של נשק גרעיני, תאונות שאירעו בכורים גרעיניים העלו לסדר היום והדגישו גם את חשיבות נושא הבטיחות בפעילותם של מתקנים אלה.

הבקרה על בטיחותם של מתקני גרעין בארצות הברית הופקדה בידי סוכנות ייעודית – הוועדה לפיקוח גרעיני – האחראית לבטיחות ולביטחון של כל הקשור לאנרגיה גרעינית. הוועדה מבצעת פיקוח על מתקני הגרעין השונים, אחראית על רישוי

פעילותם וחידושו ומנהלת את סיכוני הסביבה הנובעים מעבודתם.[178] בנוסף לוועדה זאת, הקימה התעשייה בארצות הברית גוף ייעודי אחר – Institute for Nuclear Power Operations (INPO) – אשר מציע ומטמיע תקנים לבטיחות במפעלים גרעיניים. המודל של INPO אומץ ברחבי העולם והפך למודל גלובלי המיושם על ידי World Association of Nuclear Operations (WANO) – ארגון גג של מתקנים גרעיניים בכל העולם, המשתף מידע ומגבש מומחיות במטרה להגביר את הבטיחות במתקנים אלה.[179] המוטיבציה לשיתוף מידע התגברה בעיקר אחרי התאונה הגרעינית ב־The Three Mile Island בפנסילבניה שבארצות הברית בשנת 1979, שהדגישה את חשיבות השקיפות על פני סודות מסחריים בהפעלת כורים גרעיניים פרטיים. במקרה זה לא היה תמריץ כלכלי לשיתוף המידע, אלא בעיקר רצון של החברות השונות לעשות כל שניתן כדי למנוע את האסון הגרעיני הבא.

בתחום הבטיחות של מתקני גרעין, קיימים הסכמי ערבות הדדית בין מדינות באירופה למקרה של תאונה גרעינית.[180] ערבות זו מאפשרת לתעשייה הגרעינית להתפתח, בדומה למה שהיה בארצות הברית בעקבות חקיקת Price-Anderson Act ב־1957, המבטיח פיצוי מדינתי ליזמים פרטיים במקרה של תאונת בטיחות גרעינית במפעלם.

עידוד התעשייה הגרעינית, מתן ערבות פיננסית על ידי המדינה וקיומם של מכניזמים לשיתוף פעולה גם אִפשר את הקמתו של שוק ביטוח בתחום הגרעיני. חברות הביטוח השונות נשענות על התקנים המשותפים למפעלים האזרחיים שנקבעו במסגרת INPO, בדרך שהפכה את פוליסות הביטוח לרווחיות עבורן. הסוכנות הרגולטורית האמריקאית, הוועדה לפיקוח גרעיני, דורשת פוליסות ביטוח יקרות כתנאי למתן רישוי לפעילותם של מתקנים גרעיניים, ובכך מוודאת שלמפעלים המגישים בקשה להיתר יש החוסן הכלכלי לעמוד בתאונה גרעינית.

תחום הסיכונים השני – ייצור נשק להשמדה המונית – מטופל בעיקר על ידי הסוכנות הבין־לאומית לאנרגיה אטומית. סוכנות זו משתמשת באמצעי ניטור ויכולות מתקדמות לאיתור עקבות גרעיניות ולשימוש בחומרים האסורים בהסכמים שנחתמו. במקרה של הפרת הסכמים, הסוכנות רשאית לדווח למועצת הביטחון של האו"ם, ויש לה הסמכות להטיל סנקציות צבאיות וכלכליות על המדינות שמפתחות נשק להשמדה המונית בניגוד למותר. הסוכנות חתמה על הסכמים עם ארגון WANO לקידום בטיחות

178 U.S. Nuclear Regulatory Commission, "Information Technology/Information Management Strategic Plan", U.S. Nuclear Regulatory Commission Strategic Plan, Vol. 1, 2008.

179 Ramon Revuelta, "Operational Experience Feedback in the World Association of Nuclear Operators (WANO)", *Journal of Hazardous Materials*, Vol. 111, No. 1, 2004, pp. 67-71.

180 John Braithwaite and Peter Drahos, *Global Business Regulation*, Cambridge, Cambridge University Press, 2000, pp. 297-319.

במתקנים גרעיניים כדי להימנע מניגוד עניינים ולקדם בצורה משותפת את בטיחותם של מתקני גרעין ברחבי העולם. למעשה, הסוכנות הבין־לאומית לאנרגיה אטומית מבצעת תפקיד כפול – ניהול סיכוני בטיחות בתחום הגרעין ופעילות למניעת הפצתו של נשק להשמדה המונית – וכפילות זו פוגעת ביעילות פעילותה. אחת הביקורות על הסוכנות, שהפכה לקולנית במיוחד אחרי האסון בתחנת הכוח הגרעינית בפוקושימה שביפן ב־2011,[181] הייתה על חוסר היכולת שלה לקבוע תקנים מחייבים לתעשיית הגרעין האזרחית.

אימוץ מודלים רגולטוריים מתחום האנרגיה הגרעינית למרחב הסייבר

אתגרי הבטיחות והביטחון בתחום האנרגיה הגרעינית ייחודיים לסביבתם. יחד עם זאת, ניתן ללמוד רבות משיתופי הפעולה התעשייתיים והבין־לאומים לקידום הבטיחות ולמניעת הפצת נשק להשמדה המונית ברחבי העולם, כמו גם מהמעורבות המדינתית הענפה במתן פיצוי במקרה של תאונה גרעינית. מעורבות זו אפשרה פיתוח תעשייה ושוק ביטוח, באופן שהגדיל את מספר בעלי האינטרסים ברגולציה בתחום האנרגיה הגרעינית.

שיתופי הפעולה בתחום הגרעין הביאו להקמתם של מרכזי ידע לאומיים ובין־לאומיים, הן ברמה הציבורית והן ברמה הפרטית, המסייעים בשמירה על בטיחות המפעלים. הקמת מרכזי שיתוף ידע כאלה בין שחקנים במרחב הסייבר תסייע רבות לפיתוח הידע וההגנה בתחום זה. אף שישנן יוזמות פרטיות לשיתופי ידע סביב איומי סייבר, הן אינן חוצות מגזרים ואינן זוכות לתמריץ מדינתי; נהפוך הוא, יש חוסר אמון בולט בין התעשייה ובין המדינה, בעיקר בארצות הברית, בנושאי הגנת הסייבר. ייתכן כי הסיבה לכך היא שטרם התרחש אסון סייבר בקנה מידה של תאונה גרעינית, כפי שהייתה ביפן ב־2011, בברית המועצות ב־1986 או בארצות הברית עצמה ב־1979, – מה שגורם לתחושה של היעדר דחיפות ביצירת שיתופי פעולה גורפים בתחום זה.

מבחינת התערבות מדינתית, המדינה מעורבת כיום כמעט בכל תחומי הפעילות של המתקנים הגרעיניים שבשטחה. בארצות הברית הדבר מבוצע דרך רשות ייעודית המרכזת תחת קורת גג אחת את הסמכויות והמומחיות לפעילות בתחום זה. ריכוז סמכויות כזה עדיין לא קיים באופן גורף במרחב הסייבר, אך מתחיל להתפתח דווקא במדינת ישראל מאז שנת 2015 בחסות מערך הסייבר הלאומי. זאת ועוד, התקנים עליהם

181 אסון גרעיני שאירע כתוצאה מנזקי רעידת אדמה וצונאמי שבא בעקבותיה. במהלך התאונה שוחררה כמות משמעותית של חומר רדיואקטיבי לאטמוספירה, לקרקע ולמי האוקיינוס השקט. כמה מעובדי התחנה נפגעו ונפצעו קשה במהלך האירוע, ויותר מ־300 עובדים ספגו כמויות קרינה משמעותיות. פעולת הטיהור סביב התחנה צפויה להימשך עשרות שנים.

נשענת הרגולציה בסייבר נתפסים לרוב על ידי החברות הפרטיות כלא אפקטיביים מול ההתפתחויות הטכנולוגיות.

ראוי לאמץ את הפרקטיקה של מתן רשיון לפעילות בתחום האנרגיה הגרעינית גם למרחב הסייבר. כדי לקבל רשיון, מתקן גרעיני נדרש לעמוד תחת בחינה ופיקוח שיטתיים, וכלי אסדרה זה יוכל לסייע גם במיגור מבעוד מועד של סיכוני סייבר במגזר הפרטי. ראוי לאמץ במרחב הסייבר גם את שיתופי הפעולה בין הגופים השונים בתחום האנרגיה הגרעינית המאפשרים פיתוח תקנים ברמה נאותה.

במישור הבין־לאומי, תחום האנרגיה הגרעינית מטופל על ידי הסוכנות הבין־לאומית לאנרגיה אטומית שהינה בעלת סמכויות של ניטור ואכיפה, ומגבשת נורמות שעל פיהן פועלות המדינות החברות. לעומת זאת, בתחום הסייבר אין כיום שיתוף פעולה בין־לאומי המתקיים במסגרת יישות אחת. הקמת גוף בין־לאומי כזה במרחב הסייבר תוכל לאפשר גיבוש נורמות בין־לאומיות להתמודדות עם תקיפות סייבר, להשפיע על מרחב האיומים בסייבר ולסייע בהכנסת שיקולים אתיים בעת שימוש בכלי תקיפה.

ברמת התמריצים, המדינה מעורבת כיום וערבה לפיצויים נדיבים במקרה של תאונה גרעינית. מנגנון הפיצויים מאפשר לתעשייה להתפתח עם פחות דאגות כלכליות ולשוק הביטוח לפזר סיכונים בין כל בעלי הפוליסות. הידיעה של חברות הביטוח כי במקרה של נזק כולל המדינה תספק ערובות כלכליות, מתמרצת חברות אלו להציע פוליסות ולסייע בקידום האינטרס הציבורי בתחום הבטיחות של מפעלים גרעיניים. מעורבות מדינתית דומה תסייע מאוד למאמצי ההגנה בסייבר. כינונו של שוק ביטוח מתפקד בערבות המדינה יאפשר להעלות את רמת ההגנה בסייבר ולשמש תמריץ להוזלת פוליסות לארגונים ולחברות. בנוסף לכך, הוא יכניס שחקן משמעותי נוסף – חברות הביטוח – לתחום הסייבר, שיהיו לו אינטרסים להגן על מרחב זה גם במגזר העיסקי.

פרק ד׳: מודל מוצע לרגולציה של מרחב הסייבר בישראל

בפרקים הקודמים נסקרו האתגרים שבניהול סיכוני סייבר על ידי משטרי רגולציה, הובאה סקירה השוואתית של הנעשה במדינות מפתח בעולם בתחום הרגולציה בסייבר, כולל תחומי אסדרה בולטים, ונגזרו תובנות מרגולציה בתחומי הגנת הסביבה והאנרגיה הגרעינית. האיומים המתפתחים על מרחב הסייבר מחייבים התערבות מדינתית חכמה, שמצד אחד תחייב נקיטת אמצעי הגנה ראויים ומידתיים, ומצד שני תעודד את השוק להגן על עצמו באמצעות תמריצים, תוך איתור יעדי התערבות מרכזיים, שהתועלת הנובעת מהגנת עליהם עולה על עלות ההשקעה.

המודל המוצע לרגולציה במרחב הסייבר הישראלי מתמקד באסדרה והנחייה בשגרה. הוא מתבסס על הקיים, אך גם מחדש ומוסיף, וכולל חלוקה המבחינה בין רגולציה עצמית, הנחיות מדינתיות מחייבות, ורגולציה וולונטרית מבוססת תמריצים, כמפורט להלן:

1. **רגולציה עצמית** – ארגוני ביטחון כגון צה"ל, שב"כ, המוסד ומשטרת ישראל, יהיו כפופים להנחיות פנימיות בלבד, אשר יתוקפו באופן מחזורי על ידי מנגנוני ניהול הסיכונים של כל ארגון ויהיו נתונים לבקרה חיצונית.
2. **רגולציה מחייבת** – המדינה תשית רגולציה מחייבת על גופים אשר פגיעה בתשתיות הסייבר שלהם משמעותה פגיעה חמורה בביטחון הלאומי של ישראל. גופים אלה יחולקו למגזרים על פי חמש קטגוריות:
   א. מתקנים, תעשיות ביטחוניות בבעלות פרטית או ציבורית, כמו גם פרויקטים, בעלי רגישות גבוהה, יונחו על ידי הממונה על הביטחון במשרד הביטחון (המלמ"ב).
   ב. תשתיות קריטיות שיהיו כפופות הן להנחיית השב"כ והן להנחיית מערך הסייבר הלאומי: השב"כ ידרוש ממפעילי תשתיות תקשורת במדינה, כגון חברת "בזק", להכיל רגולציה מחייבת, שתכלול תקנים, מבדקי חדירות תקופתיים ומתן מענה לאיומים מתפתחים; מערך הסייבר הלאומי ינחה ויסייע לגופי תשתיות קריטיות בכל שאר המגזרים – תחבורה, אנרגיה, מים, נמלים ותעופה – לעמוד בתקנים מחמירים להגנת סייבר.

ג. מגזרי המשק החיוניים לרציפות התפקודית בישראל יונחו על ידי הרגולטור המגזרי בכל משרד ממשלתי, בתיאום עם מערך הסייבר הלאומי ובהנחייתו. לדוגמה, המפקח על הבנקים יטיל רגולציית הגנה בסייבר על מגזר הבנקאות; הרשות לניירות ערך תטיל רגולציה מחייבת על התשתיות המאפשרות מסחר בשוק ההון; משרד הבריאות ידרוש מבתי חולים לעמוד בתקני הגנה בסייבר; משרד האנרגיה יחייב מפעילי תשתיות אנרגיה פרטיים לפעול תחת רגולציית הגנה בתחומם.

ד. בעלי עסקים פרטיים החייבים רשיון עסק או אישור ממשרדי התכנון השונים יהיו נתונים תחת רגולציה שתפעל מול ארגונים וחברות במגזר העיסקי־אזרחי, על בסיס תסקיר עמידות קיברנטית שכל יישות עיסקית תידרש למלא. מטרת הרגולציה הזו תהיה להקטין את פוטנציאל הפגיעה בציבור בעת אירוע סייבר נקודתי בחברה/ארגון פרטי.

ה. מרחב הסייבר בכללותו – תופעל רגולציה מחייבת להגברת חוסנו של מרחב הסייבר, וזאת דרך התערבות נקודתית בצומתי מפתח. למשל, ספקי שירותים עליהם נשען המשק, המהווים מרכיב קריטי בשרשרת האספקה של ארגונים רבים; חברות לאירוח אתרי אינטרנט; מטמיעים של מוצרי אבטחת מידע בחברות השונות.

3. **רגולציה מבוססת תמריצים** – תפקידם של תמריצים מדינתיים הוא לעודד מנגנוני הגנת סייבר בתוך ארגונים. למשל, עידוד ובנייה של שוק הביטוח בסייבר; מתן הקלות מס לרכישת הגנה בסייבר; מתן תמריצים לשיתוף מידע בין ארגונים על איומי סייבר.

להלן פירוט של שלושת ענפי הרגולציה המרכיבים יחדיו את המודל המוצע לרגולציה של הגנת הסייבר במדינת ישראל.

רגולציה עצמית

כאמור, ארגוני ביטחון כגון צה"ל, שב"כ, המוסד ומשטרת ישראל, יהיו כפופים להנחיות פנימיות בלבד. בתחום זה שומר המודל המוצע על הקיים. לצד זאת, ראוי כי הגופים הכלולים בקטגוריה זו יפתחו יכולות בקרה עצמיות באופן שימצה את פיתוח הידע ההגנתי המתגבש במרחב בכללותו וידווחו לגורם חיצוני, כמו מבקר המדינה, על פעילותם בנושא. לדוגמה: מומלץ לגופים אלה לבצע באופן קבוע, על בסיס שנתי או דו־שנתי, תהליכי ניהול סיכונים באמצעות גורמים חיצוניים המורשים לפעול בסביבה הרגישה של הארגון.

הסכנה בפיקוח עצמי של מוסדות כה רגישים היא שחסמים ארגוניים משמעותיים, המונעים הגנה מיטבית, יישארו במקומם. זהו סיכון שמומלץ לנהלו על ידי בקרה מחזורית חיצונית בתיאום עם הגופים עצמם.

רגולציה מחייבת

רגולציה מדינתית מחייבת מופעלת על גופים במשק אשר פגיעת סייבר בהם פירושה פגיעה בביטחון הלאומי של מדינת ישראל. רגולציה זו תופעל על ידי גופים מדינתיים שונים בעלי מומחיות תוכן בעולמם של הגופים המפוקחים, כמפורט בסעיפים הבאים.

פיקוח המלמ"ב על תעשיות ביטחונית ומתקנים רגישים

הפיקוח והרגולציה של הממונה על הביטחון במשרד הביטחון על התעשיות הביטחוניות ומתקנים רגישים מיועדים לשמור על הסודיות בעבודתם. הרגולציה של המלמ"ב כוללת הן הנחיות ביטחוניות במרחב הסייבר עבור הגופים המפוקחים והן אסדרה רגולטורית. הדבר נובע מהרצון לשמור הן על ביטחון המדינה והן על הרציפות התפקודית של הגוף המפוקח.

הנחיית הגופים על ידי המלמ"ב כוללת מתן מודיעין במידת הצורך, הנחיות להגנה וקביעת קריטריונים לבעלי תפקידים בתחום הגנת הסייבר. הגוף המונחה הוא שאמור להעמיד את המשאבים ולבצע את המבוקש על ידי הגורם המנחה. הנוסחה המוצעת היא שהמלמ"ב יקבע לרוב את עקרונות ההגנה, והגופים המונחים יבחרו את אופן המימוש. בכל מקרה, ההנחייה חייבת להתממש תוך שיתוף פעולה מלא בין שני הצדדים.

רגולציה מחייבת על תשתיות קריטיות

רגולציה מחייבת תחול גם על גופים המוגדרים כתשתית חיונית־קריטית. הפיקוח יבוצע הן על ידי מערך הסייבר הלאומי והן על ידי שירות הביטחון הכללי, כפי שמקובל היום. מערך הסייבר יפַתח ידע ומומחיות, בשיתוף עם השב"כ, במטרה להגן על ארגוני התשתית הקריטית. אלה ייבחנו ויוגדרו מחדש במידת הצורך על ידי ועדת היגוי ייעודית, ויעמדו בתקנים מחמירים, כולל בדיקות חדירות תקופתיות – כל תשתית בהתאם לתחום העיסוק שלה.

ועדת ההיגוי תורכב מנציגים של השב"כ, מערך הסייבר הלאומי, משרדי התשתיות הממשלתיים וחברות פרטיות העוסקות בהגנה על תשתיות קריטיות. הוועדה תבחן באופן תקופתי את האפשרות להכניס גופים נוספים למסגרת ההנחיות המחייבות, או להוציא ממנה גופים חייבים.

רגולציה מחייבת במגזר הממשלתי

בנוסף על גופים המוגדרים כתשתית קריטית, יש מערכות וגופים רבים שחשיבותם לביטחון הלאומי היא עליונה, אך הם טרם הוגדרו כקריטיים על יד המדינה. כך, למשל, בתי חולים, מערכות רמזורים, מערכות בחירות, בנקים, ותעשיות המזון אינם נכללים תחת ההגדרה של תשתית קריטית. לפיכך, מומלץ שהרגולטור בכל אחד ממגזרים אלה, יגבש מומחיות בתחומי פעולתם וינחה אותם כדי למנוע פגיעה בהם ובאמצעותם – בביטחון הלאומי של מדינת ישראל.

המודל המוצע ממליץ להמשיך ולהסתמך על רגולטורים מגזריים הפועלים מול גופים בעלי פוטנציאל של גרימת נזק לביטחון הלאומי של ישראל. כמו כן, המודל מצדד בהישענות הרגולטור המגזרי על מומחי תוכן, תוך הסתמכות על הנחייתו של מערך הסייבר הלאומי. בדרך זו יאפשר המודל מצד אחד להנחות מקצועית גופים משמעותיים לביטחון הלאומי, ומצד שני להמשיך במתן הנחיות מחייבות להם מצידו של הרגולטור המגזרי. הרגולטור המגזרי יוכל לפעול בדרך של פרסום הנחיות הגנה מפורטות לתחום העיסוק של המפוקחים על ידיו, כפי שנעשה על ידי בנק ישראל והרשות לשוק ההון, וגם דרך מתווכים רגולטוריים אשר יפתחו מומחיות תוכן בנושא, כפי שנעשה על ידי משרד האנרגיה (אשר הסמיך גורם מקצועי חיצוני פרטי כמתווך רגולטורי להגנת הסייבר במגזר תשתיות האנרגיה הפרטיות).

רגולציה מחייבת לעסקים הנדרשים לרשיון עסק

המודל המוצע בחר עד עתה לאמץ לרוב את המצב הקיים. להלן יתואר בהרחבה החידוש המוצע, המבקש להכפיף את כלל המשק לדרגות שונות של רגולציה בהגנת מרחב הסייבר, וזאת בהתאם לקריטריונים בהם עומד כל גוף. המטרה היא למצוא את האיזון בין העמקת הגנת הסייבר ברמה הלאומית מצד אחד ובין המשך פיתוח היכולת של גורמים עיסקיים לפעול ולקדם את הכלכלה הישראלית מצד שני.

המודל המוצע מתבסס על מודל הרגולציה הקיים מתחום הגנת הסביבה, המחייב כל גוף עיסקי המבקש לקבל או לחדש את רשיון העסק שלו לערוך תסקיר ובדיקת היתכנות לפגיעה בביטחון הלאומי כתוצאה מפגיעת סייבר.

להלן סקירה של הפער הקיים בתהליך קבלת ההחלטות סביב החלת דרישות ההגנה המחייבות במרחב הסייבר, תיאור הרגולטור המדינתי הרלוונטי למרחב זה ופירוט התהליך המוצע.

קבלת ההחלטות בישראל בשאלת ההגנה במרחב הסייבר

הגברת חוסנו של מרחב הסייבר ברמה הלאומית דורשת שכל ארגון הפועל במרחב זה יבין וימפה בצורה שיטתית את פוטנציאל הנזק של כל פגיעה בו. בעוד שמדינות

שונות פיתחו דרכים להגן על התשתיות והמערכות הקריטיות לתפקודן,[182] תהליך קבלת ההחלטות בישראל העוסק בשאלה על מה להגן ובאיזה אופן לעשות זאת אינו שקוף ושיטתי, אינו מבטיח הגנה נאותה מבעוד מועד ואין בו כדי למנוע פגיעה בביטחון הלאומי.

כימות פוטנציאל הנזק הנשקף ממערכות מידע הוא משימה מורכבת הדורשת היכרות מעמיקה עם התהליכים הארגוניים בכל יישות. הנזק נמדד לא רק בהיבטים כספיים או בהשפעת הפגיעה על התוצר הלאומי הגולמי של המדינה, אלא יכול לבוא לידי ביטוי גם בפגיעה בנכסים בעלי חשיבות לאומית וסמלית. בארצות הברית, לדוגמה, תוכניות הגנה מופעלות גם על אתרי מורשת וזיכרון.[183] מנעד ועוצמת הנזק במרחב הסייבר רחבים דיים כדי לגבש מדרג חד־ערכי שעל פיו תיושם הגנה מחייבת במרחב זה. המודל מבקש להציע מנגנון אפשרי לכימות הנזק ולהחלת "חליפות הגנה" ייעודיות להגברת חוסנו של מרחב הסייבר ולמניעת פגיעה בביטחון הלאומי.

המשרד לביטחון המולדת בארצות הברית מפעיל מתודולוגיה הנקראת "סקירת עמידות קיברנטית" (Cyber Resiliency Review) עבור גופים ותשתיות השייכים למגזרים השונים.[184] הסקירה נוגעת בהיבטים מרכזיים של אופן הפעולה של ארגונים ומספקת תמונת מצב על הנכסים הקריטיים להגנה, על ניהול תשתיות התקשורת של הארגון, על גורמים המשפיעים על הרצף התפקודי שלו, על ניהולו הטכנולוגי, על היקף התלות שלו בגורמים חיצוניים, על צורת הניהול של מצבי חירום ותאונות, על יכולתו לאתר ולנהל חולשות וכן על יכולתו לבצע הערכת מצב אובייקטיבית. סקירת היבטים אלה מאפשרת למקבלי ההחלטות בכל ארגון לקבל תמונת מצב כוללת ולגבש תוכנית פעולה לשיפור העמידות הקיברנטית. יחד עם זאת, התהליך אינו שיטתי דיו וגם אינו מחייב ולכן אינו מבטיח אי־פגיעה בפועל.

המצב בישראל דומה למדי. ועדת ההיגוי מתכנסת מעת לעת ומביאה לאישור רשימה של גופים שיש לבחון את הגדרת מעמדם כתשתית קריטית. הגדרתם במעמד זה תחייב גופים אלה להעמיק את הגנתם ולעמוד בהנחיות האבטחה של שירות הביטחון הכללי (במקרה של ספקי תקשורת) או של מערך הסייבר הלאומי (בכל מקרה אחר). אלא שאין כיום תהליך סטטוטורי שיטתי ומחייב, בעל קריטריונים ברורים, שיאפשר

---

182 במדינת ישראל הוקמה ב־2002 הרשות הממלכתית לאבטחת מידע (רא"ם) שבידיה הסמכות והאחריות על מערכות מידע, זאת על בסיס החלטות ועדת היגוי ייעודית של המטה לביטחון לאומי, שתפקידה לבחון את סיכוני אבטחת המידע הגלומים בכל מערכת במרחב.

183 Patrick Beggs, "Securing the Nation's Critical Cyber Infrastructure", U.S. Department of Homeland Security, February 25, 2010.

184 מגזרים אלה כוללים, בין היתר, את מגזר המים, האנרגיה, התקשורת, התחבורה, התעשייה הכימית, החקלאות ותעשיית המזון, מערכות מידע, בנקאות ושירותים פיננסיים ומסחריים, שירותי הבריאות וכן נכסים בעלי חשיבות לזיכרון הלאומי האמריקאי (אנדרטאות, אתרי מורשת וכדומה).

איתורם של גופים כאלה מבעוד מועד.[185] משאותר הארגון או הגוף שעליו יש להפעיל את הנחיות האבטחה, מתחיל עצם תהליך ההנחייה, אם על ידי השב"כ ואם על ידי מערך הסייבר הלאומי. הנחייה זו כוללת איסוף ומחקר על פוטנציאל האיומים על הארגון, התרעות על כשלי סייבר אפשריים בתוכו, הנחייה כיצד להגן על נכסיו וביקורת ותרגילי פתע לביצוע אכיפה.

השאלה המרכזית היא כיצד ניתן לאתר את הגופים שהם בעלי פוטנציאל להיות תשתית קריטית, לפני שייגרם נזק. מורכבות הנושא היא גדולה, נוכח העובדה שכמעט לכל חברה עיסקית או משרד ממשלתי יש ממשק עם מגזרים המוגדרים כתשתיות קריטיות. לדוגמה, הגנה על תשתיות אספקת המים ואיכותם בישראל אינה נוגעת רק לתהליכים בחברת "מקורות", כי אם גם לעשרות ספקי מים אחרים, אגודות, תאגידי מים, מתקני התפלה והולכה, מתקני טיפול בשפכים, מתקני טיפול והולכת קולחים ועוד. חלק גדול ממתקנים אלה מופעל על ידי יזמים פרטיים, שהפעלה של מנגנוני הגנה במרחב הסייבר אינה תמיד בראש סדר העדיפויות שלהם. דוגמה נוספת הן מערכות מיקור חוץ, או ספקי משנה של מערכות שהוגדרו כתשתית קריטית על ידי המדינה. למשל, מפעל תעשייתי שנקבע כי הוא חיוני ופועל תחת הנחייה מחייבת של מערך הסייבר הלאומי, תלוי בפעולתו ביצרנים אחרים ("יצרני לוויין" קטנים יותר) המספקים תשומות (לעיתים קריטיות) לתהליך הייצור של המפעל המוגן. במקרים רבים נמצא כי אחדים מאותם "גורמי לוויין" אינם נכללים בקבוצת התשתיות הקריטיות, ולכן רמת ההגנה שלהם אינה מספקת. פגיעה קיברנטית בהם עלולה לגרום לנזקים משמעותיים במפעל המוגן.

החשיבות של מיפוי פוטנציאל הנזק בקרב כלל המגזר העיסקי־אזרחי היא גדולה. השימוש בטכנולוגיות מידע בישראל הוא נרחב מאוד, הן במגזרים הציבוריים והן במגזרים הפרטיים. ישראל מספקת, אפוא, כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי, המעוניין לפגוע בחוסנה ובביטחון הלאומי שלה. על כן, איתור גופים נוספים, שפעילותם מחייבת הנחייה של מערך הסייבר הלאומי או רגולטור מגזרי, היא מטלה חיונית לצורך בניית מערכת הגנה אופטימלית.

סקרים הנערכים מעת לעת ומידע המועבר ממשרדי הממשלה השונים מצביעים על צורך זה, אך אינם מספקים מענה כולל. יש ליצור תהליך מובנה שיאפשר שיפור משמעותי בהגנה על מיזמים במגזר הפרטי החשופים לפגיעה קיברנטית, שהשפעתה עלולה להיות רחבה ולהגיע לרמה הלאומית.

185 הקריטריונים המובאים בפני ועדת ההיגוי אינם גלויים והדרך בה נקבע מהי תשתית קריטית במדינת ישראל חסויה מעיני הציבור.

זהות הרגולטור בתחום הסייבר

תהליך המיפוי של המגזר העיסקי והתערבות המדינה לצורך הגנת מרחב הסייבר כבר בשלב קבלת רשיון העסק יהיו כרוכים בבדיקה חוצה מגזרים של עסקים, הגם שפיתוח הידע בנושא הגנת הסייבר הינו משותף ותקף לכלל המגזרים. על כן, הרגולטור בתחום הסייבר בעסקים המחוייבים ברשיון יתבסס הן על מערך הסייבר הלאומי, שתפקידו לפתח ידע, כלים ושיטות לאופן בו ארגונים יכולים להעלות את רמת הגנת הסייבר שלהם, והן על הרגולטורים המגזריים, המפתחים מומחיות בהתאם לצרכים של המגזר הספציפי ומבצעים את ההתאמות הנדרשות מההנחיות הכלליות של מערך הסייבר הלאומי. שני הגופים נדרשים לפעול בסינרגיה, מתוך הנחת עבודה שרוב הסדרי הרגולציה במרחב הסייבר אינם משתנים בין מגזרי הפעולה השונים. עם זאת, יהיה צורך לעדכן את ההנחיות הקיימות על פי עולם התוכן של הגוף המפוקח.

דוגמה לפעילות משולבת כזו ניתן למצוא כבר היום בשיתוף הפעולה המתקיים בין רשות התקשוב הממשלתית ובין משרד הבריאות. תפקיד הרשות הינו להנחות את מאמצי ההגנה של כלל משרדי הממשלה, ומשרד הבריאות גוזר מההנחיות הללו את ההתאמות הנדרשות עבור בתי החולים שתחת אחריותו. יש ליצור תהליך, שמערך הסייבר הלאומי כבר החל בו, שיגדיר את הרגולטור הרלוונטי להגנת סייבר בגוף מסוים, כדי להימנע ממצב (שבחלקו כבר קיים) שבו מספר גופים רגולטוריים פועלים מול אותו גוף מפוקח ובאותו הקשר.

התהליך המוצע: שימוש בכלים סטטוטוריים קיימים

כפי שפורט בפרק סקירת הספרות, גופים בישראל שהוגדרו כתשתית קריטית מפוקחים באופן מחייב על ידי שירות הביטחון הכללי (במקרה של גופי תקשורת נתונים) או על ידי מערך הסייבר הלאומי (כלל גופי התשתית הקריטית האחרים). הרגולציה על משרדי הממשלה, יחידות סמך והגופים הכפופים להן נעשית על ידי רשות התקשוב הממשלתית. רשות זאת מפקחת גם על מגזרים נוספים, שעל פי רמת הקריטיות שלהם מפוקחים גם על ידי גופי רגולציית סייבר מדינתיים נוספים (לדוגמה, רשות החשמל). משרדי הממשלה השונים מפקחים על גופים הנמצאים בתחום אחריותם ונתפסים כחשובים. כך, למשל, משרד הפנים מפקח על רשויות מקומיות ועל החברות הכלכליות הפועלות במסגרתן.

רוב המגזר העיסקי־אזרחי בישראל אינו מפוקח כיום. כדי לשפר את המצב בתחום זה מוצע להכניס את תחום הגנת הסייבר כמרכיב מובנה בתהליך הסטטוטורי הקיים במגזר העיסקי. זאת, הן בשלבי ההקמה של מיזם (אישורו בוועדות התכנון השונות) והן בתהליך התפעול שלו (חוק רישוי עסקים). הצעתנו היא, שכל מיזם שיוגש לאישור בוועדות התכנון במדינה יחויב למלא שאלון על פוטנציאל הנזק כתוצאה מפגיעה

קיברנטית בו. שאלון זה יהווה את הכלי הסטטוטורי העיקרי לצורך איתור ובחינת חשיפתו של המיזם לאפשרות של התקפות סייבר, וכן לגיבוש תהליכי הגנה נגד התקפות כאלו. השאלון גם יספק למערך הסייבר הלאומי כלי לאיתור וניהול מערך התשתיות הקריטיות במדינה עליהן יש להגן. לצד זאת, תוכל הרשות הרלוונטית הממונה על רישוי המיזם לבדוק את העמידה המתמשכת של הגוף הנבחן בהוראות ההגנה במרחב הסייבר.

כדי להסביר הצעה זו יש להרחיבה ולפרטה. הקמה של כל מיזם בישראל, ובכלל זה מיזמי תשתיות לאומיות, מחייבת עמידה בתהליכי התכנון הסטטוטורי הנוהג במדינה. כך, מיזמים הכרוכים בבניית מתקנים ומבנים מחויבים לקבל את אישורן של ועדות התכנון השונות בהתאם לעניין: מקומיות, מחוזיות וארצית. הבדיקה של מסמכי התכנון המוגשים לאישור הגורם התכנוני בישראל הינה כלי הבקרה המרכזי של הרשויות על מיזמים אלה. בין המסמכים המוגשים לבחינת ועדות התכנון כיום ניתן למצוא מסמכים הנוגעים לכיבוי אש, להיבטים שונים של בריאות הציבור, להיבטים סביבתיים, לטיפול בחומרים מסוכנים, להגנת העורף ועוד. מסמכים אלה מגדירים את הצעדים אותם על היזם לנקוט כדי לעמוד בדרישות המתחייבות בכל תחום. צעדים אלה כפופים לבקרת גורמי הרגולציה המוסמכים, המפעילים מומחים שתפקידם הוא להביא לכך שהמיזם יוקם תוך שמירה על האינטרס הציבורי ועל הביטחון הלאומי.

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

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

לצד המרכיב התכנוני למיזמים חדשים ניתן, כאמור, לעשות שימוש גם בתהליך רישוי העסקים, המחייב חידוש עיתי, כדי לוודא שהפעלת המיזם לאורך השנים עומדת בקריטריונים המתחייבים בתחומים השונים, ובכלל זה בתחום ההגנה מפני

מתקפות סייבר. שופט בית המשפט העליון לשעבר, מישאל חשין, קבע באחד מפסקי דינו: "מטרתו של החוק [לרישוי עסקים] היא לשמור ולהגן על ערכים שונים הנתפסים בחברתנו כערכים חשובים... כך הוא הערך של שלום הציבור, כך הוא הערך של שמירה על בריאות הציבור ובטיחותו, כך הוא הערך של שמירה על איכות הסביבה ואיכות החיים... להגנה על מטרות [ה]חברה...".[186] מדברי השופט חשין ניתן להסיק כי הכלים אותם מספק חוק רישוי עסקים ניתנים לשימוש גם לצורך הגנת סייבר. בכך הם יוצרים כלי בקרה חוקי נוסף בידי מערך הסייבר הלאומי, שבאמצעותו הוא יוכל לוודא כי גם מיזמים קיימים יעמדו בקריטריונים מתחייבים. במקרים מסויימים הוא אף יוכל לדרוש מבעלי עסקים פרטיים להגיש תסקיר עמידות קיברנטית ולחייבם למלא אחר הנחיות ההגנה.

שאלון פוטנציאל נזק מפגיעת סייבר

תהליך קבלה או חידוש של רישיון יהיה כרוך בפנייה של בעלי מיזמים אל מערך הסייבר הלאומי, אשר יציג בפניהם שאלון שבו הם יתבקשו לדווח על עוצמת החשיפה לציבור במקרה של פגיעת סייבר בארגון. השאלון יתחקה אחר רמת הפעילות הרשתית, מידת החשיפה שלה לציבור במקרה של נזק וחשיבות הארגון לרציפות התפקודית של מדינת ישראל ולביטחון הלאומי. השאלון יאפשר לקבוע מדרג קיברנטי עבור המיזם ואת תוכן תסקיר העמידות הקיברנטית שעליו לבצע. ככל שתגדל חשיבותו של המיזם לביטחון הלאומי תגדל, כך התסקיר שהוא יצטרך לערוך יהיה מפורט יותר. גם עלויות הגישור על הפערים שיימצאו במיזם בתחום הגנת הסייבר יהיו, קרוב לוודאי, גבוהות יותר.

על מערך הסייבר הלאומי לקבוע בשאלון אמות מידה שיגדירו את המיזמים והפרויקטים שלגביהם תתקיים חובת הגשת התסקיר. אמות מידה אלו יוכלו להתבסס על מספר מרכיבים, כמו גודלו של המיזם, חשיפתו לרשת האינטרנט, חשיפתו לגורמי סיכון בסייבר, המגזר אליו הוא משתייך, הממשקים של מיזם זה עם גורמים הנמצאים כבר תחת הנחיית מטה הסייבר הלאומי או שירות הביטחון הכללי, וכן היבטים שונים הנוגעים לתוחלת הנזק של התקפת סייבר על המיזם המועמד לרישוי.

ראוי להבהיר, שהצורך בביצוע מהלכי ההגנה הנגזרים מתוך האבחון שייערך לארגון ייקבע אך ורק מתוך בחינת עוצמת הנזק לביטחון הלאומי העלול להיגרם כתוצאה מפגיעה בתשתיות הסייבר שלו. למדינה לא צריך להיות כל עניין בנזק הכלכלי שיגרם לארגון כתוצאה מפגיעה בסייבר. תחום זה ימשיך להיות עניין פנימי הנוגע לניהול העיסקי ולאינטרסים של בעלי המניות. יחד עם זאת, אם הנזק הכלכלי יהיה בסדר גודל העלול להשפיע על הכלכלה הישראלית בכללותה, תיבחן התערבות מדינתית.

186 רשות ערעור פלילי (רע"פ) 4270/03, מדינת ישראל נגד תנובה.

תסקיר עמידות קיברנטית

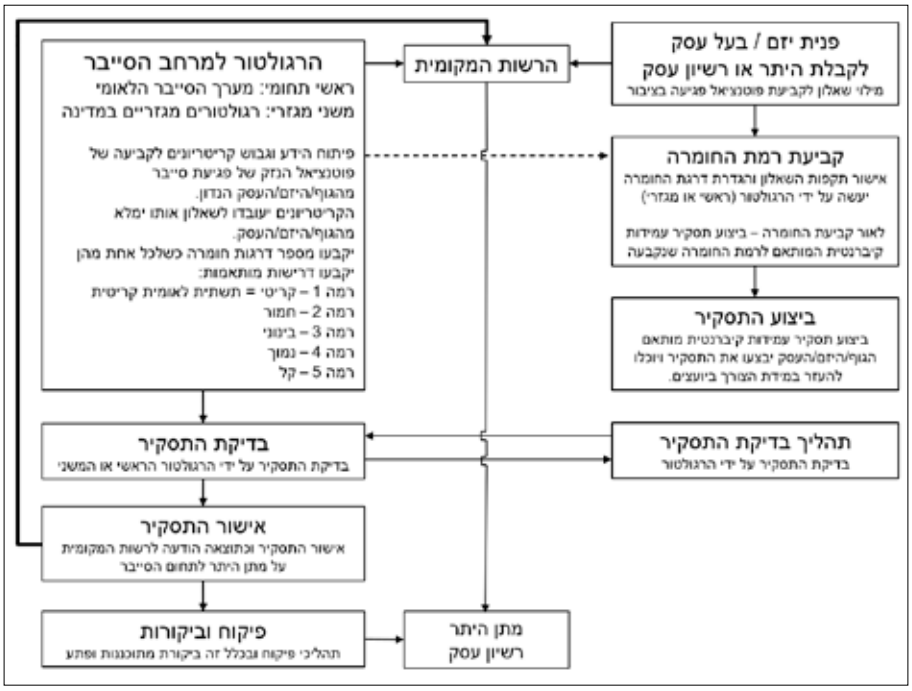
כאמור לעיל, מיזמים בתהליך הקמה, ובמקרים מסויימים כאלו שכבר הוקמו, יידרשו להגיש למערך הסייבר הלאומי תסקיר עמידות קיברנטית, וזאת בהתאם לשאלון פוטנציאל הנזק עליו השיבו. ניתן להציע מספר קווים מנחים לתוכנו של תסקיר זה, כמו גם לגורמים כגון יועצים חיצוניים שיוסמכו לערוך אותו ולהגישו, וכן לגורמים שיוסמכו לבדוק אותו. מבחינה סטטוטורית, תכולת התסקיר צריכה להיות גורפת ועליו לחול על כל הבקשות להקמת מיזמים, אלא אם ניתן לכך פטור על ידי הגורם המוסמך.

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

1. **הנחיות לתסקיר** – מערך הסייבר הלאומי יהיה אחראי להכנת הנחיות לביצוע התסקיר. על הנחיות אלו להיות מותאמות ספציפית למיזם או לגוף הקונקרטי. מוצע כי ההנחיות יכללו מספר מרכיבים, בהם: מיפוי פוטנציאל הנזק כתוצאה מתקיפה קיברנטית; מיפוי נקודות התורפה של המיזם או התוכנית; הוראות שיאפשרו מזעור החשיפה והנזק.
2. **הכנת התסקיר** – התסקירים יוכנו באחריותו ובמימונו של היזם המבקש רישוי. לצורך הכנתם ייעשה שימוש ביועצים שייבחרו מתוך קבוצת יועצים ייעודיים שיוכשרו ויוסמכו על ידי מערך הסייבר הלאומי. יועצים אלה יפעלו לאור ההנחיות להכנת התסקיר.
3. **בדיקת איכות התסקיר** – בדיקת התסקיר תבוצע באחריות מערך הסייבר הלאומי. המערך יוכל לעשות שימוש ביועצים חיצוניים שיוכשרו ויוסמכו לבדיקה של תסקירים. עלות הבדיקה תוכל להיות מוחלת על היזם. בתהליך זה ייתכנו מספר מעגלי הערות ותשובות בין גורמי מערך הסייבר הלאומי ובין הנבדק.
4. **אישור התסקיר** – בחינת התסקיר ואישורו ייעשו על ידי הגורמים המוסמכים במערך הסייבר הלאומי, שגם יקבע את המשך ההנחיות לגוף שמסר את התסקיר. האישור גם יוכל להתייחס להיבטים הנוגעים להתניות לרישוי העסק, כמו גם להוראות שיש להחיל על תוכניות היזם.

כאמור, חוק רישוי עסקים מהווה פלטפורמה מתאימה למתן הנחיות וליישום הוראות בתחום ההגנה מפני מתקפת סייבר עבור גופים קיימים. יחד עם זאת, מידת הציות לחוק המדובר אינה מספקת, וסוגייה זו תקבל מענה במסגרת ההמלצות ליישום. בנוסף, בשל מגבלות החלות על ביטחון מידע וזליגה של מידע, נדרש יהיה להגדיר תהליך זה כתהליך ממודר, שאינו פתוח לציבור הרחב אלא מוגבל רק לגורמים מוסמכים.

השלבים של המודל המוצע מתוארים באופן סכימתי בתרשים 7:



תרשים 7: מודל רגולציה מוצע למגזר העיסקי

על פי תרשים המודל, בשלב הראשון מתבצעת פנייה של היזם או בעל העסק לקבלת רשיון עסק, במסגרתו ימולא שאלון פגיעות קיברנטית. בהמשך, על פי החלטת הרגולטור במרחב הסייבר, (רגולטור ראשי תחומי – מערך הסייבר הלאומי – שיפעל בצוותא עם רגולטור משני מגזרי – המשרד הממשלתי), תיקבע רמת החומרה לפי פוטנציאל הפגיעות בסייבר ויינתנו הנחיות לביצוע תסקיר עמידות קיברנטית. התסקיר ייבדק ויאושר בסופו של התהליך על ידי הרגולטור המגזרי בצוותא עם מערך הסייבר הלאומי. אישור זה יהווה את אחד התנאים לקבלת רשיון העסק המבוקש.

יתרונות המודל נובעים, בראש ובראשונה, מן האיזון שהוא יוצר בין הצורך בהעמקת הגנת הסייבר ובין הרצון לפתח את הכלכלה. המודל משתמש במתודולוגיית התסקיר מתחום הגנת הסביבה, אשר הוכחה כיעילה בטיפול במפעלים מזהמים ומבטיחה מיפוי יסודי ומעמיק של פוטנציאל הסיכון. בנוסף, מדובר בתהליך סטטוטרי שיטתי ומחייב, המאפשר הבנה עמוקה של הפגיעה הפוטנציאלית בארגונים. המגזר העיסקי בישראל מהווה כר מטרות נרחב לתוקף הקיברנטי הפוטנציאלי, ולפיכך איתור שיטתי של גופים עיסקיים הוא משימה בעלת חשיבות עליונה. על פי התהליך המוצע, עסקים

ייבחנו באופן חוצה מגזרים, ועל ידי כך תגבר המודעות של בעלי העסקים והציבור בכללותו לסכנות הנשקפות במרחב הסייבר.

חיסרון בולט של המודל הוא הישענותו על הליך רישוי העסקים שנאכף ברמת הרשות המקומית. מאחר והנחיות הרשות המקומית אינן הנחיות מדינתיות קשיחות, עסקים רבים נוטים שלא לעבור תהליך אסדרה זה עבור פעילותם. יתרה מזאת, הליך רישוי העסקים מסועף על פני סוכנויות רגולטוריות רבות ואורך זמן רב.[187] כדי להתמודד עם עובדה זו נערכו רפורמות לאורך השנים והוכנסו מנגנוני "היתר זמני" ו"היתר מזורז" לקבלת רישוי עסק, עד השלמת התהליכים של קבלת הרשיון המלא.

כחלק מהניסיון להחיל מאמצי הגנת סייבר על המשק בכללותו, המודל המוצע קורא לאכוף ביתר שאת את חוק רישוי העסקים במדינת ישראל ולפשט את התהליך הכרוך בקבלת רישוי עסק. הרגולציה צריכה להיעשות מול גוף אחד במשרד הכלכלה, שיפעל ביעילות מול הרגולטורים הרלוונטיים למתן אישור לפתיחת עסק. יחד עם זאת, הנתונים של השנים האחרונות, המצביעים על כך שכארבעים אחוזים מהעסקים בישראל פועלים ללא רשיון,[188] עלולים להפוך את המודל המוצע לחסר שניים. על כן, יש לפשט את התהליך הרגולטורי ולהקנות למשרד הכלכלה סמכויות אכיפה לסגירת עסקים שלא יעמדו בתנאי הסף לקבלת רשיון.

רגולציה של שרשרת אספקה ושל צמתים חיוניים

רגולציה מחייבת על פי המודל המוצע תכלול גם צמתים חשובים שהתערבות מדינתית בהגנתם תוביל לתועלת רבה בעלות נמוכה. צמתים אלה יזוהו בעבודת מטה שתבחן את המשק באופן מעמיק ותזהה תשתיות מרכזיות וחיוניות, עליהן נשענת מסה קריטית של שחקנים במשק. הרציונל מאחורי זיהוי צמתים אלה הוא מציאת נקודות מפתח קריטיות שהתועלת בפיקוח עליהן לביטחון הלאומי היא גדולה. חשוב להדגיש כי המדינה לא תהיה זרוע ביצוע בעבודה מול צמתים אלה; תפקידה יסתכם בזיהוי הצמתים ובשיתוף פעולה עם הספקים הרלוונטיים לעידוד אבטחתם, מתוך הצורך והרצון להגביר את חוסנו של מרחב הסייבר הישראלי.

דוגמה לצמתים כאלה הם ספקים מרכזיים בשרשרת האספקה, מארחי שרתי האינטרנט (ספקי Hosting), המהווים תשתית למספר גדול של שירותי אינטרנט במדינת ישראל, יישומים ומערכות מידע אחודות המנהלים סליקות כרטיסי אשראי, עליהם נשענים מרבית העסקים הפרטיים, חברות אינטגרציה (טלדור ומל"ם למשל) העוסקות בתמיכה במערכות מידע במרבית המשק, קופות תשלומים של חברת Retalix

187 צבי לוינסון וגיל דרור, "רגולציה סביבתית מתקדמת... לאחור", **מים והשקיה**, 3 ביולי 2016.

188 שמעון איפרגן, "40% מבתי העסק בארץ פועלים ללא רישיון עסק", חדשות mako, 27 בדצמבר 2012, http://www.mako.co.il/special-mako-news/Article-a434351304cdb31006.htm

הנמצאות בשימוש אצל רוב ספקיות המזון, חברת "ברינקס" לשינוע מזומנים עליה נשענים הבנקים השונים, יישומים שונים לניהול חשבונות בנק הנמצאים בשימוש כלל הבנקים, וספקיות האינטרנט דרכן מתבצעים גלישה וחיבור למרחב הסייבר הגלובלי.

לאחר זיהוי הצמתים, על המדינה להעסיק ספקי צד שלישי שיהיו אחראים על בקרת האיכות של נותני שירותים קריטיים אלה. בפסקאות הבאות יובאו העקרונות עליהם נשען מודל זה, ייסקר האופן בו יש לזהות צמתים כאלה במשק, ויפורט כיצד על המדינה להתערב ביישומו.

זיהוי צמתים בעלי השפעה במשק: שרשראות האספקה ודוגמאות נוספות

בעולם אבטחת המידע קיימת חולשת אבטחה הנקראת Class Break, העלולה לפגוע לא רק במערכת אחת, אלא במכלול מערכות המכילות חולשה זו. דוגמאות לכך הן חולשה במערכת הפעלה המשמשת משתמשים רבים ומערכות שונות, או פגיעה במצלמות מסוג מסויים הנמצאות בתפוצה נרחבת ודרכן ניתן להפיל אתרים רבים (כפי שהיה בתקיפת ספק האינטרנט Dyn בארצות הברית באוקטובר 2016).

Class Break אינו מושג חדש בתחום ניהול הסיכונים. שטפונות ורעידות אדמה הם דוגמאות מהעולם הפיזי לסיכונים הפוגעים באופן בלתי מובחן בתשתיות ובבני אדם רבים. סיכונים אלה מהווים בדרך כלל סייגים בפוליסות של חברות הביטוח, שאינן מעוניינות להתמודד עם נזק רב ממדים המתרחש בו־זמנית במערכות רבות. תוקפים בעולם הסייבר מחפשים את נקודות החולשה באבטחה כדי לנצלן שוב ושוב, במיוחד כשתקיפה דרך נקודת חולשה אחת ובאמצעות כלי אחד מאפשרת לתקוף מִנעד רחב של מערכות. יש אפוא לזהות את אותם Class Breakers מבעוד מועד גם בתחום הרגולציה בסייבר.

אחת הדוגמאות המובהקות ביותר לנקודות תורפה בעלות פוטנציאל השפעה על כלל המשק מתייחסת לשרשראות האספקה של נותני שירותים. שרשראות האספקה הן קבוצת משאבים ותהליכים הקשורה לספקים, רוכשים וקבלני ביצוע הדרושים לתהליך הפיתוח, הייצור, הטיפול והמשלוח של מוצרים ושירותים לרוכשים שונים.[189] ניתן לפגוע במערכת באמצעות שרשרת האספקה בכל שלב ומקום במחזור החיים שלה, וההגנה עליה הופכת למורכבת יותר ויותר. הספקים השונים, עליהם נשענים ארגונים רבים לצורך פעולתם, עשויים לא לעמוד בדרישות ההגנה המחייבות את הארגון המקבל את שירותיהם. יתרה מכך, הארגון עשוי לא לקחת בחשבון אותם ספקים בתכנון ניהול הסיכונים שלו.

189 רם לוי ועמי רוחקס דומבה, "שרשרת האספקה – איום הסייבר השקט", *IsraelDefense*, 19 בפברואר, 2014.

על פי דוח של OECD משנת 2013,[190] למעלה ממחצית המוצרים בעולם משמשים לייצור מוצרים אחרים. זהו נתון שמעיד על הפיצול הנרחב בשרשראות הייצור בעולם כתוצאה מההתקדמות הטכנולוגית ומהגלובליזציה של השווקים, וטומן בחובו סיכונים לספקי שירותים ברחבי העולם. לשרשראות אספקה יש מאפיינים שמקשים מאוד על הגנתן ונותנים יתרון לתוקף: הן מורכבות, מפוזרות ברחבי העולם, מחוברות ביניהן (interconnected), ארוכות וכוללות חוליות לוגיות רבות, מסלוליהן אינם קבועים והן כוללות שכבות שונות של מיקור חוץ. משמעותם של מאפיינים אלה מבחינתו של המגן היא קושי להבין את המרכיבים המשמשים בכל מערכת ובכל תת־מערכת, ביחד ולחוד. זאת ועוד, בשוק העבודה הגלובלי של ימינו, ייתכן שרכיבים שונים של אותו מוצר ייוצרו במספר מדינות ויורכבו במוקדים שונים, מצב המגדיל את מספר נקודות התורפה בשרשרת האספקה והופך התקפות סייבר עליהן לכדאיות במיוחד עבור התוקפים.

חברת "מיקרוסופט" חשפה בשנת 2017 תקיפה שעשתה שימוש בשרשרת האספקה לצורך התקפת יעדים במגזר הפיננסי. התקיפה השתמשה בעדכון של תוכנה צד ג', שמערך העדכון שלה נפרץ על ידי התוקפים, כדי להשיג בדרך זו נגישות למחשבים המותקפים.[191]

ההסתמכות על שרשראות האספקה טומנת בחובה שני איומים מרכזיים. הראשון – ירידה בפונקציונליות כתוצאה מהקושי לוודא את איכות ספקי השירות, החומרה והתוכנה; השני – פונקציונליות לא רצויה, כלומר החדרת קוד עוין לחומרה או לתוכנה במהלך הייצור, שינוצל כאשר החומרה או התוכנה יגיעו ליעד. אפשרות נוספת היא שימוש בתוכנה שפותחה ברמה נמוכה ומאפשרת ניצול חולשותיה. המורכבות הגדולה של ניתוח שרשרת האספקה גורמת לכך שגילוי או ניצול חולשות בתוכה עלולים לארוך זמן רב. לפיכך, נדרש מיפוי מבעוד מועד, בחסות המדינה, של נותני השירותים וקבלני המשנה המרכזיים, תוך סיווגם לקטגוריות שונות בהתאם לרמות האבטחה אליהן הם יכולים להתחייב. מודל קיים בנושא זה ניתן למצוא בדרישות המדינה מקבלנים: לכל קבלן יש סיווג הנקבע באחריות המדינה, ומי שמאשר את הסיווג הוא רשם במשרד הבינוי והשיכון.[192] יש לקבוע סיווג כזה גם עבור נותני שירותים וחוליות בשרשרת האספקה של ארגונים, וזאת בהתאם לפוטנציאל הנזק של הארגון המפוקח לביטחון

190 OECD, "Interconnected Economies: Benefiting From Global Value Chains – Synthesis Report", OECD, https://www.oecd.org/sti/ind/interconnected-economies-GVCs-synthesis.pdf

191 לפרטי התקיפה ראו דיווח של מערך הסייבר הלאומי מ־9 במאי 2017: https://www.gov.il/he/departments/publications/reports/micro_finance

192 ראו: מדינת ישראל, "תקנות רישום קבלנים לעבודות הנדסה בנאיות (סיווג קבלנים רשומים)", 1988.

הלאומי. קביעת תו תקן כזה תביא לסיווגם של נותני השירותים המרכזיים במשק בהתאם לרמת האבטחה שלהם, דבר שיסייע לארגונים מקבלי השירות לנהל את סיכוני הסייבר הנובעים מההתקשרות עימם. יצירת שלושה־ארבעה מִדרגים לספקי המשנה תאפשר לכל ארגון לקבוע בעצמו את קבלני המשנה שאיתם יעבוד. בנוסף, יצירת המדרג תאפשר לחייב ארגונים להעסיק קבלני משנה בהתאם לתחום העיסוק של אותם ארגונים.

מעֵבר להסדרת השירותים השונים במשק על בסיס סיווג רמת ההגנה שלהם, ישנם תחומים מרכזיים נוספים בהם המדינה יכולה להתערב כדי להגביר את החוסן הלאומי. כזאת היא, למשל, התערבות אפשרית מול מטמיעי אבטחת מידע – אינטגרטורים הפועלים בחברות, שתפקידם הוא לשלב בין טכנולוגיות מידע ובין הגנה על מידע בארגונים גדולים, ובכך הם חולשים על אבטחת המידע במרבית המשק. כישלון במימוש מדיניות אבטחה, או התקנת מוצר אבטחה באופן לא מיטבי, יובילו לכשל אבטחתי "מתגלגל" ולפגיעה משמעותית במרחב הסייבר הישראלי. המודל מציע התערבות מדינתית כדי לוודא את איכותם של האינטגרטורים, מתוך הנחה שחיזוקם יביא לחיזוק מרחב הסייבר הישראלי כולו.

דוגמה נוספת ניתן לראות בספקיות האינטרנט, המהוות את הצומת שדרכו גולשים כל המשתמשים ברשת האינטרנט במדינת ישראל. הספקיות מנקזות לתוכָן גם את מרבית התעבורה בעולם הסייבר וגם את המתקפות וניסיונות ההתגוננות נגדם. העלאה של רמת האבטחה בקרב הספקיות תביא מניעת תקיפות מבעוד מועד. יש לישראל יכולות הגנה מתקדמות שאינן מיושמות בשוק ספקיות האינטרנט. קביעת כללים להגנה נאותה על הספקיות, באופן שאינו פוגע בפרטיות לקוחותיהן, היא צעד חשוב לחיזוק מרחב הסייבר הישראלי.

עוד צומת מרכזי במרחב הסייבר בישראל הוא ספקי האירוח (hosting) של שרתי Web. מדובר בחברות המספקות חוות אירוח, שעל שרתיהן נמצאים אתרי אינטרנט רבים המשרתים את האזרחים במדינה. חוות שרתים אלו מרכזות לתוכן אתרי אינטרנט רבים, וכשל באבטחתן עלול להוביל לכשל אבטחתי במספר רב של אתרים. על אף מרכזיותן, חוות שרתים אלו מאובטחות כיום על בסיס החלטה של החברות המארחות בלבד. חסרה שקיפות לגבי האופן בו חוות אלו מאובטחות, אין מדרג המייצג רמות אבטחה שונות הניתנות באמצעותן ללקוחות, ונקודת תורפה זו מטופלת, ככלל, על אף מרכזיותה, באופן בלתי מספק. גיבוש תקנים לאירוח אתרי אינטרנט יגביר משמעותית את חוסנם ויצמצם את יכולתם של גורמים עוינים לנצל חולשות כדי לפגוע באזרחים.

התערבות מדינתית בעוגנים בעלי השפעה במשק

לאחר זיהוי עוגנים קריטיים בעלי השפעה על כלל המשק, המדינה צריכה לסווגם לקטגוריות עיקריות ולוודא קיום תמיכה ובקרת איכות של השירותים הניתנים על ידי ספקים אלה. ההתערבות המדינתית תיעשה הן על ידי שיתוף פעולה בין־לאומי עם ארגוני תקינה רלוונטיים, הן על ידי הרגולטור המגזרי והן על ידי ספקי צד שלישי שביכולתם לוודא את איכות השירות המוצעת, הכל בהתאם לשירות המפוקח. כך, למשל, אינטגרטורים ותומכי מערכות מידע יצטרכו לעבור מבדקי הכשרה והסמכה תקופתיים בפיקוח המדינה כדי להיות מעודכנים באיומים המתחדשים ובמוצרי ההגנה המתקדמים. בחינות הכשרה והסמכה כאלו יכולות להיעשות על פי התקנים הקיימים של ISO או ISACA, המתעדכנים מעת לעת.

דוגמה נוספת להתערבות מדינתית הן מערכות קריטיות שיש להן דומיננטיות רבה במגזר מסויים, כגון מערכות כספומט, ניהול חשבונות בנק וסליקת תשלומים. מערכות אלו ייבחנו על סמך תקנים של גופי תקינה בין־לאומיים, כמו מכון התקנים של ארצות הברית, וזאת על פי התקן המתקדם ביותר ובהתאם לידע הנצבר על התקפות סייבר קודמות על מערכות כאלו.

הרגולטור המגזרי ייקח גם הוא חלק במאמץ זה. כך, לדוגמה, כשמדובר במערכות שיתוף מידע מתחום הביטוח, במערכות המשמשות למסחר בניירות ערך על ידי גופים רבים במשק או במערכות שכר, הרגולטור המגזרי יבחן את המערכות המקבילות להן בעולם, ויעסיק לפי הצורך ספקי צד שלישי כדי לוודא את אבטחתן של המערכות הישראליות. באופן זה, תבחר המדינה את המקומות הרגישים במגזרים השונים, בהם עליה לוודא רמת הגנת סייבר ראויה, וזאת מבלי לגלוש לרגולציה קבועה על כלל המגזרים במשק.

אחד החסרונות הבולטים במודל זה הוא יצירת מעמד של "מנצחים". לפי המודל, המדינה בוחרת באופן סלקטיבי להבטיח את איכותן של המערכות שכבר נהנות מדריסת רגל משמעותית במשק, ובכך היא עלולה להפלות את המתחרים. יחד עם זאת, ערך התחרותיות הוא משני בחשיבותו לרציפות התפקודית ולסכנה הנשקפת לביטחון הלאומי כתוצאה מפגיעה במערכות שנבחרו על ידי המדינה. לפיכך, יתרונותיו של המודל המוצע גוברים על חסרונותיו בסוגיה זו.

רגולציה על בסיס תמריצים

ביטוח אירועי סייבר על בסיס חובת דיווח

כניסת חברות הביטוח לשוק הגנת הסייבר תהווה תמריץ לחברות בשוק להגן על עצמן מצד אחד ולחברות הביטוח להוזיל את פוליסות הביטוח שלהן מצד שני. יחד עם זאת, בניית שוק ביטוח משגשג מחייבת להתבסס על מודלים סטטיסטיים הנשענים

על מידע אקטוארי הנוגע לאירועי סייבר ולסיכונים בפועל. על כן, הקמת שוק ביטוח כזה כרוכה בהנחיות מחייבות לשקיפות באירועי סייבר, או לכל הפחות ליצירת מאגר מידע אקטוארי ראוי עבור חברות הביטוח. במדינת ישראל אין כיום הנחיות שקיפות כאלו, והדבר מונע משוק הביטוח להתפתח בתחום הסייבר באופן שיסייע לכלל המשק.

אירועי סייבר בישראל אינם מעוגנים בחובת דיווח, למעט במקרים של פריצות למאגרי מידע. תקיפות לגניבת שמות משתמשים, ריגול או דרישות כופר לא חייבות בדיווח. התדירות הנמוכה של דיווחים על פגיעות סייבר בחברות ישראליות, לעומת תדירות הדיווחים על פגיעות כאלו ברחבי העולם, מובילה למסקנה כי מרבית אירועי הסייבר בישראל אינם מדווחים ונשארים בין כותלי הארגונים. ממסמכי הרשות הלאומית להגנת הסייבר[193] ניתן ללמוד כי בשנת 2017 עמד ממוצע החדירות לארגונים בישראל על כמאה בחודש. מספרים אלה אינם עולים בקנה אחד עם המדווח לציבור ומלמדים על היעדר שקיפות בתחום זה. יתר על כן, גם אם מערך הסייבר הלאומי מקבל מידע על פריצת סייבר לחברה מסויימת, אין לו סמכות לכפות חקירה או אכיפה, כפי שיש למשטרת ישראל.[194]

ההשלכות של היעדר שקיפות ציבורית על חוסנו של מרחב הסייבר בישראל הן משמעותיות. חברות וארגונים שאינם חייבים בדיווח בוחרים במדיניות של שמירה על סודיות בעת אירוע סייבר ומעריכים שבדרך זו מוניטין החברה לא ייפגע. היעדר שקיפות ציבורית גם מקשה, כאמור, על חברות הביטוח לאגור מידע אקטוארי שישמש לתמחור פוליסות ביטוח בתחום הגנת הסייבר. קיומו של שוק ביטוח בסייבר יאפשר לשחקנים כבדי משקל, כמו חברות הביטוח, להצטרף לבעלי האינטרסים בהגנה על הארגונים השונים. כמו שוק הרכב, בו חברות הביטוח עודדו התקנת אמצעי בטיחות ומיגון, כך ארגונים שונים שירצו לבטח עצמם נגד אירועי סייבר יידרשו לנקוט צעדים משפרי הגנה אותם בחרו שלא לנקוט לפני כן.

המודל המוצע מבקש לחייב שקיפות ציבורית בעת אירועי סייבר מסֵדר גודל בינוני ומעלה, ובדרך זו לעודד את שוק הביטוח בסייבר. הדיווח לא חייב לבוא במקביל לתהליך ההתמודדות עם האירוע, אך לאחר שהאירוע מוגר ברמה סבירה, יש לדווח עליו בפרטי פרטים לציבור דרך אמצעי התקשורת. דיווח כזה צריך לכלול תובנות על אפיק החדירה שנבחר ועל הנזק שנגרם (אם נגרם) לפרטיות הלקוחות. חובת הדיווח צריכה להיות מלווה בפיצויים מתאימים על אובדן מידע או פגיעה בפרטיות כתוצאה מאירוע הסייבר המדובר. במקביל, על המפקח על הביטוח ושוק ההון לגבש פוליסת

193 הרשות הלאומית להגנת הסייבר, "סיכום שנות ההקמה 2016-2017", הרשות הלאומית להגנת הסייבר, 2018, https://www.gov.il/he/Departments/news/summary

194 רפאל קהאן, "האקר: נסתדר לבד: התעשייה בארץ לא סומכת על מערך הסייבר", **כלכליסט**, 28 ביוני 2017, https://www.calcalist.co.il/internet/articles/0,7340,L-3716104,00.html

ביטוח סייבר אחודה לחברות הביטוח השונות, שתאפשר גם לבעלי עסקים קטנים ובינוניים לרכוש פוליסה לפיצוי לקוחותיהם במקרה של אירוע סייבר.

חובת הדיווח והקמת שוק ביטוח פעיל גם עבור עסקים קטנים ובינוניים יגדילו משמעותית את התמריצים של ארגונים להתמגנות בסייבר. כאשר המוניטין העיסקי נמצא על כף המאזניים, וחברות עם גב כלכלי איתן, כמו חברות הביטוח, שותפות לאינטרסים להגן מפני התקפות סייבר, חוסנו של מרחב הסייבר הישראלי צפוי לגדול. ראוי לציין בהקשר זה כי מערך הסייבר הלאומי בוחן אפיקי פעולה לגישור על הפערים בתחום ביטוח הסייבר ולסיוע בבניית שוק ביטוח הסייבר במדינת ישראל.

הקלות מס להגנה בסייבר

רכישה של מוצרי הגנה בסייבר כרוכה בעלויות גבוהות. חברות מתעדפות מוצרי הגנה מסויימים על פני אחרים לא מעט משיקולי עלות. על המדינה ורשות המיסים לעודד רכישה של מוצרי הגנה בסייבר על ידי מתן הקלות מס והוזלת המוצרים לארגונים. הקלות המס יינתנו על פי אמצעי ההגנה הקיימים בארגונים השונים, באופן שיאפשר להם ליצור הגנה רב־שכבתית. למשל, ארגונים שברשותם מוצרים להגנה רשתית, אך אין להם פתרון לתחנות הקצה, יזכו להקלות ברכישת מוצרי קצה, אך לא יהיו זכאים להקלות מס כשהדבר נוגע להגנה רשתית. כלומר, תמונת ההגנה בחברות תהיה מדווחת לרשויות המס, כדי שאלו יוכלו לדעת באילו תחומים לסייע לאותן חברות במתן תמריצים בדמות הקלות במס.

שיתוף מידע פנים־מגזרי ובין־מגזרי לצורכי הגנת סייבר

שיתוף מידע במרחב הסייבר הינו תחום מתפתח במדינת ישראל. מערך הסייבר הלאומי פועל, יחד עם משרדי הממשלה השונים, להקמת מרכזי בקרה וניהול אירועים מגזריים שישפרו את מנגוני התפעול וקבלת ההחלטות ויתרמו בכך להגברת החוסן הלאומי. יחד עם זאת, שיתוף מידע בשגרה מתרחש לרוב דרך צד שלישי – הרגולטור המגזרי – ולא ישירות בין הארגונים השונים השייכים לאותו מגזר ומתחרים ביניהם.

החשיבות של שיתוף מידע להגנת הסייבר היא גדולה. שיתוף מידע כזה הינו אחד מעקרונות ההגנה האסטרטגיים ומטרתו היא להגביר את החוסן הכולל במרחב הסייבר.[195] שיתוף מידע לצורכי הגנה כולל מידע על חולשות סייבר קיימות, אופני תקיפה ואיומים קונקרטיים במרחב, זיהוי גורמים מתקיפים וניסיונות להערכת המניע שמאחורי התקיפות. מטרת השיתוף הינה, בראש ובראשונה, למנוע את התפשטות

195 גבי סיבוני והדס קליין, "אתגרי שיתוף מידע בסביבה פנים מגזרית", **צבא ואסטרטגיה,** כרך 8, גיליון 1, יולי 2016.

האיום, ולכן הוא נעשה, בדרך כלל, על בסיס פנים־מגזרי, אם כי גם לשיתוף בין־מגזרי עשוי להיות ערך רב בחיזוק ההגנה במרחב הסייבר.

היתרונות בפרקטיקות של שיתוף מידע נעוצים בעובדה כי הן שופכות אור על כל מחזור חייה של מתקפת סייבר – מן השלבים המוקדמים של איסוף המודיעין ועד לשלב המעשי של שימוש בכלי תקיפה. שיתוף מידע מאפשר לעדכן ולחדד מנגנוני הרתעה, להעשיר את מאמצי המניעה, לשפר את מאמצי גילוי המתקפות וליצור תגובה טובה יותר, תוך למידה מאחרים. למרות זאת, שיתוף מידע אינו פרקטיקה המאומצת באופן נרחב על ידי חברות מסחריות ויישויות מדינתיות. חברות מתחרות חוששות לשתף פעולה מתוך אינטרסים עיסקיים, בעוד שמדינות אינן ששות לשתף מידע מודיעיני רב ערך, בין השאר מתוך רצון לשמור על יתרונן היחסי.

מחקרים מראים כי החשש של חברות מקבלת מידע באיכות ירודה ומפגיעה במוניטין שלהן כתוצאה מחשיפת העובדה שהותקפו, וכן החשש שהדבר יועיל למתחריהן, מונעים מאותן חברות להישען באופן עקבי על פרקטיקות שיתוף המידע. בעיות נוספות, אינהרנטיות לשיתוף מידע על ידי שחקנים רבים, הן היעדר הדדיות ומצב שבו מתחרים משתמשים במידע שקיבלו לתועלתם, בעוד שהם עצמם אינם תורמים מידע משלהם.

כל מודל של שיתוף מידע כולל בתוכו יצרני מידע וצרכני מידע. במסגרת המודל המוצע, שיתוף מידע אפקטיבי במרחב הסייבר יתבצע דרך מנהלה מרכזית שתנהל את הפצת המידע ליתר הצרכנים. הקמת מרכז מידע לשיתוף תאפשר לרַכז את קבלת ההחלטות מעֵבר לאינטרסים העיסקיים בכל מגזר, ובכך לקדם את הגנת הסייבר כאינטרס ראשון במעלה. דוגמה לכך ניתן לראות בנעשה בין חברות המספקות שירותי הגנת סייבר על רבדיה השונים – מהגנה על תחנות קצה, דרך הגנה על רשתות ועד מוצרי ניטור ובקרה. מסדי הנתונים עליהם נשענות החברות המספקות הגנת סייבר הם חומר הגלם העומד בליבת המוצר שהן מייצרות. שיתוף מידע כזה בין אותן חברות ישפר משמעותית את כל מוצרי ההגנה בסייבר, אך מצד שני הוא עלול לחזק שחקן אחד על חשבון האחר.

חסם נוסף לשיתוף מידע, שקיים במגזר הפרטי, אך ביתר שאת במגזר הציבורי, הוא הרצון להחזיק בידע, ועל ידי כך להיות גורם משמעותי בתהליך קבלת ההחלטות. סוגיות של ריבונות על מידע, התקבעות על תרבות ארגונית מסויימת, אסימטריה בין משתפי המידע והיעדר תמריצים לשיתוף מוֹנעות מארגונים במגזר הפרטי והציבורי לשתף מידע בנוגע לאיומי סייבר.

ארצות הברית פעלה ועודנה פועלת וביתר שאת, כדי לעודד שיתוף מידע בין המגזרים השונים. המשרד לביטחון המולדת הקים אחרי פיגועי 11 בספטמבר 2001 פורומים לשיתופי ידע (Information Sharing and Analysis Centers – ISACs) במגזרים השונים, אליהם מצטרפים ארגונים מתוך הבנה כי שיתוף ידע הוא מרכיב הכרחי בביטחון

הלאומי. פורומים אלה נתמכים טכנולוגית וכלכלית על ידי המדינה ומאפשרים שיתוף ידע בדרך נוחה יחסית, במיוחד כאשר המהות העיסקית של החברות אינה נמצאת בתחום הסייבר.

מערך הסייבר הלאומי בישראל עוסק בפתיחת צווארי בקבוק בתחום זה, ובמיוחד בחשיבות העלאתן של רמות שיתוף הידע בין השחקנים השונים. העיקרון המנחה בפעילות המערך הוא הקמת פורום שיתופי, בראשותו של יושב ראש מערך הסייבר הלאומי, שיטפל באירועי הסייבר שיוגדרו כמשמעותיים ויכריע בסוגיות שעולות בין פורומים אחרים לשיתוף ידע. מיזם נוסף של מערך הסייבר הלאומי הוא יצירת מכניזמים לשיתוף פעולה במגזר הפיננסי או במגזר האנרגיה, וזאת באמצעות שיתוף פעולה ומעורבות של כל השחקנים הרלוונטיים. כדי לעודד שיתוף מידע מסוג זה, המודל מציע תמריצים שיאפשרו להרחיב את הקיים.

פרק ה׳: המלצות ליישום המודל המוצע

האתגרים הכרוכים ביישום מודל הרגולציה המוצע הם רבים. הם נובעים מהקושי לשנות מערכות והסדרי פעולה קיימים, מההתנגשות בין אינטרסים שונים בעיצוב מדיניות ציבורית בתחום זה וממבנים מוסדיים ותיקים המתנגדים לשינוי ובנייה מחדש. כל גוף מעוניין בשליטה על אופן הפיקוח, כאשר הנחייה במרחב הסייבר משמעותה כוח והשפעה רבים במשק. סביר להניח כי גופים קיימים יתקשו להשלים עם כללי משחק חדשים הבאים לשנות את המערכת הקיימת.

בנוסף לכך, לכל גוף מפקח יש אינטרסים שונים, במסגרתם הוא מעוניין להיות בעל סמכות בקבלת החלטות בנושאי הגנת הסייבר. האינטרסים הללו לרוב מתלכדים ויוצרים מאבקי כוח איתם והפעלת לחצים עליהם כדי שיעצבו מדיניות ציבורית בכיוון מסויים. המוסדות והסדרי הפעולה המדוברים במודל, כגון חוק רישוי עסקים, הם מוסדות והסדרי פעולה הקיימים זמן רב, אך אינם אפקטיביים מספיק. יישום המודל המוצע יקנה להם כוח וסמכות נוספים שאינם קיימים אצלם כיום.

פרק זה מפרט המלצות ליישום המודל המוצע לרגולציה בסייבר. ההמלצות מחולקות על פי השכבות השונות של המודל – רגולציה עצמית, רגולציה מחייבת ורגולציה מבוססת תמריצים – מתוך כוונה להצביע על צעדים קונקרטיים שיאפשרו למקבלי ההחלטות הטמעה מוצלחת של ההנחיות החדשות. חשוב לציין כי כל ההמלצות הן חדשות ואינן בשימוש במשק הישראלי.

מודל רגולציה עצמית

המלצה: לבחון את הצורך לפתח גוף ביקורת מקצועי ועצמאי במערך הסייבר הלאומי, שיפעל מול גופים הפועלים כיום במסגרת רגולציה עצמית (ארגוני הביטחון, צה"ל, משטרת ישראל וכדומה).

ראוי שגופים אלה יהיו חשופים לידע ההגנתי המתפתח במערך הסייבר ובשוק האזרחי. מוצע להקים גוף ייעודי שיסייע בשיתוף הידע ובהנחלת גישות הגנה מתקדמות לגופים אלה. גוף ייעודי זה יעסיק את מיטב המומחים ויהווה את זרוע שיתוף הידע של מערך הסייבר הלאומי, אשר יפעל באופן דיסקרטי מול גופים רגישים ויאפשר להם לוודא את איכות הגנת הסייבר במערכותיהם. המלצה זו תקפה גם בהקשר לפעולת המלמ"ב, שיוכל בדרך זאת ליהנות מפיתוח הידע במערך הסייבר ובמגזר האזרחי.

מודל רגולציה מחייבת

מודל הרגולציה המחייבת מתחלק למספר מרכיבים, כאשר לכל מרכיב ניתנות המלצות ייעודיות קונקרטיות.

רגולציה מחייבת דרך רגולטורים מגזריים

המלצה: גיבוש פורום במערך הסייבר הלאומי, אשר יאפשר קבלת תמונה רוחבית של הטכניקות הרגולטוריות באמצעותן בוחרים משרדי הממשלה והרשויות לפקח על הגנת הסייבר במגזרים שבתחום אחריותם.

סקירת הספרות הבחינה במגוון של טכניקות רגולציה להנחייה ולפיקוח על מגזרים שונים במשק על ידי משרדי הממשלה והרשויות. ההנחיה והפיקוח יבוצעו דרך חוזרי מנכ"ל והוצאת הנחיות מחייבות (של בנק ישראל, הרשות לשוק ההון), באמצעות מתווכים רגולטוריים בדמות חברות פרטיות (תחום האנרגיה), או בהקמת אגף ייעודי למתן מענה עבור הגופים המפוקחים (משרד הבריאות). כל אלו הן טכניקות רגולטוריות ראויות, אך מומלץ כי גוף ייעודי ביחידה להגנת הסייבר בממשלה יהיה בקדמת הידע באשר לאיכות ולרלוונטיות של רכיבי ההנחייה השונים בהם נעשה שימוש במשרדי הממשלה, וזאת לצורך יצירת הפריה הדדית וקידום המאמץ הרגולטורי הכולל.

רגולציה מחייבת במתן רשיון עסק

רכיב זה בהמלצות הינו אחד המרכיבים המרכזיים בפיתוח הרגולציה להגנת הסייבר במדינת ישראל. ליישום חלק זה לא נדרשת חקיקה מיוחדת, אלא ניתן לעשות שימוש בחוק רישוי עסקים הקיים (כך גם עולה מפסק הדין של השופט חשין בתביעת המדינה נגד חברת "תנובה").[196] ייתכן שניתן יהיה להסתפק בהחלטת ממשלה שתחיל את חוק רישוי עסקים גם על נושא הגנת הסייבר, בהתאם למודל המוצע בחיבור זה. בהקשר זה מוצעות מספר המלצות קונקרטיות כמפורט להלן:

המלצה: הגברת האכיפה במשרדי הכלכלה והפנים לצורך שיפור הציות לחוק רישוי עסקים במדינת ישראל.

המודל המוצע, הנשען על חוק רישוי עסקים כמנגנון סטטוטורי מחייב, יפעל כראוי רק על ידי חיזוק הסמכות לאכיפתו ושיפור הציות לו. לשם כך, מוצע להסמיך יישות אחת, לאכוף את החוק ביתר שאת וליצור מאזן הרתעה כלפי חברות ועסקים פרטיים הפועלים ללא רשיון. כאשר חוק רישוי עסקים יהפוך לכלי מחייב הנאכף על כלל המשק באופן שיוויוני, יוכל התהליך השיטתי המוצע להפיק את מלוא הפוטנציאל שבו.

המלצה: הקמת זרוע ביצוע במערך הסייבר הלאומי שתקיים פיקוח על תסקירי עמידות קיברנטית בכלל המשק.

---

196 רשות ערעור פלילי (רע"פ) 4270/03, מדינת ישראל נגד תנובה.

מערך הסייבר הלאומי יפתח ידע על האופן בו יש למלא שאלון ותסקיר עמידות קיברנטית, וזאת בהתאם להתפתחות הידע בישראל ובעולם. התסקירים יצטרכו לכלול מענה לכלל האיומים המשתנים במרחב הסייבר, כדי להמשיך להיות רלוונטיים עבור עסקים חדשים, לבל יהפכו לנטל על התעשייה.

המלצה: קידום תקינת מקצועות הסייבר.

מאחר ושימוש בשאלון ובתסקיר עמידות קיברנטית יעלה את הדרישה למומחים וליועצים בתחום הסייבר, מומלץ לקדם את התקינה של מקצועות הסייבר השונים ולשים דגש מיוחד על יכולתם של יועצים לספק מענה בדמות תסקיר עמידות קיברנטית, באופן שיקיף את כלל סיכוני הסייבר שעלולים להיווצר כתוצאה מפעילות הארגון וממשקיו. יועץ קיברנטי יקבל הסמכה רשמית מן המדינה, אותה הוא יצטרך לתקף מדי שנה כדי להישאר מעודכן באיומים ובאופן ביצוע התסקירים במקומות שונים בעולם.

רגולציה של צמתים חיוניים לשיפור החוסן הלאומי בסייבר

המלצה: להקים פורום משותף למערך הסייבר הלאומי, ליחידה להגנת הסייבר בממשלה (יה"ב) ולמובילים טכנולוגיים במשק לצורך זיהוי, ניתוח והגנה על צמתים חיוניים במטרה לחזק את החוסן הלאומי.

התערבות מדינתית בצמתים מרכזיים לצורך שיפור חוסנו של מרחב הסייבר מחייבת מיפוי ברור של כלל התשתיות המרכזיות במשק ושל האופן בו התערבות נקודתית עשויה להועיל או לשבש את פעולות השוק. מיפוי כזה דורש ידע טכנולוגי והכרת ההתנהלות הטכנולוגית במשק הישראלי באופן חוצה מגזרים. פורום משותף של מערך הסייבר הלאומי, יה"ב והמגזר הפרטי יספק, מצד אחד, ידע טכנולוגי ומצד שני הכרה אינטימית עם משרדי הממשלה, המגזרים המפוקחים והנעשה במשק בכלל. לאחר זיהוי העוגנים במרחב, מומלץ לפעול לסקירה של הנעשה בעולם בתעשיות מקבילות, תוך זיהוי הניתן ללמוד מהן ובכלל זה כיצד להגן טוב יותר על עוגנים אלה.

רגולציה מבוססת תמריצים

עידוד ביטוח עבור אירועי סייבר על בסיס חובת דיווח

המלצה: קידום חוק המחייב את כלל המשק בדיווח בעת תקיפת סייבר משמעותית.

החוק המוצע יגדיר קריטריונים ברורים לתקיפת סייבר "משמעותית". זאת, בהתבסס על כמות המידע שנגנב ורגישותו, ועל השאלה האם ובאיזו מידה היה מוצפן. החוק יחייב דיווח למערך הסייבר הלאומי, מתן פיצוי ללקוחות שנפגעו, ולאחר שהארגון יצא מכלל סכנה – גם דיווח לציבור הרחב. חוק כזה ימריץ ארגונים להגן על עצמם מבעוד מועד בשל המוניטין שלהם שיהיה מונח בכף, וכן יספק מידע אקטוארי שוטף לחברות הביטוח, אשר יסייע להן לתמחר ולספק פוליסת ביטוח ארגונית לפגיעות סייבר.

המלצה: הקצאת תקציב ממשלתי ייעודי עבור הרשות לשוק ההון, ביטוח וחיסכון, לצורך מתן ערבות מדינתית לחברות הביטוח במקרה של אירוע סייבר רחב היקף.

המדינה צריכה לספק ערבות לחברות הביטוח במקרה של אירוע סייבר בקנה מידה גדול מאוד כדי לעודד אותן לספק פוליסות נגד התקפות סייבר במחירים תחרותיים. הקצאת תקציב ייעודי לכך תאפשר לקבוע קריטריונים ברורים לגבי אירוע סייבר המאפשרים לחברות הביטוח שימוש בערבות הממשלתית לצורך מתן פיצוי לארגונים שנפגעו מאירוע כזה. הערבות המדינתית תקטין את הסיכון שבהנפקת פוליסת סייבר במשק וצפוייה לתמרץ את חברות הביטוח לעסוק בתחום זה.

הקלות מס להגנה בסייבר

המלצה: הממשלה תבחן את האפשרות למתן הקלות מס עבור הטמעת הגנת סייבר ברמה ראויה.

משרד האוצר יבצע חשיבה על אפשרות קידומן של הטבות מס לחברות במשק בעבור הטמעתה של הגנת סייבר ברמה ראויה. המשרד יגדיר את הקריטריונים למתן ההטבות על בסיס רמת ההגנה של הארגון והיקף פעילותו במשק. ככל שהיקף הפעילות יהיה רחב יותר וההגנה ראויה יותר, כך ההטבה תהיה משמעותית יותר.

המלצה: הקמת יחידת סייבר ייעודית ברשות המיסים.

יחידת הסייבר שתוקם ברשות המיסים תהיה בעלת יכולת לבחון ולדרג את רמות ההגנה בארגונים המבקשים לקבל הקלות מס כתוצאה מיישום אמצעי הגנה בסייבר. התמקצעות רשות המיסים בתחום זה צפוייה ליצור תחרות בריאה בין חברות שונות על הזכות להקלות מס בתמורה להגנת סייבר, ובכך לתרום לחיזוק החוסן הלאומי במרחב זה.

שיתוף מידע פנים־מגזרי ובין־מגזרי לצורכי הגנת סייבר

המלצה: קידום חקיקה למתן פטור מאחריות במקרה של פגיעת סייבר ופטור מעמידה ברגולציית הגבלים עיסקיים כתוצאה משיתוף ידע בין־ארגוני על איומים במרחב הסייבר.

חקיקה כזאת, בדומה לחקיקה שהתקבלה בארצות הברית בדצמבר 2015, תעודד שיתוף מידע במטרה לאפשר הגנה פרו־אקטיבית נגד איומי סייבר. בנוסף למאמצים הנוכחיים להקמת מרכזים לשיתוף מידע מגזרי, חקיקה כזו תאפשר לקבל "תמונת־על" של איומי הסייבר במשק הישראלי בכל רגע נתון. לחברות יהיה אינטרס לשתף מידע רב ככל הניתן כדי לזכות בפטור מאחריות במקרה של אירוע סייבר שהתרחש לאחר שננקטו אמצעי ההגנה כתוצאה מניתוח האיומים ששותפו.

סיכום

סקירה וניתוח של הנעשה בעולם ובישראל סביב המאמצים לחיזוק הגנת הסייבר מלמדים כי אסדרת מרחב זה מתרחבת ומתעדכנת באופן תדיר. מרכזיותו של מרחב הסייבר בחברה המודרנית, יחד עם אתגרי הביטחון שהוא מזמן, הביאו מדינות רבות בעולם המערבי, כולל ישראל, להרחיב את פעילותן בנושא, להקצות לו משאבים רבים ולעדכן מבנים מוסדיים, כך שיתאימו להתמודדות עם האתגרים החדשים שהוא מציב. יחד עם זאת, המגזר העיסקי־אזרחי נותר ברובו לא מפוקח, והתמריצים הניתנים לו לחיזוק הגנת הסייבר אינם מקיפים או אטרקטיביים מספיק. כוחות השוק מעדיפים חדשנות ופיתוח טכנולוגי על פני אבטחת ושמירה על מידע, ומערכות הרגולציה המדינתיות אינן משכילות לשנות סטטוס־קוו זה.

מערכות מדיניות עוסקות בעשורים האחרונים באופן תדיר בניהול ובמיגור סיכונים עבור החברה בשלל תחומי חיים, כגון תחבורה, סביבה, פיננסים ובטיחות. לעומת זאת, טרם גובשה אסטרטגיה אפקטיבית להקטנה משמעותית של סיכוני הסייבר ולמניעת פגיעה שלהם בביטחון הלאומי. מודל הרגולציה המוצע במסמך זה מבקש להתמודד עם האתגר על ידי הצעת גישה אינטגרטיבית לטיפול בסיכוני סייבר בעלי פוטנציאל של פגיעה בביטחון הלאומי. המודל מתייחס אל מרחב הסייבר הישראלי כמכלול ומציע דרך סדורה לניהול סיכוני סייבר על פני המגזרים השונים בחברה, תוך שימוש במגוון כלי רגולציה – רגולציה עצמית, רגולציה מחייבת ורגולציה על בסיס תמריצים. החלוקה לשלושה סוגים של רגולציה נועדה לספק מענה רב־שכבתי לאתגר הרגולציה שמציב מרחב הסייבר.

הרגולציה העצמית, שבאמצעותה מפקחים על עצמם גופי הביטחון הרגישים במדינה, תהיה תחת פיקוח תקופתי של גורם חיצוני, שיוקם במערך הסייבר הלאומי כגוף ביקורת מקצועי ועצמאי. החלטת ממשלה ייעודית, אשר תחייב גופים הנתונים לרגולציה עצמית בלבד לעבור ביקורת חיצונית תקופתית, תאפשר פיקוח על האופן בו מגנים על עצמם גופי הביטחון הרגישים ביותר. האתגר במימוש פיקוח כזה הוא התנגדות אפשרית של גופים שאינם רגילים להיות נתונים לביקורת חיצונית. התנגדות כזאת עלולה להגביר את החיכוך המוסדי ולהוציא את העוקץ מפעולות הביקורת.

רגולציה מחייבת, הכוללת בעיקרה רגולציה על תשתיות קריטיות ומשרדי ממשלה וכן רגולציה מול המגזר העיסקי, תבוצע בשלושה אופנים:

1. הסתמכות על הרגולטור המגזרי המבצע הנחייה ופיקוח על המשק בתחום שיפוטו, תוך הקמת פורום שיפקח באופן רוחבי על האופנים השונים והטכניקות הרגולטוריות שעל פיהן מנחים משרדי ממשלה את המגזר הפרטי. האתגר המרכזי בהסתכלות רוחבית על רגולטורים מגזריים היא המורכבות שבפעילות כל אחד מהם. כל משרד ממשלתי צבר מומחיות בתחומו, והרצון להקים צוות־על שיפקח ויכווין את עבודתם של הרגולטורים המגזריים עלול להיתקל בקושי מול המשרדים הקיימים ובאתגר של גיוס הון אנושי בעל מומחיות מתאימה.
2. יצירת תהליך סטטוטורי חדש, באמצעות הכלי הקיים של חוק רישוי עסקים, לזיהוי פוטנציאל הנזק לביטחון הלאומי כתוצאה מפגיעת סייבר במגזר העיסקי במדינת ישראל. במסגרת זו יבוצע תסקיר עמידות קיברנטית למגזר הפרטי על סמך שאלון שיפרט את פוטנציאל הנזק הגלום בפעילותו של כל ארגון עיסקי. עריכת התסקיר תפוקח על ידי זרוע ביצועית במערך הסייבר הלאומי ותיתמך על ידי יועצים שיפעלו תחת תקינה מקצועית ויעברו הסמכה תקופתית. יועצים אלה יסייעו לארגונים במילוי התסקירים ובהתייחסות לכלל האיומים. האתגר בשימוש בחוק רישוי עסקים הינו מעמדו החלש של חוק זה בתרבות הרגולציה הישראלית: הוא נשחק רבות במהלך השנים, וכדי לעשות בו שימוש יעיל, יש לרכז את יישומו במשרד אחד – משרד הכלכלה – תוך הגברת האכיפה.
3. מיפוי צמתים מרכזיים במשק הישראלי שהם בעלי השפעה מכרעת על החוסן הלאומי, והתערבות מדינתית נקודתית להעלאת רמות ההגנה בצמתים אלה. האתגר בפעילות כזו הוא כפול: פעולת הזיהוי עלולה להיות מורכבת ודורשת הסתכלות רוחבית ועמוקה על המשק הישראלי; אופן ההתערבות עלול להיות כזה שיתעדף שחקנים בעלי אחיזה דומיננטית במשק וימנע תחרות מצד שחקנים אחרים השואפים לתפוס את מקומם. ההתערבות המדינתית תצטרך להיעשות במקרה זה ברגישות, תוך התחשבות בכל האינטרסים, ותוך שקיפות מוחלטת בנוגע לאופן ההתערבות והיתרון היחסי שהיא מעניקה לשחקנים דומיננטיים.

רגולציה מבוססת תמריצים נועדה להניע את כוחות השוק להשקיע יותר בהגנת סייבר. רגולציה זו מתבססת על המרכיבים הבאים:

1. הקמת שוק ביטוח סייבר, תוך העברת חוק המחייב דיווח ושקיפות על תקיפות סייבר בארגונים והקצאת תקציב ממשלתי לרשות שוק ההון לצורך מתן ערבויות לחברות הביטוח שיפעלו במשק, למקרה של אירוע סייבר בסדר גודל חריג. האתגר הטמון במרכיב זה הוא הקושי של חברות לעמוד בחובת הדיווח, בין השאר מהחשש לפגיעה במוניטין של החברה. אי־הודאה של חברות בתקיפות סייבר שהתרחשו בהן

מאפשרת להסתיר את עצם קיומה של הפגיעה. חשיפת תקיפות סייבר בארגונים עלולה להנחית מכה אנושה על המשך פעילותם של עסקים קטנים ובינוניים. יש לגבש פוליסות ביטוח בערבות המדינה למקרים כאלה, ובכך לאפשר לחברות קטנות ובינוניות לשאת בנזקים.

2. הקלות מס להגנה בסייבר. זאת, באמצעות צוות ייעודי שיוקם ברשות המיסים כדי לבחון בקשות של ארגונים להקלות במס במקרה שיתעדפו הגנת סייבר ויספקו מענה הגנה ברמה גבוהה ללקוחותיהם. האתגר במתן הקלות כאלו תמורת הגנת סייבר הוא הצורך בפיתוח ידע טכנולוגי ברשות המיסים, שיאפשר לה להיענות לבקשות ולדרג את החברות המבקשות הקלות. קביעה כי תשתית סייבר מסוימת היא בטוחה היא אתגר קשה לביצוע. רשות המיסים תצטרך לקבוע קריטריונים ברורים ולהיעזר בתקנים בין־לאומיים כדי לקבוע מודל התנהלות בסייבר לחברות השונות.
3. מתן פטור מאחריות במקרה של שיתוף מידע פנים־מגזרי ובין־מגזרי על איומי סייבר ארגוניים, באופן שיאפשר הגנה פרו־אקטיבית במרחב זה. האתגר במקרה זה הוא לפרטיות הלקוחות של החברות העיסקיות. עידוד לשיתוף מידע בין המגזר העיסקי ובין המגזר המדינתי עלול להוביל לזרם מידע שיאפשר למדינה להכיר באופן ישיר את פעילותם של לקוחות החברות, למשל בשוק הקישוריות. על המדינה לבצע אנונימיזציה מלאה למידע שיגיע אליה. זהו אתגר מורכב, אך התועלת שבו עולה על העלות ותאפשר הגנה פרו־אקטיבית במרחב הסייבר.

ארבע שאלות מחקר נשאלו בפתיחתו של מסמך זה: הראשונה עסקה בבסיס, בחוקים ובמוסדות שעליהם מושתתים מאמצי מדינת ישראל בהגנת מרחב הסייבר. בפועל, מדינת ישראל מפעילה מאז שנות התשעים של המאה העשרים מאמצי הגנה עבור התשתיות המדינתיות הקריטיות. מאז ראשית המאה ה־21 הצטרפו לכך הנחיות נקודתיות ומגזריות מטעם משרדי הממשלה והרשויות למגזרים הרגישים במשק, כגון בריאות ופיננסים. בעשור הנוכחי עוברת ישראל מירכוז בתהליך קבלת ההחלטות ובחרה לנהל את אתגר הסייבר באמצעות ריבון אחד – מערך הסייבר הלאומי. זאת, תוך שימת דגש על עמידות המשק, חוסנו של מרחב הסייבר וההגנה הלאומית. גם אחרי צעדים אלה, עדיין חסרה תפיסה כוללת וסדורה להגנה על המגזר העיסקי־אזרחי, גם אם ננקטו צעדים משמעותיים בכיוון זה.

השאלה השנייה הייתה כיצד מבצעות מדינות בעולם רגולציה להגנת סייבר על המגזר העיסקי־אזרחי. סקירת הספרות מלמדת כי ישנן גישות שונות להגנת סייבר במדינות שונות וכי האסדרה של מרחב הסייבר מאורגנת לרוב טלאי על גבי טלאי, תוך המשך סיכונים לתשתיות קריטיות ולפשיעת סייבר, במקביל לבנייה של מוסדות ותהליכי קבלת החלטות שהולכים ומתמרכזים סביב סוכנות ממשלתית אחת. גם

במדינות שנסקרו חסרה התייחסות עקבית למגזר העיסקי, מלבד לגורמים נקודתיים הפועלים במסגרתו ולמתָן תמריצים באמצעות תווי תקן ותעודות.

השאלה השלישית היא מה ניתן ללמוד מהנעשה בתחומי רגולציה נוספים, כגון הגנת הסביבה ואנרגיה גרעינית, עבור רגולציה של המגזר העיסקי־אזרחי. מסקירת תחום הגנת הסביבה עולה כי יש מקום לאמץ גישה כוללנית, הלוקחת בחשבון את ההשלכות קצרות הטווח וארוכות הטווח של הסיכונים הפוטנציאליים. כמו כן, עולה מכך החשיבות שיש לתמריצים כגורם להחלת תקנים למיגור סיכונים על המגזר הפרטי. התמרכזות תהליך קבלת ההחלטות סביב יישות אחת גם היא בעלת השפעה חיובית על העבודה מול המגזר הפרטי, והשימוש בכלי רגולטורי של תסקיר סיכונים מול המשק מסייע בהערכת סיכונים ובמניעתם מבעוד מועד.

מתחום הרגולציה של אנרגיה גרעינית ניתן ללמוד על שיתופי הפעולה בין התעשייה ובין המדינה בהקמת מרכזי ידע לקידום הביטחון. בנוסף, קיומם של מנגנוני פיצוי ענפים למקרה של פגיעות משמעותיות מלמד על האפשרות לפיתוח של שוק ביטוח ומכירת פוליסות בתחום הסייבר המתָמרצת את המגזר העיסקי להתגונן מבעוד מועד. לבסוף, שימוש במתן רשיונות בתחום הסייבר כגורם היוצר מחויבות אצל ארגונים להגן על עצמם יאפשר לקבוע כי מתן רשיון כרוך גם בפרקטיקות של הגנת סייבר ראויה.

השאלה רביעית והאחרונה שואלת מהו מודל אפשרי לרגולציית הגנה בסייבר עבור המגזר העיסקי־אזרחי במדינת ישראל. על סמך הפערים המוצגים בסקירת הספרות והתובנות מתחומי רגולציה אחרים, אנו מציעים מודל רב־שכבתי לאסדרת הגנת הסייבר בישראל. המודל המוצע מבקש לשלב בין הצורך בפיתוח התעשייה ובפעילות גוברת במרחב הסייבר מצמד אחד, ובין שמירה על הביטחון הלאומי מצד שני, וזאת על בסיס כלים רגולטוריים מתחום הגנת הסביבה, ובראשם תסקיר עמידות קיברנטית. כמו כן, זיהוי עוגנים מרכזיים בעלי השפעה משמעותית על המשק כולו מאפשר למודל המוצע לפעול ישירות להגברת חוסנו של מרחב הסייבר הישראלי, וכתוצאה מכך לחזק את הביטחון הלאומי של מדינת ישראל. התמריצים המוצעים, שחלקם שאולים מתחום הגנת הסביבה והאנרגיה הגרעינית וחלקם חדשניים למודל זה, מבקשים לפעול לעידוד שקיפות בנוגע לאירועי סייבר ולהקמת שוק ביטוח יעיל לפיזור סיכונים במרחב זה. כמו כן, המודל מבקש לאפשר הקלות מס עבור הגנת סייבר ברמה ראויה, ובכך לשנות את המצב הנוכחי שבו פועלים כוחות השוק.

אסדרת מרחב הסייבר, בדיוק כמו הפרקטיקות הארגוניות להגנה במרחב זה, היא מאמץ רב־שכבתי הנוגע למגזרים שונים ומחייב מתן תשומת לב לייחודיות של כל מגזר מצד אחד, ולצורך לבחון באופן שיטתי את הסיכונים הפוטנציאליים של כלל המגזרים מצד שני. זהו מודל הנותן לראשונה מקום מרכזי למגזר העיסקי־אזרחי ומבנה תהליכי

עבודה שיתופיים שיסייעו בהגברת חוסנו של מרחב הסייבר באופן משמעותי ושונה משגרות הרגולציה הנוכחיות.

חשיבותו של המודל המוצע גוברת נוכח הקריאות להתגוננות עצמית ואקטיבית של המגזר העיסקי. במצב של היעדר מענה הגנתי מספק, נוכחות גוברת של איומים ועלויות הגנה גבוהות, נשמעים קולות המבקשים לאפשר לחברות פרטיות לבצע תקיפות סייבר חוזרות במקרים של זיהוי מקור הפגיעות. זאת ועוד, היעדר רגולציה בתחום זה יוצרת ואקום המאפשר לחברות להאיץ את מירוץ החימוש במרחב הסייבר. היתרונות במודל המוצע הם שינוי מאזן התמריצים הנתפס כעת כמתגמל מידי עבור התוקפים, הקטנת נטל התגובה על ממשלות וצמצום ההתקפות, והקטנת נזקים פוטנציאליים למגזר העיסקי. יחד עם זאת, גישה כזאת עלולה ליצור חיכוך והסלמה בין ארגונים שונים בשל אסימטריה מובנית ביכולותיהם לבצע הגנה אקטיבית על פעילותם ולהוביל להעסקתם של "שכירי חרב", שיהפכו את מרחב הסייבר לעוד פחות בטוח מכפי שהוא היום.

הדילמות בתחום זה הן היכן (ואם בכלל) ניתן לקבוע את גבולותיה של פעילות זו, במיוחד כאשר היעדר המענה הרגולטורי מוביל חברות ליטול יוזמה בתחום ההגנה האקטיבית גם ללא הרשאה מפורשת.[197] נדרש לאזן בין התועלת ובין הנזק שבפעילות כזאת ולחשוב על ההשלכות קצרות הטווח וארוכות הטווח שלה. מטרות ההגנה האקטיבית הן הרתעה של האקרים ברמה נמוכה, סיוע בחקירות אירועים תוך הטמנת Tokens מנוטרים לגניבה, ובאופן כללי עידוד צעדים אקטיביים יותר, מעבר לתחקור מעמיק, אחרי שהתרחשה תקיפה. העובדה שחברות בוחנות ברצינות אימוץ פרקטיקה כזאת מלמדת גם היא על הפער שנוצר באסדרת המגזר העיסקי־אזרחי במרחב הסייבר ועל הצורך בגיבוש פתרונות אחרים, מעֵבר לרגולציה בשגרה.

לסיכום, עם הקמתה של הרשות הלאומית להגנת הסייבר ב־2015 ועם האיחוד של כלל הגורמים העוסקים בסייבר במדינת ישראל במסגרת מערך הסייבר הלאומי ב־2018, תוך בניית מומחיות תוכן בנושאי סייבר על פני מגזרים רבים, בשלו התנאים לכינונו של מודל רגולציה חדש שיבחן לעומק את מרחב השחקנים במשק ויאפשר לזהות ולמגר סיכוני סייבר מבעוד מועד. האתגרים הניצבים לפתחו של המודל המוצע במסמך זה הם חיזוק הסמכות של חוק רישוי עסקים והגברת הציות לו וכן התאמת המודל לאתגרי הרגולציה החדשים.

תחום הבינה המלאכותית ויכולות הלימוד העצמאיות של מערכות השלובות בהתקנים מקושרים מזמנים לפתחם של מקבלי ההחלטות אתגרים, שכדי להתמודד

197 Wyatt Hoffman and Ariel Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?", Carnegie Endowment for International Peace, 2017.

איתם יש צורך במודל רגולטורי אפקטיבי להגנת הסייבר. כאשר תהליכי קבלת החלטות ותשתיות המדינה הופכים בהדרגה לדיגיטליים לחלוטין, כל מודל רגולטורי יצטרך לקדם ביתר שאת את האינטרס הציבורי במרחב הסייבר, ולו גם במחיר של התנגשות בין בעלי אינטרסים שונים. האינטרס הציבורי כולל את השמירה על אבטחת המידע, על הרציפות התפקודית, על הביטחון הלאומי, על סודות מסחריים ועל פרטיות המשתמשים, לרוחב כל פניה ורבדיה של חברת המידע.

נספח: מילון מונחים

מונח	המשמעות
כללי	
מרחב הסייבר	שם תואר למרחב אינטראקטיבי של מערכות דיגיטליות המשמשות לאחסון, שינוי והעברת מידע, הפועל בחלקו מעל קישוריות רשת האינטרנט.
הגנת הסייבר	סט תהליכים ריאקטיביים ופרו־אקטיביים הפועלים להסרת איומים על שלמות, אמינות וזמינות מחשבים, רשתות ומידע, המרכיבים יחדיו את מרחב הסייבר. המושג מכיל בתוכו אבטחת מידע, הגנת תשתיות קריטיות, שמירה על הביטחון הלאומי, והגנה מפני פשיעת סייבר וטרור בסייבר.
רגולציה	פעולת ארגון, פיקוח ואכיפה, המבוצעות על ידי המדינה או סוכנויות מדינתיות עצמאיות במטרה לכפות באופן חוקי כללי התנהגות מחייבים.
משטר רגולטורי	סך כל החוקים, ההנחיות, ההוראות והסוכנויות המוסדיות העוסקים בתחום מסויים לאורך זמן ומשקפים את הסדרי הפעולה, ניטורם ואכיפתם.
רגולציה	
רגולציה מדינתית	רגולציה מטעם המדינה, הנעשית על ידי קביעת חוקים ומתן הנחיות, ניטורם ואכיפתם, במטרה להסדיר או להבנות שוק באופן מסויים. רגולציה מדינתית יכולה להיות מחייבת או וולונטרית, בהתאם לדרכי הפעולה הנבחרות.
רגולציה עצמית	רגולציה שבה אחד או יותר מתהליכי הרגולציה – קביעת כללים, ניטור ואכיפה – מבוצע על ידי הגוף המפוקח.
המדינה הרגולטורית	כינוי לשינוי בתפקיד המדינה, החל משנות התשעים של המאה העשרים, ממדינה המספקת שירותים, גובה מיסים, ומסייעת לשכבות חלשות, למדינה המקימה סוכנויות ומסדירה את הכלכלה והחברה בכל תחומי החיים.
מודל רגולציה	מודל המפרט את אופני ההתערבות המדינתית לצורך פתרון בעיה למען האינטרס הציבורי.
תיווך רגולטורי	פעולת תיווך רגולציה בה גורם שלישי, שאינו הגורם המסדיר או המוסדר, לוקח על עצמו תפקידי רגולציה של קביעת כללים, ניטור או אכיפה, ופועל בתווך שבין הגוף המסדיר לגוף המוסדר.

מונח	המשמעות
רגולציה מחייבת	רגולציה שבנוסף לקביעת תקנים אחידים לשחקנים השונים, כוללת סנקציות במקרה של אי־ציות להם.
אסטרטגיית ניהול סיכונים לרגולציה	מאמצי המדינה להפחתת סיכונים עבור החברה מתחלקים לארבע אסטרטגיות מדינתיות. הנפוצה שבהן היא אסטרטגיה ל**מניעת** סיכונים, הכוללת התערבות מדינתית על ידי קביעת תקנים והנחיות למניעת סיכונים מבעוד מועד. אסטרטגיה שנייה היא אסטרטגיה ל**מזעור** נזקים, הכוללת צעדים לניהול אירוע או משבר כתוצאה מסיכון שהתממש. אסטרטגיה שלישית היא אסטרטגיה של **פיזור** סיכונים, בה המדינה מעודדת את קיומו של שוק ביטוח, המפזר סיכונים על פני כל בעלי הפוליסה. אסטרטגיה רביעית היא אסטרטגיה של **הסטת** סיכונים, המעבירה סיכונים מיישות אחת לשנייה כדי לתמרץ קבלת מידע על סיכון מבעוד מועד או כדי לעודד שחקנים במשק לפעול באופן שנתפס כאינטרס הציבורי.
מגזר עיסקי	מגזר המורכב מבעלי עסקים פרטיים הפועלים למטרות רווח (נקרא גם "המגזר השני").
מבנה מוסדי	המבנה המינהלי דרכו מתקבלות החלטות. במקרה של המדינה, מדובר על הרשויות והסוכנויות השונות, ועל חלוקת הסמכויות ביניהן. המבנה המוסדי סביב מרחב הסייבר בארצות הברית כולל עשרות סוכנויות פדרליות, שקיבלו את סמכותן מתוקף חקיקה בקונגרס, החלטות נשיאותיות והתפתחות העיסוק בנושא. תחום השיפוט של סוכנות אחת עשוי לחפוף באופן חלקי לתחום השיפוט של סוכנות אחרת.
רשיון עסק	תעודה המעידה כי ננקטו כל האמצעים והסידורים המתאימים להפעלתו התקינה של עסק על פי הקבוע בחוק ולטובת הציבור הרחב ובעל העסק.
תמריצי רגולציה	תהליך שנועד לעודד פעילות של שחקנים שונים במשק לטובת האינטרס הציבורי, באופן לא כפוי ותוך מתן תמריצים. לדוגמה, הקלות מס על מתווה פעילות מסויים, סבסוד של שירותים לעידוד תחרות ומתן היתרים לעבודה עם גופים מדינתיים.
הגנת סייבר	
הֶתקנים מקושרים	עצמים פיזיים הקשורים ביניהם ברשת האינטרנט לצורך זיהוי בפני עצמים אחרים וניהול מבני נתונים ומידע ללא התערבות אדם. הֶתקנים מקושרים נחשבים לאבני הבניין של עידן "האינטרנט של הדברים". לפי הגדרת סוכנות הסחר הפדרלית של ארצות הברית, "האינטרנט של הדברים" הוא "התקנים וחיישנים, שאינם מחשבים, טלפונים ניידים או טאבלטים, המתחברים, מאחסנים ומעבירים מידע אחד לשני דרך רשת האינטרנט".

מונח	המשמעות
ביטוח סייבר	ביטוח – אסטרטגיית פיזור סיכונים, בה בעלי פוליסת ביטוח רוכשים את הזכות לפזר סיכון מסויים על פני כל בעלי הפוליסה הנוספים. ביטוח סייבר – אסטרטגיית פיזור סיכונים העוסקת בנזקי צד ראשון וצד שלישי כתוצאה מפגיעת סייבר. נזקי צד ראשון כוללים פגיעות סייבר בתשתית הארגונית של הארגון המבוטח. נזקי צד שלישי הם נזקים הנגרמים לגורם שלישי הקשור לגורם המבוטח, למשל, נזקי פרטיות הנגרמים ללקוחות החברות כתוצאה מפגיעות סייבר ואובדן מידע אישי.
חובת דיווח באירועי סייבר	חיוב ארגונים לדווח ליישות ציבורית, הנושאת באחריות המגזרית כלפי הארגון המדובר, על אירועי סייבר שחוו. חובת דיווח יכולה להיות גם כלפי הציבור בכללותו, או כלפי לקוחות שפרטיותם נפגעה כתוצאה מדליפת מידע. למרות שהאינטרס הפנימי של הארגון הוא לרוב להשאיר אירועי סייבר בין כתליו, חובת הדיווח מתמרצת ארגונים להגן על עצמם מבעוד מועד ועשויה לסייע להעלאת השקיפות ולכינונו של שוק ביטוח הנשען על מידע על אירועי סייבר בארגון.
שיתוף מידע על איומי סייבר	שיתוף מידע הנעשה לצורכי הגנה וכולל מידע על חולשות סייבר קיימות, אופני תקיפה ואיומים קונקרטיים במרחב הסייבר, זיהוי גורמים מתקיפים וניסיונות להערכת המניע מאחורי התקיפות, הכל מתוך מטרה למנוע את התפשטות האיום.
תקינת מקצועות סייבר	פירוט של רמת המקצועיות הנדרשת לעוסקים בהגנת סייבר על רבדיה השונים. התקינה מגדירה את סוגי המקצועות, יכולות הידע הנדרשות, ניטור ואכיפה.
תסקיר	תסקיר – כלי תכנוני שנועד לצמצם סיכונים במהלך הקמה וניהול של פרויקטים חדשים ומתמשכים. התסקיר נועד לזהות מבעוד מועד השפעה שלילית אפשרית ולספק מענה פרו־אקטיבי לסיכונים שיווצרו. לדוגמה, תסקירי השפעה על הסביבה בעת הקמת פרויקטים חדשים ותסקירי השפעה על פרטיות בעת הקמה או ניהול של חברות המחזיקות במידע אישי.
תסקיר עמידות קיברנטית	תסקיר עמידות קיברנטית, הינו כלי תכנוני העוסק במיפוי סיכונים קיברנטיים העלולים להגרם לציבור כתוצאה מפעילות חדשה או קיימת.

מונח	המשמעות
חוסן מרחב הסייבר	חוסן – מושג הכולל את סך כל פעולות ההגנה, הגילוי והתגובה לאיומים, תקיפות, משברים ואירועים העלולים לפגוע באינטרסים חיוניים, כגון הביטחון הלאומי, אספקת מזון ותפקוד תקין של החברה. חוסן במרחב הסייבר – תוצאה של פעולות התורמות לנטרול האיומים ובניית יכולות, באופן ששומר ואף מחזק את יציבות ואמינותו של מרחב הסייבר.
שרשרת האספקה	תשומות של שירותים, מוצרים, תוכנה וחומרה, המשמשות בתהליך העיסקי של ארגון ונרכשות מספקים חיצוניים, תוך קישור למערכות המידע והמחשוב של הארגון ברמות חשיפה משתנות. נסיון העבר מראה כי במקרים רבים תוקפים מצליחים לחדור את המערכות הארגוניות באמצעות תקיפה של ספק המשנה וחדירה דרכו למערכות הארגון.
צמתים חיוניים לחוסן מרחב הסייבר	מקומות שזוהו כמשמעותיים לשמירה על חוסנו של מרחב הסייבר. לדוגמה, ספקי שירותי אירוח (hosting) של אתרי אינטרנט, ספקיות תשתיות אינטרנט, מטמיעי אבטחת מידע בכלל המשק ושירותי תוכנה יעודיים המשמשים את כל המגזר הפיננסי. התערבות מדינתית בצמתים אלה היא בעלת אפקט רחב על מרחב הסייבר בכללותו.
הגנה אקטיבית	אסטרטגיית הגנה במרחב הסייבר, המתבססת על מתן היתר להגנה עצמית ואפשרות לתקיפה חוזרת במקרה של פגיעת סייבר בעלת מקור מזוהה.
פרטיות והגנת מידע	פרטיות והגנת מידע – מרכיב באבטחת המידע, החופף באופן חלקי להגנת הסייבר, אך עוסק גם בנושאים עקיפים שאינם קשורים באופן ישיר להגנת סייבר, כגון האופן בו יש לסווג מידע, משך הזמן שמידע יכול להישאר במערכת, מידע אישי, רמות השקיפות בעיבוד מידע אישי, היכולת של מושאי המידע לשלוט על מידע הנוגע בהם, וכן איכות המידע המוחזק. תחום הפרטיות הוא תחום ותיק יותר מבחינה רגולטורית מאשר תחום הגנת הסייבר, ועל כן הגנת הסייבר מקיפה ומרחיבה את הגנת מערכות המידע יותר ממנו.
צוותי CERT	צוותי CERT – ראשי התיבות של Computer Emergency Response Teams – צוותים שתפקידם הוא לנהל אירועי סייבר בזמן אמת על ידי ריכוז כל הגורמים המעורבים תחת מעטפת אחת, שיתוף מידע רלוונטי בין השחקנים השונים בזמן אמת וקבלת החלטות למיגור האירוע על פי האינטרסים המדינתיים. צוותי CERT נפוצים במדינות רבות בעולם, ולאחרונה החלו לקום צוותי CERT מגזריים, כמו במגזר הפיננסים או במגזר האנרגיה, מתוך רצון לתת מענה ייעודי למגזר המותקף, תוך התייחסות למורכבות המאפיינת אירועי סייבר בכל מגזר בנפרד.

INSS Memoranda, January 2018–Present

No. 180, August 2018, Gabi Siboni and Ido Sivan-Sevilla, *Cyber Regulation* [Hebrew].

No. 179, August 2018, Udi Dekel and Kim Lavi, eds., *A Strategic Framework for the Israeli-Palestinian Arena* [Hebrew].

No. 178, July 2018, Carmit Padan and Meir Elran, *Communities in the Gaza Envelope – Case Study of Social Resilience in Israel* (2006-2016).

No. 177, June 2018, Yotam Rosner and Adi Kantor, eds., *The European Union in Turbulent Times: Challenges, Trends, and Significance for Israel.*

No. 176, June 2018, Udi Dekel and Kobi Michael, eds., *Scenarios in the Israeli-Palestinian Arena: Strategic Challenges and Possible Responses* [Hebrew].

No. 175, May 2018, Yotam Rosner and Adi Kantor, eds., *The European Union in a Time of Reversals: Challenges, Trends, and Significance for Israel* [Hebrew].

No. 174, April 2018, Avner Golov, *The Israeli Community in the United States: A Public-Diplomacy Asset for Israel* [Hebrew].

No. 173, March 2018, Meir Litvak, Emily B. Landau, and Ephraim Kam, eds., *Iran in a Changing Strategic Environment*.

No. 172, February 2018, Meir Litvak, Emily B. Landau, and Ephraim Kam, eds., *Iran in a Changing Strategic Environment* [Hebrew].

No. 171, January 2018, Carmit Valensi, Udi Dekel, and Anat Kurz, eds., *Syria – From a State to a Hybrid System: Implications for Israel*.

No. 170, January 2018, Doron Matza, *Patterns of Resistance among Israel's Arab-Palestinian Minority: A Historical Review and a Look to the Future*.

חוסנו של המגזר הפרטי במרחב הסייבר משפיע באופן מכריע על הביטחון הלאומי. מגזר זה מהווה לרוב חוליה חלשה דרכה מתפתחת מתקפה קיברנטית ומשמש כקרש קפיצה עבור תוקפים המעוניינים לפגוע במטרות מדינתיות. יחד עם זאת, כשלי שוק מובנים מובילים להיעדר השקעה ארגונית מספקת בהגנת סייבר ראויה.

החצנה שלילית של נזקי סייבר בארגונים, הקושי בכימות התועלת שבהשקעה שכזו, היעדר אחריות של ספקי תוכנה וחומרה עבור בעיות אבטחה במוצריהן, ושוק תחרותי המתגמל חדשנות וקידמה על פני הגנת סייבר ראויה יוצרים פער הדורש התערבות מדינתית.

סקירת משטרי רגולציה להגנת הסייבר בעולם המערבי מלמדת על היעדר מענה שיטתי עבור המגזר העסקי ועל פער במיפוי איומי הביטחון הלאומי כתוצאה מנזקי סייבר פוטנציאליים במגזר זה.

מזכר זה – שנשען על הנעשה בעולם בתחום הסייבר ובתחומי רגולציה נוספים – מציע מודל רגולטורי רב־שכבתי להסדרת הגנת הסייבר במגזר הפרטי. המזכר מציע מודל משולב של חלופה רגולטורית מדינתית הכולל רגולציה מחייבת, הקמת מנגנוני בקרה לפיקוח על רגולציה עצמית, ומתן תמריצים לעידוד ארגונים להגן על עצמם. בעידן של שימוש נרחב בהתקנים מקושרים, כניסה של בינה מלאכותית לשלל תחומי החיים, והקמה של שוק ביטוח להגנה בסייבר, הסדרת המגזר העסקי הינה אינטרס לאומי חיוני ראשון במעלה.

ד"ר גבי סיבוני הוא מנהל תכנית המחקר 'צבא ואסטרטגיה', מנהל תכנית המחקר 'בטחון סייבר' ועורך כתב העת **סייבר, מודיעין וביטחון**, במכון למחקרי ביטחון לאומי. ד"ר סיבוני הצטרף לסגל החוקרים במהלך 2005. במהלך שירותו הצבאי שירת כלוחם וכמפקד בחטיבת גולני ושירת במגוון תפקידים במילואים בהם: סגן מפקד של אגד לוגיסטי וראש מטה של אוגדה. במסגרת עבודתו בצה"ל הוא המתודולוג הראשי של המרכז להכוונת בניין הכוח – המעבדה התפיסתית. סיבוני הינו בעל התארים .B.Sc ו־.M.Sc בהנדסה מכנית מאוניברסיטת תל אביב ותואר דוקטור במערכות מידע גיאוגרפיות (GIS) מאוניברסיטת בן גוריון בנגב. ד"ר סיבוני משמש כיועץ במגוון תחומים, בהם: טכנולוגיה צבאית, הנדסת מים וסביבה, ניהול סיכוני סייבר ומערכות מחשוב.

עידו סיון־סביליה הוא עמית מחקר בתכנית הסייבר של המכון למחקרי בטחון לאומי ומיישם מתודולוגיות מחקר על בסיס נתוני־עתק במכון. הוא דוקטורנט למדיניות ציבורית באוניברסיטה העברית וחוקר באופן השוואתי מבני ממשל לניהול סיכונים בתחום הסייבר. מר סיון־סביליה הוא בעל ניסיון רב בנושאי הגנת סייבר ממשרד ראש הממשלה, חיל האוויר והמגזר הפרטי. היה מלגאי בתכנית פולברייט של מחלקת המדינה האמריקאית ושירת כחוקר בתחום החקיקה בקונגרס האמריקני בוושינגטון.

INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
TEL AVIV UNIVERSITY אוניברסיטת תל אביב