רגולציה במרחב הסייבר בישראל – תשתית מושגית, אתגרים ודרכי התקדמות

גבי סיבוני ועידו סיון

בעיית ביטחון מרחב הסייבר (Cybersecurity) חוצה תחומים, מגזרים וגישות. מאמר זה מציג את עמודי התווך של הבעיה, מאמץ פרדיגמה לפיה המדינה היא מנהלת סיכונים עבור הציבור דרך רגולציה, וסוקר את הרקע וההסברים להתפתחות הרגולציה בעולם המודרני. בהמשך, המאמר עומד על הדומה והשונה בין ארצות הברית, האיחוד האירופי ומדינת ישראל באופן בו הן בוחרות להתמודד עם אתגר ביטחון מרחב הסייבר, ומדגיש את החשיבות והקשיים בהכלת רגולציה מדינתית בתחום זה על המגזר האזרחי. המאמר גם סוקר כיווני התקדמות אפשריים בשאלת ביטחון מרחב הסייבר ומעלה הצעות כיצד להבטיח את חוסנו הקיברנטי של המגזר האזרחי.

מילות מפתח: רגולציה, סיכונים, ביטחון סייבר, מגזר אזרחי

מבוא

ההתנהלות במרחב הסייבר הינה אתגר עבור מקבלי ההחלטות. האתגר נובע בראש ובראשונה מתלות המדינה והחברה במרחב הסייבר, שהוא מיסודו פגיע. מרחב זה מאפשר זרימת מידע, המסייעת ברוב המקרים לפריחה כלכלית, להגברת היעילות ולרווחה חברתית, אך הוא גם נתון לאיומים ביטחוניים, פליליים ומסחריים. האתגרים לחוסנו של מרחב הסייבר[1] נובעים ממספר סיבות עיקריות:

- ראשית, ישנה אסימטריה מובהקת בין חסמי הכניסה הנמוכים לתוקפים ובין עלויות הגנה גבוהות. בעוד שתקיפה מוצלחת זקוקה לווקטור התקדמות יחיד, מאמצי ההגנה מתיימרים לכסות את כלל הפגיעויות האפשריות.

ד"ר גבי סיבוני הינו ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. עידו סיון הינו חוקר ניובאואר בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

- שנית, מרחב הסייבר נשען על פרוטוקולי תקשורת מיושנים המאפשרים אנונימיות רבה לתוקפים ומקשים על רשויות אכיפת החוק לזהות את מקור התקיפות.[2]
- שלישית, מרחב הסייבר מאפשר הן ניצול החולשות הרבות של חומרה/תוכנה והן שימוש בכלי תקיפה קיימים שכבר פעלו בהצלחה בתקיפות קודמות. תופעה זו גוררת מרוץ חימוש מואץ המדרדר עוד יותר את רמת האבטחה, וראיה לכך הוא השוק המשגשג לניצול חולשות zero-day.[3] לאחרונה נחשפה פעילות של חברות מסחריות הסוחרות עם ממשלות בחולשות תוכנה ובכלי תקיפה לצורכי ריגול נגד אזרחים ומתנגדי משטר.[4]
- רביעית, היעדר כלים לשיתוף מידע על האיומים במרחב הסייבר ועל אמצעי ההגנה שנוקטות חברות מסחריות מקשה על גיבושו של מאמץ קולקטיבי ופרו־אקטיבי למניעת תקיפות במרחב זה. הדבר נובע בראש ובראשונה משיתוף מידע חלקי ומשקיפות מוגבלת של חברות מסחריות במגזר האזרחי.[5] עם זאת, גם המגזרים הצבאי והמדינתי לא תורמים את חלקם בשיתוף מידע כזה.
- 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 או של איום סייבר שהתממש. אי לכך, עלויות הנזק כתוצאה מפריצה מוצלחת ומוניטין החברה הנפרצת אינם מונחים על הכף באופן שיתמרץ חברות להגן על עצמן מבעוד מועד. למרות מודעות גוברת של בעלי מניות וקהל הלקוחות במגזר הפרטי לתחום הסייבר, אין הנחייה גורפת ומחייבת לפרסם אירועי סייבר ולדווח על נזק שנגרם. בנוסף לכך, יכולותיו של ארגז הכלים הטכנולוגי הקיים היום בשוק אינן מספיקות ליצירת הגנה הרמטית.[6]
- לבסוף, מרבית המשתמשים במרחב הסייבר אינם מודעים לסכנות שהוא טומן בחובו ומזינים אותו במידע רגיש וקריטי שאינו מוגן כראוי. בנוסף, משתמשים רבים נופלים קורבן לניסיונות חדירה באמצעות הנדסה חברתית, בוחרים סיסמאות באופן חלש מדי, ובמרבית התקיפות מהווים את החוליה החלשה דרכה נפרצות מערכות.[7]

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.[8] הקלות בה חברות מסחריות ומדינות אוספות ומאחסנות מידע קריטי אינה תואמת את יעילות המאמצים הנעשים כדי להגן על מרחב הסייבר, אף שהמדינה מנסה להתערב ולמנוע התממשותם של סיכוני סייבר, או לצמצמם בדיעבד. כך אנו מוצאים עצמנו תלויים לחלוטין בתפקודו התקין של מרחב שביסודו הוא פגיע.

הסיכונים הנשקפים ממרחב הסייבר הינם המשך טבעי של סיכוני המדינה המודרנית, כפי שתיאר הסוציולוג אולריך בק בספרו פורץ הדרך מ־1986, *Risk Society*.[9] לדברי בק, החיים המודרניים על פיתוחיהם הטכנולוגיים טומנים בחובם הזדמנויות רבות, אך גם יוצרים סכנות חדשות לאדם ולסביבה. הכלכלן דיוויד מוס (Moss) התייחס ב־2002 למורכבות של ניהול סיכונים אלה על ידי הממשלה.[10] מוס הראה כיצד ממשלת ארצות הברית, כמנהלת סיכונים עבור החברה האמריקאית, עברה דרך שלושה שלבי התפתחות עוקבים באסטרטגיית ניהול הסיכונים שלה. ראשיתו של התהליך הייתה במאה ה־19, כאשר ארצות הברית התערבה באופן אגרסיבי בניהול סיכונים לעידוד השקעות וצמיחת המשק (על ידי חוקים, כגון חוק חברה בע"מ, המגביל את הסיכון עבור המשקיעים בחברה, וחוק פשיטת רגל, המגן על משקיע מלרדת מכל נכסיו). בהמשך עברה המדינה לניהול סיכונים עבור בטיחות העובדים ויציבות חיי שוק העבודה (חוקים לפיצויים ולביטחון סוציאלי לעובדים כביטוי להולדתה של מדינת הרווחה האמריקאית). לבסוף, בשלב הנוכחי בעת המודרנית, המדינה עוסקת בניהול סיכונים עבור כלל החברה – תחילה סיכוני סביבה, בטיחות במזון וכדומה, וכעת סיכוני סייבר, הנובעים מפיתוחים מודרניים ומהסיכונים הכרוכים בהם.[11]

אסטרטגיות ניהול הסיכונים שנוקטת המדינה המודרנית נעות על הרצף שבין הפחתת הסיכונים ובין חלוקתם מחדש בחברה. מצד אחד, הפחתת סיכונים כוללת בעיקר מניעה של סיכונים מבעוד מועד (למשל, רגולציה לבטיחות, שלטים המזהירים מפני מהירות מופרזת, ובשדה הסייבר – דרישות אבטחת מידע למניעת פריצה למערכות), וכן צעדי צמצום נזקים (mitigation) שמטרתם להפחית את הנזק כתוצאה מסיכון שכבר התממש (למשל, רגולציית כיבוי אש; או בשדה הסייבר – צעדים לצמצום נזק מהתקפות סייבר[12] ודיווח לאזרחים וגורמים מדינתיים על פריצה שקרתה כדי שיתגוננו מפניה).

מצד שני, חלוקה מחדש של סיכונים עוסקת בהעברת האחריות לסיכון בין הישויות השונות. למשל, חוקי בטיחות מוצרים (Product Liability Laws) מסיטים את האחריות מהצרכן ליצרן. דוגמה עכשווית משדה הסייבר הם חוקי שיתוף מידע במרחב הסייבר (Cyber Information Sharing Act) המגבילים את האחריות של חברות מסחריות הבוחרות לשתף מידע עם הממשלה על פריצות סייבר. חלוקה מחדש של סיכונים יכולה לבוא לידי ביטוי גם כפיזור סיכונים על פני מבוטחים שונים, למשל בחברות ביטוח, כאשר כל מבוטח משלם פרמיה מסוימת כדי לכסות את הנזק מסיכון שיתממש אצל אחד המבוטחים. פיזור הסיכונים על ידי המגזר הפרטי בעולם הסייבר נעשה בעיקר עבור סיכוני צד שלישי,[13] עד כה ללא התערבות מדינתית.

על אף אסטרטגיות ניהול הסיכונים הרבות שעומדות בפני המדינה, היא טרם השכילה למצוא את האופן הראוי בו עליה להתערב, בעיקר במגזר האזרחי, כדי להבטיח את רציפותו התפקודית, חוסנו ויציבותו של מרחב הסייבר. החשיבות של המגזר האזרחי לחוסנו של מרחב זה היא עצומה: המגזר האזרחי מהווה את חלק הארי במרחב הסייבר, נחשף למרבית האיומים, ולפגיעה בו יש השלכות כלכליות וביטחוניות על חוסנה של החברה.

רגולציה מדינתית: רקע והתפתחות

רגולציה ברמה הבסיסית ביותר היא פעולת הסדרה, פיקוח ואכיפה המבוצעות על ידי המדינה או סוכנויות מדינתיות עצמאיות במטרה לכפות באופן חוקי כללי התנהגות מחייבים. רגולציה כזאת חלה על "נמעני רגולציה" שאותם הגוף הרגולטורי שואף להסדיר.

מושג הרגולציה נולד בארצות הברית בסוף המאה ה־19 כדרך פוליטית ומינהלית להסדיר את השוק. הרגולציה הפכה לכלי מרכזי בידי אנשי ממשל, שכן היא הייתה תגובה טבעית לכשלי שוק, להיעדר פיקוח ולהיווצרותם של "מונופולים טבעיים". לעומת זאת, באירופה הדגש היה לא על הרגולציה, אלא על הלאמה של השוק. פיקוח באמצעות הלאמה עיכב את התפתחות המסורת הרגולטורית באירופה לעומת ארצות הברית. יחד עם זאת, מסוף שנות השבעים של המאה הקודמת ואילך חלה התרחבות של השימוש ברגולציה והוקמו סוכנויות אכיפה עצמאיות בארצות הברית, וכן נעשה שימוש מסיבי בכלים רגולטוריים באירופה כחלק מהאצת האיחוד הכלכלי של היבשת.[14]

עם עלייתם לשלטון של מרגרט תאצ'ר בבריטניה (1979) ורונלד רייגן בארצות הברית (1981) חלה התרחבות בפעילות של סוכנויות רגולטוריות עצמאיות שפעלו להסדרת השוק, במה שזכה לכינוי "המדינה הרגולטורית".[15] תפקיד המדינה עבר אט־אט ממסבסדת שירותים ומסייעת לצמצום פערים, לייעול השוק באמצעות רגולציה (או דה־רגולציה)[16] מוגברת.

רגולציה נתפסת לרוב כחקיקה/חקיקת משנה על ידי המדינה או סוכנויות רגולטוריות עצמאיות. היא יכולה לבוא לידי ביטוי גם בהוראה/צו/הנחייה מחייבת. תפקיד הרגולציה הוא להסדיר את פעילות השוק, בעוד שקביעת המדיניות נעשית על ידי הדרג המדיני. ב"מדינה הרגולטורית" יש תפקיד מרכזי למומחים, והדרישה למומחיות גבוהה היא המוטיבציה הראשונית להקמת סוכנויות רגולטוריות עצמאיות.[17]

ניתן להסביר את חשיבותה של רגולציה עבור הציבור במספר אופנים:

- ראשית, הרגולציה שואפת להגן על ערכים ועל חירויות האזרח שעלולות להיפגע על ידי בעלי הכוח או איומים מבחוץ. משימה זו מסבירה את הצורך בכוחות צבא וביטחון מצד אחד, אך גם ברשויות שיבלמו ויאזנו אותם במידת הצורך מצד שני.
- שנית, רגולציה מוצדקת מבחינה כלכלית. תפקיד הרגולציה הוא לתקן כשלי שוק הנובעים מהתנהלות השוק החופשי באופן שלא משרת את האינטרס הציבורי.[18] לדוגמה, מונופול המתמחר ומספק מוצרים כראות עיניו, ועל כן יש להטיל עליו פיקוח.
- שלישית, רגולציה מתחייבת במצב של היעדר מידע או של אסימטריה במידע. מצב כזה גורם לצרכנים, לחברות או למדינות להתנהג בצורה שלא משרתת את האינטרס הציבורי, ובמקרה זה תפקידו של הרגולטור הוא לאפשר שקיפות וזרימת מידע.
- לבסוף, רגולציה נובעת מהרצון להבטיח את קיומם של משאבים ציבוריים מִתכלים שאי אפשר למנוע את השימוש בהם, החל מאיכות האוויר וכלה בכמות הדגים בים. על הרגולטור לדאוג שמשאבים כאלה ימשיכו להתקיים, על אף שכוחות השוק נוטים לכלותם.

אופן הפעילות של הרגולטור במדיניות הציבורית והיווצרותה של רגולציה מוסברים בספרות בצורות שונות ומגוונות. תיאוריית האינטרס הציבורי (פונקציונאליזם) גורסת כי רגולציה פועלת לקידום טובת הכלל ולהגדלת הרווחה החברתית.[19] לעומתה, תיאוריית האינטרס הפרטי גורסת כי הרגולטור מונע מתוך אינטרסים פרטיים במטרה להגדיל את רווחתן של קבוצות אינטרס מרוכזות המייצגות בדרך כלל פלח קטן באוכלוסייה. הרגולציה בהיבט הזה היא תוצר של היחסים בין קבוצות אינטרס ובין המדינה ובינן לבין עצמן.[20] בנוסף, אפשר לתת למשטרים רגולטוריים הסבר מוסדי. במקרה זה יכולותיו (capacity) של המוסד הרגולטורי[21] או מיקומו ההיסטורי בהליך המדיניות הציבורית[22] מסבירים את הבניית הרגולציה באופן בו היא נוצרה. בעשרים השנים האחרונות התפתח זרם נוסף, המסביר רגולציה מתוך תיאוריה רעיונית. על פי תיאוריה זו, לפרדיגמות יש תפקיד מרכזי בהליך העיצוב של המדיניות הציבורית.[23] רעיון מסוים נתפס כ"נכון" ב"חלון הזדמנות" מסוים וסוחף אחריו את מקבלי ההחלטות ליצירת רגולציה ברוח הפרדיגמה והאינטרסים העוטפים אותה.[24] קרי, רעיונות ואינטרסים שזורים במקרים רבים זה בזה, כאשר רעיון מסוים עוזר לתת לגיטימציה וביטוי לאינטרסים שבכוחם ליצור רגולציה שתשרת את מטרותיהם.[25]

גישות רגולציה במרחב הסייבר בעולם המערבי ובישראל

הרגולציה הולכת ומתרחבת בחיים המודרניים, וההסברים לקיומה והאופנים בהם היא מתהווה שונים ומגוונים. עם זאת, רגולציה במרחב הסייבר טרם נבחנה בספרות

באופן מספק. להלן יפורטו האתגרים שטומנת בחובה רגולציית מרחב הסייבר, דרכי ההתמודדות של רגולטורים עם בעיית ביטחון מרחב הסייבר, והאופן שבו ארצות הברית והאיחוד האירופי[26] מבַנות את משטרי הרגולציה שלהן במרחב זה בהשוואה לישראל. בהמשך יתמקד המאמר ברגולציה הישראלית על מרחב הסייבר ויצביע על הפער המהותי הקיים במשטר זה – המגזר האזרחי.

רגולציה במרחב הסייבר נוגעת להגנה לא רק במובן הקלאסי; היא טומנת בחובה היבטים רבים הקשורים באופן ישיר לביטחון הלאומי, להגנה על נכסים וקניין רוחני, למניעת פשיעה ולשמירת מידע והזכות לפרטיות. יחד עם זאת, הרגולציה מציבה אתגרים בפני הרגולטורים משלוש סיבות עיקריות:

- ראשית, העלויות המושתות על אלה הנדרשים להגנה על מרחב הסייבר הן גבוהות ויוצרות התנגדות נחרצת מצד המגזר הפרטי, המהווה את חלק הארי של מרחב זה, לרגולציה מכל סוג שהוא.[27]
- שנית, אין הנחייה מדינתית המורה על מידת השקיפות של חברות מסחריות בכל הנוגע לרמות ההגנה ולחומרת התקיפות המתרחשות בפועל. הן התוקפים והן המתגוננים משתפים ביניהם מידע,[28] אך מאמצי ההגנה אינם נהנים לרוב מהתארגנות קולקטיבית בקנה מידה נרחב. כאשר סודות מסחריים ומוניטין של חברות מונחים על כף המאזניים, אין זה מפתיע כי המגזר האזרחי אינו שש לשתף מידע על המתרחש במרחב הדיגיטלי שלו.
- שלישית, רגולציה במרחב הסייבר, כבכל מקום אחר, טומנת בחובה קונפליקט בין אינטרסים, שהבולטים הם המאבקים בן אטטיזם[29] לליברליזם ושל הזכות לפרטיות מול הזכות לביטחון.[30] מאבקים הקשורים לאינטרסים של הביטחון הלאומי מול הרצון בפיתוח כלכלי (המשתקפים בפיקוח על ייצוא מוצרים), כמו גם מכשולים בשיתוף מידע בין חברות הנובעים מהוראות מחמירות מצד הממונה על ההגבלים העסקיים, משקפים רק במעט את הקשיים בכינון רגולציה בתחום הסייבר. הקונפליקטים הללו נותנים דרור לאינטרסים מנוגדים ולמאבקי כוח סביב האופן בו יש להבנות את הרגולציה במרחב הסייבר.

נוכח אתגרים אלה, רגולציה של מרחב הסייבר כוללת בדרך כלל ארבע דרכי התמודדות עם בעיית האבטחה של מרחב זה.[31] הדרך הנפוצה היא התוויה של סטנדרטים ודרישות בתחום אבטחת המידע, הכוללים בין היתר הצפנה, ניטור, גיבויים, הזדהות חזקה וכיוצא באלה. בנוסף, בעיקר בארצות הברית, הרגולציה עוסקת בעידוד וביצירה של מכניזמים לשיתוף מידע בין חברות מסחריות ובין המדינה מתוך רצון להתמודד עם בעיית חוסר המידע, ועל ידי כך להתגונן מבעוד מועד מפני התקפות ולצמצם נזקים של התקפה שכבר התרחשה. שדה הרגולציה מתאפיין גם ביצירה של סוכנויות רגולטוריות ובמתן סמכות למוסדות מדינתיים לאכיפת סטנדרטים ופרקטיקות הגנה בתחום ביטחון מרחב הסייבר.[32] לבסוף,

משטרים רגולטוריים כוללים בתוכם צעדים לצמצום נזקי פריצה עבור צד שלישי, הכוללים דיווחים ל־CERT הלאומי[33] וללקוחות שמידע אישי עליהם נגנב. הדבר עולה בקנה אחד עם "מעגל ההגנה השלם",[34] הכולל צעדי מניעה, שיתוף מידע וצמצום נזקים אחרי מתקפה, היוצרים מעטפת הגנה קוהרנטית לארגונים במרחב הסייבר.

כלי הרגולציה המשמשים דרכי התמודדות אלו הינם לרוב חקיקה, הנחיות מדינתיות מחייבות מצד סוכנויות רגולטוריות[35] ורגולציה עצמית שמקורה באימוץ תקנים מומלצים – תקני ISO לאבטחת מידע[36] או תקני PCI עבור חברות מקוונות העוסקות בשירותי סליקה[37] – או מומחיות פנים־ארגונית הכוללת הנחיות להגנת רשתות המחשבים של הארגון אך אינה מפורסמת ברבים. גם המדינה מפרסמת סטנדרטים והנחיות על האופן בו מומלץ להגן ועל האסטרטגיות אותן יש לנקוט. בארצות הברית, למשל, מכון התקנים הלאומי (National Institute of Standards and Technology – NIST) מקפיד לפרסם סטנדרטים להגנה והצפנה של מערכות מידע.[38] במגזר הפיננסי, (The Financial Industry Regulatory Authority (FINRA סוקרת עבור חברות פיננסיות אמריקאיות את האסטרטגיות הרצויות להגנה במרחב הסייבר.[39]

בעולם המערבי יש שתי גישות עיקריות להתמודדות המדינה עם סיכוני מרחב הסייבר. בארצות הברית הרגולציה מבוססת בעיקר על מודלים וולונטריים, סקטוריאליים, מרובי סוכנויות, עם משקל נכבד לכוחות השוק.[40] האיחוד האירופי מציג גישה היררכית עם מוסדות רוחביים בעלי סמכות אכיפה חזקה, כאשר המדינה נמצאת במרכז וחלקים גדולים במגזר הפרטי כפופים לרגולציה. ארצות הברית מאמינה כי האינטרס העסקי יוביל חברות להגן על עצמן, בעוד שהאיחוד האירופי דוגל בגישה מתערבת יותר, בה המוסד המדינתי דואג להגנת המגזרים השונים לרווחת האזרחים. שקיפות כלפי אירועי סייבר נאכפת הן בארצות הברית והן באיחוד האירופי: בארצות הברית הדבר מבוצע ברמה המדינתית, כאשר ישנן 47 גרסאות של Data Breach Notification.[41] האיחוד האירופי, מצדו, קיבל לאחרונה את דירקטיבת הגנת המידע המשודרגת שלו (General Data Protection Regulation), שנכנסה לתוקף במאי 2016 ותיושם החל ממאי 2018. דירקטיבה זו מבטיחה סטנדרט אחוד לדיווח ופיצוי על אירועי סייבר. הלוגיקה של מקבלי ההחלטות באירופה הינה ליצור תמריצים עבור השוק להגן על עצמו מבעוד מועד, כדי שלא לשאת בהוצאות הדיווח והפיצוי הנוקשות.[42] לבסוף, בארצות הברית מסתמנת הרחבה של אסטרטגיות הסיכון אותן נוקטת המדינה – לא רק מניעה וצמצום נזקים כתוצאה מפגיעות סייבר, אלא הסטת האחריות מחברות מסחריות במטרה לעודד שיתוף מידע. גישה זו טרם אומצה באיחוד האירופי, וספק אם תאומץ נוכח הפגיעה האפשרית בזכות לפרטיות, הנתפסת באירופה כזכות אזרחית

בסיסית עליה המדינה צריכה לשמור. שיתוף המידע כולל מתן לגיטימיות לאיסוף מידע מוגבר על ידי חברות מסחריות והעברתו למדינה, וקשה להאמין שגישה כזאת תאומץ על ידי האיחוד האירופי מבלי שיתלוו לה אחריותיות ושקיפות מתאימות.

שתי הגישות נותנות מענה חלקי בלבד. הן אינן כוללות הסדרה של המגזרים הביטחוניים־ממלכתיים (צבא, גופי מודיעין וכדומה), שבדרך קבע פטורים מרגולציה ממשלתית ובעיקר מיישמים מודל של "רגולציה עצמית", וגם לא מענה כולל למגזר האזרחי על רבדיו השונים, הכוללים חברות מסחריות, גופי תעשייה והאזרחים עצמם.

ישראל מהווה מעין ייצור כלאיים בין שתי גישות אלו. מצד אחד, רוב המגזר האזרחי בה אינו נתון תחת רגולציה מחייבת כלשהי, והמדינה (כמו בארצות הברית) מסתמכת על כוחות השוק שימצאו את האיזון הנכון בין צורכי ההגנה על מרחב הסייבר ובין ההשקעה הכלכלית הדרושה לשם כך; מצד שני, הגישה האטטיסטית באה לידי ביטוי בחברות פרטיות כמו הבנקים, שבשל חשיבותן האסטרטגית מדינת ישראל החליטה להתערב באבטחתן. המדינה אף מטילה סנקציות על חברות פרטיות במקרה שהן לא עומדות בתנאי הסף הרצויים. יש לכך יוצא מן הכלל בדמות חוק הגנת הפרטיות, הכולל בתוכו היבטים של הגנת מידע ומוכל על מחזיקי מידע אישי באשר הם בכל המגזרים. יחד עם זאת, חוק הגנת הפרטיות נחקק ב־1981 והיבטי הגנת המידע שבו טרם עודכנו.

תהליך התגבשות הרגולציה במרחב הסייבר בישראל כוללת שני שלבים עיקריים, שהתגבשו ללא אסטרטגיה לאומית שחלה על כלל המגזרים במשק.[43] ראשיתו של משטר הסייבר בישראל הוא בחוק להסדרת הביטחון בגופים ציבוריים (1998), שפירט את הדרישות להגנה על מערכות המידע של גופים שהוגדרו כ "חיוניים" למדינה. אלה כללו את גופי התעופה, תשתיות המים, החשמל והתקשורת. ב־2002 נקבע כי המנחה המקצועית של גופים אלה תהיה הרשות הלאומית לאבטחת מידע (רא"ם) הכפופה לשירות הביטחון הכללי (שב"כ).[44] כמו כן נקבע כי גופים "חיוניים" הזוכים להנחיה מרא"ם ייבחרו בקפידה על ידי ועדת היגוי ייעודית. רשימת הגופים החיוניים הלכה והתרחבה עם השנים. גופים שהוגדרו כחיוניים עבור המדינה על סמך עוצמת הנזק שהם עלולים להסב (למשל, ביחס לתל"ג) קיבלו הנחיה מדינתית, בעוד שגופים רבים שלא הוגדרו כבעלי פוטנציאל נזק גבוה נותרו ללא הנחיה, והגנתם נגזרה בעיקר משיקולים כלכליים של כוחות השוק. ראוי לציין כי הגופים המונחים הינם פרטיים וציבוריים כאחד (למשל, בתי הזיקוק, חברת אל על, חברת החשמל, חברת רכבת ישראל).

ישראל נכנסה בשנת 2011 לשלב ב' בפיתוח הרגולציה במרחב הסייבר, כאשר הממשלה שינתה את גישתה והחלה לתת את הדעת לעבודה הנדרשת מול המגזר האזרחי. הרצון ליצור אינטגרציה מוצלחת יותר עם כוחות השוק הוביל להקמת

הדומה והשונה בין המשטרים הרגולטוריים בארצות הברית, בישראל ובאיחוד האירופי

	ארצות הברית – משטר רגולטורי ליברלי – נשען על כוחות השוק וברובו וולונטרי	**ישראל – בין ליברליזם לאטטיזם – תשתיות קריטיות תחת פיקוח המדינה, והשוק נתון לכוחותיו**	**האיחוד האירופי – משטר רגולטורי אטטיסטי – ריכוזי ומחייב**
נוכחות מדינתית	במגזרים קריטיים בלבד – אנרגיה, בריאות, חשמל, מים וכדומה	במגזרים קריטיים בלבד – אנרגיה, בריאות, חשמל, מים וכדומה	במגזרים קריטיים ובספקי שירותים מקוונים
אסטרטגיות ניהול סיכונים	אסטרטגיה מתקדמת – מניעת תקיפות סייבר וכן חלוקה מחדש של האחריות כלפי סיכונים במגזר האזרחי	לא קיימת רגולציה המגבילה אחריות ומסיטה סיכון בין הישויות השונות, או כזו המחייבת צמצום נזקי סייבר לחברות וללקוחותיהן בהינתן פריצה מוצלחת	אסטרטגיה של מניעת התקפות וצמצום נזקים, ללא חלוקה מחדש של האחריות כלפי סיכונים בחברה
שקיפות כלפי צרכנים בעת אירוע סייבר	קיימת ברמת המדינות בצורה לא אחודה וב־47 גרסאות שונות	לא קיימת	קיימת באופן קוהרנטי ואחיד תחת הדירקטיבות שאושרו ב־2016 ויגיעו למימוש ב־2018
קונפליקט עם הזכות לפרטיות	מנוהל ברובו על ידי כוחות השוק, פרט למגזרים ספציפיים (רישומי בריאות, מידע על קטינים וכדומה)	מנוהל ברובו על ידי כוחות השוק, עם דרישות מחמירות יחסית שלא נאכפות במלואן על ידי הרשות למשפט וטכנולוגיה (רמו"ט)	מנוהל על ידי המדינה עם חוקים מחייבים, מוסדות בעלי כוח, ומונע מתוך אינטרסים של שמירה על פרטיות, כזכות האדם הגוברת על אינטרסים כלכליים. ברמת מדינות האיחוד, הזכות לפרטיות מתערערת אל מול סוכנויות המודיעין המקומיות

מטה הסייבר הלאומי במשרד ראש הממשלה. בהמשך, הוקמה ב־2015 הרשות הלאומית להגנת הסייבר, כגוף הביצועי להגנה על מרחב הסייבר במדינה, אשר הציב לעצמו כמטרה לעבוד ישירות עם המגזר האזרחי. באופן סכמטי ניתן לתאר את ההסדרה המדינתית במרחב הסייבר בישראל באופן הבא:

תרשים 1: אופן הפיקוח על הגנת הסייבר בישראל, 2016

שני היבטים עיקריים עולים מתרשים 1: ראשית, כפי שנטען תחילה, המגזר האזרחי בישראל ברובו אינו מונחה. ישנם "איים" שונים, כמו המגזר הפיננסי, מגזר האנרגיה ומגזר הבריאות, המונחים בעיקר על ידי יחידות הסמך שפועלות תחת הנחיית רשות התקשוב הממשלתית. עם זאת, רובו ככולו של המגזר האזרחי מתבסס על הנחייה עצמית, לוקה בשיתוף ידע ומבַצע צמצום נזקים מול הלקוחות כראות עיניו.

בנוסף לפיקוח הסלקטיבי על המגזרים השונים, מדינת ישראל הוציאה לאחרונה שתי הנחיות רגולטוריות משמעותיות. ההנחיה הראשונה, שמטרתה להגביר את הפיקוח שכבר מבוצע על ידי האגף לפיקוח על ייצוא ביטחוני במשרד הביטחון, עסקה בהרחבת היריעה[45] של מוצרים שידרשו פיקוח מדינתי, מתוך רצון של המדינה לפקח על ייצוא הסייבר ולשמור על היתרון היחסי הישראלי. המדינה החליטה להקפיא את המהלך, להמשיך את ההיוועצות עם תעשיית הסייבר ולהמשיך להיצמד לעת עתה להסדרי פיקוח בין־לאומיים בלבד. זאת, נוכח התנגדות התעשייה, שחששה כי לא תוכל להתחרות בתעשיות של מדינות שאינן מפוקחות.[46] הרצון לשמור על מעמדה של ישראל בעולם כיצואנית סייבר מובילה ביחס לגודל האוכלוסייה במדינה,[47] הביא בין היתר לשמירת הסטטוס קוו בנושא הפיקוח. ניתן ללמוד מכך על עומק ההבנה ההדדית ושיתוף הפעולה הנרחב בין התעשיות השונות בישראל ובין משרד הביטחון.[48] המשרד בא לקראת התעשייה,

אך עדיין מקבל דריסת רגל בה ונמצא במעגל קבלת ההחלטות עבור כל מוצר סייבר בעל אפיון התקפי מובהק.

ההנחיה הרגולטורית השנייה שהוציאה המדינה שמה לה למטרה לטפח את ההון האנושי העוסק בהגנת סייבר וליצור סטנדרטים עבורו. זוהי, המלצה רשמית, בה המדינה מפרטת את רמת המקצועיות הנדרשת לעוסקים בהגנת סייבר על רבדיה השונים.[49] מדובר בהנחיה משמעותית, שטרם נוסתה בהרחבה בעולם, ועשויה להעלות את רמת המקצועיות של המעורבים בהגנת מרחב הסייבר בטווח הקצר בדמות מסלולי הכשרה שונים שיפותחו במיוחד, אך גם לייתר את האופן האוטו־דידקטי בו מרבית המומחים בתחום דינמי זה צוברים ידע.[50]

רגולציית סייבר במגזר האזרחי: חשיבות וקשיים

על אף שלל המאמצים שנעשו עד כה, המגזר האזרחי בישראל אינו נתון לרגולציה בתחום הסייבר ונעדר פיקוח מדינתי על אבטחתו.[51] מדובר במצב הקיים גם במדינות אחרות ונותן את אותותיו בין השאר בארצות הברית ובאיחוד האירופי (לפחות עד לשתי הדירקטיבות האירופיות האחרונות, שלראשונה כוללות תעשיות מהמגזר האזרחי).

קשה להפריז בחשיבותו של המגזר האזרחי לעמידותו של מרחב הסייבר, וזאת מכמה סיבות: ראשית, המגזר האזרחי מהווה את חלק הארי של מרחב זה. הוא נחשף למרבית האיומים עליו ומהווה באופן מסורתי את החוליה החלשה דרכה מתחילות תקיפות רחבות על מגזרים נוספים העושים שימוש בסייבר; שנית, חברות פרטיות מספקות שירותים באופן תדיר למשרדי ממשלה וגופים מדינתיים רגישים, ועל כן עמידותן הינה אינטרס ראשון במעלה; שלישית, פגיעה במגזר הפרטי פירושה פגיעה ביציבות המשק, שעלולה בתנאים מסוימים להידרדר לפגיעה חמורה יותר בחוסן הלאומי. מדיניות ההפרטה ההולכת ומתרחבת העמיקה את הבעיה והפכה את המגזר הפרטי לגורם מרכזי עוד יותר, דבר המשליך על מאמצי הרגולציה של המדינה; רביעית, המגזר האזרחי אחראי לפיתוחים הטכנולוגיים עליהם נשענים מגזרים רגישים יותר, ופגיעה בו עלולה להוות "דלת אחורית" וכר פורה לתקיפת מידע רגיש.[52] הדבר נכון במיוחד לחברות הזנק הדלות במשאבי הגנה, אך לעיתים קרובות מפתחות מוצרי הגנה לשימוש הכלל.[53]

התנגדותו העקרונית של המגזר הפרטי לרגולציה אינה מפתיעה, שכן היא חוצה תחומים ונושאים שונים. רגולציה מדינתית ופיקוח נתפסים כמגבילים חברות מסחריות וכמביאים עמם עלויות נכבדות שאין מאחוריהן תועלת משמעותית.[54] בנוסף, המגזר הפרטי תופס את המדינה כגורם שמגיב לאט לשינויים טכנולוגיים ואינו יכול לעמוד באתגרים הניצבים בפני פיקוח על מרחב טכנולוגי דינמי ומשתנה כמו מרחב הסייבר.[55] לפי תפיסתו של המגזר האזרחי, במקום להגביר את עמידות

החברות המסחריות, רגולציה מדינתית עלולה לפיכך לאלץ אותן לאמץ סטנדרטים שאינם תואמים עוד את האיומים הנוכחיים ולמנוע מהן את הגמישות ממנה הן נהנות כיום. לבסוף, הרעיון של התערבות מדינתית אינו עולה בקנה אחד עם גישת הניאו־ליברליזם שהתפשטה כאש בשדה קוצים בחברות קפיטליסטיות במאה העשרים.[56] הפרדיגמה השלטת היא פרדיגמה של הפרטה ודה־רגולציה, לפיה על המדינה להתערב באופן מזערי, אם בכלל, בנעשה בשוק, וזאת כדי למקסם תועלות עבור החברה המסחרית.[57]

תובנות מסכמות

על אף שמדינת ישראל מקדמת את הקמתה של הרשות הלאומית להגנת הסייבר, מגזרים רבים במשק עדיין נעדרים כל הנחיה ופיקוח שיבטיחו הגנה ראויה. חסרה מפת דרכים שתבטיח את חוסנו של המגזר האזרחי ותהווה מודל שיאומץ על ידי השחקנים השונים במשק.

מודל כזה יידרש לתת מענה למספר נקודות מפתח. ראשית, יהיה עליו ליצור תהליך מובנה שיתמרץ גופים אזרחיים לאמץ הגנה קיברנטית. "רגולציית כניסה" דרך חוק רישוי עסקים ברשויות המקומיות היא דרך אחת, אך ניתן לחשוב על דרכים נוספות. השאיפה היא לייצר מעין "חותמת סייבר" מקצועית שתעיד כי הגוף האזרחי מוגן כראוי. המדינה עמלה בימים אלה על חוק הסייבר, שיקבע סטנדרט הגנה אחוד לצורך קבלת תו תקן.[58] ייתכן שהצורך בחותמת אבטחה כזאת יתמרץ גופים להגן על עצמם טוב יותר.

שנית, יש לתת את הדעת לשכבות השונות במגזר האזרחי, שכן אין פתרון אחד שמתאים לכולם ויש צורך בהתאמה מדוקדקת של "חליפת" הרגולציה בהתאם לעיסוק, לרגישות המידע, להליכי הייצור ולשרשרות האספקה של החברות השונות במשק. על כן, יש לבצע מדרוג של המגזר האזרחי על פי חשיפתו לסיכונים והנזק שפריצה למערכותיו עלול לגרום. דין חברת ביטוח אינו כדין חברת תרופות, והמודל המוצע יצטרך לתת את הדעת על הבדלים מהותיים אלה.

שלישית, יש לשקול הרחבה של אסטרטגיות הסיכון אותן נוקטת המדינה. מהסתכלות רוחבית על סקירת הרגולציה הישראלית ניתן ללמוד כי המדינה עוסקת בעיקר במניעת התממשותם של סיכוני סייבר. ייתכן שמגנוני שיתוף המתפתחים בארצות הברית[59] במטרה לעודד שיתוף מידע, מחברות מסחריות, אך עם אי־פגיעה מרבית בזכות לפרטיות, יאפשרו לפתוח את צוואר הבקבוק של העברת המידע וייצרו הגנת סייבר פרו־אקטיבית ויעילה יותר.

לבסוף, יש לפעול להגברת השקיפות על אירועי סייבר בשגרה, תוך חיוב של כל המגזרים לדווח ל־CERT הלאומי, ושיתוף מידע עם האזרחים. הדבר יסייע ללמוד ממה להיזהר ולהבין עד כמה מידע רגיש נמצא בסיכון.

כל הנקודות שנמנו לעיל עשויות ליצור תמריצים יעילים יותר להגנה ולמזעור נזקים (mitigation). חברות מסחריות יחששו מלשאת בהוצאות הכרוכות במזעור הנזקים המעוגנות בחוק, ויש להניח כי יגנו על עצמן בצורה מרבית מבעוד מועד.

לסיכום, הצורך ברגולציית סייבר במגזר האזרחי בישראל הינו ברור. עם זאת, הקשיים בפיתוח רגולציה כזאת הם רבים, החל בקשיים ובמאבקים בין מוסדות המדינה, דרך נקודות חיכוך בין אינטרסים שונים ועלויות הכרוכות בציות לרגולציה, ועד לרצון למצוא את האיזון הנכון בין שקיפות לסודיות ובין ריכוזיות לביזור.

מרחב הסייבר בישראל הוא אזרחי במהותו – רובו המכריע מבוסס כיום על תשתיות, מערכות וטכנולוגיות אזרחיות המופעלות על ידי ארגונים אזרחיים. אף על פי כן, המגזר האזרחי טרם הוסדר וסונכרן אל תוך משטר הרגולציה בישראל. אחריות ההגנה על מרחב הסייבר במגזר זה נתונה כיום בידי הארגונים האזרחיים בלבד. אין בכוחו של הארגון הבודד להעמיד את המומחיות והמשאבים הדרושים כדי להתמודד עם האיומים במרחב הסייבר ללא יצירת תשתית לשיתוף פעולה עם שאר המגזרים במשק.

ישראל פועלת באופן לא מבוטל להגנה על מרחב הסייבר ברמה המדינתית. המדינה הקימה יחידות סמך במשרד ראש הממשלה, קיבלה החלטה על הקמת זרוע סייבר והקימה מסגרות למחקר ופיתוח ומרכזי מחקר לאומיים בתחום הסייבר. עם זאת, המדינה טרם עשתה די להגנת אותם גופים במגזר האזרחי שפגיעה בהם עלולה לפגוע מהותית גם בה. מצב זה מחייב את ממשלת ישראל להמשיך את החתירה ליצירת מסגרת שתאפשר הגנה יעילה על המגזר האזרחי הרלוונטי, וזאת באמצעות מגוון כלים ויכולות בתחום הגנת הסייבר.

הערות

1 המושג "חוסנו של מרחב הסייבר" מתייחס לעמידותו לפגיעות אפשריות כתוצאה מחולשות תוכנה/חומרה, פרוטוקולים לא מאובטחים וגישה לא מורשית למידע.

2 פיתוחם של פרוטוקולים אלה תאם את הצרכים עם ראשיתה של רשת האינטרנט בשנות השישים של המאה הקודמת. הצורך באותם ימים היה לאפשר קישוריות בין כמה עשרות מחשבים, כאשר אף אחד לא חזה כי על פרוטוקולים אלה תישען רשת של מיליארדי משתמשים.

3 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.com, April 17, 2015, https://www.wired.com/2015/04/therealdeal-zero-day-exploits.

4 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, http://www.nytimes.com/2016/05/30/

technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?ref=topics&_r=0.

5 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 (2) (2014): 103-111.

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

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

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

9 U. Beck, Risk Society: Towards a New Modernity (Sage Publishing, 1986).

10 David Moss, When All Else Fail: Government as the Ultimate Risk Manager (Harvard University Press, 2002).

11 שם.

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

13 סיכוני צד שלישי בעולם הסייבר הינם סיכונים לפרטיות לקוחות של חברות מסחריות הנפגעים כתוצאה מפגיעת סייבר וגניבת מידע אישי. חברות הביטוח לא ששות לבטח סיכוני צד ראשון, מאחר ויש חוסר במידע אקטוארי שיסייע לתמחר פרמיות ביטוח עבור סיכוני סייבר לחברות עצמן (קרי, סיכוני צד ראשון).

14 שם.

15 Giandomenico Majone, "The Rise of the Regulatory State in Europe", West European Politics, Vol. 17 (1994): 77-101.

16 פרופ' לוי־פאור מסביר במאמרו "Regulation and Regulatory Governance" מדוע דה־רגולציה מזמינה עוד סוכנויות ופקידים לפיקוח על הפרטות ולשמירה על האינטרסים של המדינה: David Levi-Faur, "Regulation &Regulatory Governance", Department of Political Science & The Federmann School of Public Policy & Government, The Hebrew University, Mount Scopus, Jerusalem, February 2010.

17 שם.

18 שוריק דריישפיץ, "רגולציה – מה, איפה ומתי? מבט תאורטי ומשווה", **פרלמנט**, גיליון 64, מארס 2010: **מי הפריט את המדינה שלי? הפרטה, רגולציה, והמגזר השלישי: תיאוריה ומעשה**, המכון הישראלי לדמוקרטיה.

19 ראו לדוגמה: Harlod Demsetz, "Why Regulate Utilities?", Journal of Law and Economics, Vol. 11 (1968): 55-65.

20 למחקר אמפירי שבחן את הפעילות של קבוצות אינטרס 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): 1191-1213.

21 מחקר לדוגמה על האופן בו המדיניות להגנת הפרטיות באירופה יצרה מוסדות חזקים שהעבירו חוקי פרטיות נוקשים שנגדו את רוח התקופה: A. L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive", International Organization, Vol. 62 (01), (2008):103-130.

22 מחקר העומד על העקביות של מדינת הרווחה המודרנית: P. Pierson, The New Politics of the Welfare State (Polity Press, 2006).

23 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 (3) (1993):275-296.

24 מחקרו של John Kingdon הטביע מושגים כגון "חלון הזדמנויות" ו"יזם מדיניות" שמסבירים בצורה מדויקת להפליא את הליך המדיניות הציבורית: John Kingdon, Agendas, Alternatives and Public Policy, 2nd edition (Boston: Little, Brown, 1995).

25 D. Béland & R. H. Cox eds., Ideas and Politics in Social Science Research (Oxford University Press, 2010), Introduction.

26 אמנם, האיחוד האירופי שונה מהמוסד המדינתי הקלאסי, אך יחד עם זאת הוא מהווה אובייקט חיוני למחקר השוואתי בתחום הסייבר. ההחלטות ברמת האיחוד האירופי הובילו למדיניות הגנת מידע נוקשה בכל רחבי האיחוד, והדירקטיבות המתקבלות ברמת האיחוד מתוות את הדרך למדינות השונות. הדברים תקפים לא רק בהקשרי סייבר. ניתן לראות את השפעת האיחוד האירופי גם בהקשרים של רגולציה על בטיחות מזון ואימוץ מוצרים מהונדסים גנטית במדינות השונות. על חשיבותו הרגולטורית של האיחוד האירופי ראו: David Bach and Abraham L. Newman, "The European Regulatory State and Global Public Policy: Micro-institutions, Macro-influence", Journal of European Public Policy, Vol. 14:6 (2007): 827- 846.

27 Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security", Georgetown Journal of International Affairs, International Engagement on Cyber, Vol. IV (October 2014): 69-78.

28 לאופן בו האקרים משתפים מידע ב־Darknet ראו ראיון עם Stuart Madnick מ־MIT: Linda Tucci, "Stuart Madnick: Dark Web Hackers Trump Good Guys in Sharing Information", techtarget.com, April 30, 2016, http://searchcio.techtarget.com/news/450295259/Stuart-Madnick-Dark-Web-hackers-trump-good-guys-in-sharing-information.

29 התערבות מוגברת וריכוזית של הממשלה.

30 ראו דיון פילוסופי המאתגר את המושגים "משחק סכום אפס" ו"איזון נדרש" בין ביטחון לחירויות הפרט: Jeremy Waldron, "Security and Liberty: The Image of Balance", Journal of Political Philosophy, Vol. 11 (2) (2003):191-210.

31 דרכי התמודדות אלו עולות כאשר בוחנים את הדרך בה מבוצעת רגולציה לאורך השנים בארצות הברית (ברמה הפדרלית וברמת המדינות) ובאיחוד האירופי (ברמת האיחוד וברמת המדינות החברות בו).

32 למשל, בית המשפט בארצות הברית העניק לאחרונה סמכות ל־Federal Trade Commission (FTC) לאכוף חוקי הגנת מידע במגזר הפרטי. לפרטים נוספים ראו: Brent Kendel, "Appeals Court Affirms FTC Authority over Corporate Data-Security Practices", The Wall Street Journal, August 24, 2015, http://www.wsj.com/articles/appeals-court-affirms-ftc-authority-over-corporate-data-security-practices-1440425754.

33 Cyber Emergency Readiness Team (CERT) – סוכנות רגולטורית הקיימת היום כמעט בכל מדינה. הסוכנות מרכזת את כל אירועי הסייבר החייבים בדיווח ומתכללת תגובה לאירועים משמעותיים שקורים במרחב.

34 Siboni, "An Integrated Security Approach".

35 למשל, הנחיות של הרשות לאבטחת מידע בישראל על האופן בו יש לאבטח רשתות ארגוניות.

36 להסבר על תקני ISO ראו האתר הרשמי: http://www.iso27001security.com/html/27032.html.

37 להסבר על תקני PCI ראו האתר הרשמי: https://www.pcisecuritystandards.org/.

38 ראו לדוגמה סטנדרטים שהפיץ הארגון: http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

39 למשל, דוח אחרון של FINRA שהוצא בנושא זה: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

40 Richard J. Harknett, James A. Stever, "The New Policy World of Cybersecurity", Public Administration Review, Vol. 71 (3) (May/June 2011): 455-460.

41 ראו פירוט: "Security Breach Notification Laws", National Conference of State Legislators (NCSL), April 1, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

42 לפירוט בנושא ההשפעה של הרגולציה האירופית על רמת האבטחה של חברות מסחריות ראו: Warwick Ashford, "Breach Notification the Biggest Impact of EU Data Law Overhaul, Says Law Firm", computerweekly.com, November 27, 2015, http://www.computerweekly.com/news/4500258249/Breach-notification-the-biggest-impact-of-EU-data-law-overhaul-says-law-firm.

43 סיבוני ואסף, "קווים מנחים לאסטרטגיה לאומית במרחב הסייבר", עמ' 22.

44 בשנת 2015 הוקמה הרשות הלאומית להגנת הסייבר שקבלה על עצמה את האחריות על הנחיית עיקר גופי התשתיות הקריטיות במדינת ישראל.

45 הרחבה הכוללת בעיקר מוצרי חדירה, ניתוח פריצות וידע על קיומן של חולשות חומרה/תוכנה.

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

47 למהפכה בעיר באר שבע, שהמדינה שמה לה למטרה להפוך לבירת ייצוא הסייבר האזורית, ראו: Warwick Ashford, "Israel's Cyber Security Frontier", computerweekly.com, May 2016, http://www.computerweekly.com/opinion/Israels-cyber-security-frontier.

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

49 למסמך ההסדרה הרשמי ראו: "מדיניות אסדרת מקצועות הגנת הסייבר במדינת ישראל", **משרד ראש הממשלה – מטה הסייבר הלאומי**, 31 בדצמבר 2015, http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf.

50 ראו דוח בנושא: Professionalizing the Nation's Cybersecurity Workforce (Washington D.C., The National Academy of Sciences, 2013), http://www.nap.edu/catalog/18446/professionalizing-the-nations-cybersecurity-workforce-criteria-for-decision-making.

51 פרט לישויות ספציפיות כמו הבנקים, או לחוק הגנת הפרטיות שחל על כלל המשק אבל לא מספיק מעודכן בהיבטי אבטחת מידע. ראו סקירה בכתבה של רפאל קאהאן,

"נתניהו משווק את הסייבר הישראלי אבל החקיקה בארץ פרוצה", **כלכליסט**, 25 ביוני 2015, http://www.calcalist.co.il/internet/articles/0,7340,L-3662815,00.html.

52 לסקירה מעמיקה יותר של חלק מהסיבות הנ"ל ראו: Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security".

53 גבי סיבוני, דוד ישראל, "הריגול בסייבר והשפעתו על שיקולי חברות עסקיות", **צבא ואסטרטגיה**, כרך 7, גיליון 3, דצמבר 2015.

54 Etzioni, "The Private Sector: A Reluctant Partner in Cyber Security".

55 שם.

56 לסקירה על הגישה הניאו־ליברלית בחברות קפיטליסטיות ראו: John Dryzek, Democracy in Capitalist Times: Ideas, Limits and Struggles (Oxford University Press, 1996).

57 האם הפרטה באמת מובילה לדה־רגולציה? על אתגור הצידוקים להפרטה ראו: יצחק גל־נור, **מדיניות ההפרטה – על מי נטל ההוכחה?** (ירושלים: האוניברסיטה העברית ומכון ון ליר, 2014). על רגולציה בעידן של הפרטות ראו: דוד לוי־פאור, נעם גדרון, סמדר מושל, **הגרעון הרגולטורי של עידן ההפרטה** (ירושלים: מכון ון ליר, 2014).

58 ראו: יוסי מלמן, "קוד סגור: המדינה מקדמת חוק הגנת הסייבר על רקע התגברות התקיפות", **אתר מעריב**, 6 בפברואר 2016, http://www.maariv.co.il/journalists/Article-524985.

59 Andy Greenberg, "Congress Slips CISA into a Budget Bill that's Sure to Pass", Wired.com, December 16, 2015, http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/; Tim Greene, "CISA Legislation would Fit Liability for Businesses Sharing Cyber Threat Information", networkworld.com, October 28, 2015, http://www.networkworld.com/article/2998815/security/cisa-legislation-would-lift-liability-for-businesses-sharing-cyber-threat-information.html