הגנה על תשתיות קריטיות מפני איום קיברנטי

ליאור טבנסקי

מבוא

תפקוד החברה המודרנית מבוסס על מארג סבוך של תשתיות שונות: אנרגיה, תקשורת, תחבורה, מזון ועוד. מאמר זה עוסק באיום הקיברנטי המתפתח על תשתיות מידע חיוניות (Critical Information Infrastructure). המאמר נועד לתרום לדיון ציבורי מושכל באיום הקיברנטי על תשתיות חיוניות, תוך התמקדות בסוגיות המיוחדות לו הדורשות התייחסות בין־תחומית, בגישות להתגוננות מפניו, במענה הישראלי הקיים ובאתגרים המתפתחים. פיתוח הדיון הציבורי עשוי להוביל לשיפור ההגנה על תשתיות לאומיות במגזר האזרחי והציבורי.[1]

המאמר נפתח בהמשגת נושא התשתיות החיוניות ודן במקורותיו, ייחודו וחדשנותו של האיום. בהמשך נדונים רבדים של ההתמודדות עם האיום, בהקבלה מושגית לעולם התוכן הצבאי. המענה הישראלי הקיים נסקר בקצרה, ובעקבותיו מודגשים האתגרים המרכזיים של האיום הקיברנטי למדיניות הציבורית. לבסוף מוצגים כיווני מחקר ופעולה עתידיים.

"תשתית מידע חיונית": ביאור והמשגה

תשתית (Infrastructure) היא מערכת המשלבת מתקנים שונים ומאפשרת לבצע פעולות שונות. היא כוללת, בין השאר, צנרת הולכת מים מבארות לבתים ולשדות, כבישים סלולים, גשרים וצמתים המאפשרים תנועה של אנשים וסחורות, תעופה, תקשורת, דלק, בריאות ועוד. בעידן המידע, התשתיות המסורתיות הופכות לתשתיות מידע עקב שיבוץ המחשבים בהן. בנוסף לכך, נוצרו תשתיות חיוניות חדשות, שהן על טהרת המידע: מאגרי מידע ממוחשבים המכילים נתונים חשובים כגון רישומי ההון במערכת הבנקאית, קניין רוחני מדעי וטכני ועצם הלוגיקה

ליאור טבנסקי הוא חוקר בתכנית לחקר לוחמה קיברנטית, הנתמכת על ידי קרן ג'וזף וג'נט ניובאוואר, פילדלפיה, ארצות הברית

המתוכנתת שמנהלת תהליכי ייצור ותהליכים עסקיים שונים. בעידן המידע, המושג "תשתית" כולל גם מרכיבים ממוחשבים. כשאומרים היום תשתית מתכוונים בהכרח לתשתית מידע (Information Infrastructure).

אחד המאפיינים של תשתית הוא התלות של תחומי עיסוק שונים בה. בעבר, התלות נבעה מקשרי גומלין פיזיים או גיאוגרפיים בלבד. עם התפתחות המרחב הקיברנטי, הכולל מערכות תקשורת מידע ואמצעים ממוחשבים לשליטה ובקרה אוטומטית, נוצרו קשרי גומלין נוספים היוצרים פגיעות נוספת. מדובר בקשרי גומלין ממוחשבים (למשל, שליטה ובקרה באמצעים אלקטרוניים ומרחוק) ולוגיים (למשל, השוק הפיננסי הבינלאומי כגורם המשפיע על תשומות ותפוקות של התשתיות החיוניות), המהווים חידושים שלא היו מתקיימים ללא טכנולוגיות המידע. לכן, כדאי להבחין בין תשתית במובן המילוני המסורתי ובין השימוש המודרני במושג זה, המכיל ממד קיברנטי.

תשתית מוגדרת חיונית כאשר סבורים ששיבוש תפקודה יוביל למשבר כלכלי־חברתי משמעותי, בעל פוטנציאל לערעור היציבות בחברה ועם השלכות פוליטיות, אסטרטגיות וביטחוניות. מדינות שונות מציגות הגדרות שונות למונח "תשתית חיונית",[2] אך המשותף לכולן הוא שמדובר בתשתית בעלת ממד ממוחשב, בה תלויות מערכות פיזיות נוספות, שפגיעה בתפקודה עלולה לגרום לנזק רחב בממד הפיזי.[3]

אפשר לזהות שלושה מקורות להגדרת תשתית כקריטית: הראשון – המשקל הסמלי של התשתית. כך, למשל, שיבוש עוין של אמצעי התקשורת המסורתיים המשמשים את המדינה להעברת מסרים לאזרחים יפגע באופן מיידי ביכולת התפקוד של השלטון. יתרה מזאת, בטווח הארוך יפגע שיבוש כזה קשות באמון האזרחים בממשלה או אף במשטר הקיים. מדינות דמוקרטיות אחדות כוללות את אתרי המורשת, המוזיאונים, הארכיונים והאנדרטאות שלהן בתשתית החיונית הראויה להגנה גם מפני איום קיברנטי.[4]

השני – התלות המיידית בתשתית, כגון רשת החשמל או רשת המחשבים, בהן תלויים רוב התהליכים בחברה. חדירת המחשוב וקישורו ברשתות ממוחשבות יצרו מצב שבו המערכות הממוחשבות מהוות תשתית בפני עצמה. המרחב הקיברנטי עצמו הוא דוגמה מייצגת לתשתית שהפכה לקריטית בגלל הממשק של רוב הפעילות בחברה עם רשתות התקשורת הממוחשבות.

השלישי – קשרי גומלין מורכבים: המגמה המואצת של הוספת יכולות קישוריות יוצרת השפעות לא צפויות מעבר לרמה המקומית ("אפקט הפרפר").[5] יש להניח שקשרי הגומלין בין התשתיות השונות אינם מוכרים במלואם, וכֶשל של רכיב אחד עלול לגרום למגוון רחב של תוצאות ונזקים. אפשר לחלק את סוגי הכשל לשלושה טיפוסים:

1. כשל הנגרם מִסיבה משותפת (Common Cause Failure). למשל, מתקנים שונים (מאגר דלק, שדה תעופה ותחנת כוח) הממוקמים בסמיכות גיאוגרפית עשויים להיפגע ממקרה בודד של הצפה. קשה לראות מתקפה קיברנטית שתגרום במישרין לכשל מסוג זה.
2. כשל מידרדר (Cascading): שיבוש מערכת בקרה בתשתית אחת (מים) גורם לשיבוש בתשתית שנייה (תחבורה: למשל הצפת קו רכבת), גם אם זו אינה תלויה בה במישרין. מתקפה קיברנטית יכולה לגרום במישרין לכשל מסוג זה.
3. כשל מסלים (Escalating): שיבוש תשתית אחת (למשל, רשת תקשורת) פוגע במאמץ לתקן תפקוד של תשתיות אחרות שנפגעו מגורם אחר (שירותי חירום, מסחר, שליטה מרחוק).[6] מתקפה קיברנטית יכולה לגרום במישרין לכשל מסוג זה.

להדגמת חשיבותן של תשתיות קריטיות והמשמעות של פגיעה בהן ניתן להשתמש במגזר התעופה המסחרית. מגזר זה משך את תשומת לבם של אויבי המדינות המפותחות והביא אותם לנקוט שורה של צעדים נגדו: חטיפת טיסות מסחריות, פיגועי ספטמבר 2001 בארצות הברית וניסיונות טרור נוספים באמצעות מטוסי נוסעים.

התעופה האזרחית מהווה תשתית שעל בסיסה מתקיימות פעילויות מגוונות בחברות המפותחות. התחבורה האווירית המסחרית הובילה ב־2009 יותר משני מיליארד נוסעים ב־28 מיליון טיסות של 27 אלף מטוסים הפועלים מ־3,670 שדות תעופה מסחריים בעולם.[7] בנוסף לטיסות המסחריות מאכלסים את המרחב האווירי כלי טיס צבאיים (חלקם בלתי מאוישים) ופרטיים. חוקים, תקנות ונהלים פנים־מדינתיים, לצד שיתוף פעולה בין־לאומי, מסדירים את ההיבט האדמיניסטרטיבי של ענף התעופה.

שדות התעופה קשורים זה לזה בתנועת המטוסים המתוכננת, ומערכת בקרת התנועה האווירית בכל אתר נתון היא חלק מתשתית התעופה הבין־לאומית. הבקרה האווירית מבוססת על מערכות ממוחשבות: אמצעי גילוי, ניטור, מעקב, אוטומציה, תקשורת, שליטה ובקרה ועוד. שיבוש התפקוד התקין של מערכת הבקרה האווירית יפגע בתנועה האווירית כולה.

חדשנות האיום

בשנים האחרונות אנו עדים להתגברות הדאגה מפני הפגיעות האפשרית של התשתיות המונחות ביסוד החברה המודרנית המפותחת.[8] עצם התעוררות הדיון הזה כעת אמורה להפתיע. תשתיות חיוניות היו חיוניות תמיד וחשיבותן גלויה לכול. סכסוכים בין־לאומיים ופנימיים שונים קיימים ומתפתחים ברחבי

העולם, ובמלחמה סביר לצַפות לניסיונות לפגוע בתשתית החיונית של היריב, במטרה להחליש ולהכניע אותו. לנין וטרוצקי הורו לפעיליהם במהלך המהפכה הבולשביקית ב־1917 להשתלט על הדואר, הטלפון, הטלגרף, גשרים ותחנות רכבת. במלחמות ממושכות, כמו במלחמת העולם השנייה, נעשו ניסיונות לפגוע בתשתית חיונית כדי לשבש את כושר הלחימה ואת רוח האויב.[9] תשתיות חיוניות של מדינה, יהיו אשר יהיו, הן יעד טריוויאלי במהלך סכסוך. לכן, ארגונים ומדינות עמלו לאורך כל ההיסטוריה על מערכי הגנה: הסוואה, שמירה, ביצור, כוח מגן, הרתעה וכיוצא באלה. מדוע, אפוא, גבר דווקא לאחרונה החשש מפני פגיעה בתשתיות חיוניות, ועוד במדינות החזקות ביותר?[10]

אין עוררין על העובדה כי המדינות המפותחות נהנות מעליונות צבאית מוחלטת על פני אויביהן השונים. מדינות אלו לא חוו מלחמות בשטחן בעשרות השנים האחרונות. ישראל היא המדינה המפותחת היחידה הנמצאת תחת איום צבאי מתמשך המתממש בצורות שונות (מתקפות טילים ב־1991, רקטות בצפון המדינה ובדרומה,[11] ומחבלים מתאבדים בשנים 2000–2005). כמה מהמדינות המפותחות נפגעו ממעשי איבה שפגעו ישירות באזרחיהן, תוך עקיפת עוצמתן הצבאית שהייתה אמורה להגן עליהם. מתקפות הטרור לא יכלו לאיים על המדינות המותקפות, אולם הן הצליחו לגרום לשינוי מדיניותן בצורה זו או אחרת.

תשתית חיונית היא מטרה מפתה לאויב, יהיה זה ארגון טרור או מדינה עוינת. בכל צורות המלחמה המסורתיות, זהות האויב מתגלה בוודאות לאחר התקיפה, כי זו חייבת להתבצע באמצעות הגעה פיזית של חימוש אל המטרה. גם במקרה של שיגור טילים לא קיים ספק באשר למיקום אתר השיגור. חטיפות טיסות מסחריות בשנות השבעים של המאה הקודמת, פיגועי המתאבדים בריכוזי אזרחים בישראל, הפיגועים בארצות הברית בספטמבר 2001 והפיגועים במדריד ב־2004 ובלונדון ב־2005 גם הם דרשו נוכחות פיזית של המפגעים במקום התקיפה.

זיהוי האויב חיוני לצעדי תגובה ולהרתעה. ניתן לומר שמה שמנע פגיעה בתשתיות החיוניות בעבר היה כוח המגן שניצב בדרכי האויב, ובמיוחד ההרתעה שהבטיחה לגבות ממנו מחיר כבד. מצב עניינים מוכר זה הגיע לקצו עם התפתחות המרחב הקיברנטי. לראשונה בהיסטוריה ניתן לתקוף מטרות איכות (כמו תשתית חיונית) מבלי להגיע פיזית אל המקום בו הן נמצאות, מבלי להתמודד עם כוחות המגן ומבלי להיחשף. במצב הנוכחי ניתן להשתמש לרעה בתשתית הממוחשבת הקיימת כדי לשבש או להשבית מערכת חשובה, וזאת באמצעות חדירה אל רשת התקשורת, אל התוכנה או החומרה של מחשבי הפיקוד והבקרה.[12] האיום נובע מהפגיעות שמקורה במאפייני המרחב הקיברנטי הקיים.[13] המאפיינים המיוחדים של המרחב הקיברנטי גורמים לכך שהאתגר שבאיום הקיברנטי שונה באופן מהותי מהאתגרים שבאיומים המסורתיים.

רבדים בהתמודדות

כאמור, מאמר זה עוסק רק באיום הקיברנטי על הממד הממוחשב של התשתיות, לאור ההבנה שאיום כזה הפך לאפשרי, זמין ומשמעותי ועלול לשבש את תפקוד החברה המפותחת.

ההתמודדות עם האיום על תשתיות מידע חיוניות כוללת מניעה, התרעה, זיהוי וגילוי ההתקפה, תגובה, ניהול המשבר, בקרת נזקים וחזרה לתפקוד מלא. כאשר בוחנים התמודדות עם איומים על הביטחון הלאומי, מקובל לחלק את הדיון לרמות הטקטית, המבצעית והאסטרטגית. מאמר זה מציע לדון בהתמודדות עם האיום על תשתיות מידע חיוניות בחלוקה לכמה רבדים: טכנולוגי; טכני־מבצעי; אופרטיבי; אסטרטגי־לאומי.

הרובד הטכני מתמקד במערכת ממוחשבת ארגונית, שהיא הפעילות הנפוצה ביותר בתחום. לאור נפח הפעילות הגדול, משתמשים לעתים קרובות בהיבט הטכני של "אבטחת מידע", בעוד שמדובר במושג שמתייחס הן להגנה על תשתיות חיוניות והן לביטחון הקיברנטי בכלל. בנוסף לכך, מתפתחת פעילות הבוחנת את הסוגיה במבט לאומי כולל. זו תיקרא להלן "הרובד הלאומי" של הביטחון הקיברנטי.

כל הרבדים נדרשים להתמודד עם האיום, אולם לאור המיקוד השונה כדאי להבחין בין שכבות ההגנה הללו. החלוקה המוצעת תסייע להבחין במהות אתגרי ההגנה על תשתיות חיוניות כמקרה פרטי של הביטחון הקיברנטי.

הרבדים הטכניים – הרמות הטקטית והמבצעית

מכיוון שהאיום נגזר ממאפייני טכנולוגיות המחשבים, בדרך כלל מחפשים את המענה לו בקרב אנשי המחשבים. כצפוי, הפתרונות המוצעים מבוססים גם הם על טכנולוגיות המחשבים. הבעיה נתפסת כסוגיה טכנית, ולכן הפתרון המוצע הוא הנדסי. השכבות הטכנית והמבצעית בהתמודדות עם האיום הקיברנטי, שמקורן במקצועות ההנדסה, המתמטיקה והמחשבים, מתמקדות בזיהוי פגיעויות במערכת ממוחשבת ארגונית ומחפשות מענה הנדסי שיצמצם פגיעות זאת. טבלה 1 מרכזת סוגיות נפוצות שעמן מתמודדים הרבדים הטכניים של ההגנה.[14]

האמצעי העיקרי במאמץ לבנות עמידות[15] הוא השקעה בגיבוי, ביתירות, בהפרדה וכדומה. כידוע, מערכות ממוחשבות חשובות נבנות פעמיים, באתרים נפרדים, כדי לזכות ביכולת להמשיך לתפקד במקרה של פגיעה פיזית במערכת.

אספקת המענה לבעיות ההנדסיות שזוהו מתבצעת כיום לרוב באמצעות השוק הפרטי. תעשיית אבטחת המידע היא תחום עסקי ענֵף שתיאורו חורג מגבולות מאמר זה. בחלוקה המוצעת כאן, אבטחת מידע נמצאת ברבדים הטכניים־מבצעיים. אבטחת מידע היא דיסציפלינה מתפתחת המרכזת משאבים רבים למחקר ופיתוח, שירותי יעוץ ומיקור חוץ, תעשיית מוצרי אבטחה וכיוצא

טבלה 1: מרכיבים ומאפיינים פגיעים במערכות – רשתות מחשב

תיאור המרכיב	סיווג טכני
סיסמאות גישה להתקנים ומערכות נשארו בהגדרות ברירת המחדל.	ניהול סיסמאות
סיסמאות נשמרות ומועברות ללא הצפנה.	
סיסמאות גישה לא מוחלפות.	
אבטחה פיזית לוקה בחסר.	אבטחת גישה פיזית
קיימת אפשרות גישה לציוד קריטי לאנשים שאינם עוסקים בציוד זה.	
ניהול הרשאות משתמשים לקוי מאפשר לעובד זוטר גישה לתהליך קריטי.	אבטחת גישה מחשובית
"חומת אש" מוגדרת כך שמאפשרת סוגי תקשורת מיותרים.	
הרשת התהליכית אינה מופרדת מהרשת המשרדית.	
האפשרות לגישה מרחוק למערכת המחשוב הושארה פתוחה.	
קיימת אפשרות גישה למערכת המחשוב ברשת אלחוטית.	
תהליך הגישה מרחוק משתמש בפרוטוקול פתוח ובסיסמאות חלשות.	
יצרן המערכת סיפק עדכוני אבטחה אולם אלה לא הותקנו במערכת.	ניהול תצורה
הרשאות מִנהלן הוענקו למשתמשי המערכת.	
גישה לרכיבי המערכת החיונית לא מנוטרת; לא נאסף מידע יומן (Log).	
מידע יומן לא נבדק באופן שוטף.	

באלה. שוק אבטחת המידע העולמי צפוי לגדול ל־125 מיליארד דולר ב־2015, ורוב ההכנסות ממנו יגיעו אל חברות אמריקאיות ואירופיות המציעות חבילות משולבות של שירותים ומוצרים טכניים יחד עם יעוץ עסקי־טכנולוגי.[16]

סוגיית הביטחון הקיברנטי, ובמיוחד ההגנה על תשתיות חיוניות, נוצרה עקב השינוי הטכנולוגי. תחילה היה צפוי פתרון טכני לבעיה שמקורה טכני. אולם נראה שמתפתחת הבנה שההתמודדות לא יכולה להסתכם ברובד הטכני־מבצעי לבדו, שכֵּן לא תיתכן נוסחה הנדסית מדויקת להתמודד עם האיום הקיברנטי: מבנה החברה, ערכיה ומוסדותיה הם חלק בלתי נפרד מהסביבה.

הרובד הלאומי – הרמה האסטרטגית

הרובד הלאומי העליון בוחן את האיום על תשתיות חיוניות במסגרת תפיסת הביטחון הלאומי, במיקוד לאומי החורג מגבולות של ארגון או של תהליך עסקי. זוהי גישה הרואה בהגנה על תשתיות מידע חיוניות חלק ממשימת ההגנה על החברה בכללותה. ההגנה על תשתיות המידע הופכת למעשה להגנה על חברה מבוססת־ידע.[17]

אבטחת המידע, העומדת במרכז הרובד הטכני, היא חלק הכרחי אך בלתי מספיק בראייה האסטרטגית. אפשר לומר שהרובד הלאומי העליון מבוסס על הרבדים הטכניים והמבצעיים הבסיסיים, אולם הגישה הרחבה לא מסתפקת בתיקון הבעיות המקומיות של המערכות הארגוניות. בהקבלה לתחום הצבאי, הרובד האסטרטגי זקוק לרמה מבצעית נאותה, אך זו אינה מספיקה להשגת המטרה האסטרטגית.

בראייה לאומית רחבה, נדרשת מדיניות לאומית כוללת בתחום ההגנה על תשתיות חיוניות, שבנוסף על היסודות ההנדסיים תביא בחשבון היבטים חברתיים, פוליטיים, כלכליים וארגוניים מורכבים. כן נדרש גורם ארגוני שמסוגל להביא בחשבון את מכלול קשרי הגומלין המורכבים בין התשתית החיונית ובין תפקוד תקין של החברה והמדינה. זהו ללא ספק אתגר מורכב למדיניות ציבורית, בהתחשב במגבלות המבניות של השירות הציבורי מצד אחד ובחוסר המיקוד האסטרטגי של גורמי השוק הפרטי מצד שני.

הרובד הלאומי של ההגנה זקוק לפעולות חוצות ארגונים, בגיבוי של סמכות אפקטיבית. כפי שהמדינה מגינה על כלל המרחב הפיזי שלה, כך היא רואה צורך מִתגבר להגן על כלל המרחב הקיברנטי שלה, על אף מאפייניו המיוחדים המקשים על המשימה. התפתחות האיומים הקיברנטיים הפכה את הממשלות ללקוחות העיקריים של שירותי ההגנה.

סוגיות לקובעי המדיניות

מהפכת המידע ממשיכה לשנות את הסביבה האסטרטגית ומשפיעה בדרכים מורכבות על מגוון סוגיות חברתיות, תרבותיות וכלכליות. סוגיית הביטחון הקיברנטי, ובפרט ההגנה על התשתיות החיוניות, נמצאת כבר על סדר היום הציבורי והממשלתי. הניסיון הקצר מראה שעל אף הדמיון הרב במקור האיום, קיימים הבדלים במסגרת הדיון ובסוגי הפתרונות המוצעים במדינות שונות. מכיוון שהאיום הוא דומה, ההסבר לשונות הוא תפקיד המוסדות החברתיים בדיון ובקביעת המענה.

איזו תשתית היא חיונית?[18]

הדיון בתחום ההתגוננות צריך להתחיל מקביעת סדרי עדיפויות. הערכה ומדידה של רמת הסיכון ברכיבים, מחשבים ומערכות היא תנאי הכרחי להתמודדות יעילה. במדעים המדויקים ובהנדסה קיימות שיטות מתמטיות למדידת יחסי הגומלין והתלות בין רכיבים למערכות. הכלים הללו נמצאים בשימוש גם ברבדים הטכניים של ההגנה על תשתיות חיוניות. עם זאת, דרושות שיטות משופרות להערכת סיכונים הנובעים מקשרי גומלין מסועפים בין מערכות טכנולוגיות מורכבות המשובצות בתשתיות החיוניות.

הערכת מידת החיוניות הלאומית של תשתית חייבת להתייחס למכלול הערכים, היעדים והכוחות החברתיים. לפיכך, מידת החשיבות היחסית של תשתית, וכתוצאה מכך מידת ההשקעה הציבורית הנדרשת להגנתה, אינן נגזרות מנוסחה הנדסית ודורשות דיון ציבורי רחב ומושכל. המוסדות הפוליטיים הייצוגיים הם האכסניה לדיון כזה בחברה דמוקרטית. לאור אילוצי המערכת הפוליטית, סביר להניח שדיון מסוג זה יהיה ארוך ולעתים מתסכל. עם זאת, רק בתהליך פוליטי משתף ניתן יהיה לעצב מענה מיטבי לאיום בטווח הארוך.

פגיעות קיברנטית: סוגיה טכנית, סיכון כלכלי או איום ביטחוני?

אילו משמעויות פוטנציאליות יש לצמיחת המרחב הקיברנטי בכלל ולפגיעה בתשתיות קיברנטיות חיוניות בפרט? הנושא חורג בבירור מתחומי העיסוק של מחשבים, הנדסה ואבטחת מידע אל עבר השאלה: מהו תפקיד המדינה בהגנה הקיברנטית על תשתיות חיוניות? האם זו משימה צבאית, אזרחית למחצה, "הגנת המולדת" או משימה אזרחית־מסחרית? התשובה משפיעה במישרין על הפתרון המוצע ויש לה השלכות פוליטיות, תקציביות וארגוניות רחבות. עד לא מכבר ההנחה הייתה שמדובר בסוגיה טכנית בעיקרה, והמענה הופקד לפיכך בידי אנשי המחשבים. חברות מסחריות סיפקו פתרונות טכניים למגזר הצבאי, המסחרי והאזרחי, והממשלות לא שיחקו תפקיד משמעותי. כיום ברור שתשובה מיטבית יכולה להתקבל רק בדיון משותף בין מגזרים וגורמים שונים בחברה, מכיוון שהיא נגזרת מערכי החברה, מהמבנה הפוליטי והחברתי ומתפיסת הביטחון הלאומי.

מציאת האיזון בין ערכי החופש, אידיאולוגיית השוק ודרישות הביטחון

התשתיות החיוניות, והמידע הנחוץ לתפקודן התקין נוגעים בכל תחומי החיים של האזרח. הם מעוררים סוגיות רבות הנוגעות לזכויות האזרח, כגון פרטיות, חיסיון והליך הוגן; לעוצמה יחסית של מדינה, אזרחים ותאגידים; ולהקצאת כספי ציבור. לכן, האתגר המרכזי שבעיצוב מדיניות ההגנה על תשתיות חיוניות מפני איום קיברנטי אינו טכני או מבצעי, אלא אתגר של ראייה לאומית־אסטרטגית

כוללת. הגנה על תשתיות חיוניות אינה נחלתם הבלעדית של מהנדסי המערכות ואנשי המחשוב; המענה המיטבי לאיום קיברנטי בכלל ולאיום על התשתיות החיוניות בפרט ייווצר רק באמצעות דיון ציבורי רחב במסגרת המערכת הפוליטית הדמוקרטית.

השוק הפרטי וביטחון קיברנטי

האופי המבוזר של הפעילות הכלכלית בעידן של שינוי טכנולוגי מהיר, הגלובליזציה וההפרטה משפיעים על האיום הקיברנטי. כלכלת השוק הגלובלית הביאה לכך שחלקים נרחבים מהתשתית החיונית נמצאים בבעלות פרטית.[19] התלות ההדדית חסרת התקדים בסחר בין־לאומי היא אחד הביטויים הבולטים של הגלובליזציה וההפרטה. המדינות המתועשות מייבאות את רוב המזון הגולמי שאזרחיהן צורכים ומייצאות מוצרים מוגמרים ושירותים. קמעונאי המזון אינם מחזיקים מלאים מעבר לכמה ימי צריכה טיפוסית ומסתמכים על המשך התפקוד הבלתי מופרע של המערכת הלוגיסטית המסועפת המסוגלת לספק מענה לביקושים בזמן קצר.[20] לאור החומרה של שיבושים באספקת מזון, יתכן ששרשרת האספקה הזו תהפוך ל"תשתית מידע חיונית".

חברות פתוחות (Open Societies),[21] בעלות כלכלה חופשית, נרתעות ממעורבות המדינה בתהליכים עסקיים. כל ניסיון למעורבות המדינה בתהליכי השוק נתקל בחשדנות בעולם השוק החופשי. כך, למשל, הטענות הנשמעות נגד רגולציה ממשלתית של האינטרנט מקורן באידיאולוגיה המלווה שוק זה. הפתרון שאומץ עד כה היה רגולציה ממוקדת: מאז אמצע שנות התשעים של המאה העשרים פותחו ואומצו בארצות הברית עשרות תקנים מפורטים לאבטחת מידע במגזרים ותעשיות שונות[22] ונוסדו ארגונים לפיקוח ובקרה. אולם, במשבר הפיננסי העולמי של 2008 הדגימה המערכת הפיננסית המסחרית את סכנות הבעלות הפרטית על תשתית חיונית הכפופה לרגולציה.

הדיון בנושא ההגנה על תשתיות חיוניות בארצות הברית עובר בשנה האחרונה מִדגש על מנגנוני השוק ו"שיתוף פעולה פרטי־ציבורי" וולונטרי לעבר מודל המקנה סמכויות נרחבות לממשל להנחות גופים עסקיים ולפקח על ביצוע הנחיותיו.[23] גם בישראל קיימת רגולציה של התשתיות החיוניות, ואף עלתה הצעה להרחיבה גם לעסקים קטנים.[24]

שוק מוצרי המחשב והביטחון הקיברנטי

השימוש במערכות האבטחה צריך להיות קל לכל משתמש, לצרוך משאבי מחשב מעטים ולא לפגום בתפקוד מערכת הליבה או בחוויית המשתמש. המצב בשוק בתחום זה אינו מעודד: ההשקעה בביטחון משנית לעומת היציאה המהירה לשוק;

ההשקעה הנדרשת לבדיקות העמידות והאמינות קשה שבעתיים בסביבה פרטית־מסחרית, המודדת הישגים בקיצור זמן ההחזר של השקעה ראשונית ובצמצום הוצאות שלא קשורות לפעילות הליבה, ומוגנת במנגנוני האחריות המוגבלת. ליצרני מערכות המחשב אין כיום תמריץ להשקיע בהגברת האמינות והביטחון. אבטחה נתפסת כפונקציה חיצונית הנוספת על מערכות הליבה, לעתים באמצעות יצרן אחר שלא זוכה לשיתוף פעולה מהיצרן המקורי. ניתן לסכם ולקבוע כי רמת האמינות ואבטחת המידע ברוב מוצרי התוכנה, החומרה ותקשורת מערכות המחשוב לוקה היום בחסר, וכי אין ספק שפגיעות רחבה זו תרמה לעליית האיום הקיברנטי.

לאור נסיבות חוקיות, כלכליות ותחרותיות, קשה לצפות לשיתוף פעולה וולונטרי בין פירמות פרטיות בתחומים אלה. יחד עם זאת, אין לשאוף או לצפות להלאמה כתנאי להגברת הביטחון הקיברנטי. מה שדרוש הוא הגברת מעורבות המדינה בהכוונת השוק החופשי לאור האיומים הקיברנטיים.

המענה הישראלי

אבטחת מידע רגיש והגנה על תשתיות ממוחשבות אינן מהוות נושאים חדשים במדינת ישראל. מאז 1996 קיבלה הממשלה החלטות הנוגעות להתגוננות מפני איומים קיברנטיים.[25] מתווה ההגנה על תשתיות ממוחשבות עוצב בהחלטה ב/84: "אחריות להגנה על מערכות ממוחשבות במדינת ישראל" של ועדת השרים לענייני ביטחון לאומי, מ־11 בפברואר 2002. זאת ההחלטה שעל בסיסה מופעל עד היום המענה הישראלי לאיום הקיברנטי על תשתיות מידע חיוניות. המענה שנקבע בהחלטה כולל הקמת ועדת היגוי עליונה הבוחנת מעת לעת את זהות הגופים שחיוני להגן עליהם והקמת היחידה הממלכתית להגנה על המערכות הממוחשבות (הרשות לאבטחת מידע). גוף אחרון זה נמצא במסגרת השב"כ ומנחה את הגופים שהוגדרו כחיוניים בנושא ביטחון המחשוב, מפקח על ביצוע ההנחיות ומוסמך לנקוט סנקציות נגד המפרים אותן. הגופים המונחים נושאים בעלויות ההגנה הנדרשת. גופים חשובים נוספים הנמצאים תחת אחריות משרד ממשלתי פועלים בהתאם להנחיות המקצועיות של הרשות אך אינם מפוקחים על ידה. גופי הביטחון השונים פועלים להגנה על תשתיותיהם הייחודיות באופן עצמאי, ללא הנחיה פורמאלית של הרשות לאבטחת מידע.

בהשוואה למצב בזירה הבין־לאומית, נראה שישראל הייתה בזמן קבלת ההחלטה מתקדמת יחסית למדינות אחרות בעיצוב ובביצוע ההגנה על התשתיות החיוניות ברמה הלאומית. אולם המרחב הקיברנטי המשיך להתפתח מאז בקצב מהיר ונוצרו מערכות וקשרי גומלין חדשים, שלא בהכרח ניתנים להגדרה כתשתית לאומית חיונית. כך, למשל, עסקים קטנים ובינוניים תלויים בספקי תקשורת

מסחריים ומבצעים את פעילויות הליבה על גבי האינטרנט הפתוח. התפתחות זו של חדירת יישומים מסחריים וצרכניים על בסיס "מחשוב ענן" מעלה סוגיות חדשות ומצביעה פעם נוספת על חשיבותו הגוברת של המרחב הקיברנטי בכל תחומי החיים.

המענה הישראלי לצורך בהספקת הגנה לתשתיות מרכזיות חיוניות נוסד לפני קרוב לעשור, אולם אינו מסַפק ראייה כוללת של התחום האזרחי־מסחרי המתפתח במרחב הקיברנטי. לפיכך, כדאי לבחון מחדש את האתגרים הקיימים והצפויים, ובעקבותיהם את המענה הרצוי.[26]

בעקבות "המיזם הקיברנטי הלאומי" החליטה ממשלת ישראל באוגוסט 2011:

> לפעול לקידום היכולת הלאומית במרחב הקיברנטי ולשיפור ההתמודדות עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי: לשפר את ההגנה על תשתיות לאומיות שהן חיוניות לקיומם של חיים תקינים במדינת ישראל ולחסנן ככל הניתן מפני התקפה קיברנטית, תוך קידום מעמדה של ישראל כמרכז לפיתוח טכנולוגיות מידע, וזאת תוך עידוד שיתוף הפעולה בין האקדמיה, התעשייה והמגזר הפרטי, משרדי הממשלה והגופים המיוחדים... לאור זאת, בהמשך להחלטת ועדת שרים לענייני ביטחון לאומי ב/84 מיום 11 בדצמבר 2002, ומבלי לפגוע בסמכות שניתנה לגורם אחר על פי כל דין והחלטות ממשלה [מוחלט]:
>
> 1. להקים מטה קיברנטי לאומי (להלן המטה) במשרד ראש הממשלה.
> 2. להסדיר את האחריות לטיפול בתחום הקיברנטי.
> 3. לקדם את יכולת ההגנה על המרחב הקיברנטי בישראל ולקדם מחקר ופיתוח בתחום הקיברנטי וחישוב העל.[27]

החלטת הממשלה עשויה להוביל להסדרה משופרת של המענה הישראלי לאיום הקיברנטי בכלל ולאיום על התשתיות החיוניות בפרט.

סיכום

הממד הקיברנטי ניצב במוקד הדיון המחודש בהגנה על תשתיות לאומיות חיוניות. מאפייני המרחב הקיברנטי מאפשרים לפגוע בתפקוד התשתית החיונית מבלי להיות פיזית בקרבת המטרה ומבלי להסתכן בגילוי חד־משמעי בידי הצד המותקף. מכיוון שכל התשתיות הושפעו ממהפכת המידע וכולן כוללות כיום מרכיבים ממוחשבים המשמשים בעיקר לשליטה ובקרה, השינוי הטכנולוגי המהיר יצר גם איום ביטחוני חדש. זה עורר דיון מחודש על התשתיות החיוניות והגנתן, דיון המוקדש כולו לאיום הקיברנטי. האיום הקיברנטי על תשתיות מידע חיוניות הוא אולי הביטוי המסוכן ביותר של תחום הביטחון הקיברנטי. איום חדש זה מצטרף לשורה ארוכה של איומים ולא מחליף אותם.

המאמר הציג את המושג "תשתית חיונית" ודן בהגדרת החיוניות, בתיאור מקורות הפגיעות ובמאפייני האיום. בהמשך תיאר המאמר רבדים בהתמודדות עם האיום החדש, המוחשי והמיידי, המציב אתגרי מדיניות מורכבים הדורשים התמודדות. המאמר סקר בקצרה את הסוגיות המרכזיות לדיון; כל אחת מהן ראויה לדיון אקדמי ויישומי רב־תחומי ללא דיחוי.

רוב המדינות מפעילות כיום רגולציה משפטית וטכנית במגזרים נבחרים. מדינת ישראל מגינה מאז 2002 על תשתיות שהיא הגדירה כחיוניות באמצעות פיקוח והנחיה של גוף ייעודי. עם זאת, התפתחות המרחב הקיברנטי הותירה את חלקו האזרחי הלא־חיוני בלתי מוגן, ובמקביל העלתה את רמת הפגיעות.

אף שבמבט ראשון נראה כי נושא ההגנה על תשתיות מידע חיוניות משתייך לתחום המחשבים, כשעוסקים בו מתברר שרצוי להרחיבו מעֵבר לעיסוק הטכני. ההמלצה המרכזית היא, אפוא, להגביר את הדיון הציבורי בנושאי הביטחון הקיברנטי, כדי לכלול בו שיקולים חברתיים ותרבותיים רחבים, ובהמשך לאפשר התמודדות מיטבית איתו ברמה הלאומית־אסטרטגית, מתוך ראייה לאומית כוללת.

לאחרונה יזמה ממשלת ישראל את "המיזם הקיברנטי הלאומי", הצפוי להתניע טיפול במכלול הסוגיות. המלצות הוועדה הבין־תחומית שעסקה בנושא זה טרם פורסמו, אולם ברור שרק תהליך מושכל של עיצוב מדיניות יכול לצמצם את רמת הסיכון בה נתונות מדינת ישראל ויתר המדינות המפותחות.

האתגר המרכזי בתחום ההגנה על תשתיות חיוניות מפני איום קיברנטי אינו אתגר טכני; זהו אתגר אסטרטגי ופוליטי.

הערות

1 המאמר נכתב לפני התנעת "המיזם הקיברנטי הלאומי", אשר עסק בהרחבה גם בנושא הנדון במאמר, אולם המלצותיו טרם פורסמו בפומבי.

2 להלן הגדרה אמריקאית מ־2003 לתשתיות מידע חיוניות: "תשתיות מידע חיוניות הן מערכות ומתקנים שהריסתם או שיבוש תפקודם (באמצעים ממוחשבים) יגרמו לאחד או יותר מאלה: מספר נפגעים הדומה לתוצאה של הפעלת נשק להשמדה המונית; פגיעה ביכולת זרועות הממשל לספק לציבור שירותים בסיסיים ולהבטיח את ביטחון האזרחים; פגיעה ביכולת תפקוד של פירמות עסקיות ושיבוש התפקוד הכלכלי; השפעה לרעה על המשק עקב פגיעה בתפקוד של מערכות תשתית חיוניות; שיבוש התפקוד חותר תחת אמון הציבור במוסדות השלטון והמשק הלאומי:US Government, White House, Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification, Prioritization and Protection*, December 17, 2003.

3 Elgin Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Zurich, Center for Security Studies (CSS), ETH Zürich (Swiss Federal Institute of Technology), 2008; John Moteff, Claudia Copeland and John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*,

Washington, D.C., Congressional Research Service, Library of Congress, 2002; Myriam Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *International Journal of Critical Infrastructures,* Vol. 1, No. 2-3, 2005; US Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2009*, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm; Tyson Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies*, Boca Raton, FL., CRC Press, 2009; Robert Radvanovsky, *Critical Infrastructure: Homeland Security and Emergency Preparedness*, Boca Raton, FL., CRC/Taylor & Francis, 2006.

4 למשל: אוסטרליה וארצות הברית. נראה שמדינות אלו מיחסות חשיבות רבה להיסטוריה הפוליטית שלהן כמרכיב מרכזי בזהות הלאומית הקבוצתית ובחוסן החברתי והמדיני:
International CIIP Handbook 2008/2009, Table 1; DHS, DoI: *National Monuments & Icons: Critical Infrastructure and Key Resources, Sector-Specific Plan,* May 2007, p. 17, http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf

5 "תורת הכאוס" מנסה להתמודד עם קשיים מסוג זה בשיטות מתמטיות.

6 פגיעה ברמת התפקוד של השלטון, שפוגעת בשירות לאזרח, יוצרת הסלמה: אמון הציבור בממשל צונח, מה שעשוי להתבטא בשינוי פוליטי (במשטר ייצוגי הדבר יתבטא בהחלפת ממשלה) ואף משטרי (מהפכה במשטר סמכותני, או שינוי מבנה המשטר בדמוקרטיה).

7 IATA (International Air Transport Association), *Air Transport Facts* (2009), http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/economic-social-benefits.aspx. ארגון IATA מייצג 93% מהתנועה האווירית הסדירה בעולם.

8 ארצות הברית הייתה החלוצה בתחום זה, כאשר ב־1996 יזמה דיון ברמה נשיאותית בנושא:
United States. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection*, Washington, D.C., U.S. G.P.O., 1997.

9 במבצע ההפצצות האסטרטגיות במלחמת העולם השנייה בעלות הברית ריכזו מאמץ אווירי לתקיפת מפעלים גרמניים לייצור מסבים כדוריים, שמני סיכה, מתקני זיקוק וצמתי מסילות רכבת. המבצע נועד לפגוע בכושר הייצור של אמצעי לחימה.

10 כאמור, ארצות הברית מובילה את הטיפול בנושא הפגיעות הקיברנטית מאמצע שנות התשעים של המאה הקודמת, בהיותה בעלת עוצמה טכנולוגית וצבאית עצומה ומעמד של מעצמת־העל היחידה.

11 מאז שנת 2001 משגרים ארגוני הטרור רקטות ופצצות מרגמה מרצועת עזה לעבר יישובי הנגב. עד היום גרמו הרקטות ל־19 הרוגים, ופצצות המרגמה ל־10 הרוגים, ושיבשו קשות את אורח החיים באזור. לאחר הסלמה יצאה ישראל בדצמבר 2008 למבצע "עופרת יצוקה", שהסתיים בהצלחה צבאית. ירי תלול מסלול מרצועת עזה נמשך עד היום, אם כי בהיקף קטן יותר מאשר לפני המבצע.

12 היתכנות השימוש באמצעי קיברנטי לגרימת נזק פיזי הוצגה בניסויים. רשת CNN שידרה כי בניסוי Aurora שהוזמן על ידי המשרד לביטחון הפנים של ארצות הברית ונערך ב־Idaho National Labs, שידור הוראות למערכת שליטה ובקרה של מערכת ייצור חשמל הביא לכך שגנרטור יצא משימוש ובהמשך התפוצץ.

13 להלן סיכום האתגרים הנובעים ממאפייני המרחב הקיברנטי הקיים היום: הפגיעות

הרבה של מערכות ממוחשבות; קושי להבחין בין תקלה לתקיפה; קושי לקשר בין אירוע לתוצאה; קושי להתחקות אחר מקור הפגיעה; קושי לזהות את התוקף, גם אם מקור הפגיעה ידוע; שימוש רחב בטכנולוגיות מסחריות מן המדף; ריבוי השחקנים בתחום לאור סף הכניסה הנמוך. לדיון על המרחב הקיברנטי בהקשר לביטחון הלאומי ראו: ליאור טבנסקי, "לחימה במרחב הקיברנטי: מושגי יסוד", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

14 Jason Stamp, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, 2003, http://www.sandia.gov/ccss/documents/031172C.pdf

15 עמידות או חוסן (resilience) היא יכולת המערכת לספוג פגיעה ולחזור לפעולה תקינה במהרה. במערכות ממוחשבות התוצאה מושגת על ידי שחזור המצב המקורי ("חזרה בזמן") או על ידי התאמה מהירה לאילוצים החדשים (הסתגלות).

16 http://www.strategyr.com/Information_Security_Products_and_Services_Market_Report.asp

17 James der Derian and Jesse Finkelstein, "Critical Infrastructures and Network Pathologies: the Semiotics and Biopolitics of Heteropolarity", in: Myriam Dunn Cavelty and Kristian Søby Kristensen, *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security*, London, New York, Routledge, 2008.

18 קיימת שונות רבה בין הגדרת התשתית הקריטית ובין האמצעים הננקטים להגנתה במדינות השונות. ראו: Brunner and Suter, International CIIP Handbook 2008/2009. ההיבט האזרחי של הגנה על תשתיות חיוניות בישראל נקבע ב"חוק להסדרת הביטחון במקומות ציבוריים, התשנ"ח־1998". החוק מסמיך את שירות הביטחון הכללי להנחות גופים ציבוריים שונים בתחומי האבטחה הפיזית, אבטחת מידע ואבטחת מערכות ממוחשבות חיוניות, לפי פירוט המופיע בתוספות לחוק. בחוק זה נקבעו עונשים על אי מילוי הוראותיו, הכוללים קנס אזרחי ומאסר בפועל. ב־2003 הוקמה הרשות הממלכתית לאבטחת מידע (רא"ם), "המופקדת על הנחיה מקצועית של הגופים המונחים שבאחריותה בתחום אבטחת תשתיות מחשב חיוניות מפני איומי טרור וחבלה, בתחום אבטחת מידע מסווג ומפני איומי ריגול וחשיפה", http://www.shabak.gov.il/about/units/reem/pages/default.aspx

19 רוב התחבורה הציבורית בארצות הברית ויותר מ־85% ממגזר האנרגיה בארצות הברית נשלטים בידי חברות מסחריות פרטיות. כ־85% מהתקשורת של משרד ההגנה האמריקאי עוברים ברשתות מסחריות.
http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/energy1.htm

20 מדינת ישראל, מכוח מצבה הגיאו־פוליטי, מחזיקה מלאי מזון וציוד כדי להבטיח את צרכי המשק בשעת חירום. "הרשות העליונה למל"ח – מזון ומשכ"ל" במשרד התמ"ת היא הגוף האחראי על נושא זה.

21 הכוונה למושג של פילוסוף המדע קרל פופר. ראו: קרל רימונד פופר, **החברה הפתוחה ואויביה**, מתרגם: אהרן אמיר, עורך: יוסף אגסי, הקדמה: יובל שטייניץ, ירושלים, שלם, 2003.

22 ראו למשל ריכוז פרסומים של מכון התקנים האמריקאי: http://csrc.nist.gov/publications/PubsFL.html
וכן התקנים למגזר החשמל של North American Electric Reliability Corporation Standards (NERC) CIP-002-3 through CIP-009-3, http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf http://www.nerc.com/fileUploads/File/Standards/Revised_

Implementation_Plan_CIP-002-009.pdf

23 CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency,* Washington, D.C., Center for Strategic and International Studies, 2011.

24 גבי סיבוני, "הגנת נכסים ותשתיות קריטיות מפני תקיפה קיברנטית – הממד הסטטוטורי", **צבא ואסטרטגיה**, כרך 3, גיליון 1, אפריל 2011.

25 ראו לדוגמה: החלטת ממשלה 1886 בק/9 מ־20 במארס 1997: הקמת ועדת היגוי לנושאי מחשוב בכל משרד ממשלתי; החלטת ממשלה 3582 בק/77 מ־16 במארס 1998: אחריות לנושא אבטחת מידע במשרדי הממשלה; החלטת ממשלה 4956 בק/179 מ־23 במארס 1999: הוקמה המועצה לאבטחת מידע רגיש במשרד ראש הממשלה; החלטת ממשלה תמ/80 מ־26 בנובמבר 2000 בעניין האחריות על אבטחת המידע הממוחשב בצה"ל ושיתוף הפעולה עם הגורמים האזרחיים; החלטת ממשלה תמ/14 מ־18 ביולי 2001: רשת פנימית מאובטחת לשימוש משרדי הממשלה.

26 כאמור, המאמר נכתב לפני פרסום המסקנות של "המיזם הקיברנטי", אשר עסק בין היתר בנושא ההגנה על המרחב הקיברנטי האזרחי.

27 הודעת מזכיר הממשלה בתום ישיבת הממשלה מיום 7 באוגוסט 2011, סעיף ד': קידום היכולת הלאומית במרחב הקיברנטי, http://www.pmo.gov.il/PMO/Secretarial/Govmes/2011/08/govmes070811.htm