ניתוח והמלצות לאסטרטגיית הסייבר הלאומית החדשה של ישראל

מאת אל"מ (מיל') שי שבתאי

מבט מבס"א מס' 2,349 ,20 ביולי 2025

תקציר: מערך הסייבר הלאומי פרסם עדכון של האסטרטגיה הלאומית להגנת הסייבר (גילוי נאות: הכותב סייע בתהליך החשיבה). האסטרטגיה החדשה מפתחת ומעדכנת את עקרונות קודמתה מ-2017, אך שונה בתפיסת היסוד ומתמקדת בהגנה על מדינת ישראל ונגזרותיה כאמצעי להבטחת תהליכים ותשתיות ליבה לאומיים. היא נוגעת ומחדשת בסוגיות כמו מהו 'השלם הסייברי הלאומי', איך מתמודדים עם 'רשת האספקה הטכנולוגית' (ולא 'שרשרת אספקה'), ואף מושפעת מהמלחמה בכך שהיא מדגישה, כי בשל הגורם האנושי לא ניתן למנוע הפתעות. המלצה מרכזית לתהליך היישום היא הצורך בבניית עוצמות מערך הסייבר הלאומי, על מנת שימצב את מעמדו כגורם המוביל את רשת שיתופי הפעולה הממשלתית והלאומית המוגדרת כבסיס ליכולת המימוש.

מה כוללת האסטרטגיה החדשה

בפברואר 2025 פרסם מערך הסייבר הלאומי עדכון של האסטרטגיה הלאומית להגנת הסייבר [גילוי נאות: הכותב סייע בחשיבה על האסטרטגיה החדשה באמצעות פרסום מסמך אסטרטגיית סייבר לאומית: סוגיות לדיון במרכז בס"א ובשיח עם אנשי המערך]. המסמך, אשר מחליף את קודמו מ-2017, בנוי בצורה ברורה ואינטואיטיבית. הוא מגדיר את החזון הלאומי: "מרחב דיגיטלי אמין, זמין ובטוח המאפשר את היתרונות של עולם משגשג ומתקדם".

המסמך מפרט ארבעה עקרונות על למימוש, שמהווים בסיס למאמצי המענה: הגנה משותפת - חיוניות הפעולה המשותפת בתוך הממשלה ובינה לבין יתר המגזרים; הגנה אקטיבית - גישה פרו-אקטיבית להגנה; הגנה שממנפת חדשנות ומצוינות טכנולוגית - התבססות על היתרון היחסי של האקוסיסטם הטכנולוגי הלאומי בתחום; וחוסן והיערכות למשברים - היערכות למשברים שבוודאות יתרחשו.

גוף האסטרטגיה הוא פירוט של מאמצי המענה המרכזיים ותת-רכיבי המענה שלהם במסגרת שלושה נדבכים. הנדבך הראשון הוא הגנה במרחב הלאומי - קרי, מאמצי ההגנה על נכסי המדינה. המאמצים המרכזיים במסגרת זו הם שיפור ההגנה בקרב האזרחים והעסקים (פרק 1); הגנה ממוקדת בתשתיות הלאומיות הקריטיות (פרק 2);

והגנה על המרחב הדיגיטלי המשותף (פרק 3). הנדבך השני הוא התארגנות משולבת של כלל גורמי המדינה. המאמצים המרכזיים במסגרת זו הם פעולה משותפת (פרק 4); מוכנות לאירוע משברי (פרק 5); והסרה פרואקטיבית של איומים (פרק 6). הנדבך השלישי הוא פיתוח של שותפויות אסטרטגיות לאומיות ובינלאומיות ושל יכולות עתידיות טכנולוגיות והון אנושי. המאמצים המרכזיים במסגרת זו הם הגיבוש של שותפויות אסטרטגיות (פרק 7); וטיפוח מצוינות מדעית - טכנולוגית על מנת לשמר את ישראל בחזית הסייבר העולמית (פרק 8).

השוואה למסמכים מקבילים

תפיסת היסוד של האסטרטגיה החדשה שונה במהותה מהאסטרטגיה שפורסמה ב-2017. האסטרטגיה הקודמת מיקמה את הסייבר כרכיב בהקשר לאומי רחב, והגדירה את "חזון הסייבר של מדינת ישראל: מדינת ישראל תהיה מדינה מובילה ברתימת מרחב הסייבר לטובת צמיחתה הכלכלית, רווחתה החברתית וביטחונה הלאומי". האסטרטגיה הזו עסקה - כפי שאפיין את הטיפול בסוגיה מאז 'המיזם הקיברנטי הלאומי' ב-2011 - בסייבר כמחולל עוצמות לאומיות ובסוגיית ההגנה כנגזרת ממנה. ההגנה לא מאוזכרת בחזון אלא רק בייעוד האסטרטגיה: "להסדיר את כלל המאמצים הלאומיים בתחום הגנת הסייבר, ליצור 'שפה משותפת' בין העוסקים במלאכה ולהבטיח מענה יציב וארוך טווח...". האסטרטגיה החדשה מעמיקה לתווך הסייבר ומתמקדת בהגנה על מדינת ישראל ונגזרותיה. עם זאת, קיימת המשכיות בתפיסות הפעולה, שבאסטרטגיה הקודמת התמקדו בשלוש שכבות: עמידות משקית, חוסן מערכתי והגנה לאומית. שלושת הנדבכים של האסטרטגיה החדשה מהווים פיתוח ועדכון של שכבות אלו לאור ההתקדמות שהושגה מאז פרסומה של האסטרטגיה הקודמת, בין היתר במסגרת מימושה, למשל, במערכי ההגנה על המגזרים הממשלתיים ובתשתיות המחשוב הממשלתיות.

שינוי הגישה בתפיסת היסוד מתבטא בהתייחסות המסמך החדש לחדשנות טכנולוגית ולשיתופי פעולה בינלאומיים. המסמך הקודם הדגיש את אלו כמאמצים תומכים למימוש האסטרטגיה. במסגרת זו בניין הכוח המדעי-טכנולוגי הלאומי כלל התייחסות לתפקיד המדינה בטיפוח יזמות וחדשנות טכנולוגית בתעשיית הגנת הסייבר הישראלית ובתמיכה במרכזי מחקר ייעודיים במוסדות מחקר אקדמיים. האסטרטגיה החדשה מעבירה את המשקל בהתקדמות בתחום זה לשוק הפרטי, וקובעת, כי יש "להרחיב את פעילות מרכזי המצוינות והמעבדות מול האקו-סיסטם, בין היתר בהגדלת מעורבותן של חברות מהמגזר הפרטי במרכזים אלה". פיתוח ההון האנושי בתחום הסייבר נשאר כיעד הממשיך - בעדכונים הנדרשים - באסטרטגיה החדשה.

המאמץ התומך בתחום שיתוף פעולה בזירה הבין-לאומית כלל במסמך הקודם שיתופי פעולה להעלאת רמת ההגנה הלאומית והעולמית בסייבר וסיוע למדינות עמיתות בחיזוק יכולתן הלאומית. באסטרטגיה החדשה המאמץ ממוקד בצרכיי ההגנה, וכולל את העמקת הקשרים עם 'שותפות מובילות' ולצרכים מוגדרים יותר של התרעה ואכיפה, ואילו הסיוע למדינות ידידות ממוקד לעתות של 'משבר סייבר לאומי'.

עיקרי תוכנית העבודה של מערך הסייבר הלאומי לשנת 2025 מופיעה במסגרת ספר תוכניות העבודה של משרדי הממשלה ויחידות הסמך, שהתפרסם באפריל 2025 לאחר העברת תקציב המדינה. חמשת עקרונות תוכנית העבודה והיעדים המוגדרים למימושם עדיין לא משקפים את תהליך המימוש של האסטרטגיה החדשה. זאת, אף שאופן הגדרת היעדים והפרויקטים למימושם חופפים במידה רבה את האסטרטגיה שהושלמה במקביל. כך, לדוגמה, תוכנית העבודה אינה מגדירה יעדים של עידוד והמרצת עסקים להעלות את רמת ההגנה בסייבר (יעד 1.3 באסטרטגיה), שימור אפס נזקים משמעותיים לתשתיות מדינה קריטיות (יעד 2.1) או ניהול חירום לאומי במרחב הדיגיטלי (יעד 5.2).

מסמך נוסף אליו ניתן להשוות הוא אסטרטגיית הסייבר של ארצות הברית ממרץ 2023 בתקופת הממשל הקודם. הממשל האמריקני מיקד את האסטרטגיה בתהליכים הנדרשים להגנת מרחב הסייבר, כפי שנעשה באסטרטגיה הישראלית המעודכנת. העיקרון הראשון של המסמך היה הגדרת הדרך להשגת חסינות במרחב הסייבר על-ידי איזון האחריות להגנתו ותמריצים להשקעות ארוכות טווח. הממשל הטיל את כובד משקלו על מנת ליצור מספר שינויים מהותיים: הסדרת והעמקת ההגנה על תשתיות קריטיות בתוך הממשל ואל מול הגופים העסקיים הפועלים בתחומים אלו (יסוד 1), טיפול בגורמי התקיפה על-ידי שיבוש ופירוק (יסוד 2) ועיצוב כוחות השוק בתחום הגנת הסייבר על-ידי הטלת אחריות ומתן תמריצים לחברות הטכנולוגיה הגדולות תוך איזון מחדש של האחריות בין מנהלי שירותי התשתית לבין הגורמים שהם משתמשי הקצה (יסוד 3).

ניתן לראות חפיפה נושאית לאסטרטגיה הישראלית, ומוטרדות מבעיות מקבילות המצביעה על ניתוח דומה של האתגרים, אך כוונה אמריקנית להשתמש בעוצמות הממשל בתחום הרגולציה והמשאבים על מנת להביא לתיקון אגרסיבי של המצב. זאת בניגוד לאסטרטגיה הישראלית אשר בשל אילוצים - עליהם אתייחס בהמשך - חותרת למיצוי 'עוצמה רכה' ביצירת קואליציות ושיתופי פעולה ופחות לשימוש אגרסיבי ב'עוצמה קשה' של חקיקה והתניות משאביות.

היסודות הנוספים באסטרטגיה האמריקנית: השקעה בחוסן עתידי (יסוד 4) וקידום שותפויות בין-לאומיות (יסוד 5) מנותחים בראייה של מעצמת על טכנולוגית ומדינית המובילה תהליכים גלובליים ולא מהווה חלק מהם - ולכן מנסה רק להשפיע עליהם - כמו ישראל.

העיקרון השני של האסטרטגיה האמריקנית היה המשכיות המאמצים שבוצעו במסגרת המדיניות הקיימת. יצירת רצף בין תהליכים קיימים לבין אסטרטגיה חדשה הוא מהלך רצוי, שישראל אימצה. יש להדגיש שמהלכים שביצע ממשל טראמפ - במיוחד בתחום פעולות ההתייעלות - משנים בפועל רכיבי מפתח ביכולת מימושו של המסמך, למשל, הפגיעה בסוכנות הלאומית להגנת הסייבר CISA ובמוסד התקנים הלאומי NIST, שמהווה בסיס לפרקטיקות מיטביות (Best practices) בתהליכי הגנה בכל העולם.

התייחסויות לתכני האסטרטגיה

מסמך האסטרטגיה הוא מסמך מקיף וברור המכיל את המאמצים הנדרשים בתחום הגנת הסייבר, כפי שהם מקובלים כיום בעולם. מתוכו עולות מספר תובנות מפתח:

א. מטרת המסמך: החזון הלאומי המוגדר כ"מרחב דיגיטלי אמין, זמין ובטוח..." שם את הגנת הסייבר במקומה הטבעי והנכון כאמצעי להבטחת תהליכים ותשתיות ליבה לאומיים ביטחוניים, תשתיתיים, כלכליים, חברתיים ועוד. חסרה בהגדרת החזון התייחסות להסתגלות מהירה בראייה צופה פני עתיד בשל תהליכי השתנות מהירים המתרחשים כיום בעולם בתחום הדיגיטלי. עם זאת, כותביה מדגישים כי היא נכתבת באופק של שלוש שנים (עד 2028) באופן המבטא את הצורך בדינמיות המענה.

ב. הסוגיות 'הנוספות' ו'השלם הסייברי': האסטרטגיה כוללת שתי סוגיות שאינן מליבת הגנת הסייבר המקובלת: ההגנה מפני מאמצי השפעה תודעתיים שליליים של גורמים זרים ותוכנית לאומית להזדהות דיגיטלית בטוחה (מתוקף אחריות מערך הסייבר הלאומי על סוגיית ההזדהות הביומטרית ולאור הכללת סוגייה זו באסטרטגיה האמריקנית). הכללת סוגיות אלו מעלה את השאלה מהו 'שלם הגנת הסייבר' והאם לא נכון לצרף לעקרונות ברמה הלאומית היבטים נוספים (למשל, להגדיר את ההגירה של משרדי הממשלה לענן הציבורי כרכיב מפתח בתפיסת ההגנה הלאומית או לעסוק במדיניות ההצפנה הלאומית).

ג. השוני בין גישת 'הרשת' ל'שרשרת אספקה': המסמך מזהה, כי "המשתמשים ובעלי הנכסים הדיגיטליים במרחב הסייבר אינם שולטים בכל שלבי הייצור והיבטי התפעול... עובדה המדגישה את הצורך בהסדרת האחריות ברמה המדינתית". הדבר מבטא הבנה בסיסית, כי מעטפת ההגנה לארגונים חייבת להיות רחבה בהרבה מבקרת 'שרשרת האספקה' או 'צדדים שלישיים' (המסמך בוחר בביטוי המתקדם יותר: 'רשת אספקה טכנולוגית' וראה להלן).

ד. גישה פרואקטיבית ל'משברי סייבר': המסמך מדגיש את הצורך להיערך היטב ולתת מענה ל'חירום לאומי במרחב הדיגיטלי', וכולל שני עקרונות רלבנטיים של הגנה אקטיבית ושל חוסן והיערכות למשברים. עם זאת, בשונה מהדיון המעשי והמשפטי המתפתח כיום בעולם – ראה ארצות הברית ויפן – תחת הכותרת 'גישה פרואקטיבית' לגבי שילוב הממד ההתקפי – ברמה הלאומית והארגונית - במענה לאירועי סייבר, המסמך בוחר לעמעם את המענה הלאומי בסוגיה תחת הכותרת 'מענה לתוקף' (יעד 6.1). ניתן להניח שהסעיף מתייחס גם לפעולות לאומיות שמבוצעות נגד גופי התקיפה והמדינות או הארגונים המפעילים אותם, כפי שיוחס לישראל בשנים האחרונות. מבחינה זו מדובר בתחילתו של דיון עקרוני ולא בסיומו. סוגיה נוספת בתחום המענה שבה המסמך עושה צעד משמעותי הוא האמירה הברורה, ש"ממשלת ישראל דוגלת במדיניות של הימנעות מתשלום דמי כופר" לתוקפים.

ה. התמודדות עם ספקי טכנולוגיות גדולים: ישראל - בשונה מארצות הברית ובשל יכולת השפעתה המוגבלת - בוחרת להתמודד עם ספקי הטכנולוגיה הגדולים בדרך של "פיתוח שותפויות אסטרטגיות עם חברות... הענק הטכנולוגיות" (יעד 7.1). לצד זאת, אל מול 'רשת האספקה הטכנולוגית' ["הצמתים המרכזיים באספקת שירותי טכנולוגיית מידע ותקשורת (מגזר ICT)"] נדרש מיפוי עדכני ו"העלאת חוסן רחבה" (יעד 3.2). מדובר בגישה ריאלית לאתגר.

ו. המודעות ראשונה: "העלאת מודעות ואוריינות לאיומי סייבר" (יעד 1.1) מופיעה כיעד הראשון של האסטרטגיה. ההחלטה לעשות כן מהווה מסר ברור ונכון, שהגנת הסייבר מתחילה בהבנה של האתגר, כל גוף ובעל תפקידו בו ברמה הרלבנטית לו.

ז. הדגשת שיתוף פעולה על פני אכיפה: במספר מקומות המסמך בוחר בדרך רכה של שיתוף ולא של אכיפה. כך, למשל, מוגדר כיוון עשייה של "מערכת לאומית אחודה לדיווח וולונטרי" (במסגרת יעד 1.2). בהתייחסות לסוגיית הגנת הפרטיות במסגרת "הגנה על נכסי מידע" (יעד 3.3) מוגדר, לצד האזכור של הרשות להגנת הפרטיות ופעולתה, הצורך ב"זווית ראייה משלימה" בעיקר ביכולת להגיע כיום לתובנות חודרניות ממצרף של מידע הנחשב לא מסווג. נקודות אלו מייצגות הבנה, שכפיית כללי דיווח ופעולות אכיפה מחמירים מדי לא מהוות את המענה המיטבי או המקסימלי להגנת הסייבר.

ח. המלחמה והשפעותיה: בשני מקומות יש אזכורים המעידים על הפקת לקחים והתחברות למשמעויות מלחמת חרבות ברזל. בהיערכות למניעה והתמודדות עם הפתעה בסייבר (יעד 5.1) נכתב: "לגורם האנושי תפקיד מכריע בהתרחשות הפתעה ובניהול המשבר בעקבותיה. קיימות הטיות טבעיות, הן קוגניטיביות והן פסיכולוגיות...", ולכן נדרשים מנגנונים מפצים להתמודדות עם מצב של הפתעה. במסגרת "פיתוח הון אנושי מיומן" (יעד 8.3) נקבע, כי "ישראל תפעל לעידוד העסקת פצועי מלחמת 'חרבות ברזל' בוגרי לימודי סייבר, בתפקיד ראשון בממשלה ובתעשייה...". קשה להמעיט עד כמה ראוי ונכון מאמץ זה.

המלצות למימוש

האסטרטגיה תימדד כתמיד באופן מימושה, וכפי שנכתב עליה להיהפך לבסיס תוכנית העבודה של מערך הגנת הסייבר ויתר גופי הגנת הסייבר הלאומיים בשנים הקרובות. בתוך כך אפשר להצביע על ארבע המלצות מרכזיות בתהליך המימוש:

א. בניית עוצמות המערך: האסטרטגיה הלאומית בחרה להעמיד את מערך הסייבר הלאומי במרכזה של רשת שיתופי פעולה ממשלתית ולאומית. במצב זה עוצמתו של המערך לא נבנית מתוקף חקיקה ורגולציה המאפשרות לו יכולות אכיפה משמעותיות (למעט בתחום החיוני של התשתיות הקריטיות) אלא מהעוצמות המקצועיות וההפעלתיות שהוא מביא לשולחן המשותף. מבחינה זו מצבו דומה לזה של המוסד: גם הוא אחראי על פעילות בתווך (במקרה שלו חוץ לארץ, במקרה שלפנינו סייבר), אף שהסמכויות המשפטיות לפעולתו מועטות (אין 'חוק מוסד'...). במצב זה הארגון נבנה על עוצמות הידע וההפעלה הייחודיים והיצירתיים, שבנה מזה 70 שנה, ואת היתרונות המובהקים הללו הוא מביא לשיח עם גורמים ממשלתיים אחרים הפועלים בחוץ לארץ. זו צריכה להיות גם דרכו של המערך: עליו לבנות יכולות ייחודיות - גם עצמאיות וגם בשיתופי פעולה בעלי ערך מוסף מהותי לכל הצדדים - כבסיס לתביעתו להיות נוכח בכל עניין הקשור בהגנת הסייבר הלאומית.

ב. גבולות ההגנה (מה לא עושים): אחד האתגרים בתרגום של אסטרטגיה לתוכנית עבודה היא לצמצם את היעדים למימוש ממוקד ומתועדף באופן ברור. ניסוחים כמו "פעילות נרחבת של הסברה לציבור" (יעד 1.1), "הנגשה מדורגת של כלים ושירותי הגנת סייבר בסיסיים" (יעד 1.2), "השגת רמת אבטחה הולמת ואיכותית של מערכות המחשוב הממשלתיות" (יעד 2.3), 'כיפת סייבר' הכוללת "מגוון יכולות מתקדמות ותציע פתרון רוחבי להתמודדות מהירה יותר עם האיומים" (יעד 4.2) או "הטמעתם של עקרונות לבניית משק חסין יותר מפני משבר דיגיטלי" (יעד 5.1) ועוד, כל אלו מחייבים עבודת מטה נוספת של קביעת תיעדוף ברור בין היתר אל מול איום ייחוס מוגדר טרם הפיכתם לתהליכים ולפרויקטים.

ג. הגישה הפרואקטיבית: המדינות המובילות בעולם מתכנסות להחלטות המגדירות את גבולות הגישה הפרואקטיבית שלהם, שיכולה להשתרע מפעולות משפטיות בזירה הבינלאומית, דרך פגיעה מרחוק בתשתיות התוקף ועד הפעלת כוח נגד או בשל איומי סייבר. נכון למדינת ישראל לקיים דיון עקרוני בסוגיה ולקבוע מדיניות ברורה, גם אם הדבר ייעשה באופן לא פומבי.

ד. מחשוב קוואנטי: האסטרטגיה הנוכחית פוסחת על סוגיית המחשוב הקוואנטי, וזאת, במידה מסוימת של צדק נוכח ההתמקדות בשלוש השנים הקרובות. עם זאת, הסוגייה הקוואנטית חייבת להעלות לדיון ולטיפול כבר עתה ולו רק לאור השפעתה על סוגיית ההצפנה, שהיא רכיב מפתח בהגנת הסייבר.

לסיכום, סיכומה ופרסומה של אסטרטגיית סייבר לאומית היא אירוע ראוי לציון בעולם הגנת הסייבר ובכלל. מסמך האסטרטגיה כולל הכרעות מעניינות של מערך הסייבר הלאומי בסוגיות מפתח. מבחנו הגדול יהיה מעתה יישומו הממוקד והמתועדף - בדגש על בניית עוצמות המערך כליבה המחוללת של הגנת הסייבר הלאומית – והיכולת להניע תהליך מחזורי של עדכונו מידי שלוש שנים ולא המתנה של שמונה שנים עד למסמך הבא.

אל"מ (מיל') שי שבתאי הוא סגן מנהל מרכז בס"א, מומחה לביטחון לאומי, תכנון אסטרטגי ותקשורת אסטרטגית. אסטרטג בתחום הגנת הסייבר ויועץ לחברות מובילות בישראל.