

# דרושה - מדיניות לאומית

לפני למעלה מעשור ישראל הבינה את האיום הגלום בפגיעה בסייבר, כשהממשלה החליטה על הגנת תשתיות קריטיות. עתה הזמן להתבונן על האיום הזה בצורה רחבה ולקיים תהליך בניין כוח לאומי רב-שנתי. התייחסות שיטתית למכלול אבני היסוד בבניין הכוח תוכל להצמיד את ישראל לחזית העולמית ביישום תפיסה כוללת לפעולה לאומית במרחב הסייבר | אל"מ (מיל.) ד"ר גבי סיבוני

לצד פיתוח טכנולוגי של כלים ושיטות נדרשים להיות משולבים ומסונכרנים באופן שימצא את כלל המשאבים הלאומיים לטובת ביצור יכולות הסייבר של מדינת ישראל. שני מרכיבים אלה בבניין הכוח נדרשים להיבנות לאור האסטרטגיה ותורת הפעולה בסייבר.

המערך הטכנולוגי והאנושי שיפותח נדרש לתמוך את יעדי המדינה הלאומיים בסייבר, כפי שבאו לידי ביטוי בתהליך הפיתוח המחשבתי המקדים. כך גם ההשקעות בטכנולוגיה שמדינת ישראל מעודדת, כמו גם כיווני בניית ההון האנושי בבתי הספר ובאקדמיה.

כל אלה נדרשים להתאים לתפיסה ולטכנולוגיות המפותחות. לדוגמה, הצורך בפיתוח הגנת הסייבר במגזר האזרחי מחייבת פיתוח כוח אדם ייעודי באקדמיה, שיוכל להשתלב בשוק ההגנה האזרחית בקרב מפתחי טכנולוגיה, הארגונים, החברות וצרכני הביטחון, כמו גם בקרב גורמי הרגולציה של המדינה, שידרשו לאכוף את תפיסת ההגנה האזרחית שתסוכם.

## למצות את מלוא הפוטנציאל הלאומי

מערך מאורגן של אנשים וכלים טכנולוגיים מחייב פיתוח טכניקות פעולה, הכשרות, אימונים ותרגילים. פיתוח התחום הזה מהווה את שיאו של תהליך בניין הכוח. ארגוני הביטחון מקיימים שגרת הכשרות, אימונים ותרגילים. יש להרחיב תחום זה גם למגזר האזרחי שהוא החשוף ביותר לפגיעת במרחב הסייבר ולשלב מאמצים עם שאר הארגונים כדי למצות את מלוא הפוטנציאל הלאומי. יש לייצר אפוא מסגרות להכשרת בעלי תפקידים במגזר הזה שיוכלו למלא את מגוון התפקידים הנדרש.

הכשרות אלה ניתן לבצע בשילוב מוסדות האקדמיים וכן באמצעות קורסים ייעודיים. בנוסף ובדומה לתרגילי הגנת העורף השנתי, יש לקיים תרגילי לאומי להגנת סייבר. בתרגיל זה נדרש יהיה לאתגר את כלל מרכיבי בניין הכוח וללמוד ממנו כדי לשפר ולשכלל את המענה הלאומי באופן קבוע. בנוסף, התרגיל יהווה מנוע לפיתוח תוכניות אופרטיביות, שיסייעו לישראל לשפר את המוכנות לתקיפת סייבר רחבת היקף.

מדינת ישראל הובילה כבר לפני למעלה מעשר שנים בהבנת איום הפגיעה בסייבר כשהממשלה החליטה על מענה להגנת תשתיות לאומיות קריטיות. עתה הזמן להתבונן על האיום הזה התבוננות רחבה ולקיים תהליך בניין כוח לאומי רב-שנתי. התייחסות שיטתית וסדורה למכלול אבני היסוד בבניין הכוח תוכל להצמיד את מדינת ישראל לחזית העולמית בגיבוש ויישום תפיסה כוללת לפעולה לאומית במרחב הסייבר.

הכותב הוא ראש תוכנית הסייבר במכון למחקרי ביטחון לאומי וראש התוכנית להנדסת סייבר בבית הספר להנדסה של מכללת שנקר



תייחס להגנת מערכי הביטחון והתעשייה הביטחוני-נית הרגישה, להגנת התשתיות הלאומיות הקריטיות, להגנת שירותי הממשלה ולהגנת המגזר האזרחי. שלושת הראשונים מטופלים ברמה כזו או אחרת, אולם אף שבימים אלה מתקיים דיון ער בנושא הזה הרי שטרם סוכמה תפיסת ההגנה למגזר האזרחי.

## פיתוח כוח אדם ייעודי

תורת הפעולה במרחב הסייבר נדרשת גם להתייחס למענה הלאומי בשגרה, בחירום ובמלחמה ולהגדיר היטב כיצד צריכה מדינת ישראל להתמודד לא רק עם אירועי תקיפה שבשגרה, אלא גם עם תקיפות סייבר רחבות היקף, שיופעלו על מדינת ישראל במנותק או במשולב עם אירועי לחימה פיזיים. פיתוח כוח האדם וההון האנושי

נדרשים להתייחס למגוון מרכיבים ובהם תפיסת הפעלת הכוח ההתקפי במרחב הסייבר. תפיסה זו נוגעת למבצעי מודיעין ולמבצעים התקפיים במרחב האסטרטגי בו פועלת מדינת ישראל. אולם לא רק שם, אין להמעיט בחשיבות השימוש בכלי תקיפה בסייבר גם במרחב המערכתי והאסטרטגי של שדה הקרב מול אויבים קרובים ורחוקים. בנוסף, התפיסה צריכה להתייחס לאפשרות לקיים תקיפה מקדימה כדי לסכל את פעולתם של גורמים המתכננים לפעול נגד מטרות ישראליות, או מטרות יהודיות בעולם.

לצד ההתייחסות לנושא התקיפה יש לפתח ולגבש תפיסת הגנה כוללת המשלבת את הארגונים הרלוונטיים, במטרה לספק למדינת ישראל מענה הגנתי מקיף ואפקטיבי. תפיסת ההגנה צריכה לה-

## המענה הלאומי חייב לכולל את המרחב האזרחי

מרכיב הארגון בבניין הכוח מביא לידי ביטוי את ההסדרה הנדרשת בנוגע לאחריות ולסמכות ההפעלה של אנשים ואמצעים למימוש האסטרטגיה הלאומית ותורת הפעולה במרחב הסייבר בישראל. באופן טבעי התפתח העיסוק במרחב הסייבר בארגונים רבים בישראל. ארגוני הביטחון בונים לעצמם יכולות פעולה במרחב הסייבר כדי לתמוך את משימות היסוד שלהם. כך למשל, צה"ל הפועל למצות את הפוטנציאל של מרחב הסייבר לצרכים מבצעיים ולצרכי מודיעין. כל זאת במקביל לפיתוח יכולות ההגנה על מערכי הליבה של הצבא מפני התקפות סייבר. כך גם שאר ארגוני הביטחון דוגמת המוסד, השב"כ ומשטרת ישראל. ההגנה על תשתיות לאומיות קריטיות מונחת לפתחה של הרשות לאבטחת מידע הפועלת במסגרת השב"כ בתוקף אחריותם להגנת גופים אלה לאור החלטת ממשלה. בנוסף לכך פועלים גופים נוספים להגנת משרדי ממשלה, לשמירת הפרטיות ברשת ועוד. אך בשלב זה טרם סוכמה בממשלת ישראל תפיסת ההגנה האזרחית במרחב הסייבר. ראוי יהיה שההחלטה לגבי ארגון המענה הכולל לתקבל מתוך ראייה רחבה לצד חתירה למיצוי הפוטנציאל הקיים בארגונים השונים.

**מ**רחב הסייבר מייצר אתגרים מורכבים לצד הזדמנויות רבות. ישראל הינה מדינה עתירת טכנולוגיה וכך גם מגוון השירותים, העסקים והתעשייה שפועלים בה. אלה תלויים במידה רבה בפעולתם התקינה של מערכות מחשב, בקרה ותקשורת רבות. תמונת המצב הזו אינה יחידית רק לישראל, שכן זו תופעה גלובלית, אך ככל שתלות זו גדלה עם התפתחות היכולת לספק שירותים ולתפעל עסקים באמצעות מערכות מחשב ותקשורת, כך גדלה הפגיעות וגדל הסיכון לשיבוש חמור בשגרת החיים התקינה כתוצאה מפגיעה בעסקים ושירותים הנסמכים על מרחב הסייבר. דוגמאות לשימוש לרעה במרחב הסייבר ניתן למצוא למכבי. אירועי השנים האחרונות ממחישים עד כמה הפך המרחב הזה לזירת התגוששות ופילול ערה. במרחב הסייבר האלים ניתן למצוא מדינות וארגונים הנתמכים על-ידי מדינות הפועלים כנגד מדינות אחרות, ארגונים ואף חברות עסקיות, כשמנעד המניעים נע ממניעים פוליטיים ועד ריגול וגניבת קניין רוחני. לצידם ניתן למצוא ארגוני טרור המוצאים ברשת כר נרחב לפעילותם, תוך ניצול היכולת לשמור על אנונימיות.

לא נפקד גם מקומם של פושעים וארגוני פשיעה הפועלים בסייבר לצורך גניבת כספים, סחיטה והונאות פיננסיות. לבסוף, ניתן למצוא גם פרטים והתארגנויות אד-הוק של אקטיביסטים הפועלים ברגע מסויים כנגד מטרה משותפת. ההתפתחות הזו מחייבת מדינות בכלל ואת מדינת ישראל בפרט לייצר תפיסה כוללת, שממנה יגזרו תהליכי בניין כוח לאומי במרחב הסייבר.

## תורת הגנה כוללת

תהליך בניין כוח לאומי בתחום הסייבר הינו תוצר של תכנון רב-שנתי הגוזר מגוון פעולות, פיתוח ופרייקטים המאפשרים התעצמות בת קיימא באופן שיטתי ומוכוון. לכן, תהליך לאומי לבניין כוח בתחום הסייבר הינו אתגר מורכב המחייב שידוד מערכות לאומי.

לתהליך בניין כוח מספר אבני יסוד, אשר הראשון שבהם הינו גיבוש של אסטרטגיה ותורת פעולה כוללת במרחב הסייבר. רכיב זה הינו הבסיס עליו נשען כלל התהליך הכולל מרכיבים נוספים ובהם: פיתוח כוח האדם וההון האנושי, פיתוח טכנולוגי של אמצעים, ארגון כוח האדם והאמצעים במסגרות מתאימות, המאפשרות עמידה ביעדי האסטרטגיה ותורת הפעולה שגובשה, ולבסוף, קיומן של הכשרות, אימונים, ותרגילים במטרה לוודא שכלל המערכים פועלים כיאות וכדי לשכלל ולפתח את הידע באופן שיטתי.

כאמור, פיתוח האסטרטגיה הלאומית הינו מחורלל תהליך בניין הכוח. הקמתו של מטה הסייבר הלאומי על-ידי ראש הממשלה סימנה את תחילתו של התהליך, אולם זה רחוק עדיין מאוד מהשלמה. האסטרטגיה ותורת הפעולה במרחב הסייבר