

דרושה - אסטרטגיה לאומית

מדוע דרושה אסטרטגיה לאומית לפעולה במרחב הסייבר ומה אמורה אסטרטגיה כזו לכלול? | ד"ר גבי סיבוני



ד"ר גבי סיבוני

אם כי אופיו של המרחב הקיברנטי והתפתחותו מחריפים את הסוגיה. יש עיסוק נרחב בסוגיה זו במדינות המערב, כפי שפרשיית אדוארד סנאודן הציפה. הנקודה הרביעית היא אחריותה של המדינה לבנות יכולת קיברנטית ולהשתמש בה באופן שיאפשר השגת האינטרסים הישראליים. ולבסוף, הנקודה החמישית היא יכולתה של המדינה להבטיח את התשתית, שתאפשר מימוש האסטרטגיה בסייבר לאורך זמן. תשתית בהקשר זה היא טכנולוגיה מתקדמת, אנשים מוכשרים ומיומנים, שיתוף פעולה עם מדינות וגופים מחוץ למדינה ובניית תהליכי עבודה וארגונים ממלכתיים אפקטיביים בהתאמה לדינאמיות וטווחי הזמן הקצרים המאפיינים את תחום הסייבר.

אכיפה של שיטות עבודה

בכל אחת מהנקודות הללו ניתן להחליט על כיווני פעולה שונים, אולם חשוב ומהותי להבין את הקשרים שיש בין הנקודות הללו. לדוגמה, החלטה שהמדינה אחראית להגנת המגזר הפרטי יכולה לגרום אחריה אכיפה של טכנולוגיה ושיטות עבודה, שהמדינה חושבת כנחוצות להגנה, וכן איסוף מידע רחב על הנעשה במרחב הקיברנטי על-ידי המגזר הפרטי בישראל. פעולות כאלה עלולות לסתור חלקים מסוימים על שמירת פרטיות ומתן חופש פעולה מסוים לחברות להחליט בעצמן על רמת ההגנה הקיברנטית שלהן. מכאן שהאסטרטגיה שתגובש צריכה להיות מעשית וקוהרנטית וצריך לגבש אותה בשיטות מירב הגורמים המעורבים - ממשלה, מגזר אזרחי, חברות טכנולוגיות וגופי ביטחון.

אסטרטגיה כזו היא בחלקה גלויה ובחלקה חשאית, באופן טבעי, והיא מצריכה תיקוף עדכון עיתי. היא תושפע רבות מטכנולוגיה מתפתחת, שיטות ותפיסות התמודדות שיתפתחו וצרכים משתנים של המדינה על המגזרים השונים שלה והיא מאתגרת במימוש שלה. כאמור, אין בכל אלה לייצר את העיסוק באסטרטגיה לאומית לפעולה בסייבר. מאמר זה מתפרסם במקביל ליציאתה לאור של עבודה רחבת יריעה שכותרתה "קווים מנחים לאסטרטגיה לאומית במרחב הסייבר". עבודה שנכתבה במסגרת מחקר של התכנית לבטחון סייבר במכון למחקרי בטחון לאומי. יש לקוות שעבודה זו תוכל לתרום לתהליך גיבוש, ניסוח ואישור אסטרטגיה לאומית לפעולה במרחב הקיברנטי. אסטרטגיה החיונית לבניין הכוח ופיתוח היכולות בתחום חשוב זה בישראל.

הכותב הינו ראש תכנית ביטחון סייבר במכון למחקרי בטחון לאומי

במרחב הקיברנטי היא יריעה רחבה ונדרשת בה התייחסות לסוגיות טכנולוגיות, משפטיות, מדיניות, ביטחוניות, ארגוניות, ערכיות וכלכליות. אין במורכבות הזו כדי להוריד מחשיבות גיבוש אסטרטגיה, או מהתמודדות עם מימוש האסטרטגיה הלאומית אחרי שתגובש. יש לתת את הדעת לתהליך בו מגבשים את האסטרטגיה, לסוגיות מפתח בתהליך הזה ולקשר ההדוק בין החלטות שמתקבלות בכל אחת מהנקודות המרכיבות את האסטרטגיה. כדוגמה ניתן לבחון חמש נקודות שהחלטות בהן מהותיות לקביעת האסטרטגיה.

אחריותה של המדינה

הנקודה המשמעותית כמוצא לקביעת אסטרטגיה לאומית היא אחריות המדינה להגנת המגזר הפרטי. בשל אופיו של המרחב הקיברנטי ואופי

בסייבר, שיגדיר את יעדי העל של המדינה בתחום הפעולה בסייבר ואת דרכי השילוב שלהם במאמץ הביטחון, הכלכלה ושאר המאמצים הלאומיים. לבסוף, כל ארגון מדינתי הפועל במרחב הזה יידרש לגבש את האסטרטגיה הארגונית שלו לפעולה במרחב הזה.

מרחב הסייבר המדינתי

מרחב הסייבר המדינתי בישראל, כמו בכל מדינה אחרת, ניתן לחלוקה לשני תת-מרחבים עקריים: המרחב הביטחוני - בו פועלים כלל ארגוני הביטחון, גורמי המדינה, הגנת תשתיות לאומיות קריטיות וכדומה - והמרחב הפלילי אזרחי, הכולל את ארגוני האכיפה השונים, דוגמת משטרת ישראל ורשויות אכיפה נוספות המתמודדים מול גורמי פשיעה במרחב הסייבר. לכן,



הפעילות שמתרחשת בו נדרשת הגדרה לגבי אחריותה של המדינה בסוגיית הביטחון הקיברנטי של ארגונים פרטיים ואזרחים. כפועל יוצא מהגדרת האחריות של המדינה עולה הנקודה השניה, שהיא הצורך והסמכות של המדינה לאכוף שימוש בטכנולוגיות ושיטות פעולה בתחום הגנת הסייבר על המגזר האזרחי, שמהווה במקרים רבים חלק מתשתית חיונית קריטית לביטחונה ו/או לתפקודה התקין של המדינה, מוסדותיה ואזרחיה.

הנקודה השלישית היא עד כמה זכאית המדינה לאגור פרטים על פעילות המגזר האזרחי במרחב הקיברנטי לצורך הגנתו. סוגיית החדירה לפרטיות האזרחים היא ערכית ואינה רלוונטית רק לסייבר,

האסטרטגיה שתגובש תדרש להתייחס לשני המרחבים האלה המייצרים את מרחב הסייבר המדינתי השלם. זאת כמוכן מבלי להזניח מרכיבים שלובים נוספים דוגמת פיתוח התעשייה, ההון האנושי שיתוף פעולה בין לאומי ועוד.

כמובן שבבסיס העיסוק בהיבטי אסטרטגיה לפעולה במרחב הקיברנטי עולה השאלה של כדאיות ורלוונטיות בניסוח אסטרטגיה בתחום שכמות העוסקים בו גדולה, הוא מקיף אט-אט את כל תחומי החיים, כמות הכסף המושקעת בו בשוק החופשי היא גדולה ומהווה ממילא מניע להתפתחות והתחווה היא שאין יכולת של ממש למדינה לממש בו תכנית סדורה. תכנון אסטרטגיה לאומית

וכח התעצמות השימוש שנעשה במרחב הקיברנטי להשגת אינטרסים של מדינות וארגונים, ולאור העובדה שישראל, כמדינה מפותחת טכנולוגית, פעילה מאד במרחב הסייבר, נראה נכון להציע קווים מנחים לאסטרטגיית פעולה של ישראל במרחב הקיברנטי. את היעדים של ישראל ניתן לנסח בפירוט, אך בסיסם, כמו בכל מדינה, הוא הבטחת ביטחון לאומי ואישי ושגשוג ורווחה כלכליים לכלל אזרחי המדינה.

המרחב הקיברנטי הוא מרחב נוסף בו ישראל פועלת כדי להבטיח את היעדים הללו. מימוש היעדים מחייב הגנה יעילה על מוסדות המדינה, תשתיות קריטיות, עסקים ואף פעילות אזרחים, תוך שימוש מושכל במרחב הזה להשגת האינטרסים של ישראל. הדרך למימוש יעדים אלה נדרשת להתבסס על אסטרטגיה שהינה תכנית-אב להשגת היעדים ועל טקטיקה המגדירה את אופן מימוש

מסמך המדיניות
הלאומית לפעולה
בסייבר יגדיר את יעדי
העל של המדינה בתחום
ואת דרכי השילוב
שלהם במאמץ הביטחון,
הכלכלה ושאר המאמצים
הלאומיים

האסטרטגיה בפועל. במציאות, כפי שכולנו חווים, הקשרים בין המרכיבים האלה אינם חד-כיווניים, אלא מקבילים ודו-כיווניים והעשייה בכל רובד משפיעה כל העת על הרבדים האחרים.

לאור זאת, גיבושה וניסוחה של אסטרטגיה לאומית לפעולה במרחב הסייבר הן בסיס חיוני להכוונת הפעלת הכוח ובניין היכולות בתחום הסייבר בכל מרחב הפעולה, כולל: טכנולוגיה, הון אנושי, ארגון והטמעה, לצד הכוונה של הפעולה של כלל הגורמים והארגונים הלאומיים העושים שימוש במרחב זה. לכן, על מדינת ישראל לפעול בהקדם כדי לגבש מסמך אסטרטגיה לאומית לפעולה בסייבר. מסמך האסטרטגיה שייכתב צריך להיות רכיב במסמכי היסוד, כשהמוביל שבהם צריך להיות מסמך המדיניות הלאומית לפעולה