שותפות אסטרטגית - מכפיל כוח להתמודדות עם האיום המתגבר בממד הסייבר

א' - ראש החטיבה העוסקת בהתמודדות עם איומי סייבר בשב"כ

מבוא

מאמר זה עוסק בהתארגנות קהילת המודיעין להתמודדות עם איומי סייבר, ובתוכה השותפות האסטרטגית בין צה"ל/חטיבת ההגנה בסייבר (חטה"ג) לשב"כ/החטיבה לסיכול איומי סייבר, שותפות שהיא "ראש החץ" של ההיערכות הביטחונית מול האיומים בממד זה. המאמר סוקר את אתגרי ההגנה והסיכול מול האיום המתעצם בסייבר ואת התפתחות ההתארגנות הבין־קהילתית והשותפות בין שני הגופים ביחס למדרג של מערכות יחסים בין ארגוניות (תיאום, סיוע, שילוביות, שיתופיות ושותפות).

הטענה העיקרית במאמר זה היא ששילוביות, שיתופיות ושותפויות על גווניהן, ובתוך כך שותפויות אסטרטגיות שמביאות לידי ביטוי קשר לטווח ארוך, המחבר במטרות הליבה, בחזון ובערכים, עם אינטרסים פרגמטיים, הן מפתח הכרחי להתמודדות עם רוחב היריעה של האתגרים בממד הסייבר

הטענה העיקרית המובאת במאמר זה היא ששילוביות, שיתופיות ושותפויות על גווניהן, ובתוך כך שותפויות אסטרטגיות שמביאות לידי ביטוי קשר לטווח ארוך, המחבר במטרות הליבה, בחזון ובערכים, עם אינטרסים פרגמטיים, הן מפתח הכרחי להתמודדות עם רוחב היריעה של האתגרים בממד הסייבר.

השותפות האסטרטגית בין שב"כ לחטה"ג, המתבססת על ייעודי הארגונים ועל החפיפה ביניהם, מאפשרת לכל אחד מהארגונים לממש את ייעודו באמצעות נכסים ויכולות שיש ברשות הארגון האחר. לצד היכולת למקסם משאבים ולנהל בצורה מושכלת מאמצים משותפים בבניין והפעלת הכוח, השותפות מאפשרת לרתום את כלל היכולות המודיעיניות, המבצעיות והסיכוליות של הארגונים לטובת בניית תמונת המודיעין הכוללת והתמודדות רב־ממדית ואפקטיבית עם האיומים בממד הסייבר, בשילוב כלים ויכולות מחוץ לממד.

בשותפות כזו הערך והכדאיות נבחנים לאורך זמן ולא בהשוואה לאירוע בודד. היא מחייבת ניהול מתמיד, כדי לשמר ולהעצים את האינטרסים המשותפים, לפרק מתחים בהתהוותם, לבצע התאמות נדרשות ביחס למציאות המשתנה ולקדם אזורי ערך חדשים. מנהיגות, אמון, שקיפות, קרדיטציה מוסכמת ומנגנונים לניהול חילוקי דעות הם המפתח **למעבר מ"אגו־סיסטם" ל"אקו־סיסטם" ולהבקעת היעדים המשותפים**.

פרק א' - אתגר ההגנה והסיכול מול האיום המתעצם בממד הסייבר

בשנים האחרונות חלה עלייה דרמטית ברמת האיום שנשקפת מפעילות יריבים בממד הסייבר ככלי מרכזי בשגרה וכחלק מארסנל הכלים במערכה כוללת. עלייה זו היא תוצאה של השינוי באופי העימותים הנוכחיים והעדפה של מדינות להימנע ככל האפשר מכניסה למערכות צבאיות רחבות היקף, וכן של התלות הגוברת של תהליכים עסקיים, תעשייתיים, חברתיים וכלכליים במערכות תקשו"ביות. תלות זו והמאפיינים הייחודיים של הממד מייצרים לתוקפים מכל הסוגים והרמות כר פורה של הזדמנויות:

- קישוריות שמאפשרת להגיע מכל מקום לכל מקום;
- משטח תקיפה הולך ומתרחב: החל מרכיבים טכנולוגיים (IOT) ועד לגוף האדם, הנשען על טכנולוגיות כדי לנהל את חייו, לעבוד, לנוע ממקום למקום ולשמור על בריאותו IOB – (Internet of the body);
- חולשות וכלים זמינים ברשת ברמות שונות;
- יכולת השתנות מהירה (תשתיות, כלים ושיטות תקיפה);
- מרחב הכחשה – הממד מזמן לתוקף מגוון אפשרויות להסוות ולטשטש את זהותו.
- משטח התקיפה המתרחב מאפשר גם לתוקפים בעלי יכולות נמוכות לייצר נזק משמעותי, ולתוקפים בעלי יכולות גבוהות להגיע למידע ברשתות רגישות, מכיוון שמרבית הרשתות מחוברות באופן כלשהו לאינטרנט.

תחת משפחות התכליות המוכרות לפעילות בסייבר - איסוף/ריגול (CNE), טרור/פגיעה (CNA) והשפעה (CNI), התפתחו בשנים האחרונות איומים חדשים:

- **פגיעה כלכלית באמצעות סייבר** – תקיפות כופרה, דלף שתכליתו לפגוע במוניטין או CNA שתכליתו נזק כלכלי לחברה/משק. פעמים רבות מאחורי תקיפות אלה עומדים (ישירות או בעקיפין) גורמים מדינתיים שתכליתם לייצר, באמצעות הפגיעה הכלכלית, אפקט תודעתי. אפקט זה עלול להיות, בתרחישי קיצון, בעל משמעויות אסטרטגיות. מתקפת NotPetya (2017), שכוונה נגד אוקראינה היא דוגמה למתקפה שיצרה נזק כלכלי נרחב עם משמעויות אסטרטגיות למשק האוקראיני וכן לחברות ענק מערביות.
- **בלמ"ס + בלמ"ס + בלמ"ס = סוד** - אם בעבר הנחת העבודה הייתה כי הנזק שעלול להיגרם כתוצאה מנגישות יריבים למאגרי מידע מקומיים ובלתי מסווגים הוא נמוך, כיום יכולות זמינות של כריית מידע ואלגוריתמים של לימוד מכונה מאפשרים לחבר ולהתיך מידע ממגוון מקורות בלתי מסווגים לכדי מודיעין שעלול לסכן שיטות, יכולות ונכסים.
- **התרחבות השימוש בשרשרת אספקה דיגיטלית כווקטור נגישות –** דוגמה בולטת לכך מהעת האחרונה היא מתקפת SolarWinds, שייצרה נגישות ראשונית למספר רב של גופי ממשל וחברות ענק בארה"ב דרך עדכון תוכנה לגיטימי של פלטפורמת ניטור רשתות של החברה האמריקאית SolarWinds. בהמשך, כאשר היה גוף שסומן כמעניין, מימשו התוקפים מבצע רשת עמוק, ככל הנראה לתכלית איסוף/ריגול.

- **טרור ממוקד באמצעות סייבר** - התרחבות מגמת ה־IOT ומגמת ה־IOB הופכת את הסייבר גם לאמצעי לפגיעה ממוקדת ומדויקת באנשים.

במציאות כזו, אתגר ההגנה והסיכול הוא אתגר עצום ומתעצם. אומנם לתוקף מספיקה נקודת תורפה אחת כדי להבקיע, אך הצד המגן והמסכל נדרש לסגור ולנטר מספר עצום של פרצות פוטנציאליות. האיום לעיתים קרובות יהיה "סמוי מן העין" – יריב יכול לפעול במשך תקופה ארוכה בתוך רשת, להתפשט ממנה לרשתות נוספות, לאסוף ולהזליג מידע ולבצע פעולות מניפולציה שנשארות זמן רב "מתחת לרדאר". מאפיין זה מייצר ליכולת של הצד המגן/מסכל אתגר לבחון את אפקטיביות הפעולות שהוא מבצע. האם העובדה שאיננו מזהים פעילות היא אכן אינדיקציה לכך שאין פעילות כזו?

האיום המתעצם מממד הסייבר מצטרף למגמה נוספת, של היטשטשות הגבולות בכל היבט של האיום:

- מי תוקף אותי? יריבים מגוונים ובעלי מאפיינים שונים – מדינות, ארגוני טרור, שחקנים "אזרחיים" דוגמת קבוצות האקרים שהם לפעמים "קבלן ביצוע" של מדינה/ארגון טרור ולפעמים מבצעים את הפעילות לטובת רווח עצמאי, האקרים בודדים ועוד.
- מיהו היעד הנתקף? ממטרות ביטחוניות קלסיות ועד תשתיות וחברות אזרחיות.
- לשם מה? פגיעה בביטחון פיזי/אישי עד פגיעה בביטחון לאומי. ישנן יותר ויותר תקיפות שממממשות כמה תכליות בציר הזמן – דוגמת תקיפה שמתחילה כאירוע איסופי, ממשיכה כאירוע CNA על ידי הפעלת כלי מחיקת TI ובכך מייצרת אפקט תודעתי שעלול לפגוע בתחושת הביטחון.
- איך מתבצעת התקיפה? טשטוש גבולות בין הקינטי לקיברנטי:
  - במאקרו – מרחב הסייבר כמרחב נוסף לתגובה ולניהול המאמצים בין המערכות.
  - במיקרו – שימוש בכלים מחוץ לממד ההתמודדות עם איומי סייבר כדי לממש שיבוש, סיכול והרתעה בצורה אפקטיבית.

המאפיינים הייחודיים של הממד וטשטוש הגבולות מחדדים את הצורך בהסתכלות כוללת ורב־ממדית על האיום: מצד היריב, המשך בתשתיות האינטרנט והתקשורת הבין־לאומיות שבהן ממוקמת שרשרת התקיפה והבידול של התוקף ועד למרחב המדינתי הישראלי, עליו נדרש להגן, לצד יכולת לנטר ולנתח את פעילות היריבים (הגיונות, כוונות ויכולות) ולייצר התמודדות מבצעית ומאמץ סיכולי במגוון כלים, בממד הסייבר ומחוצה לו. איך נערכים, אם כך, להתמודדות עם אתגר עצום זה?

פרק ב' - מערכות יחסים בין־ארגוניות בתיאוריה ובפועל

גודל האתגר וההבנה כי הוא צפוי להתעצם משמעותית, תורגמו כבר ב־2013–2014 לשינוי בהתארגנות של גופי הביטחון - בהגנה, בהתקפה ובשילוב בין מגן ותוקף והקמת התארגנות, שבה חברים כלל גופי הקהילה שעוסקים בהגנה וסיכול איומי סייבר. תכליתה של התארגנות זו היא לייצר הסתכלות כוללת על פעילות היריבים בסייבר וההקשרים הרחבים שלה, וכן לנהל אופרציה

צילום: SHUTTERSTOCK

מתמשכת או נקודתית ("מבצע") מול איומי סייבר. החזון שהיה הבסיס להקמת התארגנות זו לא היה תוצאה של משבר ארגוני אלא נבע מניתוח בהיר וצופה פני עתיד של האיום ומאפייניו, והבנה כי רוחב היריעה של האיום מחייב התארגנות משותפת של כלל הארגונים העוסקים במלאכה.

כדי להבין את הייחודיות של ההתארגנות הקהילתית בתחום ואת הייחודיות של השותפות האסטרטגית בין צה"ל/אגף תקשוב/חטיבת ההגנה בסייבר לחטיבה העוסקת בסיכול איומי סייבר בשב"כ, שבה אתמקד בהמשך, אציג את מדרג מערכות היחסים הבין ארגוניות: **מדרג של מערכות יחסים בין־ארגוניות.**[1]

- תיאום (Coordination) – סנכרון פעילות בתא שטח או מול יעד מסוים. תיאום מאפשר לכל צד לגזור את המשמעויות למניעת פגיעה הדדית.
- סיוע (Assistance) – תהליך שבו גוף אחד מעמיד משאב/יכולת/מידע לטובת גורם אחר. בתהליך זה נשמרת האוטונומיה בקבלת ההחלטות של הגוף המסתייע.
- שילוביות (Jointness) – התארגנות משימתית משותפת לפרק זמן מוגדר. בתהליך זה מתקיים חיבור בין גופים תוך מיצוי היתרון היחסי של כל אחד מהם לטובת מענה לאתגר מבצעי/תהליך בניין כוח.
- שיתופיות (Cooperation) - עבודה משותפת בין גופים, לרבות שיתוף במידע, משאבים ויכולות לצורך השגת מטרותיהם. שיתופיות מחייבת אמון ושיתופיות בקבלת ההחלטות.
- שותפות (Partnership) – קשר לטווח ארוך המשלב חיבור במטרות הליבה, בחזון ובערכים

1 סולם השילוביות לעיל הוא תוצר של עבודה שבוצעה בשב"כ על שילוביות בין־ארגונית, המתיבה ידע תיאורטי בנושא עם פרקטיקה.

עם אינטרסים פרגמטיים. בשותפות לא חייב להתקיים מצב של win win ביחס לאירוע או תהליך בודד. הערך והכדאיות נבחנים לאורך זמן.

בשנותיה הראשונות הייתה ההתארגנות הקהילתית מנגנון שעסק בעיקר ב**תיאום** פעילויות ומאמצים על בסיס הערכת מצב שבועית משותפת, ומימש **שילוביות** בריכוזי מאמץ מבצעיים. היבטים מסוימים של ההתארגנות, דוגמת חילופי מזהים טכנולוגיים ומודיעין, כבר נגעו במדרג של **שיתופיות.**

גודל האתגר באיומים הנשקפים בממד הסייבר הוביל לשינוי בהתארגנות של גופי הביטחון - בהגנה, בהתקפה ובשילוב בין מגן ותוקף והקמת התארגנות, שבה חברים כלל גופי הקהילה שעוסקים בהגנה וסיכול איומי סייבר

ההתארגנות מאפשרת לכל אחד מהגופים החברים בה להביא לשולחן את יתרונו היחסי ולהתבסס על יכולות הארגונים האחרים כדי לממש את ייעודו במרחב. צה"ל אחראי להגנה על קיומה של מדינת ישראל, על עצמאותה וביטחון אזרחיה ותושביה בכלל הממדים, ובתוך כך חטה"ג אחראית על הבטחת העליונות והרציפות התפקודית הצה"לית והגנה על המערכות והרשתות התקשוביות של צה"ל. שב"כ אחראי על סיכול ריגול וטרור בכלל הממדים, כולל בסייבר, וכן מוביל את ההתארגנות הקהילתית בשגרה.

המכנה המשותף הרחב של ההתארגנות הקהילתית הוא חוסן ועמידות המרחב הישראלי וטיפול באירועים במרחב המדינתי. היא מתבססת על שני "שרירים" שפועלים בצורה משולבת – "שריר" ביטחוני, הממוקד ביריבים ובשרשרת הערך של התוקף מצד היריב ועד למרחב המדינתי הישראלי, בהובלת צה"ל ושב"כ ובשותפות המוסד, ו"שריר אזרחי" שממוקד בקידום העמידות והחוסן של המשק בהובלת מערך הסייבר הלאומי. היערכות משולבת ורב־שכבתית זו מאפשרת לייצר תמונה מלאה וארגז כלים להתמודדות עם האיום על כלל היבטיו – הביטחוניים והאזרחיים.

החיכוך המתעצם בממד הסייבר והצורך במעבר מהתמודדות עם איומי CNE של היריבים למתקפות CNA, חייבו לעבור מעבודה ב־offline למענה online המשלב את יכולות כלל הארגונים בזמני תגובה קצרים. הדבר הביא לקפיצת מדרגה משמעותית בתהליכים הבין־ארגוניים וברמות האמון והאינטימיות בין שותפי ההתארגנות בכל הרמות: מבניין הכוח הטכנולוגי, ניהול השגרות המודיעיניות והאופרטיביות ועד לניהול אירועים ואופרציות מבצעיות מורכבות. במידה מסוימת אפשר להשוות בין קצב האירועים שפגש את המרחב הישראלי בשנה האחרונה בסייבר לאינתיפאדה השנייה: מהפכת הסלולר בתחילת שנות ה־2000, שאפשרה תקשורת טקטית ותיאומים חוצי גזרות יצרה איום בעל אופי טכנולוגי וחייבה קפיצת מדרגה בשילוביות הקהילתית כדי להתמודד בצורה אפקטיבית עם הטרור הפלסטיני הגואה.[2] גם האיום המתעצם בשדה הקרב של הסייבר מחייב קפיצת מדרגה בהיערכות הטכנולוגית והמבצעית ובשותפות הבין־ארגונית, תוך כדי פיתוח של יכולות, שיטות פעולה והתארגנויות.

הגם שתפיסת התמודדות רב־שכבתית כזו (Layered Deterrence) שמשלבת "שרירים"

אזרחיים וביטחוניים, היא תפיסה רווחת גם בקרב שותפים מרכזיים במערב, **ההתארגנות הישראלית היא יוצאת דופן בעומקה, ברמת האינטימיות שלה ובהישגים שהיא מצליחה להביא לשולחן – בבניין ובהפעלת הכוח**. לשותפות האסטרטגית בין חטיבת ההגנה בצה"ל לחטיבה העוסקת בסיכול איומי סייבר בשב"כ, שמובילות את "השריר הביטחוני" בהתארגנות, יש חלק משמעותי בהצלחה זו.

פרק ג' - השותפות האסטרטגית בין שב"כ לחטה"ג - ייעוד, אתגרים ומתכון לשותפות מוצלחת

הרעיון להקים שותפות אסטרטגית בין שב"כ לחטה"ג נבט ב־2017, מתוך היכרות של ראשי החטיבות דאז עם מודלים של יחידות משותפות בעולם. המשמעות הפרקטית הייתה הקמת יחידה משותפת לשני הארגונים. בתחילה, התארגנות זו התמקדה באתגרים טכנולוגיים בלבד, אולם בשנים הבאות העמיקה השותפות גם לאזור המודיעיני-הכוונתי. הבסיס לשותפות הוא החיבור בין הייעוד והמשימות של כל אחד מהגופים והחפיפה ביניהם, לצד הנכסים והיכולות שמחזיקים כל אחד מהגופים:

- חטה"ג, לצד אחריותה להגנה על רשתות צה"ל ושימור הרציפות התפקודית הצה"לית, היא חלק מהאקו־סיסטם שפועל מול היריבים בממד.
- החטיבה העוסקת בסיכול איומי סייבר בשב"כ מובילה את מימוש ייעוד הארגון לסיכול טרור וריגול בממד הסייבר, תוך חיבור לחטיבות הסיכול "הקלסיות", המובילות את הסיכול בממד הקונבנציונלי. ומתבססת, בין היתר, על מארג של יכולות אשר יוצרות תפיסה של "מכ"ם סייבר".

החיכוך המתעצם בממד הסייבר והצורך במעבר מהתמודדות עם איומי CNE של היריבים למתקפות CNA, חייבו לעבור מעבודה ב־offline למענה online המשלב את יכולות כלל הארגונים בזמני תגובה קצרים. הדבר הביא לקפיצת מדרגה משמעותית בתהליכים הבין־ארגוניים וברמות האמון והאינטימיות בין שותפי ההתארגנות בכל הרמות

תועלות השותפות והערך שהיא מייצרת

- עיצוב וניהול מערכות משותפות להתמודדות עם פעילות הסייבר של היריבים כפלטפורמה מרכזית להסכמה על תכליות, יעדים ומיקוד משותף, ששותפים לו גם שאר הארגונים החברים בהתארגנות הקהילתית.
- תכנון משותף בטווח הקצר והארוך בבניין והפעלת הכוח, בהתבסס על יתרונות יחסיים, המאפשר למנוע כפילויות, למצות משאבים בצורה מיטבית ולמקסם את שמיכת המשאבים הקצרה.

2 ראה מאמרו של משה שוחט בגיליון זה אודות התפתחות תפיסת הסיכול המשולב באינתיפאדה השנייה.

- מנגנוני פעולה מוסכמים להתמודדות עם האתגרים בממד בשגרה, בחירום בסייבר ובעימות כולל, בהתבסס על תוכניות משותפות, תרגילים ותהליכים בריאים ומשותפים של הפקות לקחים.
- יכולת רתימה של כלל היכולות המודיעיניות, המבצעיות והסיכוליות של הארגונים (שב"כ וצה"ל) – החיונית לבניית תמונת המודיעין הכוללת של האיומים, לתיעדוף מושכל וליצירת היכולת להתמודד באופן אפקטיבי ורב־ממדי עם האיומים – מצד הירי ועד המרחב המדינתי הישראלי, מהתרעה עד סיכול, בממד הסייבר והטכנולוגיה ובשילוב עם כלים ויכולות מחוץ לממד.

על השותפות האסטרטגית בין הארגונים אפשר להסתכל בשלושה מעגלים:

- היחידה המשותפת לשני הארגונים.
- כלל היכולות והנכסים של החטיבות.
- כלל היכולות והנכסים של צה"ל ושב"כ - סיכול אפקטיבי של איומי סייבר מחייב מערכה משולבת בממד ומחוצה לו - **"ביטים לא מנצחים רק בביטים".**

את המעגלים הללו מניעים מנגנוני התכנון של ההתארגנות הקהילתית ומנגנוני התכנון המשותפים לשני הארגונים, שמאפשרים לנהל בשוטף את הפעלת הכוח, לייצר אגרוף משותף כשיש אירוע או אתגר מבצעי, לרתום משאבים מתוך צה"ל או שב"כ למימוש היעדים והתכליות המשותפות, ולבצע תכנון ארוך טווח.

התארגנות כזו, מטבעה, כרוכה בלא מעט **אתגרים שדורשים ניהול מתמיד** כדי לשמר ולהעצים את האינטרסים המשותפים, לפרק מתחים בהתהוותם ולזהות ולקדם אזורי ערך חדשים:

- תרבות ושפה ארגונית שונה;
- **איך מתמודדים עם כישלונות ואיך מחלקים קרדיט בהצלחות**;
- **מי מוביל**? ישנם אירועים שבהם התשובה לשאלה זו היא ברורה, אבל ישנם מקרים אפורים שבהם נדרש לנהל את ההובלה או לייצר העברות מקל מורכבות, ויש מקרים שמחייבים מסוגלות לנהל אירוע או מאמץ בהובלה משותפת;
- **מערכות מידע נפרדות** – אתגר שקיים גם בשגרה אבל מתעצם במבצעים ובהיערכות בחירום שדורשים סנכרון ויכולת עבודה מתואמת בקצבים גבוהים;
- הסכמה על תיעדוף המשאבים ששייכים לגוף אחד (חטה"ג) אך מוצבים בגוף אחר (שב"כ);
- שימור תחושת הערך שכל אחד מהצדדים מקבל מהשותפות בציר הזמן.

מה הם העקרונות לשותפות מוצלחת?

- **מנהיגות** – הבנה כי האינטרסים הלאומיים, מורכבות הממד ומגבלת המשאבים הם הבסיס לצורך, וכי הערך לכל אחד מהצדדים לא נמדד בטווח קצר או ביחס לאירוע ספציפי אלא הוא עיקרון מרכזי בשותפות. הבנה כי האלטרנטיבה של היעדר שותפות תביא לתחרות הרסנית שתפגע באינטרס הלאומי ובאינטרס של כל אחד מהארגונים.
- **אמון ושקיפות מלאה** – אפשר, ולעיתים אף חייבים, שלא להסכים, אבל אסור להסתיר.

- מנגנונים שמאפשרים לייצר סדר עדיפות מוסכם ולנהל דיון ענייני על אי־הסכמות.
- לאפשר לכל גוף את היכולת לייצר רלוונטיות וקרדיטציה ארגונית במקביל ובתיאום.
- **שרטוט קווים אדומים ועקרונות קריטיים לכל ארגון** – נכסים להסתרה, שמירה על מקורות וביטחון כוח אדם ועוד.
- **מעורבות מנהלים** בכירים באירועים ותהליכים אסטרטגיים ובאירועים טקטיים רגישים.
- **עיצוב מורשת משותפת**, הנשענת על ערכים, סמלים וטקסים משותפים, ונבנית דרך אירועים וחוויות מעצבות בשותפות.

עם הפנים קדימה

השותפות האסטרטגית בין צה"ל/חטה"ג לשב"כ מתקיימת ומתעצמת כבר כארבע שנים. בתקופה זו השותפות הייתה פלטפורמה פורה להתמודדות אפקטיבית עם האתגרים בממד, על ידי שיבוש וסיכול של מתקפות סייבר מצד יריבים, ויזימה ומימוש של מהלכים מבצעיים רבים, לצד תכנון והוצאה אל הפועל של בניין כוח משמעותי בתחום פיתוח מערכות ושיטות פעולה ותהליכי פיתוח כוח אדם משותפים. בימים אלה של תכנון רב־שנתי אנו בעיצומו של שיח על העמקת השותפות בין הארגונים ועל בניית מודלי שותפות מתקדמים עם השחקנים הנוספים בהתארגנות הקהילתית.

קפיצת מדרגה בשילוביות, שיתופיות ושותפות על גווניהן - מול הקהילה, מול שותפים בעולם ומול האקו־סיסטם האזרחי היא המפתח להתמודדות עם האתגר העצום והאיומים בממד הסייבר. ככל שנשכיל לבנות, לפתח, להעצים ולטפח שותפויות כאלה - נוכל להיות צעד אחד לפני היריבים.

אני מאמין שכדי לעצב בהסתכלות חזונית את ההיערכות המדינתית להתמודדות עם איומי סייבר בחמש השנים הקרובות, נדרש, לצד חיזוק ההתארגנות והשותפויות בתוך הקהילה וקידום שותפויות עם ארגונים מקבילים בעולם, לבחון ולקדם שיתופי פעולה עם האקו־סיסטם האזרחי העוסק בתחום, תוך שבירת פרדיגמות והתמודדות עם המורכבויות בהיבטים הביטחוניים והמשפטיים.

קפיצת מדרגה בשילוביות, שיתופיות ושותפות על גווניהן – מול הקהילה, מול שותפים בעולם ומול האקו־סיסטם האזרחי היא המפתח להתמודדות עם האתגר העצום והאיומים בממד הסייבר. ככל שנשכיל לבנות, לפתח, להעצים ולטפח שותפויות כאלה – נוכל להיות צעד אחד לפני היריבים גם בסייבר.