# האסטרטגיה הישראלית להגנת הסייבר

**משרד ראש הממשלה** | מערך הסייבר הלאומי

# האסטרטגיה הישראלית להגנת הסייבר

# תוכן העניינים

# דברי פתיחה

## ראש מערך הסייבר הלאומי, ד"ר אביתר מתניה

מרחב הסייבר מגלם הזדמנות לצמיחה כלכלית ולרווחה חברתית ותופס מקום גדל והולך בחיינו כפרטים וכחברה. לצד זאת, איומי הסייבר מתגברים והולכים, יוצרים השפעות שליליות על פרטים, על חברות ועל ארגונים ומציבים סכנות חדשות ברמה הלאומית - לביטחון הלאומי, לסדר החברתי ולכלכלה.

בהתאם, החליטה ממשלת ישראל, בשורה של החלטות, על היערכות מדינתית כוללת להעלאת רמת הגנת הסייבר ולהגדרת אחריות להגנת הסייבר ברמה הלאומית, זאת לצד שמירתו של הסייבר כמרחב פתוח המאפשר זרימה חופשית של ידע, הון ושירותים, מחולל חדשנות ותורם לרווחה חברתית, ותוך הקפדה על זכויות יסוד, ובהן הזכות לפרטיות וחופש הביטוי.

מתוקף החלטת הממשלה מס' 3611 הוקם ב-1 בינואר 2012 **מטה הסייבר הלאומי** והוטל עליו לגבש אסטרטגיה לאומית כוללת להגנת הסייבר. האסטרטגיה אומצה ע"י הממשלה ב-15 בפברואר 2015, ותוך כך הוחלט להקים גוף הגנה אופרטיבי מרכזי להגנת הסייבר בישראל - **הרשות הלאומית להגנת הסייבר**, שתפעל לצד מטה הסייבר כחלק **ממערך הסייבר הלאומי**.

האסטרטגיה הישראלית להגנת הסייבר מהווה את התשתית הרעיונית והמעשית לבניית מענה יציב וארוך טווח לאיום הסייבר והיא בנויה משילוב של שלושה מרכיבים: תפיסת פעולה להגנת המשק בהתבסס על מודל של שלוש שכבות הגנה; שלושה מאמצי-על לקידום ההגנה באופן שלם - בניית הסייבר כמרחב בטוח, הקמת הרשות הלאומית להגנת הסייבר ומחקר ופיתוח של יכולות וטכנולוגיות הגנה מדינתיות; ולבסוף, מאמצים תומכים לפעילויות אלה, והם בניין הכוח המדעי-טכנולוגי של ישראל בתחום הסייבר ושיתוף פעולה בזירה הבין-לאומית.

המסמך שלהלן פורס ומפרט את הרציונל ואת מרכיבי האסטרטגיה, על-מנת לשמש כעזר בידי העוסקים במלאכה וככלי ליצירת "שפה משותפת" בתחום. המסמך נכתב במטה הסייבר הלאומי, על-ידי האסטרטג הראשי, טל גולדשטיין, בשיתוף ר' תחום בכיר לתכנון אופרטיבי, ליאור יפה, ובסיוע של בעלי תפקידים רבים במערך הסייבר.

# מבוא

## התפתחות ההיערכות הישראלית בתחום הגנת הסייבר

התארגנות ייעודית ראשונה להגנת הסייבר הלאומית התרחשה בשנת 2002, כאשר הטילה ממשלת ישראל על **הרשות הממלכתית לאבטחת מידע** (רא"מ) בשב"כ אחריות להנחיית גופים אזרחיים, המפעילים מערכות ממחושבות חיוניות ברמה הלאומית. בעקבות ההחלטה הוקמה **ועדת היגוי עליונה** בראשות ראש המטה לביטחון לאומי, שיעדיה היו סנכרון והסתכלות כוללת על מאמצי הגנת הסייבר המדינתיים. כינון הוועדה ופעולות ההגנה של רא"מ היו מאמץ ממשלתי פורץ דרך ברמה העולמית בתחום הגנת הסייבר, והייתה להם תרומה ניכרת לביסוס ההגנה על התשתיות החיוניות ולפיתוח הידע והיכולות בישראל.

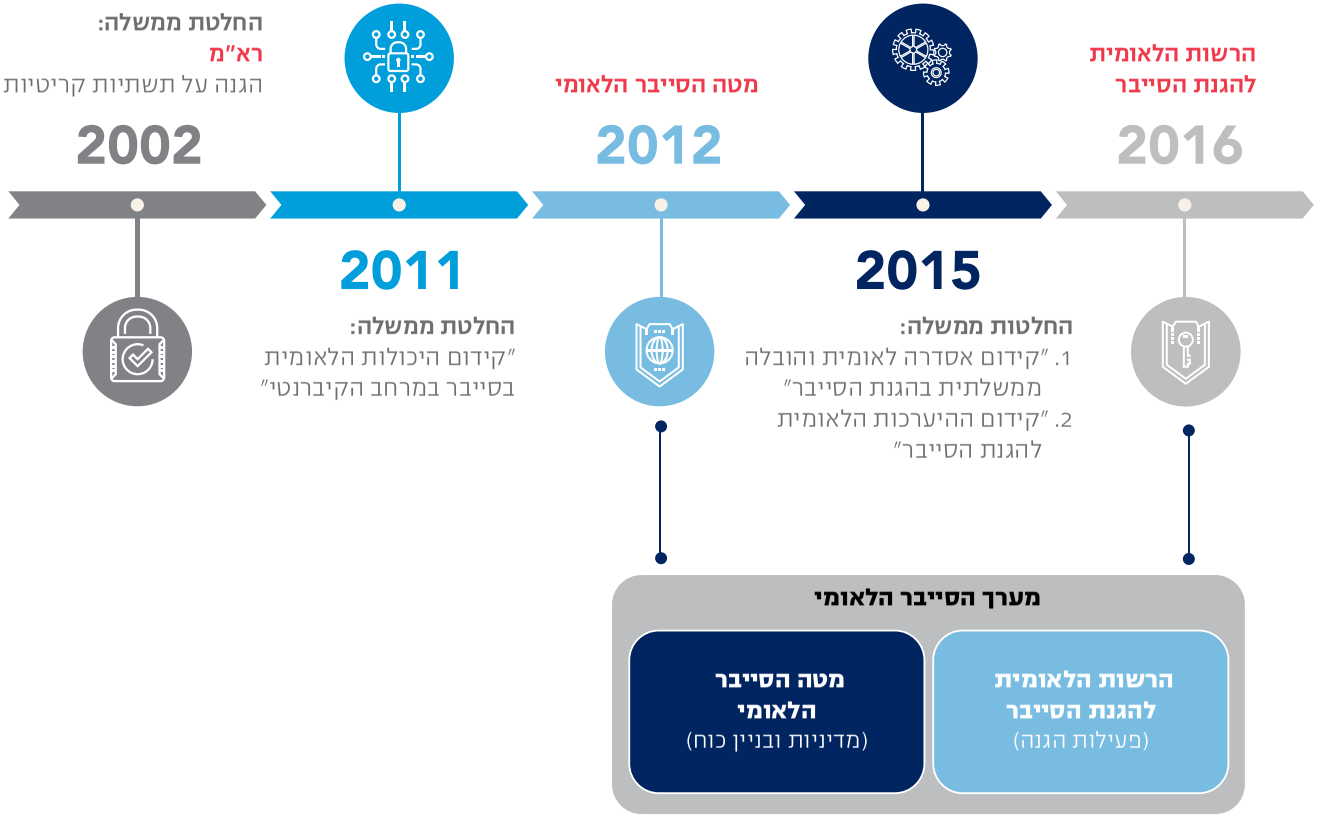
הצעד המשמעותי הבא שבו נקטה מדינת ישראל בתחום הגנת הסייבר היה בהחלטת הממשלה מס' 3611 מיום 7 באוגוסט 2011, לקידום היכולות הלאומיות בסייבר, שהתקבלה על בסיס המלצות של ועדת מומחים רחבת היקף בראשות ראש **המועצה הלאומית למחקר ופיתוח** (המולמו"פ) דאז. במרכז ההחלטה עמדה הקמתו של **מטה הסייבר הלאומי**, בכפיפות לראש ממשלת ישראל. על המטה הוטלה, בין היתר, האחריות לגיבוש המדיניות והאסטרטגיה הלאומית בתחום הסייבר, לקידום תהליכי הגנה לאומיים ולהסדרתם, לפיתוח היכולות הלאומיות בתחום הסייבר ולביסוס שיתופי פעולה בין-לאומיים ומעמדה של מדינת ישראל כמדינה מובילה בתחום. בנוסף, מונה ראש המטה כיושב ראש ועדת ההיגוי העליונה.

על בסיס האסטרטגיה שגיבש המטה עם כלל הגופים הרלוונטיים קיבלה ממשלת ישראל ב-15 בפברואר 2015 שתי החלטות. הראשונה, החלטה מס' 2443, עוסקת באסטרטגיית בניין העמידות והחוסן בסייבר של המשק האזרחי, ובפרט בהיערכות הממשלתית מול המשק ובתוך הממשלה. השנייה, החלטה מס' 2444, עוסקת באסטרטגיית ההגנה האופרטיבית על המשק האזרחי, בחיבור כלל גופי ההגנה הלאומיים לעשייה משותפת בהגנת סייבר, ובפרט בהקמה של **הרשות הלאומית להגנת הסייבר**. הרשות החלה לפעול להגנת המשק האזרחי ב-1 באפריל 2016.

בשנת 2017 אוגדו כל הפעילויות הטכנולוגיות של מטה הסייבר **ליחידה לטכנולוגיות סייבר**, המהווה את הזרוע הטכנולוגיות הלאומית לקידום יכולות וטכנולוגיות סייבר לרמה הלאומית. במקביל, נקלטה במטה הסייבר **היחידה להזדהות וליישומים ביומטריים**, כחלק מבניית השלם בתחום הסייבר.

הרשות, כגוף האופרטיבי להגנת הסייבר, ומטה הסייבר, כגוף המדיניות ובניין הכוח בסייבר, מהווים **ביחד את מערך הסייבר הלאומי**, הפעול במשרד ראש הממשלה, בכפיפות ישירה לראש הממשלה.

**איור 1** | התפתחות ההיערכות הישראלית בתחום הגנת הסייבר.



# האסטרטגיה הישראלית להגנת הסייבר בעשר נקודות

### חזון וייעוד

1. **חזון הסייבר של מדינת ישראל:** מדינת ישראל תהיה מדינה מובילה ברתימת מרחב הסייבר לטובת צמיחתה הכלכלית, רווחתה החברתית וביטחונה הלאומי.
2. **ייעוד האסטרטגיה:** להסדיר את כלל המאמצים הלאומיים בתחום הגנת הסייבר, ליצור "שפה משותפת" בין העוסקים במלאכה ולהבטיח מענה יציב וארוך טווח, באופן המבטא את מחויבותה של מדינת ישראל להמשיך ולפעול להגנת הסייבר ולשימורו של מרחב הסייבר כמרחב בטוח של שגשוג כלכלי וחברתי.

### שער 1 | תפיסת הפעולה

3. **עמידות משקית:** היכולת של ארגונים במשק ושל תהליכים בין-ארגוניים ומשקיים להתמיד בפעילות תחת שגרת איומי סייבר, באמצעות צמצום משטח התקיפה ופוטנציאל התממשותן של תקיפות. המדינה מקדמת יכולת זו באמצעות אסדרה ישירה ועקיפה של ארגונים במשק ותהליכי אסדרה בשוק הגנת הסייבר.
4. **חוסן מערכתי:** יכולת ההתמודדות של המדינה והארגונים בה עם תקיפות סייבר באופן שיטתי, לשם צמצום הנזק המצטבר במשק לקראת אירוע, במהלכו ולאחריו, בדגש על תקיפות מתפשטות ובעלות השלכות רוחב. זאת בהתבסס על תהליכים מדינתיים לשיתוף מידע, ליצירת מידע ערכי והפצתו ולסיוע לארגונים במשק אשר הותקפו.
5. **הגנה לאומית:** ניהול מערכה מדינתית נגד איומים חמורים, אשר עומדים מאחוריהם תוקפים נחושים ובעלי משאבים, המהווים סיכון ממשי לביטחון המדינה, תוך שילוב בין מאמצים מגננתיים להכלת תקיפות והשלכותיהן ובין מאמצים אקטיביים להתמודדות עם מקורות האיום.

### שער 2 | יישום האסטרטגיה – שלושה מאמצי-על להגנת הסייבר בישראל

6. **בניית הסייבר כמרחב צמיחה בטוח:** מאמץ כלל-ממשלתי, הכולל מאמצים לחיזוק ההגנה בארגונים במשק, באמצעות אסדרה ישירה ועקיפה של ארגונים, חיזוק ואסדרה של שוק הגנת הסייבר בישראל וקביעת אמת מידה גבוהה בהגנה על גופי הממשלה, וכן מאמצים ליישום פתרונות, תהליכים ותשתיות טכנולוגיים ברמה הלאומית.

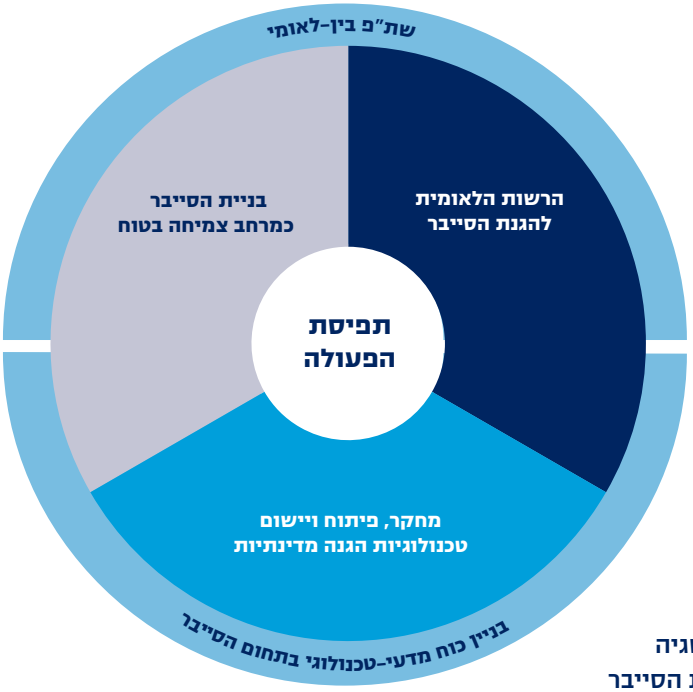
7. **הקמת הרשות הלאומית להגנת הסייבר וקידום היערכות לאומית משלימה:** הקמת גוף מרכזי להגנת סייבר, שזהו ייעודו היחיד, והוא משמש כמוקד הידע הלאומי בתחום הגנת הסייבר ומוביל את מאמצי ההגנה על המשק הישראלי מפני תקיפות סייבר. זאת לצד העצמת ההיערכות במערכת הביטחון, בגורמי אכיפת החוק וברשויות האסדרה.

8. **מחקר, פיתוח ויישום של יכולות וטכנולוגיות הגנה מדינתיות:** פיתוח טכנולוגיות לצורכי הגנת הסייבר ברמה הלאומית ויישומן.

### שער 3 | מאמצים תומכים לביסוס היכולת הלאומית בסייבר

9. **בניין הכוח המדעי–טכנולוגי הלאומי בסייבר:** המשך חיזוק התשתיות המדעיות-טכנולוגיות של מדינת ישראל בסייבר (התעשייה, האקדמיה וההון האנושי) כיתרון היחסי של מדינת ישראל בתחום וכחלק מהמאמץ העולמי להתמודדות עם האתגר.

10. **שותפות במאמצים בין–לאומיים לעיצוב מרחב הסייבר:** פיתוח שותפויות בין-לאומיות בילטרליות ומולטילטרליות לחיזוק יכולות ההגנה של מדינת ישראל ושל עמיתותיה, השפעה על השיח הבין-לאומי לעיצוב המרחב ורתימת היכולות הלאומיות לבניית מרחב הסייבר הגלובלי כמרחב בטוח של שגשוג כלכלי וחברתי כלל-עולמי.




**איור 2 | האסטרטגיה הישראלית להגנת הסייבר**

# שער 1
# תפיסת הפעולה

# רקע

**"הגנת הסייבר (Cyber Security) היא מכלול הפעולות למניעה, לנטרול, לחקירה ולהתמודדות עם איומים, תקיפות וחדירות למרחב הסייבר הארגוני והמדינתי ולצמצום השפעתם והנזק הנגרם מהם, וזאת בטרם התרחשותם, במהלכם ולאחריהם."**
(מתוך החלטת ממשלת ישראל מס' 2444 מיום 15 בפברואר 2015)

### מרחב איומי סייבר

מרחב הסייבר חשוף למשרעת איומים ייחודית בהיקפה. איומים אלה מתעצמים והולכים עם צמיחתו של הסייבר והעלייה בתלות בו והעמקת החיבור למרחב הפיזי. איומים אלה עלולים להוביל הן לפגיעה בתוך המרחב (למשל, במידע או בתפקוד) והן לפגיעה היוצאת ממנו אל העולם הפיזי (למשל, פגיעה פיזית או תודעתית).

סיכונים לביטחון הלאומי ולסדר החברתי, חשש מכשל מערכתי של שירותים חיוניים, סכנת חיים לאזרחים ותרחישי השפעה מאקרו-כלכליים, הובילו מדינות להפנים את נחיצותם של מאמצי הגנה מדינתיים, שאינם עוד נחלת המגזר הפרטי בלבד.

מאחורי איומי הסייבר עומדים מגוון גורמים עוינים: מדינות וגורמים הנתמכים על-ידי מדינות, ארגונים לא-מדינתיים זדוניים, ובהם ארגוני טרור, קבוצות פשיעה, אקטיביסטים ויחידים. האידיאולוגיות שמאחורי התקפות הסייבר נעות החל מפגיעה בביטחון לאומי, ריגול וטרור, עבור בפשיעה, בגנבת קניין רוחני ובתחרות עסקית ועד מחאה אזרחית ומטרות פרטיות אחרות.

הסיכון ברמה הלאומית אינו נובע רק מאיומים שהם ביטחוניים מטבעם, אלא מקשת האיומים בכללותה, שכן השפעות מערכתיות עשויות להיווצר גם כתוצאה מהצטברות של נזקים. סיכון זה, בשילוב עם הקושי האינהרנטי בסייבר להבחין בין גורמי התקיפה השונים והמוטיבציות שלהם, מובילים לכך, שתפיסת הפעולה נדרשת לספק מענה והתייחסות מתאימים לטווח האיומים המלא - כלומר לרמות איום שונות ברמה הלאומית ולהקשרי פעולה שונים של התוקף.

### המאפיינים הבסיסיים של הגנת הסייבר

בהתמודדות עם איומים במרחב הפיסי, שואפת המדינה לרוב לפעול בתווך שבין הגורם התוקף למושא התקיפה, כלומר למנוע מהגורמים העוינים להתקרב לגורמים המאוימים. לעומת זאת, במרחב הסייבר כמעט ולא קיימת אפשרות מעשית לעבוד בתווך, והאיומים, כלומר התקיפות, באים לידי ביטוי בתוך המרחב הארגוני והפרטי.

בשל כך, תפיסת פעולה להגנת סייבר נדרשת להתמודד עם שני מאפיינים ייחודיים של איום הסייבר. המאפיין הראשון הוא שמפעילי מערכות הסייבר, ולצורך הפשטות ה"ארגונים", הם הגורם המרכזי הנמצא בחזית המאמצים להגנת הסייבר: הם מושא התקיפה, הם התווך בו היא עוברת בדרך לאחרים והם ה"לוחמים בחזית". מאמצי הגנת הסייבר מחייבים ומתבססים על תהליכים וצעדים טכניים, המתקיימים בתוך מרחב הסייבר הארגוני, וניהול הסיכונים נוגע לרוב ישירות בתהליכים ה"עסקיים", שרק הארגון מסוגל לבצע. בהתאם, הארגונים הם חלק חיוני בכל מאמץ הגנה לאומי.

המאפיין השני הוא הבידול בין ה"תוקף הסייבר" לבין "תקיפת סייבר" - בשונה ממרבית המקרים של איומים פיסיים בהם התוקף והתקיפה משולבים. תקיפת סייבר היא מכלול הפעולות הזדוניות המתקיימות בתוך מרחב הסייבר עצמו, תוך התבססות על תשתיות, נכסים, אמצעים ושיטות המאפיינות אותה. התקיפה מתפרסת על-פני מערכות סייבר רבות, מתמשכת לאורך זמן וכמעט תמיד מתרחשת הרחק מהתוקף עצמו. תקיפת הסייבר היא המהלך שמביא להתממשות בפועל של הנזקים והסיכונים הנובעים מאיום הסייבר, ולכן גם מהווה את המושא המרכזי למאמצי ההגנה - בדומה לאופן בו מתייחסים לאירועים כגון שריפה או למגיפה, המחייבים התמודדות עם האירוע עצמו גם ללא תלות ישירה בגורם שעומד מאחוריהם. לעומת זאת, ההתמודדות עם תוקף הסייבר מהווה אתגר ומצריכה משאבים רבים, בעיקר בשל הקושי האינהרנטי בזיהוי התוקף.

### מרכיבי תפיסת הפעולה

לנוכח המאפיינים של הגנת הסייבר, תפיסת הפעולה שמה דגש לחיזוק מאמצי ההגנה של הארגונים ולבניית שיתוף פעולה של המדינה איתם, ממוקדת בהתמודדות שוטפת עם תקיפות סייבר, ומתייחס לתוקפים עצמם במקרים בהם מדובר בתוקפים מתקדמים ונחושים, שאינם ניתנים להתמודדות בדרכים אחרות והמהווים איום חמור במיוחד.

תפיסת הפעולה מכוונת לספק מענה לכלל האיומים ורמות הסיכון הלאומי, בהתייחס למאפייני הפעולה השונים של המדינה. תפיסת הפעולה נועדה לספק את המסגרת הרעיונית לכלל המאמצים והתפקידים של המדינה במסגרת הגנת הסייבר הלאומית והיא מורכבת משלוש שכבות הנבדלות ביחסים בין המדינה ובין הארגונים במשק, למושא הפעולה המדינתי ולרמת האיום הנשקף ברמה הלאומית:

- **שכבה ראשונה – עמידות משקית:** הגברת היכולת של ארגונים במשק ושל תהליכים בין-ארגוניים ומשקיים להתמיד בפעילות תחת שגרת איומי סייבר, באמצעות צמצום משטח התקיפה ופוטנציאל התממשותן של תקיפות. שכבה זו ממוקדת בעיקרה בארגונים ובקידום מאמציהם, היא אינה מוכוונת אירועים ("off-line") והיא שואפת להביא ליצירת מענה מותאם לכל רמות האיום - החל ממענה לתשתיות קריטיות ועד קידום המודעות בציבור הרחב.

- **שכבה שנייה – חוסן מערכתי:** ביסוס היכולת השיטתית של המדינה והארגונים בה להתמודדות עם תקיפות סייבר ולצמצום הנזק המצטבר במשק לקראת אירוע, במהלכו ולאחריו, בדגש על תקיפות מתפשטות ובעלות השלכות רוחב. שכבה זו מכוונת להתמודדות מדינתית עם תקיפות, כתלות באירועים ("on-line"), מושתתת על מאמצים מדינתיים המתקיימים בשיתוף עם הארגונים במשק ומיועדת גם היא להתמודד עם קשת האיומים בכללותה.
- **שכבה שלישית – הגנה לאומית:** ניהול מערכה מדינתית כנגד איומים חמורים, אשר עומדים מאחוריהם תוקפים נחושים ובעלי משאבים, המהווים סיכון משמעותי לביטחון המדינה, כולל התמודדות עם מקורות האיום. שכבה זו מוגדרת על-פי רמת הסיכון והיא נועדה לאפשר את מיקוד המאמצים במקרים של איומים חמורים. היא כוללת התמודדות הן עם התוקף והן את עם התקיפה ונזקיה, במטרה להבטיח מענה שלם. בשכבה זו המדינה היא הגורם הפועל.


**איור 3** | שלוש שכבות להגנת הסייבר:

עמידות משקית – מכלול המאמצים לקידום רמת ההגנה של הארגונים והתהליכים במשק; חוסן מערכתי – המאמץ המדינתי להכיל, להתמודד ולמנוע התפשטות של תקיפות במשק; והגנה לאומית – מאמץ מדינתי מסונכרן להתמודדות עם האיומים החמורים ביותר

# שכבה ראשונה
# **עמידות משקית**

### עמידות

**עמידות סייבר היא היכולת של ארגונים ותהליכים להתמיד בפעילות תחת שגרת איומי סייבר באמצעות מניעה והדיפה של מרבית התקיפות.**

עמידות סייבר מכוונת לצמצום משטח התקיפה, כלומר יצירת סביבה המקשה על פעילות התקפית ומקטינה את פוטנציאל התממשותן של תקיפות, ולא כמהלך תגובתי לתקיפה ספציפית. ברמה הארגונית, עמידות מושגת בהתבסס על תהליכים ארגוניים, כגון ניהול סיכונים, תכנון נכון של ארכיטקטורת המערכות וניהולי השימוש בהן, תהליכים שוטפים לזיהוי כשלים וחולשות, המהווים הזדמנות לתוקפים, והסרתם, הדרכות והתמודדות עם סיכונים הנובעים מהגורם האנושי, וכמובן יישום פתרונות טכנולוגיים. מאמצי העמידות נדרשים להתעדכן באופן תדיר במבנה, באמצעים, בשיטות ובמאפיינים.

העמידות היא המרכיב הבסיסי וההכרחי בהגנת הסייבר, המקדים את מאמצי התמודדות עם האיומים עצמם. רמת עמידות גבוהה מאפשרת למנוע את נזקיהן של מרבית התקיפות הפשוטות והנפוצות ואף מקשה על תוקפים מתקדמים ונחושים יותר, ובכך מצמצמת את המוטיבציה שלהם לפעול.

### עמידות משקית

**עמידות סייבר משקית היא העמידות המצרפית של כלל הארגונים במשק, של ממשקים בין-ארגוניים ושל תהליכים משקיים.**

עמידות משקית נועדה ליצור סביבת סייבר בטוחה ולהפחית את היקף האירועים במשק ואת חומרתם. רמת עמידות משקית גבוהה מקשה על היכולת לממש פעילויות סייבר זדוניות, בין היתר בזכות הפחתת הסיכונים, הנובעים מניצול חוליות חלשות בתהליכים חוצי-ארגונים ומניצול ארגונים בעלי עמידות נמוכה בשרשרת האספקה. זאת, בדומה ל"חיסון עדרי", המאפשר מניעה של הפצת מחלות כתוצאה מחיסון של חלק מהאוכלוסייה. צמצום היקפם של האירועים מאפשר גם את מיקוד המאמצים המדינתיים בהתמודדות עם התקיפות שצלחה הוצאתן לפועל.

בניית עמידות משקית דומה למאמצים ליצירת סביבה עירונית בטוחה על-ידי הצבת תאורת רחוב, פעילויות חינוכית למניעת אלימות בקרב בני נוער, נוכחות משטרתית מרתיעה ברחובות, הסרת אמצעי לחימה מהמרחב הציבורי ועוד.

# שכבה שנייה
# **חוסן מערכתי**

### חוסן סייבר

חוסן סייבר הוא יכולת של המדינה והארגונים בה להתמודד עם אירועי סייבר לפני התרחשותם, במהלכם ולאחריהם במטרה לחזור במהרה לשגרה תוך צמצום הנזקים הנלווים.

מאמצי העמידות שתוארו בשכבה הראשונה אינם קשורים לאירועים ספציפיים ונועדו לצמצם מראש את ההשפעות השליליות של פעילויות זדוניות. לעומתם, מאמצי החוסן הם מכווני אירועים ותקיפות (Event-driven) ונועדו להתמודד עם מקרים שבהם התקיפה לא נמנעה, או שהשפעותיה אינן מוכלות במסגרת תהליכים שגרתיים.

מאמצי החוסן הם נדבך משלים למאמץ העמידות ומתבססים עליו. המאמצים כוללים, בין היתר, פעילויות גילוי וחקירה של תקיפות, מעקב וניסיונות מניעת התבססות והתפשטות מהלך התקיפה ביעד, ניהול נזקים והשלכות של תקיפות ומניעת הישנות אירועים דומים. מאמצים אלה מחייבים חיבור למקורות מידע חיצוניים (מודיעין), נהלים סדורים להתמודדות עם אירועים, עומק טכנולוגי ויכולת תגובה מהירה לאיומים מתפתחים. בשנים האחרונות התפתח מאוד השוק התומך בבניית החוסן הארגוני, כגון: שירותי חקירת אירועי סייבר וסיוע בהכלתם, מערכות שליטה ובקרה לניהול אירועים ואמצעים להונאת תוקפים.

### חוסן סייבר מערכתי

**חוסן סייבר מערכתי הוא יכולת להתמודד עם תקיפות סייבר במשק באופן שיטתי ולצמצם את הנזק המצטבר, בדגש על תקיפות מתפשטות ובעלות השלכות רוחב.**

בשוק הפרטי נעשות פעילויות הגנה גלובליות ומקומיות, המביאות ליצירתו בפועל של חוסן מערכתי. כך, למשל, חברות הגנת סייבר מזהות באופן שוטף מערכי תקיפה חדשים, עורכות חקירות תקיפות וניתוחן ומעדכנות בהתאם את מוצריהן בקבועי זמן קצרים.

לצד זאת, ישנה חשיבות גבוהה לבניית חוסן סייבר מערכתי ברמה המגזרית והלאומית, שכן תקיפות סייבר הפוגעות בכמה גופים שהם חלק מתהליך משקי עלולות לגרום נזקים חמורים בהרבה מאשר הפגיעה בכל אחד מהגופים בנפרד. הפעילות שנעשית בשוק הפרטי ברמה הגלובלית אינה ממוקדת בתהליכים ובהקשרים ספציפיים, ולכן במקרים רבים אינה מספקת חוסן מערכתי ברמה המגזרית והלאומית.

נוסף על כך, אפשר לזהות כמה חסמים וכשלי שוק, המקשים על השגת חוסן מערכתי - בראש ובראשונה פערים בין הרצוי למצוי בתחום שיתוף מידע בין ארגונים. שנית, קיימים בשוק פערים גדולים בכוח אדם מקצועי בתחומי המחקר והאנליזה, הנחוצים למאמצי החוסן. לבסוף, חלק מהיכולות ומהמאמצים הנדרשים לבניית חוסן מערכתי מצויים בידי המדינה - כגון הקמת מערכות שיתוף מידע, תקינת אופן העברת המידע, שיתוף מודיעין, ובידי שחקנים נוספים - כגון ספקי האינטרנט, חברות גלובליות ומדינות זרות.

**אפשר לדמות את החוסן המערכתי ברמה הלאומית למערכת בריאות לאומית, המספקת תשתית להתמודדות עם מקרים חמורים, שנדרשת בהם תשתית רפואית מיוחדת, כגון חדר ניתוחים, וכן התמודדות עם סיכון של הצטברות אירועים, למשל באמצעות מנגנונים לבקרת מחלות.**

### בניית חוסן מערכתי לאומי

למדינה יש יכולת לבסס חוסן מערכתי ברמה הלאומית, בהתבסס על איגום משאבים והיותה גורם ניטרלי ואמין. המדינה מקדמת שלושה תהליכים מרכזיים: תהליכי שיתוף מידע, מאמצים ליצירת מידע ערכי והפצתו ופעולות מדינתיות להכלת תקיפות ומתן סיוע לארגונים שהותקפו.

בליבת מאמצי החוסן הלאומיים נמצאים תהליכי שיתוף מידע בין המדינה לארגונים במשק ובין הארגונים לבין עצמם, באופן המאפשר בלימת תקיפה על-ידי העברה מהירה של תובנות וידע רלוונטי בין ארגונים שהותקפו והצליחו להתמודד לבין ארגונים שטרם הותקפו או טרם עלה בידם להכיל את התקיפה. בשל החסמים הקיימים בשוק, למדינה יש תפקיד מרכזי בעידוד התהליכים של שיתוף המידע, בין היתר בהתבסס על פיתוחם ויישומם של **תהליכים ומערכות טכנולוגיות לשיתוף מידע בטוח, אמין ודיסקרטי,** וכן בהשקעת משאבים בעיבוד המידע ובהנגשתו לגורמים הזקוקים לו.

תהליכי שיתוף נדרשים להיבנות הן ברמה המגזרית והן ברמה הלאומית. **תהליכי שיתוף מידע ותמיכה מגזריים ונושאיים** מאפשרים בניית אמון ואינטימיות, בהתבסס על היכרות עמוקה עם הארגונים ועם צורכיהם. גישה זו אף מאפשרת התייחסות מעמיקה יותר לתהליכים, לטכנולוגיות ולסיכונים המאפיינים את המגזר הרלוונטי, תוך בחינת הזיקות בין סיכוני סייבר לבין סיכונים אחרים.

**שיתוף מידע ברמה הלאומית** מאפשר שיתוף מידע בין-מגזרי, מתן מענה לארגונים שאינם משויכים באופן מובהק למגזר רלוונטי ועשויים להיות חשובים לבניית החוסן המערכתי הלאומי, וכן **גיבוש תמונת מצב** כוללת של תקיפות סייבר במשק. תמונת מצב עדכנית מהווה בפני עצמה הישג חשוב והיא נחוצה לתמיכה בתהליכי קבלת החלטות וכן לטובת זיהוי תקיפות בעלות השפעות רוחביות, הבנת תהליכים ומגמות בעלות פוטנציאל סיכון למשק ואיתור תבניות תקיפה ייחודיות כנגד המדינה. למוקד מרכזי יש חשיבות גם כמוקד של ידע ושל אנשים ותשתיות, הנדרשים למאמצי החוסן ולרוב מצויים בחסר.

תפקיד חיוני נוסף של המדינה הוא **יצירת מידע וידע על-אודות איומים ותקיפות במשק וסיוע בהכלתן.** תפקיד זה לא נועד להחליף את תפקידו של השוק הפרטי, אלא להשלים אותו במקומות שיש בהם פערים, בדגש על פערים העשויים להביא לידי סיכונים למשק. המדינה עוסקת באיסוף מידע, בגילוי, בזיהוי ובחקירה של תקיפות במטרה ליצור מידע וידע ערכיים, שיסייעו למענה עבור הארגונים במשק. מאמץ זה מבטא

למעשה איגום משאבים מדינתי, שנועד להתמודד עם פערים בשוק (כגון כוח אדם מיומן ותשתיות טכנולוגיות רלוונטיות) ולמנף נכסים מדינתיים ייחודיים. הידע המדינתי מתבסס על שלושה מקורות מרכזיים: הארגונים עצמם, המסתייעים במדינה ומשתפים עמה מידע; שיתופי פעולה אסטרטגיים עם שחקני מפתח בתחום התקשורת והאבטחה, גופים מקבילים מהעולם ועוד; יכולות ומאמצים טכנולוגיים ייעודיים לאיתור ולזיהוי ניסיונות חדירה ולניתוח כלי תקיפה.

לבסוף, תפקיד נוסף של המדינה הוא **להשתתף ולסייע בהכלה של תקיפות במשק** כתלות במידת הסיכון והאינטרס הציבורי. בידי המדינה מגוון כלים שבאפשרותה להפעיל: סיוע של צוותים טכניים בחקירה, הנחיה מקצועית ישירה לארגונים שהותקפו, גיבוש ופרסום שיטות פעולה סדורות לארגונים להתמודדות עם תקיפה ספציפית ותיאום עבודה משותפת עם שותפים מרכזיים, כגון ספקיות אינטרנט, חברות אבטחת סייבר ומערכת הביטחון.

מאמץ משלים ומרכזי להכלת התקיפות הינו כמובן תהליכי **אכיפת החוק**, המאפשרים בלימה של תקיפות ומניעתן העתידית באמצעות יצירת הרתעה והרחקה מתמשכת של תוקפים. מאמצי אכיפת החוק כנגד תוקפים מתוך המדינה מהווים גם נדבך חיוני לבניית תהליכי חוסן בין-לאומיים.


**איור 4** | מאמצי הליבה הממשלתיים לבניית החוסן המערכתי במשק:

יצירה ועידוד תהליכי שיתוף מידע בין הארגונים במשק ובין הארגונים לממשלה, יצירת מידע ערכי ושיתופו עם הגורמים הרלוונטיים, בהתבסס על מקורות המידע השונים ויכולות העיבוד העומדים בפני הממשלה, וכן מאמצי הכלה של תקיפות במשק וסיוע לארגונים שהותקפו

# שכבה שלישית
# **הגנה לאומית**

**הגנה לאומית**

**ההגנה הלאומית היא אוסף המאמצים המדינתיים שנועדו להתמודד באופן ממוקד ומתמשך עם איומי סייבר, המהווים סכנה ממשית לאינטרסים ולביטחון הלאומי.**

שתי שכבות ההגנה הראשונות מאפשרות מניעה והכלה של מרבית איומי הסייבר, תוך שהן מתמקדות בעיסוק בתקיפות ולא בתוקף. עם זאת, הנחת המוצא המקובלת בהגנה, שקו ההגנה ייפרץ - נכונה ביתר שאת גם במרחב סייבר. תוקף מתקדם ונחוש דיו יצליח בסופו של דבר להשיג את יעדו.

ההתמודדות עם איומים שמסכנים אינטרסים לאומיים ומאחוריהם עומדים תוקפים מתקדמים ונחושים מצריכה מענה מדינתי ממוקד ועוצמתי, הבא לידי ביטוי בניהול מערכה, הרותמת ומאחדת את מגוון הכלים והיכולות המדינתיות תחת היגיון משותף ומתמשך. המערכה נועדה להתמודדות ממוקדת עם האיום, תוך התייחסות לכלל היבטיו - זיהוי והכלת התקיפות, התמודדות עם נזקיהן וכן התמודדות עם התוקף עצמו. זהו מאמץ מדינתי מיסודו, המבוסס על כלים ועל סמכויות הנתונים למדינה באופן בלעדי.

**שכבת ההגנה הלאומית מקבילה למאמצים במרחב הפיזי לשמירה על הביטחון הלאומי, הכוללים שימוש בכלל האמצעים העומדים לרשות המדינה, כולל, במקרה הצורך, הפעלת כוח מחוץ לגבולות המדינה.**

ההגנה הלאומית מחולקת לרוב לשתי תת-מערכות: **מערכה מגננתית**, המתייחסת להתמודדות עם התקיפות ונזקיהן, המתקיימת באופן טבעי בתוך שטחי המדינה ובהתייחס לגורם המותקף, **ומערכה המתנהלת כנגד מקורות האיום,** כלומר התוקפים עצמם, ומתאפיינת בהפעלת כלים וסמכויות אכיפת חוק וביטחון לאומי.

אתגר מרכזי בביסוס הגנה לאומית אפקטיבית ועוצמתית הוא שילוב בין שתי המערכות, המצריך תיאום, מימוש מהלכים משותפים וניהול תהליכי קבלת החלטות משותפים בנוגע לאופן ההתמודדות עם האיום.

### מערכה מגננתית

ההתמודדות עם תקיפות מתקדמות, בעלות משמעות ברמה הלאומית, מחייבת ניהול מערכה הגנתית, בין היתר באמצעות ניהול מבצעי הגנה ייעודיים לאורך זמן ובמגוון האמצעים שנועדו לחשוף ולהכיל את האיום. מבצעי ההגנה עשויים להיות סמויים או גלויים, ממוקדים או רחבים, פנים-מדינתיים או בשיתוף פעולה בין-לאומי. לטובת כך נדרשת בנייה על בסיס קבוע של תמונת אירועים שלמה במדינה.

באירועים חמורים, כשלתקיפה יש השלכות משמעותיות על המשק, או יש חשש לכאלה, כגון בעתות מלחמה, יש לניהול המערכה ההגנתית חשיבות גם בתכלול משמעות הרוחב של האירוע. בין היתר נדרשים: גיבוש תמונת מצב מקיפה של מצב התקיפות והפגיעות במשק, ניהול היבטים ציבוריים ותקשורתיים הממשקים מול גורמים העוסקים במצבי חירום ביחס להשלכות התקיפה מחוץ למרחב הסייבר.

### מערכה כנגד תוקפים

ההתמודדות עם תוקפים נחושים, המהווים איום ברמה הלאומית מצריכה מאמצים גם מול מקורות התקיפה - התוקף עצמו - וזאת על אף האתגרים הכרוכים בכך. ההתמודדות הישירה מול התוקף נדרשת הן כדי להבטיח יתרון יחסי למאמצי ההגנה, שלעתים הוא תנאי להצלחה, הן כדי למנוע את התקיפה או את הישנותה.


**איור 5** | מערכות ההגנה הלאומית:

מערכה מגננתית, המתכללת את כלל המאמצים להבנת האיום ולהכלת נזקיו בתוך המרחב הישראלי, ומערכה מתמשכת כנגד הגורמים המאיימים עצמם

# סיכום מודל "שלוש השכבות"

תפיסת הפעולה היא בסיס רעיוני לאופן שבו מדינה צריכה להירתם ולהיערך להתמודדות עם איומי הסייבר. התפיסה מציעה חלוקה של מכלול המאמצים המדינתיים לשלוש שכבות פעולה מדינתית, הבונות שלם הגנתי: בניית עמידות משקית, יצירת חוסן מערכתי וניהול מערכה להגנה לאומית.

### הקשרים בין השכבות

שלוש השכבות נבדלות זו מזה במטרות ובהקשרי הפעולה המדינתית ובנקודת העבודה מול הארגונים:

| | עמידות משקית | חוסן מערכתי | הגנה לאומית |
|---|---|---|---|
| **מטרת הפעולה** | צמצום יכולת ההתממשות של תקיפות במשק והשפעתן | צמצום סיכון לנזקים מצטברים ורוחביים ומניעת התפשטות תקיפות | התמודדות עם איומים חמורים |
| **חלוקת העבודה** | הארגונים, בהכוונת המדינה | המדינה והארגונים | פעילות בלעדית של המדינה |
| **אופי הפעילות המדינתית** | הכוונה ותמיכה בארגונים ואסדרה בשוק | תמיכה בפעילות הארגונים על-ידי שיתוף ויצירת מידע וניהול אירועים | ישירה מול האיום |
| **מושא הפעילות המדינתית** | ארגונים ופרטים | תקיפות וארגונים | מערכי תקיפה ותוקפים |
| **הקשר הפעילות המדינתית** | ללא תלות באירועים, לכלל האיומים אך בהתאם לרמת הסיכון הלאומי | בהקשר לאירועים במשק - לפני התרחשותם, במהלכם ולאחריהם | מענה לאיום בעל משמעות לאומית |

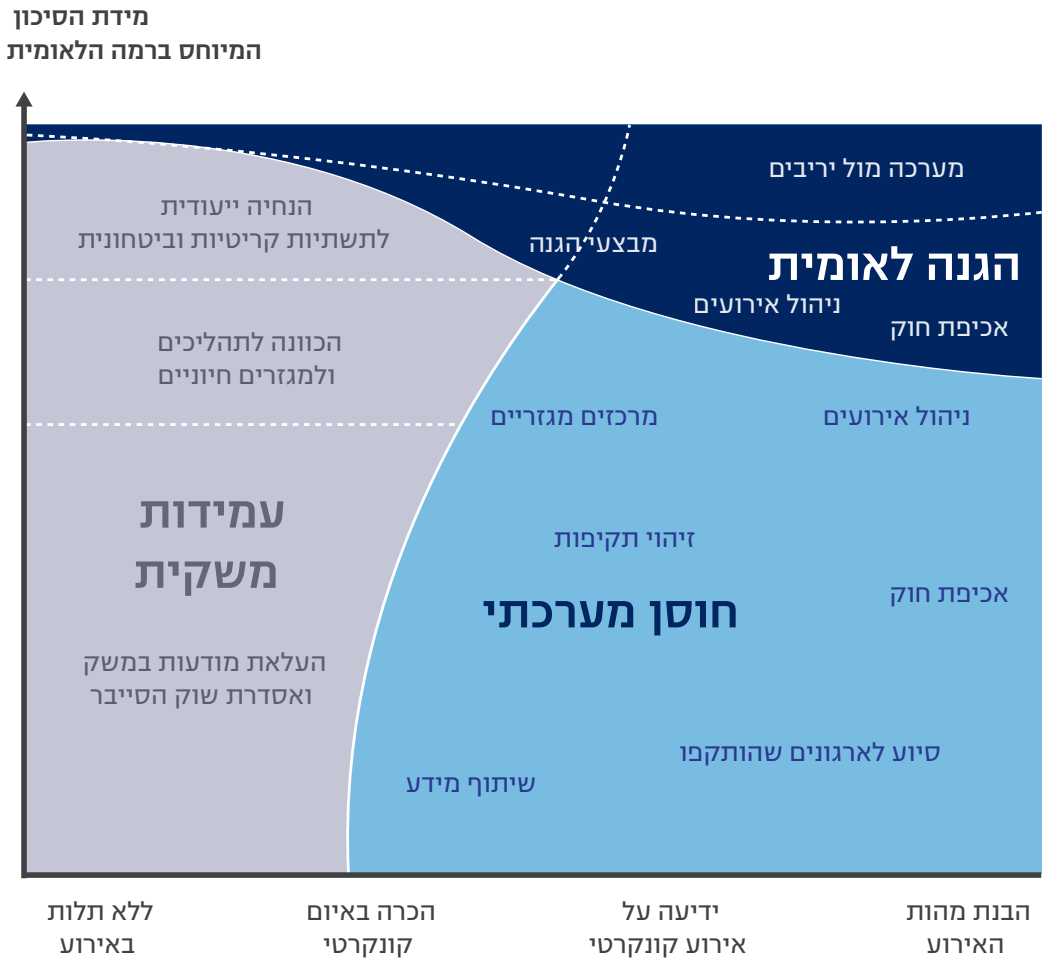
שלוש השכבות תלויות זו בזו ומקיימות סינרגיה חיונית: ראשית, הבטחת עמידות גבוהה מאפשרת לצמצם את היקף התקיפות ולמקד את מאמצי ההתמודדות המדינתיים עם התקיפות עצמן במסגרת מאמצי החוסן וההגנה הלאומית. שנית, בין השכבות מתקיימים קשרים אופרטיביים שוטפים, הממנפים את המאמץ בשכבה אחת לצורך קידום המאמצים בשכבה האחרת.

כך, למשל, העבודה השוטפת עם ארגונים במסגרת מאמצי העמידות, משמשת בסיס לקשרים הנדרשים לטובת פעילות משותפת להתמודדות עם תקיפות בתוך הארגונים בשכבת החוסן. בכיוון ההפוך - טיפול בתקיפות במסגרת שכבת החוסן וההגנה מושלם על-ידי פעולות נרחבות למניעת הישנות התקיפה במסגרת שכבת העמידות. דוגמה נוספת היא גיבושה השוטף של תמונת מצב התקיפות במשק במסגרת מאמצי החוסן. תמונת המצב היא הבסיס לריכוז המאמץ בשכבת ההגנה הלאומית. לבסוף, ההגנה על תשתיות קריטיות מהווה יעד אסטרטגי ומצריכה שילוב הדוק בין מאמצי עמידות וחוסן שוטפים ומאמצי הגנה לאומיים מפני איומים קונקרטיים על תשתיות אלו.

### שלמות המענה המדינתי

תפיסת הפעולה שואפת ליצור מענה מדינתי שלם, תוך שהיא מתמודדת עם אחד האתגרים המרכזיים בהגנת הסייבר. לרוב, המדינה פועלת להגנת אזרחיה בהתאם למאפייני האיום ולרמת הסיכון, למשל: הנזק הפוטנציאלי והשלכותיו ברמה הלאומית, הזהות והמוטיבציה של הגורם המאיים, יכולת הארגון להתמודד בעצמו ועוד. הגנת הסייבר מתאפיינת באופן מיוחד, ברמות אי- ודאות גבוהות ובפרקי זמן גדולים, הדרושים כדי לבסס הבנה בנוגע לאיומים. תפיסת הפעולה מספקת התייחסות כוללת ורציפה למרחב האיומים בכללותו, בדגש על השונות ברמות הסיכון, על מאפייני האיומים ועל האופן שבו אנו מבינים אותם.

הסכימה שלהלן מציגה את אופן הפעולה המדינתי בשלוש השכבות, בהתייחס לרמת הוודאות וההבנה של האיום (הציר האופקי) ולמידת הסיכון (הציר האנכי). הסכימה ממחישה את שלמות המענה ואת אופן הטיפול בכלל המצבים האפשריים, באמצעות בניית גישות פעולה, התואמות את רמות הסיכון ואת הקשרי הפעולה למיניהם. אחד היתרונות הבולטים בגישה זו הוא היכולת להתמודד עם אירועים, ללא תלות בהוכחת הסיכון ברמה הלאומית. כך, למשל, מענה לאירוע עשוי להתחיל ברמת החוסן ולעבור לרמת ההגנה הלאומית כאשר מתגבשת ההבנה לגבי מידת הסיכון. רמת החוסן מאפשרת גם מענה לאירועים שאינם משקפים סיכון מיידי ברמה הלאומית, אך עלולים להביא לנזקים מצטברים בעלי השלכות ברמה הלאומית.




**איור 6** | שלוש שכבות ההגנה לפי ההקשר לפעולה ההגנתית ומידת הסיכון המיוחס לאיום ברמה הלאומית:

בסכמה ניתן לראות את מאמצי העמידות המופעלים ללא קשר לאירוע ספציפי, אך ככל שרמת הסיכון גבוהה יותר מושקעים מאמצים לטובת מענה ממוקד אל מול איומים קונקרטיים ומתפתחים. שכבת החוסן מספקת מענה רחב אל מול מגוון האיומים ואירועי התקיפה, מתוך התייחסות גם לסיכונים מצטברים ולא רק לסיכון נקודתי גבוה. לבסוף, מאמצי ההגנה הלאומיים – הפנימיים והחיצוניים – הממוקדים באיומים ובסיכונים החמורים ביותר, מתרחבים ככל שמתגבשת ההבנה על אופי האיום

# שער 2
# יישום תפיסת ההגנה:
# שלושה מאמצי-על להגנת הסייבר בישראל

# רקע

מדינת ישראל פועלת ליישום תפיסת הפעולה שהוצגה לעיל באמצעות שלושה מאמצים מרכזיים, אשר נועדו להבטיח את ביסוסה של הגנת סייבר לאומית איתנה וארוכת טווח. שלושת המאמצים עוגנו בשנים האחרונות בשלוש החלטות ממשלה:

1. מאמץ כלל ממשלתי לקידום בניית מרחב הסייבר הישראלי כמרחב בטוח (בהתאם להחלטת ממשלת ישראל מס׳ 2443 מיום 15 בפברואר 2015).
2. הקמת הרשות הלאומית להגנת הסייבר, המובילה את מאמצי ההגנה הלאומיים, והיערכות לניהול מערכה לאומית משולבת של ביטחון ואכיפת חוק (בהתאם להחלטת ממשלת ישראל מס׳ 2444 מיום 15 בפברואר 2015). מאמץ זה מגלם את ההיערכות המדינתית למימוש תפקיד המדינה וייעודה הליבתי בהגנת הסייבר הלאומית.
3. פיתוח ויישום מערכות טכנולוגיות להגנת סייבר ברמה הלאומית (בהתאם להחלטת ממשלת ישראל מס׳ 3611 מיום 7 באוגוסט 2011). אלה נועדו להבטיח את יכולות הפעולה והיתרון היחסי בראייה ארוכת טווח.

# מאמץ ראשון
# בניית הסייבר כמרחב צמיחה בטוח

מדינת ישראל הציבה בראש סולם העדיפויות את המאמץ לבנייה של מרחב הסייבר כמרחב בטוח ושריד. זאת, מתוך המחויבות היסודית ליצירת סביבת סייבר בטוחה לאזרחים ולעסקים, בדומה למרחב הפיזי. סביבת סייבר בטוחה חיונית לשם רתימת מרחב הסייבר לצמיחתה הכלכלית והחברתית של מדינת ישראל, בהתאם לחזון הסייבר.

לצד החשיבות של מאמץ ממשלתי זה, נדרש לוודא שהמעורבות הממשלתית אינה יוצרים נטל משקי עודף, חסמים לחדשנות, ואי תאימות טכנולוגית. לפיכך, קובעת תפיסת האסדרה שאושרה בהחלטת הממשלה מס׳ 2443 את העקרונות שמטרתן לוודא זאת, בין היתר: מידתיות, דינאמיות, התבססות על סטנדרטים המקובלים בעולם, הלימה בין רמת הסיכון ורמת המעורבות הממשלתית. בהתאם לכך מסגרת הפעילות המדינתית נדרשת מצד אחד לאפשר פעילות ותגובה דינאמית לאיומים ומצד שני להיעשות במסגרת עקרונות ותהליכים שתפקידם למניעת תופעות לוואי לא רצויות של פעילויות אלה.

המאמץ הממשלתי כולל ארבעה כיווני פעולה מרכזיים: מאמצי הכוונה וסיוע לארגונים, אסדרת שוק הסייבר, והצבת אמת מידה גבוהה בהגנה על משרדי הממשלה, וכן מאמץ ממשלתי ישיר לקידום תשתיות טכנולוגיות, שנועדו לבסס תהליכים בטוחים במרחב הסייבר.

### הכוונה וסיוע למאמצי ההגנה בארגונים

במוקד המאמץ עומדות פעולות המדינה להכוונת הארגונים במשק, המהווים חלק ניכר מהמרחב ואחראים למרבית התהליכים בו. תפיסה זו מחייבת תעדוף ומיקוד בהתאם לסיכונים הנשקפים לפעילות. גישה זו מוכוונת באופן כללי לשלוש רמות, המבוססת על תאימות בין רמת הסיכון למידת המעורבות וההשקעה המדינתית:

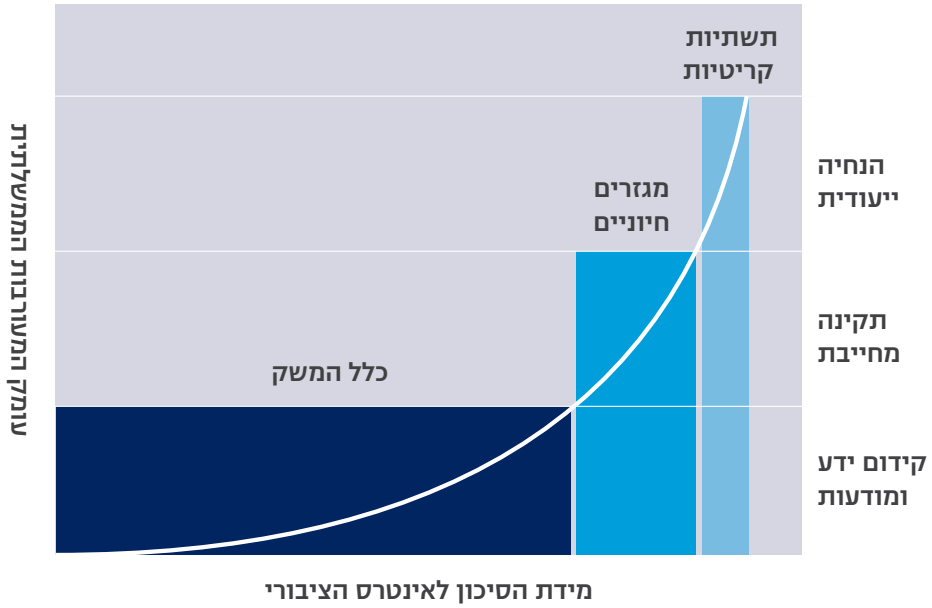
1. **הנחיה ייעודית של תשתיות ומערכות קריטיות:** רמת המעורבות המדינתית הגבוהה ביותר מתקיימת ביחס למספר מצומצם של מערכות, תהליכים וארגונים, המגלמים סיכון סייבר ברמה הלאומית. במקרים אלה מבצעת המדינה הנחיה ייעודית, המאפשרת ״תפירת״ חליפת הגנה ייחודית לגוף המונחה, הצבת רף הגנתי גבוה במיוחד וליווי צמוד ומתמשך. **ההנחיה מבוצעת באופן ריכוזי על–ידי הרשות הלאומית להגנת הסייבר (כלל התשתיות הקריטיות במשק האזרחי למעט תשתיות תקשורת) ועל–ידי גופי הביטחון (מערכות ביטחוניות ותשתיות תקשורת).**

2. **אסדרה בתחום הסייבר במגזרים ובארגונים שלתפקודם התקין השפעה על ביטחון במרחב הסייבר:** ביחס למגזרים ולארגונים שיש בהם סיכון מובהק לאינטרס הציבורי (כגון פיננסים, אנרגיה ובריאות), או לתפקודו התקין של מרחב הסייבר תיעשה אסדרה באמצעות כלי האסדרה המקובלים במשק הישראלי,

תוך יישומם בהקשר המגזרי או המרכזי הרלוונטי. בין אלה הנחיות ותקינה מחייבות, המתעדכנות מעת לעת. במרבית המקרים פעילות זו נעשית באמצעות **גורמי האסדרה המגזריים**, שהם בעלי סמכות חוקית והיכרות עם הארגונים ועם הסיכונים במגזר, ובהכוונה מקצועית של הרשות הלאומית להגנת הסייבר.

3. **קידום הגנת סייבר בכלל המשק:** מדינת ישראל פועלת לקידום העלאת העמידות בכלל הארגונים במשק באמצעות צמצום של פערי ידע, הנגשת כלים נדרשים ותמריצים או הסרת חסמים.

במקרים רבים המאמצים נעשים באמצעות גורמים מגזריים בעלי היכרות ויכולת השפעה על הארגונים במגזר. כדי לתמוך בתהליכים אלה ברמה המגזרית, החלטה מס' 2443 קידמה הקמה של יחידות מגזריות ברשויות האסדרה כדי לקדם תהליכים פנים-מגזריים.




**איור 7** | התאמה בין מידת הסיכון לאינטרס הציבורי ובין עומק המעורבות המדינתית:
החל מקידום ידע ומודעות מול מרבית הארגונים והמגזרים במשק, דרך הצבת תקינה מחייבת במגזרים ובארגונים חיוניים וכלה במאמצי הנחיה ייעודיים של מספר מצומצם של ארגונים

### אסדרת שוק הסייבר

כדי להבטיח את עיצובו הבטוח של מרחב הסייבר, מדינת ישראל פועלת לזיהוי כשלים וליצירת אסדרה נדרשת מול גורמים שיש להם חלק מרכזי בתהליכי העיצוב והבנייה של הסייבר כמרחב בטוח.

השוק הראשון שבו הוחלט לפעול הוא שוק אנשי המקצוע, שזוהה כבעל ההשפעה הרבה ביותר על תהליכי ההגנה במשק. ממשלת ישראל החלה במהלך של יצירת תשתית להסמכת אנשי מקצוע בשוק ואשר בהמשך ימומש יישומה בשלב ראשון באמצעות קביעתה כדרישה בחוזים ממשלתיים. מהלך זה מבוסס על שלושה עקרונות:

1. התבססות על מקצוע בסיס ברור - שעליו נבנים כלל המקצועות.
2. פשטות - מיקוד במעט מקצועות ליבה.
3. מחויבות ממשלתית כבסיס להשפעה על המשק.

תחומים נוספים שבהם נבחנת מידת ההשפעה המדינתית הרצויה: מוצרי ההגנה והרשת - העשויים להיות נקודות חולשה; שירותים מקצועיים - כגון ייעוץ ובדיקות חדירות; שירותים טכנולוגיים - כגון ספקי אינטרנט וענן, ביטוחי סייבר ועוד. האסדרות בשווקים אלה נועדו להבטיח היצע באיכות ובכמות ההולמות את הצרכים הלאומיים בהיבטי הגנת הסייבר, תוך הקפדה על מעורבות זהירה ומידתית ושמירה על עקרונות היסוד של שוק חופשי.

### הגנה על מרחב הסייבר הממשלתי כנקודת ייחוס

מערכות הממשל הן מרכיב מרכזי במרחב הסייבר הישראלי מבחינת היקפן, רגישות המידע המצוי בהן והשפעתן על שגרת החיים ועל ההתנהלות התקינה במשק. למאמצי הגנת הסייבר הממשלתיים יש חשיבות גם כמגדלור, המשפיע על תהליכי ההגנה במשק, בייחוד לנוכח התגברות הקישוריות בתהליכים ובטכנולוגיות בין הממשלה למגזר הפרטי. יתרה מזו, באמצעות הפנמה של היבטי הגנת הסייבר בממשלה ניתן לפתח ולבחון תפיסות הגנה ארגוניות ואתגרים למימושן.

לטובת חיזוק ההגנה במערכות הממשל, תוך הצבת דוגמה למשק כולו, הציבה ממשלת ישראל, בהחלטתה מס׳ 2443 מיום 15 בפברואר 2015 (ראו מסגרת), כיעד - להיות מובילה בתחום הגנת הסייבר, ונקטה כמה צעדים לשם כך:

1. **ההיערכות להגנת הסייבר בממשלה:** הקמת היחידה להגנת הסייבר בממשלה (יה״ב), כגוף המשמש גורם ההכוונה וההנחיה המקצועית לכלל גופי הממשלה, ופועל בהכוונת הרשות הלאומית להגנת הסייבר. כמו כן הוגדרו ממוני הגנת סייבר במשרדי הממשלה, הנושאים באחריות לניתוח סיכונים בתוך המשרד, לגיבוש מדיניות ולמעקב אחר מימושה.
2. **הסדרת תהליכים ונוהלי עבודה במשרדי הממשלה:** הסדרה ריכוזית של תהליכי רכש (בדגש על עידוד חדשנות), נוהלי העסקת כוח אדם מקצועי, מתודת ניהול סיכונים וכו׳.

**הובלה ממשלתית בהגנת הסייבר, מתוך החלטת הממשלה מס' 2443 מתאריך 15 בפברואר 2015:**

**א. "להקים יחידה להגנת הסייבר בממשלה, שייעודה להוות גוף הכוונה והנחיה מקצועית בתחום הגנת הסייבר עבור כלל משרדי הממשלה ויחידות הסמך, למעט הגופים המיוחדים, ולהקים מרכז שליטה ובקרה ממשלתי למול איומי סייבר.**

**ב. להטיל על המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך לפעול לשיפור רמת הגנת הסייבר ולשם כך – למנות ממונה הגנת הסייבר, להקים ועדת היגוי משרדית, להסדיר את אנשי המקצוע בתחום הגנת הסייבר המועסקים במשרד, להקצות תקציב ייעודי להגנת הסייבר במסגרת התקציב הקיים של המשרד ולקדם עמידה של המשרד בתקני אבטחת מידע ארגוניים.**

**ג. להטיל על מנהל הרכש הממשלתי ועל המנכ"לים של משרדי הממשלה להטמיע במסגרת הליך הרכש המרכזי או במסגרת הליך הרכש המשרדי דרישות הולמות בתחום הגנת הסייבר.**

**ד. להטיל על ראש המטה להקים ועדת היגוי לקידום ההובלה הממשלתית בהגנת הסייבר ולגבש מנגנוני סיוע למשרדי הממשלה למימוש פתרונות טכנולוגיים מתקדמים לצרכים ייחודיים..."**

3. **הבטחת תקצוב להגנת סייבר:** הוגדרה הקצאה מינימלית של 8% מתקציב טכנולוגיות המידע המשרדי לטובת הגנת הסייבר, על-מנת להבטיח הקצאה אחראית של משאבים לפרויקטים ולתהליכים להגנת סייבר בתוכניות העבודה המשרדיות.

4. **הקמת תשתיות טכנולוגיות:** פיתוח ומימוש של שירותי הגנה טכנולוגיים מרכזיים, להעצמת רמת העמידות במשרדים השונים.

כמהלך משלים הוקמה **ועדת היגוי ממשלתית לקידום ההובלה הממשלתית בהגנת הסייבר**, בראשות ראש מערך הסייבר הלאומי ובהשתתפות נציגי הרשות הלאומית להגנת הסייבר, יה"ב וממונה הגנת סייבר במשרדי הממשלה. ייעוד הוועדה הוא קידום המהלך ופיקוח על יישומו, עידוד לשיתוף מידע ותובנות בין הגופים והתאמת המדיניות לאתגרים המתפתחים.

### תשתיות ותהליכים טכנולוגיים ברמה הלאומית

מדינת ישראל פועלת באופן ישיר לביסוס תהליכי סייבר בטוחים יותר על-ידי פיתוח והקמה של תשתיות ותהליכים טכנולוגיים מתקדמים ברמה הלאומית והבין-ארגונית. בכך שואפת המדינה להשלים פערים ביכולות השוק לספק פתרונות באופן עצמאי בשל חסמי כניסה גדולים או תלות בתשתיות ציבוריות.

בשונה מפתרונות הגנה לרמה הארגונית, פתרונות ותשתיות הגנה ברמה הבין-ארגונית, המגזרית והלאומית מצויים בתחילת דרכם ומחייבים לרוב תהליכי מחקר ופיתוח בהובלת המדינה.

אפשר להצביע על כמה כיוונים מובילים בתחום זה:

1. **מימוש צעדים ותהליכים בתשתיות התקשורת הלאומיות**, שיהוו "קפיצת מדרגה" בביטחון הפעילות בסייבר וברציפות התפקודית של תשתיות הסייבר בישראל. פרויקטים אלה מבוצעים לרוב בשיתוף ספקיות האינטרנט וגורמים מרכזיים נוספים, דוגמת סינון תקיפות מובהקות או יישום פרוטוקולים בטוחים יותר.
2. **בניית תשתיות, המאפשרות לגופים ולפרטים במשק ליישם תהליכים באופן בטוח** - בין היתר באמצעות כלים ותהליכים, המאפשרים הזדהות בטוחה ואמינה.
3. **תשתיות טכנולוגיות, המספקות שירותי הגנה ארגוניים או שירותים ארגוניים מוגנים באופן מרכזי**, לרוב עבור מגזרים מרכזיים במשק: הממשלה, גופים ביטחוניים ותשתיות קריטיות.


**איור 8** | מכלול המאמצים לבניית הסייבר כמרחב בטוח:

הכוונה וסיוע למאמצי ההגנה בארגונים במשק, הסדרה וחיזוק היכולות בשוק הסייבר, קידום תשתיות ותהליכים מדינתיים התומכים במאמצי ההגנה, ומינוף מאמצי ההגנה הממשלתיים כנקודת ייחוס המשפיעה על המשק.

# מאמץ שני
# הרשות הלאומית להגנת הסייבר

בהחלטת הממשלה מס' 2444 מתאריך 15 בפברואר 2015, הוסדרה ההיערכות המדינתית בתחום הגנת הסייבר, כדי להבטיח מימוש עוצמתי וארוך טווח של תפיסת הפעולה. המהלך המרכזי שהובילה המדינה הוא ההקמה של גוף אופרטיבי חדש, לטובת הובלת מאמצי הגנת הסייבר בישראל - הרשות הלאומית להגנת הסייבר (ראו קיטוע מתוך ההחלטה במסגרת). מהלכים משלימים ננקטו במטרה להסדיר ולהעצים את המאמצים הנוגעים בהגנת הסייבר ברמה הלאומית במסגרת גופי הביטחון, רשויות אכיפת החוק ורשויות האסדרה, ושילובם כחלק ממערכה הגנתית לאומית מתוכללת.

**תפקידי הרשות, מתוך החלטת הממשלה מס' 2444 מתאריך 15 בפברואר 2015:**

**א. "לנהל, להפעיל ולבצע בהתאם לצורך את כלל מאמצי ההגנה האופרטיביים ברמה הלאומית במרחב הסייבר, בתפיסה מערכתית, לטובת מענה הגנתי שלם ורציף למול תקיפות סייבר, ובכלל זה טיפול באיומי סייבר ובאירועי סייבר בזמן אמת, גיבוש תמונת מצב שוטפת, ריכוז ומחקר מודיעין, ועבודה עם גופי מערכת הביטחון.**

**ב. להפעיל מרכז לסיוע בהתמודדות עם איומי סייבר (להלן – ה–CERT הלאומי) עבור כלל המשק, ובכלל זה לפעול לשיפור החוסן ההגנתי בסייבר, לסייע בטיפול באיומי סייבר ואירועי סייבר, לרכז ולשתף מידע רלוונטי עם כלל הגורמים במשק ולהוות נקודת ממשק מרכזית בין גופי הביטחון לבין הגורמים במשק.**

**ג. לבנות ולחזק את החוסן של כלל המשק בסייבר באמצעות היערכות, כשירות ואסדרה, ובכלל זה העלאת הכשירות של מגזרים וגופים במשק, הנחיית המשק בתחום הגנת הסייבר, אסדרת שוק שירותי הגנת הסייבר, רישוי, תקינה, עריכת תרגילים ואימונים, מתן תמריצים וכלים נדרשים נוספים.**

**ד. לעצב, ליישם ולהטמיע תורה לאומית להגנת הסייבר."**

### הרציונל של הקמת הרשות

הקמת הרשות הלאומית להגנת הסייבר מבטאת מעבר מתפיסה של סנכרון לאומי של מאמצי הגנת הסייבר לתפיסה של ריכוז המאמצים האופרטיביים והאחריות הלאומית, באופן המשרת ארבעה עקרונות:

- **גוף אחד מרכזי** - הנושא באחריות כוללת להגנת הסייבר האזרחית ומוביל תהליכים הדורשים פעולה לאומית מרכזית: בניית תמונת מצב, ניהול ריכוזי לאירועים ברמה הלאומית והכוונת המאמצים הממשלתיים. גוף זה משמש גם מוקד ידע לאומי להגנת סייבר, המסוגל לספק הכוונה מקצועית ולתמוך במאמצי כלל הגורמים הרלוונטיים.

- **גוף ייעודי להגנת הסייבר** - אשר נמדד אך ורק על משימת הגנת הסייבר ואינו מוטה בהתאם למשימות אחרות של הארגון. בשל ייעודו הייחודי, ניתן לנטרל מראש חששות הקשורים בממשקים שבין המדינה לבין ארגונים, מערכותיהם והמידע שנצבר בהם. גוף זה יכול לממש ביתר קלות את ייעודו בתור גורם טכנולוגי מוביל, שתפקידו לפעול מול הארגונים, לאסוף ולשתף מידע רלוונטי להגנה, מבלי שפעילויות אלה והאמון הנדרש למימושן מצויים בסיכון בשל תפקידים אחרים של גופי מדינה. הטלת התפקיד על גוף ייעודי מאפשרת לעצב את מסגרת הפעילות שלו תוך מיקוד בהגנת הסייבר, וקביעת מסגרת מאוזנת המפחיתה את החשש מפני פגיעה בזכויות יסוד. כך, כניסתה המחודשת של המדינה למרחב הסייבר על מנת לתמוך בפעילות הארגונים כפי שהוצג לעיל, נעשית תוך איזון קבוע עם אינטרסים אחרים החיוניים לתפקודו התקין.

- **גוף אופרטיבי** - הנושא באחריות ביצועית מלאה, עצמאי בהפעלת יכולותיו ובעל סמכויות ומשאבים הנדרשים לו. בכך מתאפשרת בנייה לאורך זמן של היכולות הנדרשות ברמה הלאומית, בהתבסס על מסה קריטית של ידע, של מומחים ושל תשתיות, תוך השלמת יכולות חסרות ופיתוח שיטות פעולה ייעודיות בטווחי זמן רלוונטיים. ריכוז חלק ניכר מהמאמצים האופרטיביים בגוף אחד מאפשר ביסוס הקשרים הנחוצים בין שלוש שכבות ההגנה. ככזה, הגנת סייבר היא תחום התמחותו והוא בעל גמישות חשיבתית לפיתוח כיווני פעולה חדשים הנדרשים בתחום. כמו כן, יש לו הגמישות לפעול במגוון הרחב של הכלים הנחוצים לטובת התמודדות עם המשימה, בין היתר: רגולציה, פעילות טכנו-מבצעית, פיתוח ידע ושיטות פעולה חדשות, עבודה פתוחה ומשתפת עם הציבור, תיאום מאמצים ביטחוניים, בניית שותפויות בין-לאומיות ועוד.

- **גוף אזרחי** - הפועל בפתיחות ובשיתוף פעולה עם הארגונים והמגזרים במשק כשותפים, בשיטות עבודה התואמות את אופייה האזרחי של הפעילות ושל יעדיה. הידע הקיים באופן בלעדי ביעדי ההגנה ובתעשיית הסייבר, כולם אזרחיים במהותם, חיוני לפעולה המדינתית להגנת הסייבר, ושיתוף הפעולה עמם הוא במקרים רבים תנאי להצלחתה. על כן נדרש גוף, הפועל בשיתוף פעולה עם הארגונים, באופן שייצר אמון בין כל הגורמים הרלוונטיים, יגדיל את האינטרס לשיתוף פעולה ויצמצם סיכון לחשיפת יתר של ארגונים.

### הרשות כמוקד ידע לאומי להגנת סייבר

הרשות היא מוקד הידע הלאומי, התומך בכלל מאמצי הגנת הסייבר בישראל. הרשות מפתחת ידע, שיטות, כלים ודרכי פעולה מומלצות ומנגישה אותם הן לגופים במשק והן לגופי הממשלה הפועלים בתחום.

תפקיד מרכזי של הרשות בהקשר זה הוא בסנכרון כלל תהליכי ההכוונה של ארגונים במשק בתחום הגנת הסייבר ותמיכה בידע ובמתודולוגיה ברשויות האסדרה השונות בממשלה. לרשויות האסדרה יש היכרות מעמיקה עם הארגונים, הן מנהלות קשרי עבודה שוטפים עמם ויש להן השפעה עליהם, ואולם מנגד, לרוב קיימים פערי ידע בתחום הסייבר, הנובעים מהעדר מסה קריטית או קשב ייעודי, הדרוש לעיסוק בתחום.

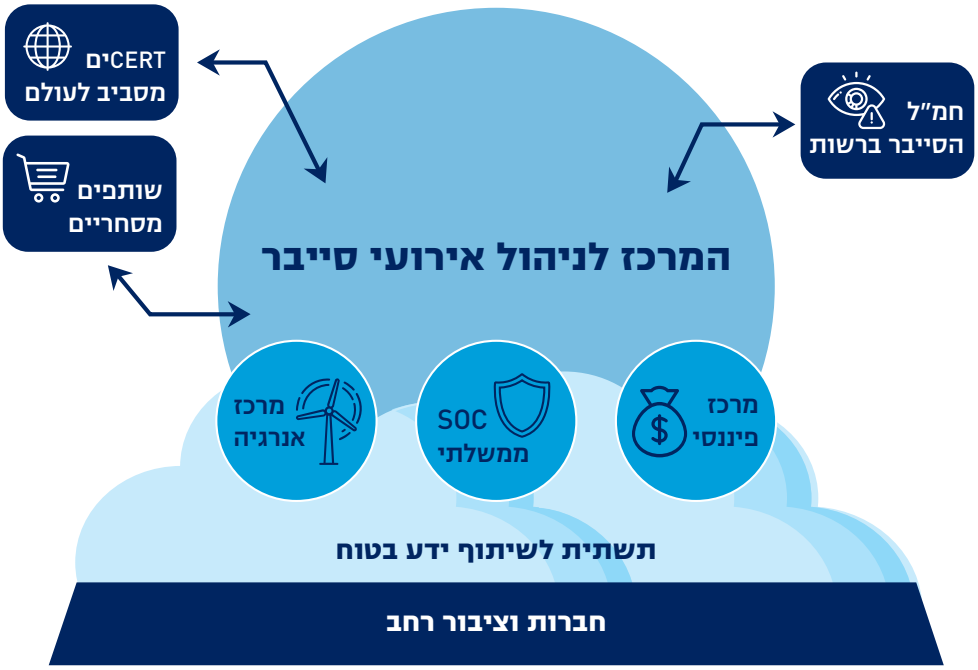
### הרשות כמוקד הלאומי לניהול ולסיוע בהתמודדות עם אירועי סייבר

הרשות היא הגוף, המרכז את ניהול ההתמודדות עם אירועי סייבר במשק ובניית תמונת מצב לאומית אחודה ועדכנית. במסגרת הרשות הוקם **המרכז לניהול אירועי סייבר** (ה-CERT הלאומי), המוביל מטעם הרשות את הטיפול באירועי סייבר בארגונים במשק. המרכז פועל לעידוד שיתוף מידע במשק ולהפצה של מידע ערכי ובר פעולה בזמן אמת, לצד מאמצי סיוע לארגונים שהותקפו ומהלכי הכלה והסברה להתמודדות עם אירועים במשק.

המרכז פועל בהתאם **לשיטה ומנגנון לאומיים לשיתוף מידע** בין המדינה לארגונים במשק ובין הארגונים לבין עצמם, אשר נועדו לרכז מידע ולהנגישו לגורמים שהוא רלוונטי להם. מרכיב מרכזי במנגנון זה הוא שילוב של מרכזי חוסן מגזריים, הפועלים בתוך המרכז הלאומי. המרכזים פועלים לשמירה על הרציפות התפקודית במגזר, תוך בניית שיח אינטימי עם הארגונים במגזר בהתאם למאפייניו. שילוב זה מאפשר מצד אחד מינוף התשתיות הטכנולוגיות והמומחיות של המרכז הלאומי לטובת הפעילות המגזרית, ומצד אחר תהליך של שיתוף מידע וניהול אירועים אפקטיבי יותר ובניית תמונת מצב לאומית רחבה.

המרכז משמש ממשק בין הארגונים במשק ליתר גופי הרשות, ובאמצעותה גם עם מערכת הביטחון, בכל הנוגע להתמודדות עם תקיפות. המרכז פועל להשגת יעדיו בשיח שוטף ופתוח מול כלל המשק, ליצירת שפה משותפת, תרבות של אמון ושיתוף מידע ולהעלאת רמת המודעות של גופים במשק לאיומים במרחב הסייבר ולאופני ההתמודדות עמם. למרכז תפקיד חיוני בקידום העמידות של הארגונים במשק, בהתבסס על שיתוף מידע שוטף ועל הנחיות עדכניות.

המרכז **הוקם בקריית הסייבר בבאר שבע** כחלק מאקוסיסטם שלם בתחום הגנת הסייבר, הכולל תעשייה, אקדמיה ופעילות ממשלתית, תוך שאיפה לחזק את הקשר של המרכז לקהילה המקצועית הישראלית והבין-לאומית באופן התומך בתהליכי חדשנות ובה בעת רותם אותם לצרכיו.




**איור 9** | המרכז לניהול אירועי סייבר:

המרכז מהווה מוקד המסייע ומשתף מידע על כלל המגזר האזרחי ומהווה ממשק מול שותפים בארץ ובעולם. במסגרתו פועלים מרכזי ההגנה המגזריים (בשלב זה: ממשלתי, פיננסי ואנרגיה).

### ניהול מערכות ומבצעי הגנה

הרשות מובילה מאמצים מדינתיים להתמודדות עם מערכי תקיפה המאיימים על מדינת ישראל לטובת צמצום נזקים מיידיים, הכלת האירוע בגבולות מבוקרים, בלימת התקיפה ולימוד מאפייניה באופן המאפשר לחזק את העמידות המשקית למנוע תקיפות דומות.

הרשות משקיעה מאמצים נרחבים ומתמשכים לזיהוי, לאיתור ולחקירה של תקיפות ומערכי תקיפה מתקדמים, בין היתר באמצעים פרו-אקטיביים, שנועדו "ללכוד" ו"להטעות" את התוקף. כמו כן, היא עוסקת בניהול האירועים, ובכלל זה בפעולות הכלה "שקטות" ו"רועשות".

### תפקידי הרשות בשלוש שכבות ההגנה

| עמידות משקית | חוסן מערכתי | הגנה לאומית |
|---|---|---|
| • הנחיית תשתיות קריטיות<br>• הכוונה ארגונית ומגזרית (כולל הכוונה למאסדרים מגזריים)<br>• מוקד ידע לאומי<br>• אסדרת שוק הסייבר | • שיתוף מידע כלל מדינתי<br>• סיוע לארגונים שנתקפו<br>• זיהוי וחקירת תקיפות<br>• יישום תהליכים ותשתיות לשיתוף וזיהוי<br>• תמיכה בפעילות חוסן מגזרית | • ניהול מבצעי הגנה<br>• בניית תמונת מצב לאומית |

### היערכות לאומית משלימה

כדי להבטיח מענה לאומי שלם, וכצעד משלים להקמת הרשות, מדינת ישראל פועלת להעצמת מכלול המאמצים הנדרשים ברמה הלאומית ולתיאום בין הרשות ובין כלל הגופים הפועלים בתחום: רשויות האסדרה, רשויות אכיפת החוק ומערכת הביטחון.

**רשויות האסדרה** השונות נוטלות חלק מרכזי במאמץ לבניית העמידות של הארגונים במשק. יש להן היכרות מעמיקה עם גופי היעד שלהן, הן מקיימות קשרי עבודה שוטפים עמם ונתונה להן השפעה עליהם. מנגד, בקרב רשויות האסדרה מתקיימים במקרים רבים פערי ידע בתחום הסייבר, הנובעים מהעדר מסה קריטית או קשב ייעודי הדרוש לעיסוק בתחום. כדי להבטיח מענה שלם ואפקטיבי, הוקמו יחידות ייעודיות להכוונה מקצועית של גופי היעד במסגרת כמה רשויות אסדרה, בהתאם לאיום הייחוס הלאומי. היחידות פועלות לעידוד ולקידום הגנת הסייבר במגזרים השונים, תוך שהן ממנפות את הנכסים והסמכויות של הרשות המאסדרת כחלק ממימוש האחריות הכוללת שלה. היחידות עובדות בשיתוף פעולה עם הרשות ובהתאם לתורת ההגנה, לשיטות הפעולה ולהנחיותיה המקצועיות של הרשות.

**רשויות אכיפת החוק** נושאות באחריות להתמודד עם פשיעת הסייבר ומקיימות שיתוף פעולה נרחב עם רשויות אכיפת חוק במדינות אחרות. פעילות אכיפת החוק כנגד תוקפים מהווה נדבך משלים וחיוני לבניית החוסן המערכתי, המאפשר בלימה של תקיפות המשפיעות על המשק, וכן משולבת במערכה ממוקדת להתמודדות עם אירועים חמורים, במסגרת ההגנה הלאומית.

**גופי מערכת הביטחון** הם חוד החנית בהתמודדות הנדרשות מול תוקפי הסייבר במסגרת שכבת ההגנה הלאומית. הם פועלים מתוקף ייעודם להתמודד עם איומי ביטחון לאומי, תוך שהם ממנפים את הידע, את המומחיות ואת היכולות הייחודיות שלהם כחלק מהמערכה ההגנתית השלמה להתמודדות עם איומי סייבר חמורים.

# מאמץ שלישי | **מחקר, פיתוח ויישום של יכולות וטכנולוגיות הגנה מדינתיות**

### רקע ורציונאל

מדינת ישראל משקיעה משאבים רבים במחקר ובפיתוח של פתרונות הגנה מתקדמים ברמה הלאומית, מתוך הבנה כי מרחב הסייבר הוא מרחב טכנולוגי וכי כדי להגן עליו באופן מיטבי יש להתבסס על אמצעים טכנולוגיים מתקדמים, המשולבים בתפיסת הפעולה המבצעית והמופעלים על-ידי כוח אדם מיומן.

מאמצי מחקר ופיתוח ייעודיים מאפשרים למדינת ישראל למנף את העוצמות הטכנולוגיות שלה על-מנת ליישם טכנולוגיות הגנה מתקדמות וייחודיות. טכנולוגיות אלה מספקות יתרון ממשי אל מול תוקפים מתקדמים, אשר לרוב מתמודדים עם מערכות הגנה מסחריות. בנוסף, המדינה פועלת לפיתוח ולקידום פתרונות הגנה ברמה העל-ארגונית, המהווים מכפיל כוח למאמצי ההגנה הארגוניים (פתרונות שאינם מושגים בכוחות השוק).

כדי לממש יעדים אלה נדרשות השקעות מדינתיות ייעודיות, תוך רתימת הידע והיכולות שמצויים באקדמיה ובתעשייה, ובהתאם לצרכים ולתפיסת הפעולה. השקעות אלה נדרשות עבור כלל שלבי הפיתוח הטכנולוגי: החל בהנבטה של גישות פורצות דרך ובעלות פוטנציאל לשנות את כללי המשחק בהסתכלות ארוכת טווח, עבור בפיתוח אבני בניין טכנולוגיות, המשרתות את מגוון המאמצים, וכלה במימוש מיזמים ובפריסת מערכות ברמה הלאומית.

### מאמצי המו"פ בישראל

ההשקעות של מדינת ישראל בפיתוח טכנולוגיות סייבר מתייחסות לשלושה מרכיבים מרכזיים: בניית התשתיות אשר מאפשרות ומקדמות עשייה טכנולוגית בתחום הסייבר; פיתוח של אבני בניין טכנולוגיות פורצות דרך, אשר עליהן עתידים להתבסס פתרונות הן ברמה הלאומית והן ברמה הארגונית; יישום ופריסה של פתרונות טכנולוגיים להגנה ברמה הלאומית - החל מתשתיות אופרטיביות לגופי ההגנה וכלה בפעילות, המאפשרת קיומם של תהליכים בטוחים יותר במשק (כגון הזדהות בטוחה).

אפשר לסמן כמה כיוונים מרכזיים לפיתוח של יכולות טכנולוגיות הרלוונטיות להגנת הסייבר הלאומית: בניית מערכות ותכנון תהליכים, העמידים יותר מפני תקיפות סייבר; קידום תהליכי הגנה, המבוססים על שירות מרכזי - במקומות שבהם יש לכך יתרון ובהתאם לאינטרס הלאומי; קידום תשתיות ופתרונות התומכים במאמצי גילוי, זיהוי, חקירה והכלה של תקיפות סייבר במשק על-ידי המדינה; קידום תשתיות המאפשרות שיח פורה ומבוסס אמון בין המדינה לארגונים ובין הארגונים בינם לבין עצמם, בדגש על תשתיות לשיתוף מידע בטוח ואפקטיבי.


**איור 10** | מאמצי המו"פ בתחום הסייבר בישראל:

מדינת ישראל פועלת לפיתוח של תשתיות ואבני בניין טכנולוגיות, בראייה ארוכת טווח, וכן מפתחת מערכות המספקות מענה לצרכים ברמה הלאומית.

### היחידה לטכנולוגיות סייבר

כדי להבטיח את המשך מימוש הפוטנציאל להגנה טכנולוגית ברמה לאומית הוקמה במסגרת מטה הסייבר הלאומי היחידה לטכנולוגית סייבר, שייעודה הוא בניית הכוח הטכנולוגי של מדינת ישראל, ובפרט מתן מענה לצרכים המבצעיים של הרשות הלאומית להגנת הסייבר.

תפקידי היחידה כוללים: חיזוק תשתיות מדעיות-טכנולוגיות הלאומיות (תעשייה, אקדמיה, הון אנושי); הקמת מעבדות ותשתיות למחקר ולפיתוח; קידום מחקר וגיבוש תפיסות טכנולוגיות פורצות דרך; פיתוח פתרונות ומימוש פרויקטים טכנולוגיים; ביצוע עבודת מטה לפיתוח תפיסות טכנולוגיות חדשניות; ביסוס מוקד ידע לאומי בנושאי טכנולוגיית סייבר.

היחידה עובדת בשיתוף פעולה הדוק עם הגורמים הרלוונטיים בגופי הביטחון ובממשלה, בונה שיתופי פעולה עם האקדמיה ועם התעשייה וכן שיתופי פעולה בין-לאומיים.

# סיכום שלושת מאמצי-העל להגנת הסייבר


**איור 11** | שלושה מאמצי-על להגנת הסייבר בישראל

# שער 3
# מאמצים תומכים לביסוס היכולת הלאומית בסייבר

# בניין הכוח המדעי–טכנולוגי הלאומי בסייבר

## הקדמה

מדינת ישראל ניצבת זה כמה עשורים בחזית העולמית של החדשנות ופיתוח הידע המדעי-טכנולוגי בתחומי הסייבר בכלל והגנת הסייבר בפרט. תרבות החדשנות, ההון האנושי הייחודי ומאמצי ההגנה הלאומיים והביטחוניים בישראל הם המנוע לתהליך מתמשך של יצירת ידע ופיתוח יכולות ופתרונות פורצי דרך בתחום, המספקים מענה הן לצרכים המקומיים והן לצרכים הכלל עולמיים.

מרחב הסייבר הוא מרחב מבוסס טכנולוגיה ביסודו, המתפתח ומשתנה ללא הפסק. לא רק שהטכנולוגיות לניצול המרחב מתפתחות בקצב חסר תקדים, אלא גם מרכיבי המרחב ופוטנציאל הפעולה בו מתפתחים כל העת - תופעה שאין לה מקבילה במרחב הפיזי. בד בבד, גם הטכנולוגיות ושיטות התקיפה מתקדמות והופכות מתוחכמות יותר ויותר, הן בהתגברות על מאמצי ההגנה, והן בהרחבת יעדי התקיפה ובמיצוי פוטנציאל הרווח והנזק הגלומים בפעילות הזדונית.

במסגרת החלטת ממשלת ישראל מס' 3611 מיום 7 באוגוסט 2011, בנושא "קידום היכולות הלאומיות במרחב הקיברנטי", סימנה מדינת ישראל את החשיבות של ביסוס היכולות המדעיות-טכנולוגיות בתחום הסייבר כמפתח לעמידה איתנה לאורך זמן בפני האתגרים בסייבר. לאור זאת פועלת המדינה לקידום היכולות המדעיות-טכנולוגיות המרכזיות: תעשייה, מחקר אקדמי והון אנושי, תוך יצירת סביבה של הפריה הדדית ("אקוסיסטם"), התומכת בתהליכי התעצמות מתמשכים.

## תעשיית הגנת הסייבר

תעשיית הסייבר הישראלית היא בין המובילות בעולם, וחברות הסייבר הישראליות נמצאות בחזית החדשנות הטכנולוגית עוד מימיה הראשונים של אבטחת המידע. ההתפתחות של תעשיית הסייבר הישראלית מבוססת על תרבות היזמות והחדשנות המאפיינת את ההיי-טק הישראלי באופן כללי, על אקדמיה מובילה ועל הניסיון הייחודי של ההון האנושי הישראלי, בדגש על יוצאי מערכת הביטחון.

מדינת ישראל פועלת להמשיך ולחזק את תעשיית הסייבר הישראלית כמקור לחדשנות וכבסיס ליכולת הלאומית בתחום הסייבר, תוך הסתמכות על היותה תעשייה רווחית ומבוססת ייצוא, המכוונת לצרכים בשוק העולמי ומהווה מנוע לצמיחה כלכלית של מדינת ישראל. המאמצים הממשלתיים על-פי-רוב אינם מחליפים את ההתפתחות העצמאית והחופשית של התעשייה, אלא נועדו לתמוך ולסייע אל מול כשלי שוק או הזדמנויות ייחודיות.

מאמץ מרכזי הוא הטיפוח של היזמות והחדשנות הטכנולוגית, שהן אחד היתרונות הבולטים של התעשייה הישראלית בעולם ומשרתות את הצרכים הלאומיים. מדינת ישראל פועלת לשמר ולטפח את החדשנות של

החברות הישראליות במגוון כלים, בין היתר על ידי מענקי מו"פ ועידוד שיתופי פעולה בין חברות ישראליות ויצירת שותפויות עם שותפים מהעולם. מאמץ מיוחד מושקע גם בסיוע לחברות הזנק, אשר מהוות מנוע חדשנות מרכזי באקוסיסטם הישראלי ומזרימות בקביעות ידע ורעיונות חדשניים לשוק הגנת הסייבר.

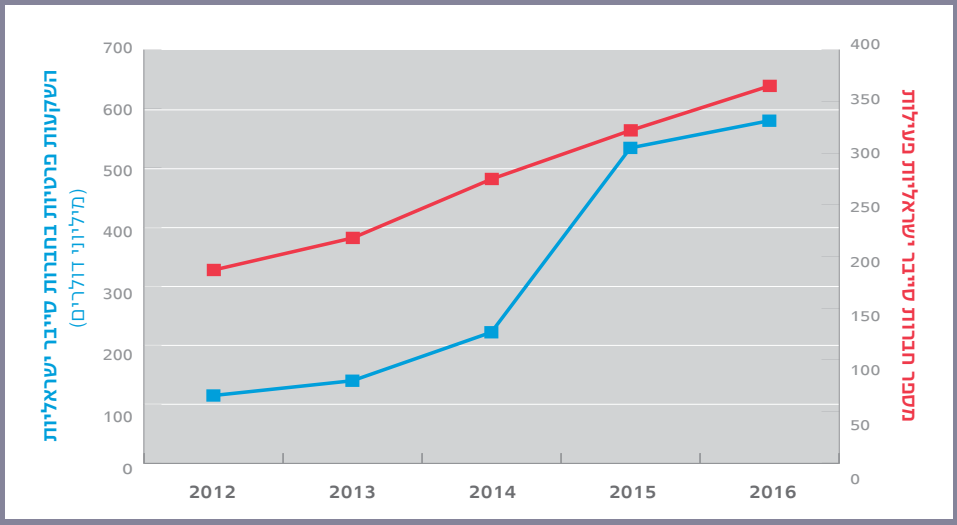
### תעשיית הגנת הסייבר הישראלית

סיפור ההצלחה של תעשיית הגנת הסייבר הישראלית מתחיל בסוף שנות ה-80 ובתחילת שנות ה-90 של המאה ה-20, עם המצאת האנטי-וירוסים הראשונים, וחומת האש של חברת צ'ק פוינט.

שנות ה-2000 היו שנים של התפתחות אטית. לצד מספר קטן של חברות שעדיין פועלות כיום והן בין המובילות בעולם, חברות רבות לא צלחו כחברות עצמאיות, אך שהיו פורצות דרך בזמנן, אך חלקן התמזגו לתוך חברות גלובליות ועל בסיסן הוקמו מרכזים מובילים בתחום הגנת הסייבר הפועלים מישראל.

בשנים האחרונות נמצאת התעשייה בצמיחה חסרת תקדים והיא מונה כיום יותר מ-300 חברות ישראליות. לאלו מצטרפות כ-30 חברות רב-לאומיות שהקימו בישראל מרכזי סייבר.

חברות סייבר ישראליות גייסו בשנים 2012-2016 – יותר ממיליארד וחצי דולרים, והיקף המכירות שלהן מוערך בכ-4 מיליארד דולרים, שמהווים כ-5 אחוזים מהשוק העולמי.



### אקדמיה

מוסדות המחקר האקדמי בישראל ניצבים בחזית העולמית בתחום מדעי המחשב ובתחומים משיקים. מדינת ישראל רואה באקדמיה מרכיב מרכזי ביכולת המדעית-טכנולוגית בתחום הסייבר. יכולת זו משמשת מנוע ליצירת ידע והבנה תשתיתיים וארוכי טווח, לביסוס פריצות דרך מדעיות-טכנולוגיות וכמובן ליצירת תשתית ההון האנושי הנחוצה לתחום. ביטוי להשפעת האקדמיה אפשר לראות כבר היום במגוון חברות ישראליות, המיישמות רעיונות מחזית הידע המחקרי לכדי מוצרים טכנולוגיים פורצי דרך, בשותפות עם חוקרים מובילים מהאקדמיה ואף ביוזמתם של האחרונים.

על-מנת להמשיך ולבסס את המחקר האקדמי בישראל, בחרה מדינת ישראל לקדם הקמת מרכזי מחקר ייעודיים, כדי לטפח את העיסוק האקדמי בתחום הסייבר, לרתום את יכולות המחקר להתמודדות עם אתגרים בתחום, וליצור שער כניסה לשיתופי פעולה בין האקדמיה, התעשייה והממשלה. בתמיכת הממשלה הוקמו שישה מרכזי מחקר באוניברסיטאות המחקר המובילות בישראל. המרכזים עוסקים בכלל התחומים הנוגעים לאתגרי הסייבר, ובכל אחד מהם מושם דגש על תחומי מחקר ועניין המביאים לידי ביטוי את החוזקות המרכזיות של המוסד האקדמי.

כיוון שהאתגרים בתחום הסייבר חורגים מסוגיות טכנולוגיות גרידא, יועדו חלק מהמרכזים מלכתחילה להרחבת העיסוק בסייבר מעבר להיבטים הטכנולוגיים שלו, ולהתמודדות עם סוגיות בתחומי החברה, הממשל, הכלכלה והמשפט.


**איור 12** | מרכזי מחקר הגנת הסייבר בשש אוניברסיטאות מובילות

### הון אנושי

המרכיב הבסיסי ביותר להצלחתה של מדינת ישראל בתחום הסייבר, כמו גם בתחומים טכנולוגיים אחרים, טמון בהון האנושי הייחודי בישראל. הקהילה הטכנולוגית בישראל מתאפיינת בתרבות של חדשנות ונועזות, הנדרשות כדי לקדם פתרונות פורצי דרך, וכן רשתיות ופתיחות לשיתופי פעולה הנחוצים בתחום. לכך מצטרף גם מרכיב ייחודי של ידע וניסיון שרוכשים העוסקים בתחום במהלך השירות ביחידות הטכנולוגיות של מערכת הביטחון.

**התפקיד המיוחד של מערכת הביטחון**

**למערכת הביטחון הישראלית יש תפקיד חשוב בפיתוח ההון האנושי בתחום הסייבר. הצרכים הייחודיים והאפשרות לבחור את הטובים ביותר, המבוססת על גיוס החובה, מציבים את מערכת הביטחון בעמדה יוצאת דופן, המאפשרת איתור, הכשרה והקניית ניסיון מעשי ואיכותי. הזרימה המתמשכת של הון אנושי לתוך מערכת הביטחון והחוצה ממנה ויוצרת השפעה דרמטית על המשק. לצד זאת, כלקוחה מרכזית של תוכניות פיתוח ההון האנושי בגילאים הצעירים, מערכת הביטחון מתפקדת גם כיוזם ושותף להכשרת בני נוער ולפיתוח תורות הכשרה פורצות דרך.**

על-מנת לקדם את כלל המאמצים של בניין הכוח המדעי-טכנולוגי בתחום הסייברבמיוחד על רקע הצמיחה האדירה בביקוש לאנשי סייבר מעולים, פועלת מדינת ישראל להעצים את ההון האנושי בתחום הסייבר באיכות ובכמות. **המאמץ מתמקד בביסוס קבוצת איכות של מומחים בעלי היכרות מעמיקה עם תחום הסייבר**, המתאפיינת בהכשרת עומק מדעית-טכנולוגיות, לרוב על בסיס אקדמי, לצד ניסיון וגישה מעשית. קבוצה זו היא הבסיס המרכזי לקידום מו"פ ייעודי בתחום הסייבר והמקור העיקרי לכוח עבודה למשימות הגנת סייבר, המצריכות עומק טכנולוגי.

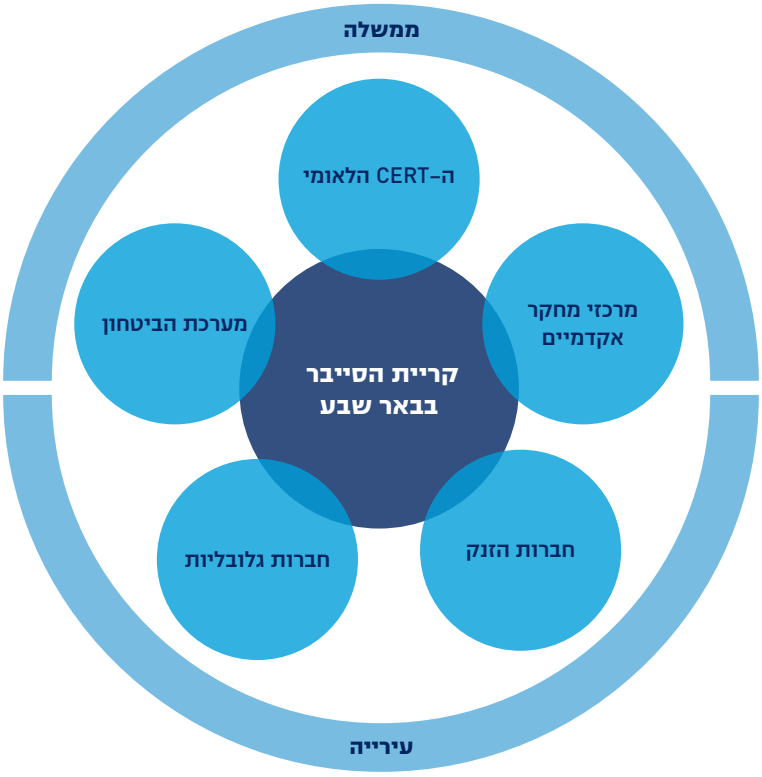
חלק ניכר מהמאמצים לפיתוח ההון האנושי בתחום הסייבר בישראל מתמקדים בחיזוק בסיס **ההון האנושי בגילאים צעירים** (תיכון ואף חטיבת הביניים), שכן רבים מבעלי המומחיות בתחום הסייבר מתחילים לצבור ידע וניסיון בתחום זה כבר בגיל צעיר, פעמים רבות בהתבסס על הכשרה עצמית, באופן שמספק להם את ההיכרות וההבנה העמוקים הנדרשים בתחום. לצורך כך, קודמו בשנים האחרונות כמה תכניות לנוער, הן במסגרת החינוך הפורמלי והן בתוכניות מצוינות חלופיות, אשר משלבות הכשרה מקצועית ברמה גבוהה עם התנסות מעשית. זאת, לצד בניית המודעות והמוטיבציה לעיסוק בנושא.

מאמץ נוסף הוא הסדרת ההכשרות המקצועיות בתחום הסייבר והעלאת רמתן המקצועית, בהתבסס על המהלך המדינתי להסדרת מקצועות הסייבר וכבסיס לבניית ההיצע של כוח האדם מיומן למאמצי ההגנה במשק. בפרט, מושם דגש על הכשרות מקצועיות לאוכלוסיות שאינן משתלבות באופן טבעי בכוח העבודה בתחום.

### קריית הסייבר הלאומית

קריית הסייבר הלאומית (CyberSpark) היא פרויקט ראשון מסוגו בעולם לביסוסו של "אקוסיסטם" מרוכז ועוצמתי בתחום הסייבר, אשר הוקם במסגרת החלטת ממשלה בעיר באר שבע. הקריה היא נקודת מפגש בין אקדמיה, תעשייה ישראלית וגלובלית, ומרכזי הגנת סייבר אזרחיים וצבאיים המצויים במרחק הליכה זה מזה. חיבור זה מהווה קרקע פורייה לשיתופי פעולה יציבים וליצירת ידע, הנחוצים לקידום החדשנות ולפתרון האתגרים של הגנת הסייבר בישראל ובעולם. בין היתר, השילוב של קרבה פיזית ורעיונית מאפשר יצירת היכרות ושיח מזדמנים וגם פיתוח של הון אנושי.

בקריית הסייבר מצויים כבר היום מרכז מחקר הסייבר של אוניברסיטת בן גוריון, חממה של חברות הזנק ישראליות, מרכזי מו"פ ושירותים של כמה חברות גלובליות, בין המובילות בעולם בתחום הסייבר, המרכז לניהול אירועי סייבר (ה-CERT הלאומי), שהינו אגף ברשות הלאומית להגנת הסייבר, (המהווה, כאמור, מוקד ידע ושער לשיתופי פעולה כחלק ממאמצי ההגנה המדינתיים), וכן עתידות להצטרף בהמשך יחידות הטכנולוגיה של צה"ל.




**איור 13** | קריית הסייבר הלאומית

# שיתוף פעולה בזירה הבין-לאומית

### מבוא

האתגרים והאיומים במרחב הסייבר הם גלובליים, ובמקרים רבים מקורם מחוץ למדינות שבתחומן הם באים לידי ביטוי. המענה לאתגרים ולאיומים אלה מחייב תיאום ושיתוף פעולה חוצה גבולות הן מול גורמים מדינתיים, הן מול גורמים פרטיים. בלא תיאום זה יעילותם של מאמצים פנים-מדינתיים מוגבלת ולוקה בחסר.

התגברות הפעילות במרחב הסייבר יוצרת, אפוא, ממשק ייחודי ואינטנסיבי בין מדינות, וביניהן ובין גופים פרטיים, אשר יש לו היבטים טכנולוגיים, תרבותיים, נורמטיביים ומשפטיים. בין כלל הגורמים הללו מתנהל שיח, שנועד להגביר את האמון בין כל הצדדים, לברר אינטרסים של מדינות, ארגונים ופרטים, לבסס תהליכים משותפים נחוצים וכן לבחון את הדין הקיים ואת יישומו והתאמתו למאפייני המרחב.

### הפעילות הישראלית בזירה הבין-לאומית

לאור כל זאת, מדינת ישראל רואה חשיבות רבה בשיתוף הפעולה הבין-לאומי כתהליך חיוני לביסוס מרחב הסייבר כמרחב גלובלי בטוח וחופשי, וכמרכיב משלים למאמצי הגנת הסייבר הלאומיים. שיתוף הפעולה הבין-לאומי כולל פעילות ברמה הבילטרלית, שיח ומאמצים בין-לאומיים וכן השתתפות בשיח רב-משתתפים עם גורמים באקדמיה ובמגזר הפרטי.

מדינת ישראל מביאה עמה לזירה הבין-לאומית הסתכלות מערכתית על נושא הסייבר לצד ניסיון בקידום ובהטמעה של פתרונות טכנולוגיים פורצי דרך ברמה הלאומית והגלובלית, והיא שואפת למנף אותם לטובת המאמצים הבין-לאומיים להגברת הביטחון במרחב הסייבר הגלובלי ולמימוש הפוטנציאל הגלום בסייבר להתפתחות האנושית.

### יישום המדיניות

מדינת ישראל פועלת בשלושה כיווני פעולה מרכזיים בשיח הבין-לאומי:

1. **שיתופי פעולה להעלאת רמת ההגנה הלאומית והעולמית בסייבר.** תחומי שיתוף הפעולה בהגנה כוללים, בין השאר, שיתוף ידע, סיוע ותיאום בעת התמודדות עם התקפות סייבר וכן הקמת תשתיות חדשניות להגנת הסייבר ולחיזוק אכיפת החוק בסייבר. לצד זאת שואפת מדינת ישראל לקדם שותפויות לפיתוח ולהקמה של תשתיות טכנולוגיות ותהליכים גלובליים, המהווים בסיס למרחב סייבר בטוח.

2. **השתתפות בשיח בזירה הבין-לאומית לשמירה על מרחב הסייבר כמרחב בטוח וחופשי**. מדינת ישראל היא שותפה פעילה בשיח הבין-לאומי לעיצוב מרחב הסייבר כמרחב גלובלי בטוח ויציב.

3. **סיוע למדינות עמיתות בחיזוק יכולתן הלאומית לטובת קידום מרחב גלובלי מוגן ובטוח**. כחלק מהמאמצים הגלובליים לבנות מרחב סייבר בטוח, מדינת ישראל פועלת לסיוע למדינות עמיתות לגיבוש היערכותן להגנה ולסיוע בהקמת תשתיות טכנולוגיות לאומיות, תוך שימוש בידע, בניסיון ובטכנולוגיה הישראליים המצויים בממשל, באקדמיה ובתעשיית הסייבר הישראליים.

# האסטרטגיה הישראלית להגנת הסייבר

# האסטרטגיה הישראלית להגנת הסייבר

**משרד ראש הממשלה** | מערך הסייבר הלאומי

**לפמ**