מערך
הסייבר
הלאומי

אסטרטגיה לאומית להגנה בסייבר

פברואר 2025

גבי פורטנוי
דבר ראש מערך הסייבר הלאומי

מלחמת "חרבות ברזל" הוכיחה ביתר שאת שישראל נמצאת **בחזית הלחימה הדיגיטלית** ושמרחב הסייבר הפך לשדה קרב לכל דבר ועניין. לצד הקרבות בשטח, עמדנו בפני מתקפות סייבר רחבות היקף מצד אויבנו, בדגש על איראן וחיזבאללה.

בעידן שבו המרחב הדיגיטלי הפך לחלק בלתי נפרד מחיי היום יום של מדינות, ארגונים ואזרחים, ישראל ניצבת בחזית ההתמודדות עם איומי סייבר המאתגרים את ביטחונה הלאומי, הכלכלי והחברתי.

המתקפות הרבות כוונו לפגיעה ולשיבוש של שגרת החיים, בהיבטים פיזיים ודיגיטליים, בהתמקד במגזרים השונים, אתרים ממשלתיים, תשתיות מדינה קריטיות, תוך חשיפת פערי הגנה לצד ניסיונות גוברים לפגוע במורל הציבורי ולהשפיע על דעת הקהל בישראל ובעולם.
אך המלחמה גם הצביעה על פתרונות אפקטיביים ברמת הארגון, המגזר, ואף ברמה הלאומית.

עלינו להמשיך לפעול לשיפור ההגנה למול איום הייחוס - בדגש על **תפיסת "כיפת הסייבר"**, המהווה הגנה רב-שכבתית דינמית ופרואקטיבית הנשענת על מפעל מידע רחב ויכולות בינה מלאכותית מתקדמות.

המלחמה אף חיזקה את העובדה **שהציבור** מהווה חלק בלתי נפרד ממערך ההגנה הלאומי.

מתקפות דיוג והחתירה להשגת מידע רגיש הדגישו את הצורך בהגברת **המודעות** בקרב כלל הציבור הרחב. על מנת להצליח להתמודד בצורה מקסימלית עם אירוע רחב היקף זה, אנו נדרשים להשקיע בחינוך לאומי בסייבר.

נוכחנו לדעת כי **טרור** הוא אינו איום מקומי אלא גלובלי ולכן נדרשת **אחדות** מול התוקפים המגיעים מכל פינה בעולם.

אנו נדרשים **לפעול כזרוע מבצעית לכל דבר**, תוך שיתוף פעולה עם קהילת הביטחון, הממשלה, המגזר הפרטי והקהילה הבין-לאומית. ככל שנשכיל לשלב בין **חדשנות, מודעות ציבורית ושיתוף פעולה אזורי ובין-לאומי** נוכל להמשיך להגן על מדינת ישראל מפני איומים עתידיים.

כאומת סטרטאפ מובילה וכמובילה עולמית בתחום החדשנות הטכנולוגית, מדינת ישראל מבינה היטב כי הבטחת ביטחון המרחב הקיברנטי הוא **תנאי הכרחי לשגשוג וחוסן לאומי.**

אסטרטגיה זו נועדה **להציב חזון ברור ויעדים מעשיים להמשך פיתוח חוסן הסייבר של מדינת ישראל**, תוך הגנה על תשתיות קריטיות וחיוניות, הנגשת שירותים וכלי הגנה למשק, מימוש תוכנית לאומית להזדהות דיגיטלית בטוחה, ביסוס מרחב תודעתי מוגן מפני השפעה זרה, ניהול משותף של מאמצי ההגנה, היערכות למניעה והתמודדות עם הפתעה בסייבר, ולבסוף – השקעה בבניין כוח, טכנולוגי ואנושי, איכותי לנוכח אתגרי העתיד.

מימוש חזון זה יבטיח את מעמדה של ישראל כמעצמה טכנולוגית עולמית, המסוגלת להתמודד עם אתגרי ההווה והעתיד בעולם הסייבר.

בברכה,

גבי פורטנוי

ר' מערך הסייבר הלאומי

תוכן עניינים

תוכן עניינים

הקדמה

האסטרטגיה הלאומית המעודכנת להגנה בסייבר גובשה בצילן של מתקפת השבעה באוקטובר ומלחמת "חרבות ברזל" שנכפתה על ישראל. **אירועים אלו מהווים נקודת מפנה אסטרטגית והיסטורית, ומחייבים הערכה מחודשת של תפיסות ההגנה הלאומיות, לרבות במרחב הסייבר**. כחלק מכך, עלינו לברר מה עלולה להיות הפתעה במרחב הסייבר, וכיצד יש להיערך אליה ברמה הלאומית.

התובנות והלקחים שהופקו במהלך המלחמה משתקפים במסמך זה, תוך התאמה למאפייניו הייחודיים של המרחב הדיגיטלי והאתגרים הגלומים בו, הנבדלים מאלו של זירות הלחימה והמרחבים המסורתיים.

בעשורים האחרונים מתחוללת בעולם מהפכה דיגיטלית, ששיאה ב"עידן המידע", המתאפיין בשילוב של נתוני עתק וכלי עיבוד מתקדמים, אשר מביא בהתאם לשינויים בהתנהלות בחיי הפרט, ארגונים וממשלות.

בתוך כך, מרחב הסייבר נמצא בהתפתחות מתמדת, ומרכזיותו בכל תחומי החיים הולכת וגוברת. תופעה זו מתבטאת בשימוש המואץ ביישומים ובמוצרים דיגיטליים, בגידול בהיקף העבודה מרחוק, ובהטמעת טכנולוגיות בינה מלאכותית, המתבססות על כוח מחשוב מתעצם. השילוב בין מרחב הסייבר למרחב הפיזי, ולדרך שבה בני אדם תופסים את המציאות, הולך ומתהדק, באופן שהופך אותו לחלק בלתי נפרד ממארג היסודות המאפשרים חיים מודרניים תקינים.

עם התלות הגוברת של חיי היומיום במרחב המקוון, מתעצמים גם האיומים - הן בהיקף, הן בקצב והן בתחכום. גורמים עוינים הפועלים ממניעים שונים, בעיקרם אידאולוגיים וכלכליים, תוקפים במרחב הסייבר, בהיקף גדל ותוך שימוש בטכניקות מתקדמות.

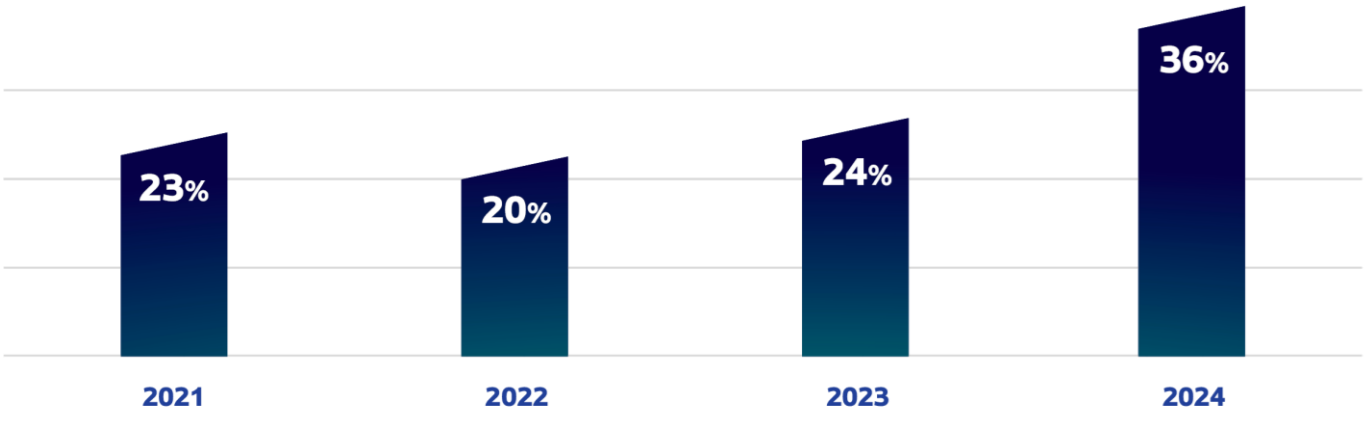
איומי הסייבר על המשק הישראלי מהווים סוגיה של ביטחון לאומי. ישראל הינה אחת המדינות המותקפות ביותר בסייבר בעולם, איומים אלו הגיעו לשיאם בתקופת מלחמת "חרבות ברזל". במהלך המלחמה גדל פי שלושה היקף התקיפות המשמעותיות על מדינת ישראל, והן כללו, בין היתר, תקיפות היברידיות המשלבות

ממדי לחימה נוספים (פיזי, קינטי, תודעתי) בניסיון לאסוף מודיעין ולהשפיע על המאמץ בשדה הקרב. **בלטו הניסיונות להשפיע על המרחב התודעתי** במטרה לערער את האמון במוסדות השלטון, לשחוק את תחושת הביטחון האישי ולסדוק את החוסן החברתי.

בשנים האחרונות חל גידול משמעותי בהיקף הנזקים הכלכליים של תקיפות הסייבר. נזקי תקיפות הסייבר בעולם מוערכים בכ-8 טריליון דולר - סכום שהוא שווה ערך לכלכלה השלישית בעולם. **בישראל, נזקי תקיפות הסייבר מוערכים בכ-12 מיליארד ₪ בשנה**. בנוסף, אירועי סייבר משמעותיים עלולים לפגוע באמון הציבור במרחב הסייבר, ולהניא אזרחים וארגונים מלמצות את השימוש במרחב הדיגיטלי – דבר שעלול לפגוע בצמיחה בטווח הבינוני והארוך.

אל מול האיומים, **תעשיית הסייבר הישראלית ממשיכה לצמוח**, ומהווה קטר צמיחה למשק הישראלי. שיעור ההשקעות בסייבר בשנת 2024 הגיע לשיא של 36% מסך ההשקעות בענף ההיי-טק, עלייה חדה בהשוואה לשנים קודמות (כ-20%-25% מסך ההשקעות), ולמרות האתגרים הביטחוניים. החדשנות והיצירתיות המאפיינות את תעשיית הסייבר הישראלית מהוות את אחד המפתחות החשובים להגנה על המשק כולו מפני האיומים המתגברים.

אחוז ההשקעות בתחום הסייבר מתוך כלל ההשקעות במגזר ההייטק הישראלי:



[1] עיבודי מערך הסייבר הלאומי לנתוני הדו"ח השנתי לשנת 2024 על האקוסיסטם הישראלי בהייטק של Startup Nation Central

הקדמה

לאור החשיבות של ההגנה על מרחב הסייבר, ההתפתחות הטכנולוגית, התעצמות מרחב האיומים, והשינויים בתכליות התקיפה בארץ ובעולם, **גוברת החשיבות של אסטרטגיית הגנה לאומית עדכנית** המתייחסת לכלל המשק ולכלל גורמי ההגנה, וחותרת ליצור מענה רחב יותר, מתוחכם יותר ומשולב יותר.

מסמך זה מציג את האסטרטגיה הלאומית של ישראל להגנת מרחב הסייבר. אסטרטגיה זו נבנית על האסטרטגיה הלאומית משנת 2017 שהגדירה את תפיסת ההגנה מפני תקיפות על מרחב הסייבר הישראלי.

כתיבת מסמך זה ועיצוב התפיסה האסטרטגית העומדת בבסיסו, הובלו על ידי מערך הסייבר הלאומי יחד עם גופי מערכת הביטחון ומשרדי ממשלה העוסקים בנושא, תוך התייעצות עם נציגי ארגונים במשק, מומחים בתחום הסייבר באקדמיה ובתעשייה, ולמידה מאסטרטגיות של מדינות מובילות בסייבר. זאת, מתוך הבנה עמוקה שכדי להגן בסייבר, נדרשת פעולה משותפת - ברמה הלאומית והבין-לאומית כאחד.

בהתאם, אסטרטגיה זו מתואמת עם אסטרטגיות דיגיטאליות לאומיות נוספות מתוך ראייה הוליסטית של המרחב הדיגיטלי.

המסמך מציג את תפיסת מרחב הסייבר, את החזון הלאומי למרחב, את העקרונות למימושו, את היעדים המוגדרים להתארגנות הממשלתית והלאומית להגנה על המשק, את הכיוונים העיקריים להגנה ולבניין כוח במגזרים השונים, ואת שיתופי הפעולה הנדרשים לכך.

ממסמך אסטרטגיה זה תיגזר תוכנית יישום לאומית המכוונת לאופק של שלוש השנים הקרובות, קרי, עד 2028. תוכנית היישום תגדיר את אופן המימוש של היעדים האסטרטגיים לכדי תוכנית פעולה, ותמומש באמצעות צוות לאומי המשלב גורמי ממשלה, גופי ביטחון, גורמים מתעשיית הסייבר ומומחים נוספים.

לאור השינויים התכופים במרחב הסייבר, ראוי יהיה לעדכן האסטרטגיה באופן תכוף וככל שתסתמנה תפניות אסטרטגיות חדשות.

מאפיינים

מרחב הסייבר ייחודי ונבדל מהותית במאפייניו ביחס למרחבים אחרים. בהיותו מרחב וירטואלי גלובאלי, הוא חוצה גבולות פיזיים, ומאפשר תקשורת ותנועה של מידע ללא מגבלות מרחק או זמן. המהירות בה עובר המידע במרחב מאפשרת יצירת אפקט מידי, הן לשימושים מועילים והן להפצת תקיפות סייבר וגרימת נזק. בנוסף, מאפייני מרחב הסייבר מאפשרים לתוקפים לפעול בו באופן אנונימי ומרוחק יחסית, עובדה המקשה על זיהוי, חקירה וביצוע פעולות אכיפה כלפי תוקפים.

עוד יש לציין, כי המשתמשים ובעלי הנכסים הדיגיטליים במרחב הסייבר אינם שולטים בכל שלבי הייצור והיבטי התפעול של היישומים והמוצרים הדיגיטליים, עובדה המדגישה את הצורך בהסדרת האחריות ברמה המדינתית.

הקשרים המסועפים בין מערכות מחשוב ורשתות מקלים על נגישות התוקפים באמצעות תקיפת שרשראות האספקה המורכבות מגופים, ארגונים ואנשים המחוברים זה לזה, היוצרים יחד רשת מורכבת של תלות הדדית, שבה פגיעה בנקודה אחת עלולה להתפשט ולהשפיע על מערכות רבות אחרות.

הממשקים המתהדקים בין מרחב הסייבר לבין העולם הפיזי, ובין האדם למכונה מתבטאים בשליטה מקוונת על הסביבה, החל מבתים חכמים, המשך ברכבים אוטונומיים, ועד למערכות ייצור ושירותים חיוניים. היבט זה מגדיל את הסיכון מפני פגיעה ברציפות התפקוד במשק, למשל באמצעות פגיעה בתשתיות קריטיות וחיוניות כגון רשתות חשמל, מערכות מים, בנקים ובתי חולים. כניסתן של טכנולוגיות מפציעות, ובפרט הבינה המלאכותית היוצרת (Generative Artificial Intelligence) המבוססת על מודלי שפה גדולים (LLM), שהופכות לנגישות לציבור הרחב, מקלה על תוקפים לשכלל את יכולות התקיפה השונות.

מורכבות נוספת של מרחב הסייבר טמונה בעובדה שמדובר ב"מגרש משחקים" משותף, בו פועלים זה לצד זה משתמשים לגיטימיים לצד שחקנים זדוניים המשתמשים באותן התשתיות.

בנוסף, הגבולות בין היריבים במרחב מיטשטשים. כך, למשל, ארגוני פשיעת סייבר מספקים שירותי תקיפה למדינות סוררות ולארגוני טרור, ומדינות משתמשות בתקיפות סייבר המאפיינות ארגוני פשיעה לתכלית אידאולוגית או כלכלית. טשטוש גבולות זה מצריך התייחסות ייעודית במענה.

קצב השינויים במרחב גבוה מאוד ביחס למרחבים אחרים, והוא ממשיך להתפשט ולהתרחב הן מבחינת היקף מערכות ומאגרי מידע שיש להגן עליהן, והן מבחינת העמקת שילובן במרחבים האחרים.

כמרחב חדש יחסית, מערכת החוקים הפנימית ונורמות ההתנהגות של מדינות וארגונים במרחב הדיגיטלי עדיין בשלבי עיצוב והתפתחות. היעדר כללים ברורים והקושי בגיבוש נורמות בין-לאומיות, בין היתר, מאתגרים יצירתה של **הרתעה אפקטיבית מול תוקפים.**

<u>מאפייניה הייחודיים של ישראל בסייבר</u>

מדינת ישראל היא מהמדינות הראשונות שזיהו את הצורך בהעלאת רמת ההגנה במרחב הסייבר בכלל המשק, וכנגזרת מכך, את הצורך בביסוס מענה לאומי לאיומי הסייבר. מטה הסייבר הלאומי שהוקם בשנת 2012 והתפתח למערך הסייבר הלאומי, פועל מתוקף מספר החלטות ממשלה, יחד עם מארג מדינתי שלם של גופים השוקדים על הגנת מרחב הסייבר הישראלי, להסדרת ההגנה על המשק, כמו גם לפיתוח ומיצוב ישראל כמדינה מובילה בסייבר.

ישראל ידועה כמובילה עולמית בחדשנות טכנולוגית. בתוך תעשיית ההי-טק המפותחת, צמחה תעשיית הגנת סייבר מרשימה בחדשנותה ובהיקפה. תעשייה זו מתבססת, בין היתר, על הון אנושי מנוסה ומיומן בסייבר ועל מצוינות אקדמית המתבטאים יחדיו באקו-סיסטם טכנולוגי פורה, המשלב בינה מלאכותית וסייבר, בהיקף השקעות השני בגודלו בעולם.

מאפיינים נוספים המקנים למדינת ישראל יתרון יחסי בהגנת סייבר הם רמת הקישוריות הגבוהה בין הגורמים השונים באקו-סיסטם הישראלי והמחויבות הלאומית הקושרת חלקים במדינה - בפרט מול איומים לאומיים. אלו, מאפשרים לרתום מומחים וחברות מהמגזר הפרטי לפיתוח פתרונות הגנה חדשניים, ולמתן סיוע הדדי למשק. המחויבות החברתית הגבוהה באה לידי ביטוי במהלך מלחמת "חרבות ברזל", עת חברות רבות במשק התנדבו לסייע בהגנה על עסקים קטנים מפני תקיפות סייבר.

מאידך, כמדינה קטנה בגודל השוק, מידת ההשפעה של ישראל לבדה על מרחב ההסדרה הבין-לאומי מוגבלת יחסית, וכנגזרת מכך, עולה הצורך בפיתוח קואליציות בין-לאומיות והשקעה בפורומים גלובליים מקצועיים.

למרות רמת הדיגיטציה הגבוהה במשק, נראה כי עדיין קיים פער במודעות לאיומי סייבר, **בעיקר בקרב הציבור הרחב והעסקים הקטנים והבינוניים, אשר מהווים מטרה לתוקפים, הן כקורבן ישיר והן כאמצעי לתקיפת ארגונים אחרים.**

במישור הנורמטיבי, קיימות הנחיות הגנה במגוון מדרגים שהתפתחו באופן אבולוציוני, אשר הובילו לשונות בחובות ובסמכויות בין המגזרים במשק. כך, למשל, תשתיות מדינה קריטיות (להלן: "תמ"ק") מונחות, בהקשרי הגנת סייבר, מכוח החוק להסדרת הביטחון בגופים ציבוריים, תשנ"ח 1998 (להלן: "החוק להסדרת הביטחון"). החוק להגנת הפרטיות, תשמ"א-1981, ובפרט לאור הרחבת סמכויות האכיפה שתוקנה השנה, מסדיר בכלל המשק חובות שחלות על המחזיקים במאגרי מידע אישי לתכלית של הגנת הפרטיות. בנוסף, חוק המחשבים, תשנ"ה-1995, קובע עבירות פליליות ועוולות נזיקיות.

מספר החלטות ממשלה בתחום הסייבר התקבלו בעשור האחרון, ביניהן ההחלטות להקמת מערך הסייבר הלאומי וקביעת תפקידיו, וההחלטה בעניין היחידה להגנת הסייבר בממשלה במערך הדיגיטל (יה"ב).

גופים הכפופים לרגולציה מגזרית נדרשים לפעול בהתאם להנחיות של רגולטורים שונים המעוגנות בנהלים, הוראות מפקחים, חוזרי מנכ"ל ומקורות נורמטיביים נוספים.

כפועל יוצא, קיים פער ברגולציה להגנת הסייבר בארגונים חיוניים לתפקוד התקין של המדינה, הכלכלה והחברה, ומסמך זה יכוון לסגירתו, בדומה לנעשה במדינות מפותחות.

ניתוח האיום על ישראל בסייבר

ישראל הנה אחת המדינות המותקפות ביותר בסייבר. מקורות האיום על מדינת ישראל במרחב זה כוללים **איומים מעצמתיים ומדינתיים**, בדגש על איראן, ואיומים מצד שלוחות הטרור שלה, המכוונים לפגע בביטחון מדינת ישראל, לאסוף מידע רגיש, לזרוע פחד בקרב אזרחיה, להעמיק שסעים חברתיים ולפגוע בלגיטימציה של ישראל, בין היתר על-ידי השפעה על דעת הקהל בארץ ובעולם. כמדינה דמוקרטית וכחלק מגוש מדינות המערב, ישראל מהווה יעד תקיפה לגורמים עוינים המנצלים את מרחב הסייבר כזירה לעימותים, תחרות והשפעה.

איום **פשיעת הסייבר**, כתופעה גלובאלית שצומחת במהירות, מהווה אחד האתגרים המשמעותיים גם לישראל, ובמיוחד האתגר המתעצם של מתקפות הכופרה (Ransomware) לסוגיהן. בנוסף, קיים איום מצד "האקטיביסטים" הפועלים ממניעים אידאולוגיים לשיבוש הפעילות השגרתית והתקינה של המשק הישראלי.

אתגר משמעותי נוסף טמון ב**סיכונים פנימיים**, במסגרתם גורמים בעלי גישה לגיטימית למידע ולמערכות בארגון כגון עובדים, ספקי שירות וכו', עלולים לגרום לפגיעה בו. סיכון זה יכול להתממש בשוגג, בהטעיה או ברשלנות, למשל עקב הפרת כללי אבטחה, או להבדיל על ידי גניבת נתונים, חבלה או ריגול.

במהלך מלחמת "חרבות ברזל", הוכפל מספר קבוצות התקיפה כנגד ישראל, ונצפו ניסיונות עצימים, בעיקר מצד איראן ושלוחות הטרור שלה לפגוע בתשתיות קריטיות. במהלך המלחמה נצפה גם גידול משמעותי בתקיפות על האזרחים והעסקים הקטנים, כמו גם בתקיפות דרך שרשראות אספקה כווקטור חדירה.

מאמצי ההשפעה הזרה על התודעה התגברו בהיקף חסר תקדים, והפכו לאיום משמעותי על הביטחון הלאומי והחוסן החברתי. מטרת תקיפות אלו הינה לערער את האמון במוסדות השלטון, לשחוק את תחושת הביטחון האישי תוך הפעלת טרור-סייבר, להעמיק את השסע החברתי ולפגוע במרקם הקהילתי.

מגמת התפוצה של כלי תקיפה מתקדמים, הנובעת, בין היתר, מהידוק הקשר בין יריבים, אויבים ופושעים, משמעה הגדלת הסיכון מתקיפות מתקדמות ומהפתעות משמעותיות. היכולת לנצל חולשות אבטחה בקלות ובמהירות חסרת תקדים הופכת את נוף האיומים למורכב עוד יותר. הדבר מחייב עדכון תפיסת האיום והעמקת ההיכרות עם יכולות התקיפה המתפתחות בקרב מנעד רחב יותר של אויבים ויריבי סייבר, על מנת להיערך לאיומים הקרבים.

משטח התקיפה של ישראל הולך וגדל, בין היתר בשל הטמעת מערכות תקשורת חדישות בעלות רוחב פס גדול יותר, שיבוצם של מכשירי IoT ויישומים בממשק עם המרחב הפיזי, המעבר לענן, והטמעת טכנולוגיית הבינה המלאכותית. כל אלו מגדילים משמעותית את הסיכון לתקיפות סייבר ואת פוטנציאל הנזק.

בשל השוני המהותי של מרחב הסייבר מהמרחבים האחרים והשינויים שחלו בו, נדרשות פרדיגמות חדשניות בבואנו לגבש מענה הולם לאתגר דינאמי זה.

חזון לאומי

מרחב דיגיטלי אמין, זמין ובטוח
המאפשר את היתרונות של
עולם משגשג ומתקדם

עקרונות למימוש

הגנה משותפת

הגנה אקטיבית

הגנה שממנפת חדשנות
ומצוינות טכנולוגית

חוסן והיערכות
למשברים

נקודת המוצא הינה ש**הגנה על מרחב הסייבר היא מרכיב מרכזי והכרחי לביטחונה הלאומי ולשגשוגה של מדינת ישראל**. לאור התפתחות המרחב והאיומים, והעמקת הממשקים עם מרחבים אחרים, על החזון לבטא ראייה רחבה יותר של כלל המרחב הדיגיטלי. על רקע הבנה זו, ישראל מציבה חזון לאומי רחב וברור:

מרחב דיגיטלי אמין, זמין ובטוח המאפשר
את היתרונות של עולם משגשג ומתקדם

החזון נשען על שלושה מרכיבים מרכזיים המשלימים זה את זה: **אמינות** – היכולת לסמוך על אותנטיות המידע, התוכן והזהויות הפועלות במרחב; **זמינות** – המבטיחה נגישות רציפה למרחב המקוון ולשירותים הדיגיטליים עבור כל שכבות האוכלוסייה והארגונים; **בטיחות וביטחון (Safety and Security)** – המתייחסים להגנה מקיפה מפני איומי סייבר על תפקוד המשק, ובכלל זה על הפעולות המתבצעות במרחב הדיגיטלי, על הנכסים הדיגיטליים, ועל פרטיות המשתמשים וביטחונם, מהאזרח ועד לרמה הלאומית.

שילוב שלושת המרכיבים הללו יאפשר למדינת ישראל ליהנות מהיתרונות הרבים של העידן הדיגיטלי ובראשם צמיחה כלכלית, חדשנות טכנולוגית, ושיפור באיכות החיים עבור אזרחיה.

כאמור, החזון הלאומי מכוון למרחב דיגיטלי כמושג רחב, המשתרע מעבר למרחב הסייבר, ומכיל את כלל היבטי החיים הווירטואליים וההשפעות הרחבות של הטכנולוגיה על החברה והתרבות.

מימוש החזון יתבסס על מספר עקרונות מפתח הנגזרים מתפיסת המרחב ומאפייניה הייחודיים של ישראל. עקרונות אלו יעמדו בבסיס הפעולות הלאומיות להגנה בסייבר וישתקפו, ברמות השונות בכל אחד מנדבכי האסטרטגיה.

<u>הגנה משותפת</u>

מאפייניה הייחודיים של משימת ההגנה ומורכבותה מובילים לכך שאין גורם בודד שיכול לשאת בנטל המטלה לבדו. בהתאם לכך, העיקרון המוביל השזור כחוט השני באסטרטגיה הוא - <u>הגנה ביחד</u>.

לממשלה תפקיד מרכזי בהובלת ההגנה בסייבר במשק ובהסדרתה. מעיקרון זה נגזר גם הצורך בהידוק שיתופי הפעולה בין גופי הממשלה העוסקים בהגנת מרחב הסייבר באופן שממנף את יתרונותיהם היחסיים ומאפשר מיצוי סמכויות וסנכרון מלא מתוך ראייה הוליסטית של המרחב. לצד זאת, חשוב לזכור כי מדובר **במאמץ של כלל החברה** (Whole of society approach), קרי, משימה משותפת לממשלה, מערכת הביטחון, המגזר הפרטי והאזרחים, לצד מדינות אחרות וחברות רב-לאומיות, בהתאם לערכים דמוקרטיים ולנורמות בין-לאומיות מקובלות.

<u>הגנה הממנפת חדשנות ומצוינות טכנולוגית</u>

עיקרון זה מביא לידי ביטוי את היתרון היחסי של האקו-סיסטם הטכנולוגי בישראל, כמדינה חדשנית וכמובילה טכנולוגית. שיפור ההגנה על המשק ימומש, בין השאר באמצעות הטמעת תפיסות הגנה מבוססות אוטומציה ובינה מלאכותית (כגון "כיפת הסייבר") והנגשת פתרונות הגנה מתקדמים להשגת יעילות מבצעית.

<u>הגנה אקטיבית</u>

עיקרון זה חותר ליישום גישה פרו-אקטיבית בהגנה בסייבר, לטובת גילוי מקדים של כוונות לתקיפה, חיסון מקדים של המשק, ושיבוש מונע של האיום באופן אקטיבי.

<u>חוסן והיערכות למשברים</u>

עיקרון זה נובע מנקודת מוצא לפיה משברים דיגיטליים יתרחשו, ולפיכך, תפיסת ההגנה הלאומית חייבת להתבסס גם על בניית משק חסין יותר ועל יכולת התאוששות מהירה כמרכיב מרכזי בתפיסת ההגנה. אירועי השבעה באוקטובר המחישו את איום ההפתעה האסטרטגית – המחייב היערכות להפתעה גם בסייבר.

הגשמת החזון תתאפשר באמצעות מערך הגנה רחב המסתגל למציאות המשתנה, ופרישתו על פני מספר מישורי עשייה, המפורטים בשלושת נדבכי האסטרטגיה:

נדבך ראשון: הגנה במרחב הלאומי - בו יתוארו מאמצי הגנה על נכסי המדינה השונים, תוך שימת דגש על יצירת מענה מותאם, המתחשב במאפייניהם הייחודיים של הנכסים והשפעתם זה על זה. רובד זה מחולק לשלושה חלקים: אזרחים ועסקים בטוחים יותר (פרק 1); שירותים חיוניים חסינים יותר (פרק 2); והגנה מרחבית (פרק 3), שתתמקד באבטחת המרחב הדיגיטלי המשותף מתוך ראייה חוצת-מגזרים.

נדבך שני: ההתארגנות המדינתית - בו תתואר תפיסת ההפעלה הקונקרטית שמנחה את מערכי ההגנה בסייבר של גופים מדינתיים. נדבך זה מחולק לשלושה חלקים: הגנה משותפת (פרק 4), הכולל את מערך ההגנה הממשלתי ושיתופי הפעולה הנדרשים עם המשק לטובת התהליך המבצעי; הפתעה בסייבר ומוכנות לחירום דיגיטלי (פרק 5); והסרת איומים (פרק 6).

נדבך שלישי: פיתוח שותפויות אסטרטגיות ויכולות עתידיות – בו מפורטים המאמצים התומכים בפיתוח היכולות העתידיות בתחום הסייבר. נדבך זה מחולק לשני חלקים: פיתוח תשתיות לשיתופי פעולה ושותפויות (פרק 7); והשקעה בבניין כוח איכותי לנוכח אתגרי העתיד (פרק 8).

נדבך ראשון:

הגנה במרחב הלאומי

המאמץ להגן על מרחב הסייבר הלאומי נועד למנוע פגיעה במשק ובביטחון הלאומי של מדינת ישראל. מטרה זו תוכל להתממש באמצעות סגירת פערים דיגיטליים, נורמטיביים והתנהגותיים, בדגש על מרכיבי המשק שאינם מוגנים ברמה מספקת בסייבר.

מערך הסייבר הלאומי

בנדבך זה יתוארו מאמצי ההגנה הלאומיים בהתבסס על שלושה רכיבים לקידום ההגנה על המרחב באופן כולל, כך שכל מרכיב יקבל מענה ייעודי ומותאם לו. הרכיב הראשון הינו **אזרחים ועסקים קטנים ובינוניים** המהווים את השכבה הגדולה והפגיעה ביותר במשק הישראלי, הן כמטרה בפני עצמה והן כאמצעי חדירה לארגונים אחרים (כשרשרת אספקה). רכיב שני הינו **שירותים חיוניים**, הכולל בתוכו תשתיות קריטיות וארגונים המספקים שירותים נחוצים, אשר פגיעה בהם עלולה להסב נזק משמעותי לתפקודה ולביטחונה של מדינת ישראל ותושביה. הרכיב השלישי הינו **הגנה מרחבית**, המתייחס למרחב הסייבר הציבורי המשותף. ההגנה תתמקד במענה לאיומים הנובעים מהממשק שבין המרחב הווירטואלי למרחב הפיזי והתודעתי, בחיזוק האבטחה של תשתיות המרחב המקוון, הגנה על נכסי המידע המדינתיים, והתמודדות עם מבצעי השפעה זרה על התודעה.

1. <u>פרק ראשון: אזרחים ועסקים בטוחים יותר</u>

הרחבת היקף תמיכת המדינה לשיפור ההגנה בקרב האזרחים והעסקים

1.1 יעד ראשון: העלאת מודעות ואוריינות למול איומי סייבר

תנאי בסיסי למניעת תקיפות סייבר ולמזעור הנזקים הנגרמים מהן הוא קיום רמת מודעות גבוהה לאיומים ולאופן התממשותם, ונקיטת התנהגות בטוחה וזהירה ברשת. מדינת ישראל תשקיע בחיזוק המודעות לאיומי הסייבר, לאמצעים הקיימים להתגוננות מפניהם, ולאפשרויות התגובה, במטרה ליצור שינוי תרבותי וחברתי שיעודד התנהגות נבונה במרחב הסייבר מצד האזרחים והארגונים בישראל.

העלאת המודעות הציבורית תעשה באמצעות פעילות נרחבת של הסברה לציבור, באופן שוטף ובתגובה לאירועים נקודתיים; פרסום אזהרות והמלצות על אודות חולשות ואיומי סייבר המסכנים את המשק; הרחבת מערך הקורסים והתכנים הפדגוגיים המונגשים לציבור; והנגשת מידע רלוונטי על כלי הגנה ושירותי סייבר. הגברת המודעות תיעשה בהתאם לאוכלוסיות היעד הרלוונטיות, ובדגש על הגיל הרך, קהילות עסקים ואוכלוסיות בעלות אוריינות דיגיטלית נמוכה. יוזמות אלו תתבססנה, ככל שניתן, על מסגרות חינוך קיימות, יוזמות חברתיות, עמותות המגזר השלישי, רשויות מקומיות, לשכות ואיגודים עסקיים ומקצועיים רלוונטיים, ובעידוד הממשלה.

1.2 יעד שני : הנגשת שירותים וכלי הגנה למשק

כדי לסייע במענה לתקיפות סייבר, מפעיל מערך הסייבר את המרכז הארצי לניהול אירועי סייבר (ה-CERT הלאומי) אשר נועד לסייע לארגונים להתמודד עם אירועי סייבר במרחב האזרחי של מדינת ישראל. המרכז מפעיל קו סיוע - מוקד טלפוני 119, המשמש כתובת ומענה עבור הציבור לדיווח מידי בעת חשד לתקיפת סייבר. המוקד מאויש 24 שעות ביממה ומעניק מענה ראשוני לאזרח או לארגון על פי רמת החומרה של התקיפה, פוטנציאל הנזק וכלל מאפייני האירוע. בהתאם, מספק המוקד הכוונה לטיפול באירוע והנחיות לחיזוק רמת ההגנה.

כמות הדיווחים שהתקבלו במרכז המבצעי 119 לפי שנים:

לטובת שיפור והרחבת המענה לציבור, תוקם מערכת לאומית אחודה לדיווח וולונטרי על כלל סוגי מתקפות סייבר, שתונגש באופן מקוון וידידותי למשתמש, תוך הקפדה על שמירת הפרטיות. מערכת זו תסייע בהעלאת שיעורי הדיווח על תקיפות סייבר מכלל המשק ותתרום להעשרת תמונת המצב הלאומית.

בנוסף, מדינת ישראל תמנף את עוצמותיה הטכנולוגיות לטובת שיפור ההגנה במגזר הפרטי, זאת באמצעות הנגשה מדורגת של כלים ושירותי הגנת סייבר בסיסיים לסריקה ואיתור חולשות ומתן התרעה מקדימה למשק, בין היתר באמצעות פורטל לאומי לשירות המשק.

1.3 יעד שלישי: עידוד והמרצת עסקים להעלות את רמת ההגנה בסייבר

מדינת ישראל תפעל להניע את המגזר הפרטי והמרחב האזרחי לחזק את רמת ההגנה בסייבר באופן וולונטרי. במסגרת זו, מדינת ישראל תעשה שימוש, בין היתר, בכלים הבאים:

א. שכלול שוק ביטוח הסייבר - ביטוח סיכוני סייבר, מלבד היותו כלי לשיפוי הנזק השיורי, מהווה גם גורם המעודד העלאת חוסן באופן רוחבי, באמצעות הצבת דרישות מקדימות מצד חברות הביטוח, בדומה לביטוחי רכב או נדל"ן. ישראל תקדם את המודעות בקרב עסקים קטנים ובינוניים ליתרונות ביטוח הסייבר, ותקדם אוריינות בקרב שוק הביטוח ככלי להעלאת חוסן.

ב. עידוד ארגונים לצריכת שירותי ומוצרי סייבר בדומה לנעשה במדינות מפותחות אחרות, תוך בחינת הענקת תמריצים לעסקים ומתן ידע רלוונטי, בין היתר על ידי : בחינת הקמת מאגר נותני שירותים אחראיים בתחום הגנת הסייבר (מאגר ספקים); בחינת אסדרת מקצועות בתחום הסייבר; וקידום הענקת תו חוסן ממשלתי לחברות העומדות בדרישות הגנת סייבר ראויה ועוד.

1.4 יעד רביעי: גיבוש ומימוש תוכנית לאומית להזדהות דיגיטלית בטוחה

הזדהות דיגיטלית היא שיטה המאפשרת לזהות אדם באופן ייחודי באמצעות שילוב מאפיינים ותכונות דיגיטליות המבחינים אותו מאנשים אחרים. כדי להוכיח את זהותם של משתמשים, ניתן להשתמש בפרטים מזהים או בתכונות ומזהים ביומטריים שונים.

הזדהות דיגיטלית בטוחה הינה מרכיב משמעותי בביטחון במרחב הדיגיטלי, שכן הוא מאפשר לאזרחים ולארגונים להתחבר ולצרוך שירותים דיגיטליים באופן אמין ובטוח, הן כמקבלי שירות מהממשלה, והן כמשתמשים מזוהים מול ספקים וחברות במשק.

גניבת זהות דיגיטלית מהווה כיום את נתיב הפריצה השכיח ביותר במרחב הסייבר. על פי פרסומים, כחמישית מתקיפות הסייבר שדווחו בעולם קשורות בגניבת זהות או בשימוש בזהות וירטואלית בדויה. השימוש הגובר ביכולות זיוף מתקדמות (deep fake) מעצים את הסיכון מתופעה זו. משכך, הזדהות דיגיטלית אמינה יכולה למנוע תופעות בלתי-רצויות, כגון שימוש בזהויות בדויות או גנובות, הפצת חדשות כזב, ביצוע מאמצי השפעה על אזרחי ישראל, הונאות, ואף טרור ופשע מאורגן.

ישראל תפעל לגיבוש מדיניות לאומית סדורה שתגדיר מסגרת נורמטיבית להבטחת הזהות הדיגיטלית של משתמשים וארגונים, כשהקו המנחה הוא ראיית המשתמש במרכז. מדיניות זו תברר את תפקיד הממשלה בהתייחס לסטנדרט ולביסוס מנגנונים לאומיים לזיהוי דיגיטלי בשוק הפרטי, מתוך רצון לעודד ולמקסם את השירותים המקוונים. המדיניות תתייחס לשמירה על הפרטיות, נגישות השימוש לכלל האוכלוסייה, ולתאימות כלל-משקית (Inter-operability) של אמצעי הזיהוי. המדיניות תתייחס לצורך לעדכן את האמצעים בהתאם להתפתחויות הטכנולוגיות של אמצעי הזיהוי, ולשינויים בשיטות התקיפה מנגד.

2. פרק שני: שירותים חיוניים בטוחים יותר

הגנה מתקדמת על התשתיות הקריטיות והשירותים החיוניים להבטחת תפקוד המשק, לבטחון המדינה ורווחת תושביה

2.1 יעד ראשון: שימור אפס נזקים משמעותיים לתשתיות מדינה קריטיות

ישראל נוקטת בגישה ייחודית, לפיה במסגרת החוק להסדרת הביטחון נקבעה רשימה של גופים במשק הישראלי המהווים תשתיות מדינה קריטיות הנדרשים להגנת סייבר מיוחדת, מתוקף חשיבותם להמשך תפקודו התקין של המשק הישראלי. השב"כ ומערך הסייבר הלאומי מלווים ומנחים את התשתיות הקריטיות על בסיס מתודולוגיה ייחודית, באופן אשר עד כה מניב את התוצאות הרצויות. מדינת ישראל תמשיך לתת דגש לאומי ייעודי להגנה על גופים אלו.

לנוכח האיומים המתפתחים, תעודכן מתודולוגיית האבטחה בגופי התמ"ק והתעשיות הביטחוניות בראייה מרחיבה, הצופה פני איומים מתפתחים, ובאופן שיטמיע את עקרונות המוכנות להפתעה, גיוון אמצעי אבטחה, סריקה וציד מתקדם של תוקפים, ויצירת תמונת מצב בזמן אמת של רמת ההגנה בגופים אלו. כמו כן, יושם דגש על הגנה קפדנית של שרשראות האספקה של גופי התמ"ק במטרה לצמצם את משטח התקיפה שלהם.

2.2 יעד שני: הבטחת רמת הגנה בסיסית בארגונים חיוניים

ארגונים רבים במשק מספקים שירותים חיוניים לציבור הרחב ולעסקים רבים. פגיעה בהם עלולה להוביל לפגיעה בתפקוד התקין של המדינה, החברה והמשק הישראלים. בשונה מהתשתיות הקריטיות המוסדרות בחוק להסדרת הביטחון, שכבה זו של ארגונים אינה מאוסדרת דיה בהקשרי הגנת סייבר כיום.

בעוד שחלק מהגופים המאסדרים הטילו חובות הגנה על ארגונים אלה מכוח סמכויות אסדרה מגזריות, הרי שבחלק מהמגזרים קיימים פערים בסמכויות ובאכיפה בהקשרי הגנת סייבר.

בדומה לנעשה במדינות מפותחות בעולם, בכוונת הממשלה לפעול ולחוקק חוק ייעודי אשר יסדיר את מאמצי ההגנה במרחב הסייבר הלאומי. בתוך כך, יוגדר בחוק מיהו 'ארגון חיוני' בתחום הסייבר, ואת החובות החלות על ארגונים אלו - ובראשן החובה לעמוד ברמת הגנה בסיסית, והחובה לדווח על תקיפות סייבר שיוגדרו. בנוסף, החקיקה הלאומית המקודמת תסדיר את סמכויות הרגולטורים המגזריים, כך שיהיו מצוידים בכלים המתאימים לפקח ולאכוף את יישום הוראות החוק על ידי הארגונים החיוניים.

2.3 יעד שלישי: הגנה על התשתיות הדיגיטליות בממשלה ובגופי הביטחון

תשתיות המחשוב הממשלתיות מקבלות מענה הגנה בסייבר ממערך הדיגיטל הלאומי, וזאת באמצעות היחידה להגנת הסייבר בממשלה (להלן: "יה"ב"), המונחית על ידי מערך הסייבר הלאומי ובשיתוף גופי הממשלה עצמם. כל אלו פועלים, על פי תפקידיהם, להטמעת תקני אבטחה, להנחיית העובדים ולבקרה.

מאמצי ההגנה על התשתיות הממשלתיות יכוונו להשגת רמת אבטחה הולמת ואיכותית של מערכות המחשוב הממשלתיות, באמצעות הון אנושי טכנולוגי מיומן ועדכני שיוביל את מאמצי ההגנה ברמה הממשלתית, לצד יכולת ביצוע רכש יעיל ומהיר של אמצעי הגנת סייבר כצורך מבצעי.

ממשלת ישראל תטמיע דרישות הגנת סייבר מתאימות במכרזים ובחוזי הרכש של המוצרים והשירותים הנרכשים על ידה, החל משלב הייזום והתכנון, ובכך תוטמע ותחלחל באופן רחב יותר הגנת הסייבר על מוצרים ושירותים, לאורך שרשרת האספקה לממשלה.

משרדי הממשלה החלו בתהליך מדורג של הגירה מתשתיות המחשוב הממשלתיות לענן ציבורי הממוקם בארץ (פרויקט "נימבוס"), מתוך כוונה לשמר ריבונות על המידע, לייעל את תהליכי העבודה והשירותים למשק, ולצורך שיפור רמת ההגנה בסייבר.

מדינת ישראל תפעל לשלב פתרונות הגנת סייבר לשימוש בענן הציבורי, לפתח כוח אדם מיומן, ולהטמיע באופן מאובטח כלי בינה מלאכותית בקרב משרדי הממשלה, במטרה להגביר את רמת האבטחה בתשתיות המחשוב הממשלתיות ולנצל את יתרונות הענן בצורה מיטבית.

לצד משרדי הממשלה, גופי הביטחון, הפועלים להגן על ביטחון המדינה ואזרחיה, מפעילים תשתיות מחשב מסווגות אשר דרושות לשם קיום פעילותם המבצעית והשוטפת. באופן טבעי, תשתיות אלו נדרשות לרמת האבטחה הגבוהה ביותר, לשמירה על ביטחון המדינה, למניעת שיבוש וזליגת סוד ולהבטחת זמינות מרבית. הממונה על הביטחון במערכת הביטחון (מלמ"ב) מנחה את משרד הביטחון והתעשייה הביטחונית בתחום זה. גופי הביטחון ימשיכו לפעול לחיזוק רמת ההגנה הגבוהה שלהם ושל שרשראות האספקה שלהם למול האיום המתפתח.

3. <u>פרק שלישי: הגנה מרחבית</u>

הגנה על המרחב הדיגיטאלי המשותף
לשמירת סביבה מקוונת בטוחה המאפשרת שגשוג

3.1 יעד ראשון: הבטחת הזמינות של המרחב המקוון

המרחב הדיגיטלי הינו חלק בלתי נפרד ממארג היסודות המאפשרים חיים מודרניים, כלכלה תקינה ורווחה.

הגנה על מרחב זה ראשיתה בהבטחת עצם קיומו וזמינותו של המרחב מפני סוגים שונים של איומים כגון מתקפות סייבר, פגיעות פיזיות, תקלות טכניות, טעויות אנוש וכיו"ב.

ישראל תעריך ותמפה את גורמי הסיכון לרשת האינטרנט, ותבטיח את רציפות השירות באמצעות ביסוס ההגנה מחד גיסא, ופיתוח יתירות במגוון שירותים מאידך גיסא. נוכח אופיו הגלובלי והמבוזר של האינטרנט, צעדים אלה דורשים שיתוף פעולה הדוק בין המגזר הציבורי והפרטי, ובין ישראל לשותפים בין-לאומיים.

3.2 יעד שני: העלאת חוסן רחבה באמצעות חיזוק 'רשת אספקה טכנולוגית'

המונח "רשת אספקה טכנולוגית" מבטא ראייה משקית רחבה וחוצת-מגזרים, המדגישה את השפעתם הייחודית של הצמתים המרכזיים באספקת שירותי טכנולוגיית מידע ותקשורת (מגזר ICT) על אבטחת המרחב המקוון. אלו כוללים את התשתיות, השירותים והמוצרים הדיגיטליים בהם תלויים רבים במשק לצורך ניהול שגרת עסקיהם.

לגופים ברשת האספקה הטכנולוגית משקל מיוחד הן בשל התלות בשירותים ובמוצרים שהם מספקים, הן לאור פריסתם הנרחבת במשק, והן בשל העובדה כי הם משמשים ווקטור כניסה לחברות אותן הם משרתים. בד בבד, נגישות רחבה זו טומנת בחובה פוטנציאל לחיזוק חוסן רוחבי בהשקעה ממוקדת ויעילה.

מדינת ישראל תפעל להבטיח מיפוי עדכני של הגופים המהווים חלק מרשת אספקה טכנולוגית זו, ולהגברת רמת הגנת הסייבר בהם.

בדומה למגמות בעולם, מדינת ישראל תפעל לחיזוק האבטחה של שירותים ומוצרים דיגיטליים, באמצעות הסטת חלק מהנטל להפחתת סיכוני הסייבר ממשתמשי הקצה אל עבר בעלי היתרון היחסי – קרי, מפעילי המערכות וספקי השירותים והמוצרים הדיגיטליים. לשם כך, יבחנו צעדי מדיניות מגוונים אשר יאפשרו אספקת מוצרים ושירותים דיגיטליים בטוחים יותר לשימוש, תוך הימנעות מהגבלה מיותרת של חדשנות טכנולוגית.

בהקשר זה, מדינת ישראל תגבש מתווה להחלת דרישות אבטחה מחייבות, טכניות ומתודולוגיות, באספקת מוצרי IoT. זאת, בדומה לסטנדרטים בין-לאומיים ולצעדי רגולציה שננקטו באיחוד האירופי (Cyber Resilience Act) לאורך כל מחזור החיים של המוצר.

במטרה לצמצם חולשות אבטחה, מדינת ישראל תקדם הטמעת מדיניות Secure by Design and Secure by Default בתעשיית הפיתוח בישראל, יחד עם התעשייה והאקדמיה, ובאמצעות קואליציה בין-לאומית.

כדי להבטיח תוכנה בטוחה לאורך כל חיי המוצר, ישראל תמשיך להפעיל ולפתח את התוכנית הלאומית שמפעיל מערך הסייבר לאיתורן של חולשות בתוכנות ובמערכות, דיווחן וחתימתן מול היצרניות כסמכות מורשה עולמית (CVE), בכל סוגי הטכנולוגיה והמגזרים.

מדינת ישראל תשאף להוות דוגמא למשק, ותקבע דרישות אבטחה הולמות ומתקדמות למוצרים ושירותים דיגיטליים בחוזי הרכש שלה. בנוסף, המדינה תבחן את השימוש במנגנוני עידוד שונים לטובת יישום פתרונות הגנה נאותים למשתמשי קצה באמצעות ספקיות האינטרנט.

3.3 יעד שלישי: הגנה על נכסי מידע

בעידן המידע, בנוסף להגנה על הטכנולוגיה, ישנה חשיבות רבה גם להגנה על המידע שלנו מפני העלייה בהיקף ובתחכום האיומים. המרחב הדיגיטלי כולל פרטי מידע ומאגרי מידע מסוגים שונים (כגון מידע אישי, עסקי, ביטחוני ועוד). השימוש הגובר במרחב המקוון והטמעת מערכות בינה מלאכותית מגדילים באופן משמעותי את היקף המידע ופיזורו - קרי, את משטח התקיפה.

לתוקפים זדוניים יכולת גוברת להשתמש במידע לגרימת נזק פיזי וכלכלי, בין היתר על ידי גניבת קניין רוחני, סודות מסחריים ונכסים פיננסיים; ריגול אחר המערכת הביטחונית; איסוף מידע רגיש על האזרחים; והשפעה על תודעת הציבור, בין היתר באמצעות איסוף מידע מצרפי מכמה מאגרים שונים והיתוכם. כך, למשל,

במלחמת "חרבות ברזל" שימשו נתונים שהוגדרו כבלתי מסווגים, אשר נאספו על ידי האויב ממקורות מידע מגוונים, לתקיפות בעלות אופי ביטחוני-פיזי-תודעתי.

ההגנה על מאגרי המידע והנתונים מוסדרת כיום בעיקר על ידי דיני הגנת הפרטיות ועל ידי חוקים שתכליתם הגנה על המסחר ועל הביטחון. לרשות להגנת הפרטיות תפקיד חשוב באכיפה במקרה של הפרת דיני הפרטיות. יחד עם זאת, נדרשת זווית ראיה משלימה, הבוחנת את הסיכון הביטחוני הנובע מאיסוף מצרפי של מידע בלמ"ס.

בכדי לוודא מענה הגנה רחב מפני העלייה בהיקף ובקצב האיומים, מדינת ישראל תפעל לזיהוי נקודות התורפה וחיזוקן; להעלאת המודעות הציבורית לסיכונים שבהחזקה ושיתוף לא זהיר של מידע; ולבחינה ממשלתית של מתודולוגית סיווג המידע בגופים בעלי מידע ביטחוני, טכנולוגי, כלכלי או מדיני רגיש, תוך התייחסות לאיומים היברידיים.

3.4 יעד רביעי: ביסוס מרחב תודעתי מוגן יותר מפני השפעה זרה

עם התפתחות אמצעי התקשורת, ובמיוחד עם התרחבות השימוש בפלטפורמות החברתיות המאפשרות שיתוף מידע תוך נגישות מהירה להמונים, הועצמה מאוד התופעה של מאמצי השפעה מצד מדינות זרות (Foreign Information Manipulation and Interference Campaigns). השימוש הגובר של היריבים בטכנולוגיית הבינה המלאכותית היוצרת מעצים את ההיקף, המהירות, התחכום וההשפעה של התופעה באופן מעריכי.

מתקפת השבעה באוקטובר והלחימה העצימה ב"חרבות ברזל" הוכיחו כי לתופעת ההשפעה הזרה, בשילוב המדיה החברתית וטכנולוגיות בינה מלאכותית, פוטנציאל איום על הביטחון הלאומי, החוסן החברתי, הדמוקרטיה ותחושת הביטחון האישי. חלק מהמבצעים הללו תכליתם לפגוע בעצם האמון הציבורי

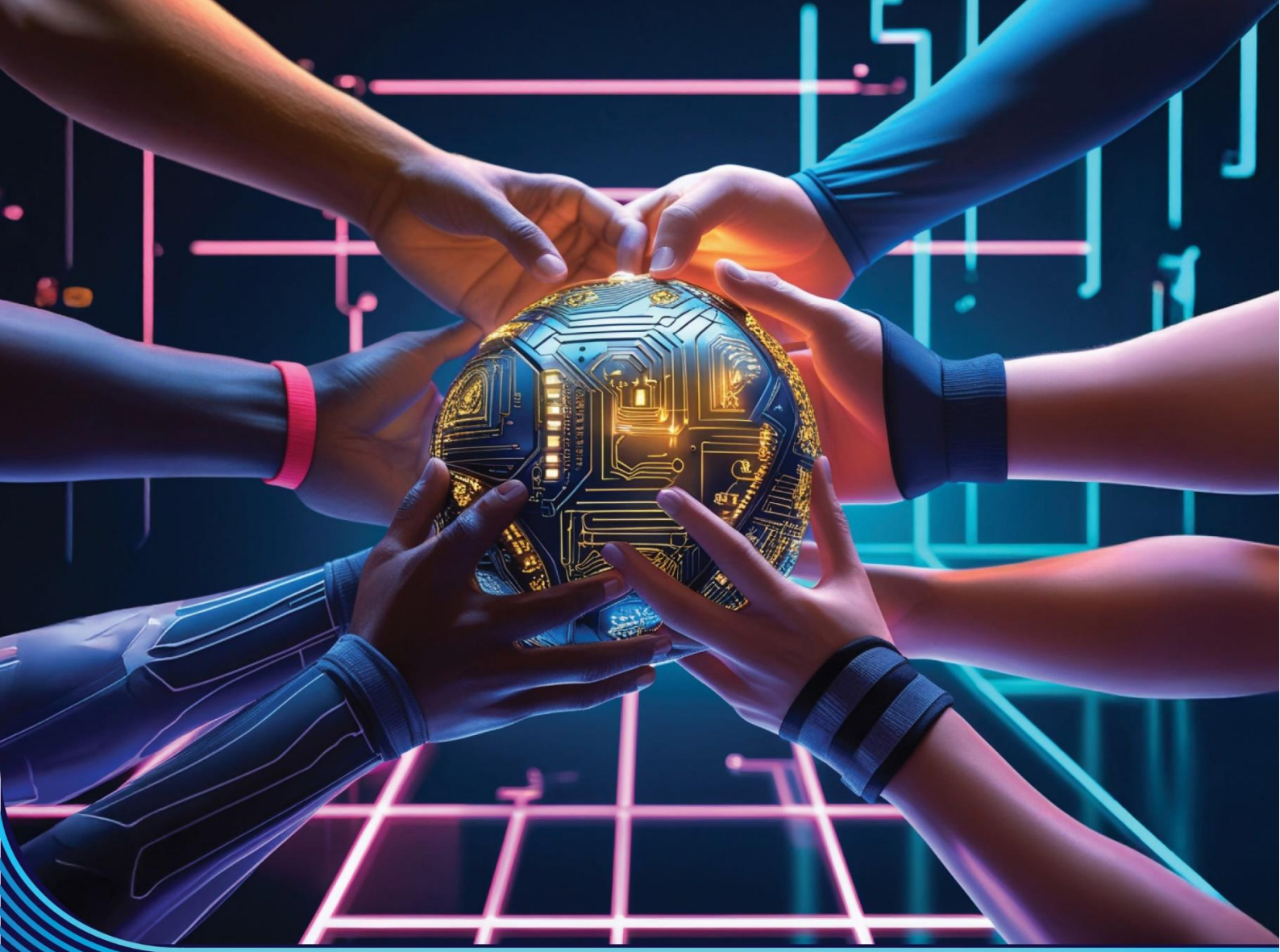
במרחב הדיגיטלי עצמו. מאמצים אלו אף השפיעו על דעת הקהל העולמית בהקשרי המלחמה.

ישראל, כמו מדינות וארגונים בין-לאומיים מובילים אחרים, מכירה באיום ההשפעה הזרה על התודעה כאיום חמור ומתעצם. אתגר ההתמודדות עם ההשפעה הזרה עומד מול אתגר שימור חופש הביטוי והבחירה של אזרחי ישראל. לפיכך, במדינה דמוקרטית כישראל, כל מעורבות מדינתית צריכה להיעשות בזהירות, בשקיפות ותחת ביקורת מתאימה.

במהלך מלחמת "חרבות ברזל", פעלו גופי ביטחון, משרדי ממשלה וגופים אזרחיים, לאיתור מעורבות זרה המפרה את החוק או את תנאי השימוש של הפלטפורמות המקוונות, ופעלו להסרת תכנים זדוניים זרים. בנוסף למאמצי ההסרה, יש צורך לבחון דרכים לטיפול באיום בשלבים מוקדמים יותר.

לצד המשך המאמצים לניטור ואיתור תכנים זדוניים במעורבות יריבים זרים, מדינת ישראל תפתח את השיח עם מדינות נוספות ועם הפלטפורמות החברתיות לעידוד סינון עצמאי, יעיל ומהיר, של תכנים זדוניים המפרים את תנאי השימוש או את החוק.

כמו כן, תקדם את הקמתו של צוות לאומי ליצירת תמונה אמינה של מאמצי ההשפעה הזרה על התודעה במרחב הדיגיטלי, ותפתח מנגנון משולב להתמודדות הוליסטית, מאוזנת ומבוקרת עם איום ההשפעה הזרה. בנוסף, ישראל תפעל להגברת מאמצי החינוך והמודעות הציבורית, החל מהגיל הרך, להבנת התופעה ודרכי התמודדות הרצויות עמה.



נדבך שני:

התארגנות מדינתית

מרחב הסייבר מתפתח ומשתנה, ועמו גם האיומים. הגבולות בין התוקפים מיטשטשים ויכולות תקיפה זולגות בין יריבים ואויבים. השינויים הללו מחייבים הידוק של הממשקים בין גורמי המדינה השונים, לטובת מענה מדינתי נרחב ומתוחכם יותר. בנדבך זה יתוארו המאמצים המדינתיים הדרושים להתמודדות עם האתגרים במרחב, לרבות ההיערכות לאיומים מתקדמים.

מערך
הסייבר
הלאומי

4. <u>פרק רביעי: הגנה משותפת</u>

מעבר משיתוף פעולה - לפעולה משותפת

4.1 יעד ראשון: ניהול משותף של מאמצי ההגנה הלאומיים

ישנה חשיבות מכרעת לכך שגופי הממשלה האמונים על היבטים שונים בתחום הגנת הסייבר יפעלו יחד באופן משולב בשגרה ובחירום. כחלק מכך, נדרשת ראייה הוליסטית ומתואמת על הנכסים במרחב הסייבר והאינטרסים הלאומיים, אשר יכווינו את מאמצי ההגנה הלאומיים.

בנוסף, נוכח השתנות המרחב ועל רקע מגמות גאו-פוליטיות של התקרבות בין אויבים ויריבים (מעצמות, מדינות וארגוני טרור), נדרשת הרחבה של אלומת האיסוף והמחקר המודיעיני. הרחבה כאמור תסייע להכיר באופן מעמיק יותר את היכולות המתפתחות בקרב מעצמות וארגוני פשיעה משמעותיים, ותאפשר להיערך לאיומים מתקדמים ולהגן על המשק הישראלי בצורה טובה יותר.

בישראל פועל מנגנון תיאום ביטחוני אופרטיבי, שהוקם לטובת יצירה וחיזוק של שיתוף הפעולה בין שירותי הביטחון בתחום הגנת הסייבר. מנגנון זה הוכיח את עצמו כאפקטיבי בתיאום סוגיות חוצות-ארגונים ובמתן מענה משותף לאירועי סייבר חמורים בזמן שגרה, וביתר שאת לאורך מלחמת "חרבות ברזל".

מדינת ישראל תפעל לשכלל את פעילות מנגנון זה באמצעות מעבר ממודל של שיתוף פעולה בין גופי הביטחון, למודל של פעולה משותפת: הן במאמצים האופרטיביים, הן בהיבטי בניין כוח, והן במחקר משותף.

כמשלים למאמץ האופרטיבי, יוקם מנגנון תיאום ממשלתי בין-מגזרי לשיתוף מידע על איומי סייבר, שיורכב מהמאסדרים המגזריים, לרבות נציגי יחידות הסייבר המגזריות, מערך הסייבר, וגופי אכיפת החוק הרלוונטיים. זאת, לטובת יצירת תמונת איום משותפת, תיאום תגובה לאירועים שוטפים ושיתוף במאמצים לקידום פתרונות.

הכוונת מאמצי ההגנה הלאומיים תתבסס גם על מדד חוסן המשק בסייבר. מדד זה יאפשר למדינה לזהות פערי אבטחה במגזרים, לשפר את יכולות ההגנה ולהתמודד עם מתקפות עתידיות בצורה אפקטיבית. מדינת ישראל תפתח מנגנון מדידה והערכה כלל משקי שיאפשר שיקוף רלוונטי ומתואם של תמונת המצב הסקטוריאלית והלאומית, הן בהיבט החוסן והן בהיבט יכולת ההתאוששות.

4.2 יעד שני: הגנה באמצעות כלים טכנולוגיים מתקדמים

מדינת ישראל תנקוט בגישה פרואקטיבית להגנה בסייבר הממנפת מצוינות טכנולוגית. **לשם כך ישראל פועלת ליישום תפיסה טכנולוגית-מבצעית לאומית מתקדמת הנקראת "כיפת הסייבר".** תפיסה זו, אשר כבר החלה לפעול באופן ראשוני, תכלול מגוון יכולות מתקדמות ותציע פתרון רוחבי להתמודדות מהירה יותר עם האיומים. המערכות של "כיפת הסייבר" יעבדו ויתיכו סוגי מידע שונים, תוך שילוב בינה מלאכותית, באופן שיאפשר ליצור תמונת מצב הוליסטית על כלל התקיפות והאיומים המיידים על המשק. "כיפת הסייבר" תמנף מודיעין לצורך מחקר איומים וסיווגם ותשתמש במגוון כלי הגנה אקטיביים לשיבוש תקיפות, לחקירה ולציד מוכוון ולהתרעות בפני ארגונים על תקיפות פוטנציאליות והדרכים למניעתן. כמאמץ משלים, מדינת ישראל תפעל להרחיב את שיתוף המידע בין המגזר הפרטי לבין מערך הסייבר הלאומי, ותתמרץ חוקרי סייבר לדווח וולונטרית על חולשות (Vulnerability Disclosure Program - VDP).

4.3 יעד שלישי: מימוש תפיסת ה-SOC הלאומי (NSOC)

תנאי בסיסי להגנה לאומית יעילה במרחב הסייבר הוא היכולת לייצר תמונת מצב לאומית הוליסטית. קיימת חשיבות לגיבוש תמונת מצב ומתן התראות בראייה סקטוריאלית ייעודית, הניזונה, בין היתר, מהמתרחש בסקטורים אחרים.

מדינת ישראל תמשיך לקדם מרכז שליטה ובקרה לאומי (NSOC - National Security Operation Center), המאגד תחתיו את המידע ממרכזי הבקרה המגזריים, שיתנו מצדם התייחסות ייעודית לכל מגזר. מרכז בקרה זה יוזן מהמידע הרב המגיע ממקורות האיסוף הקיימים במשק וממערכות "כיפת הסייבר", יבחן את כלל המידע במבט על, ואף ימליץ על פעולות מניעה והגנה בהתאם. במקביל, מדינת ישראל תשלים הקמתם של SOC-ים במגזרים החסרים, ותיצור שפה משותפת בין ה-SOC-ים השונים.

4.4 יעד רביעי: מענה לאומי לפשיעת סייבר

לפשיעה במרחב הסייבר יש מאפיינים ייחודיים הכוללים גניבת זהויות, הונאות מגוונות ומתוחכמות, אירועי כופרה ועוד.

מדינת ישראל תפעל ליצירת מערך תגובה יעיל המשלב את יכולות וסמכויות גופי החקירה והאכיפה בישראל, תוך שיתוף מידע ביניהם, בדגש על משטרת ישראל ומערך הסייבר הלאומי.

מערך התגובה יפעל בשלושה מישורי עשייה: בניית חוסן (מניעת התקיפות והגנה); התמודדות עם תקיפות (הכלה, דיווח והתאוששות); ופעולות אכיפה ושיבוש למול התוקף בשיתוף ארגוני אכיפת חוק בין-לאומיים, היכן שניתן. כחלק מכך, יבחן עדכון סמכויות גופי החקירה והאכיפה, תוך שאיפה להתאימן למציאות הטכנולוגית המתעדכנת תדיר, לשם מניעה וסיכול פשיעת סייבר.

במסגרת המאבק בפשיעת סייבר, מדינת ישראל תפעל באופן ממוקד למנוע אירועי כופרה, אשר בדומה למתרחש בעולם, מהוות את אחד הגורמים המשמעותיים ביותר לנזק כלכלי מתקיפות סייבר, ועלותן בישראל נאמדת בכמיליארד ₪ לשנה.

כחלק מכך, ממשלת ישראל דוגלת במדיניות של הימנעות מתשלום דמי כופר בכדי לסכל את כוונת התוקף, ומתוך הבנה כי התשלום אינו מבטיח השבת המצב או חסינות מפני תקיפות עתידיות.

במישור הבין-לאומי, ישראל תמשיך לפעול כשותפה במסגרת יוזמה בין-לאומית בהובלת ארה"ב, ה-Counter Ransomware Initiative (CRI), בהשתתפות עשרות מדינות. תכלית יוזמה זו הינה מאבק רב-ממדי בתקיפות הכופרה.

ישראל גם מובילה פיתוח של פלטפורמה לשיתוף מידע על תקיפות כופרה (Crystal Ball) בשיתוף פעולה עם איחוד האמירויות. מערכת זו מאפשרת העברה וניתוח של מידע על אירועי כופרה בין המדינות השותפות, במטרה להסתייע הדדית בידע, ביכולות ובכלים להכלת תקיפות סייבר.

5. <u>פרק חמישי: הפתעה בסייבר ומוכנות למשבר דיגיטלי</u>

הנחלת מודעות, מאמצים למניעת הפתעות אסטרטגיות במרחב הדיגיטאלי, ויצירת תהליכים ותשתיות הבנויים באופן עמיד יותר בעת משבר דיגיטאלי

5.1 יעד ראשון: היערכות למניעה והתמודדות עם הפתעה בסייבר

ההיסטוריה מוכיחה כי הפתעות משמעותיות מתרחשות, למרות מאמצים למניעתן. המתקפה על פרל הרבור, מלחמת יום הכיפורים, אסון התאומים ומתקפת הטרור של השבעה באוקטובר הן דוגמאות לכך.

לפיכך, יש להניח, כהנחת יסוד אסטרטגית, שהפתעה משמעותית שהמחולל שלה נובע מהמרחב הדיגיטלי הינה תרחיש אפשרי ויש להיערך אליו.

לגורם האנושי תפקיד מכריע בהתרחשות הפתעה ובניהול המשבר בעקבותיה. קיימות הטיות טבעיות, הן קוגניטיביות והן פסיכולוגיות, הנוטות להקל ראש באפשרות של הפתעה אסטרטגית. אלה נובעות, בין היתר, מהקושי להעריך מראש את עוצמת האירוע, מהעובדה שאינו וודאי, צפוי להתרחש בזמן לא ידוע בעתיד, או מייחוס סיבתי שמעוגן בקונספציות שגויות.

היערכות להפתעה כוללת פיתוח מתודולוגיה והטמעת תהליכים הצופים פני הפתעה. היערכות כזו ראוי שתיעשה בשני רבדים: ברובד הראשון, מדינת ישראל תייחד מאמצים להיערכות לאומית לצמצום היתכנות ההפתעה בסייבר באמצעות הקמת צוות לאומי לגיבוש עיתי של תרחישי הפתעה, בחינת שינויים במרחב, ואיתור נקודות תורפה.

ברובד השני, מתוך מודעות לכך שהפתעות תקרנה, ישראל תפעל להטמעתם של עקרונות לבניית משק חסין יותר מפני משבר דיגיטלי, בין היתר באמצעות גיוון אמצעי ההגנה, שימוש בהונאה ובפיתוח פתרונות פורצי דרך, ותבסס יכולת התאוששות מהירה על מנת לצמצם את הנזק ולהשיב המצב לקדמותו במהירה.

5.2 יעד שני: ניהול חירום לאומי במרחב הדיגיטלי

ככלל, מדינת ישראל מורגלת בניהול מצבי חירום בהקשרי מלחמה וטרור, אולם משבר ברמה הלאומית יכול לנבוע גם מתקיפת סייבר נרחבת או מתקלה משמעותית במרחב הסייבר, שאינם קשורים למצב חירום צבאי.

בעת מלחמה, קיימים מנגנונים מוכרים להכרזה וטיפול במצב חירום, לרבות הפעלת אמצעים המסייעים לטיפול באירועי סייבר הנלווים לו. יחד עם זאת, למצב חירום המתחולל בעקבות אירוע סייבר עשויים להיות מאפיינים שונים, ובראשם קצב הסלמה גבוה המשפיע על המרחב האזרחי באופן נרחב ובזמן קצר.

מדינת ישראל תקים צוות ייעודי, שיכלול את רשות החירום הלאומית (רח"ל) ויתר גופי החירום הלאומיים, אשר יהיה אמון על אפיון והיערכות לאומית לטיפול בחירום סייבר. הצוות ימפה את הצרכים לניהול חירום דיגיטלי לאומי ויפעל להסדרת המנגנונים, המשאבים והסמכויות, לרבות סוגיית ההכרזה על מצב חירום דיגיטלי, הנדרשים לשם כך.

6. <u>פרק שישי: הסרת איומים</u>

מדינת ישראל תפעל ביצירתיות ובאופן משולב לשיבוש פעילותם של שלל התוקפים בסייבר את ישראל, תוך ניצול מגוון כלים והיכולות שברשותה

6.1 יעד ראשון: מענה לתוקף

תוקפים מתקדמים, הן מדינתיים והן פליליים, מנסים באופן מתמשך לאתגר את האינטרסים הלאומיים של מדינת ישראל. איום זה מצריך רובד נוסף במענה המדינתי: אם עד כה תוארו מאמצים להעלאת חוסן במרחב הסייבר (קרי, למניעת תקיפות ולצמצום השפעתן לאחר שהתרחשו) – הרי שיש גם צורך להתמודד עם התוקפים באופן אקטיבי, לשם שיבוש והרתעה.

רובד זה של המענה המדינתי צריך לבוא לידי ביטוי במערכה שרותמת את מגוון הכלים והיכולות המדינתיות – הן מנגנוני אכיפה בדיעבד והן מנגנונים מניעתיים – כדי להתמודד עם תוקפי הסייבר באופן אקטיבי. מערכה זו משלימה ומשולבת במאמצים שתוארו בפרקים הקודמים, והיא מהווה מרכיב נוסף אותו יש לפתח, בתוך תפיסת ההגנה הלאומית השלמה בסייבר.

ישראל תקדם גישה אקטיבית המשלבת ביצירתיות את מגוון הכלים הטכנולוגיים, המודיעיניים, הביטחוניים, הדיפלומטיים והמשפטיים שבידיה לטובת הרתעת התוקפים על ידי גביית מחיר, שיבוש וסיכול פעולתם.

בכלל זה, גיבוש מדיניות הרתעה וייחוס, פיתוח תפיסת הפעלה, וביסוס מנגנונים לשיתוף ידע ופעולה משותפת.

לאור טבעו הבין-לאומי של מרחב הסייבר, שיבוש אקטיבי יעיל מחייב שיתוף מידע ופעולה משותפת של מדינת ישראל ומדינות ידידות, בהתאם לנורמות המקובלות, וכללי המשפט הבין-לאומי, ובמטרה לצמצם את האיום הנשקף מתוקפי סייבר.

נדבך שלישי:

פיתוח שותפויות אסטרטגיות ויכולות עתידיות

המורכבות, קצב השינוי והאופי הגלובלי של מרחב הסייבר מחייבים פיתוח מתמיד של שיתופי פעולה ברמה הלאומית והבין-לאומית, השקעה בפיתוחים טכנולוגיים מתקדמים וטיפוח הון אנושי מיומן, כמכפיל כוח אל מול אתגרי העתיד.

מערך הסייבר הלאומי

7. <u>פרק שביעי: פיתוח תשתיות לשיתופי פעולה ושותפויות</u>

מדינת ישראל תפעל לגבש שותפויות אסטרטגיות כמנוף לשיפור ההגנה הלאומית והעולמית

7.1 יעד ראשון: פיתוח שותפויות אסטרטגיות עם חברות הטכנולוגיה

לחברות הענק הטכנולוגיות עוצמה גלובאלית אדירה. ביכולתן להשפיע משמעותית על הגנת הסייבר של מדינות, לסייע למדינות במניעה, במענה ובשיקום ממתקפות סייבר. חשיבות הקשר של מדינת ישראל עם חברות אלו להגברת החוסן המשקי וקידום האינטרס הלאומי מתחדדת נוכח העלייה המתמדת בהיקפי איומי הסייבר. כמדינה בעלת תעשיית סייבר חזקה, הון אנושי מיומן, ומצוינות אקדמית - ישראל עשויה להוות נכס ערכי לחברות הטכנולוגיה, ומוקד מומחיות בתחום הסייבר המהווה מכפיל כוח בהגנה על המשק.

מדינת ישראל תפתח את השותפויות האסטרטגיות עם חברות הטכנולוגיה בישראל ומחוצה לה לקידום מספר תחומי פעילות, ביניהם: עיצוב ופיתוח משותף של פתרונות "הדור הבא" להגנה ברמה הלאומית והבין-לאומית, הטמעת פתרונות ישראליים חדשניים להגנה; שיתוף ידע לבניית חוסן; עידוד הבטחת האותנטיות של השיח ברשתות החברתיות למניעת השפעה זרה, הסתה וטרור; וקידום משותף של תפיסת ה- Security by design עבור מוצרים דיגיטאליים, ועבור מערכות בשימוש נרחב בישראל ובעולם.

7.2 יעד שני: העמקת קשרי הגנת הסייבר עם שותפות מובילות בסייבר

בשל האופי הגלובלי של מרחב הסייבר, יש צורך מבצעי בפיתוח וטיפוח קשרי גומלין עם משרדי ממשלה מקבילים, וסוכנויות הגנה זרות.

קשרי גומלין אלה יכולים להיות בתחום חילופי המידע, עיצוב וקביעת מדיניות, חקירות ופעולות משותפות, ואף פיתוחים משותפים. כבר כיום, ישראל מקבלת ומשתפת מידע על מאפייני תקיפות סייבר עם עשרות מדינות בעולם, וחברה בפורומים אזוריים ובין לאומיים שונים לפיתוח ידע, גיבוש סטנדרטים ועיצוב נורמות.

ישראל תמשיך לקדם את שיתופי הפעולה הבילטרליים והמולטילטרליים שלה ותחזקם במספר מוקדים: שיתוף מודיעין לשם קבלת התראות בזמן אמת; הפצת ידע על אודות חולשות נפוצות וחתימתן מול היצרנים; מאבק במבצעי השפעה זרה על התודעה; למידה מפרקטיקות הגנה של מדינות אחרות; הרחבת מאמצי האכיפה נגד פשיעת סייבר; מאמצי 'דיפלומטיית סייבר' לחיזוק האינטרסים הלאומיים, קידום סטנדרטיזציה ופיתוח מסגרות רגולטוריות מתקדמות.

מדינת ישראל תפעל להגברת נוכחות והשפעה במסגרות בין-לאומיות כגון ה-OECD, אינטרפול, נאט"ו ועוד. ישראל תמשיך ליזום ולפתח שיתופי פעולה בהגנת סייבר במסגרות אזוריות כמו עם מדינות "הסכמי אברהם" ומדינות ידידות באגן הים התיכון. אלה יאפשרו לישראל לקיים שיתופי פעולה פוריים לשיפור רמות ההגנה ואף לקדם את ייצוא טכנולוגיות הגנת הסייבר המתקדמות של ישראל.

7.3 יעד שלישי: השתתפות בעיצוב כללי התנהגות בין לאומיים

כשותפה לשיח הבין-לאומי המעצב את כללי ההתנהגות האחראית במרחב הסייבר, **ישראל מכוונת להשפיע על קביעת מדיניות הגנת הסייבר בזירה הבין-לאומית, לרבות במסגרת פעילויות האו"ם**. מעורבות זו הופכת דחופה במיוחד נוכח האתגרים המתפתחים בתחום ההשפעה הזרה על התודעה, המאבק בטרור-סייבר, המאבק בניצול לרעה של טכנולוגיות כגון בינה מלאכותית, השימוש לרעה בכלי סייבר התקפיים והגידול במנגנוני פשיעת סייבר כשירות (crime as a service).

נוסף על כך, ישראל מכירה בחשיבות של קידום צעדים בוני-אמון בין מדינות כתשתית לשיתוף פעולה בין-לאומי.

פעילות נוספת תתמקד בקידום ותיאום תקינה בין-לאומית מוסכמת בסוגיות שונות, כגון אבטחת שרשרת אספקה בתחום הסייבר, קידום ההגנה על מוצרים דיגיטליים, ואבטחת טכנולוגיות מבוססות בינה המלאכותית; זאת מתוך הבנה כי נורמות רלוונטיות בתחומים אלה יעוצבו בזירה הבין-לאומית.

7.4 יעד רביעי: סיוע למדינות ידידות

ישראל פועלת לשתף ידע ומידע רלוונטיים עם ידידותיה, ותמשיך לסייע למדינות ידידות בעת משבר סייבר לאומי. ישראל תפעל גם בשגרה לקדם את מאמצי בניין הכוח בסייבר באמצעות עידוד הטמעת פרקטיקות ופתרונות סייבר ישראליים, ובאמצעות מינוף פעילות הבנקים האזוריים והבין לאומיים לפיתוח וארגונים נוספים בהם ישראל חברה.

השתתפות ישראל במאמץ זה מקדמת את יעדי מדיניות החוץ של ישראל ובמקביל, מעשירה את הידע על תקיפות סייבר ואת הניסיון הישראלי לבניית החוסן והמענה ההגנתי בישראל.

8. <u>פרק שמיני: השקעה בבניין כוח איכותי לנוכח אתגרי העתיד</u>

שימור נוכחותה של ישראל בחזית הסייבר העולמית
באמצעות מצוינות מדעית-טכנולוגית בסייבר

8.1 יעד ראשון: פיתוח טכנולוגיות ויכולות עתידיות

הבטחת היכולות העתידיות של ישראל תלויה בשימור נוכחותה בחזית החדשנות העולמית, גם בכל הקשור לטכנולוגיות מפציעות ולאפשרויות ההגנה מפני האיומים הנובעים מהן.

בישראל קיימים כיום מספר מרכזי מצוינות משולבים להגנה בסייבר בתחומים שונים (תחבורה, תעשיה, ביומטריה ובינה מלאכותית). מרכזים אלו מקדמים את פיתוחם של פתרונות חדשניים.

על רקע התקדמות הטכנולוגיה ומנגנוני התקיפה נדרשת התאמה מתמדת ופיתוח יצירתי של פתרונות "הדור הבא". ישראל תקדם מאמצי מו"פ משותף הממוקד במתן מענה ופתרונות הגנת סייבר לטכנולוגיות המתפתחות ולמגמות החוזות פני-עתיד.

הסביבה הטכנולוגית משתנה ומתפתחת בקצב מואץ, וכך גם האיומים הטכנולוגיים. ישראל תקיים תהליכים שוטפים למעקב ולהיערכות לפיתוח טכנולוגיות המערערות באופן דרמטי את סביבת ההגנה בסייבר. מדינת ישראל תוביל מאמצים אלו בשיתוף פעולה הדוק עם האקדמיה, גופי הביטחון והתעשייה, תוך מיקוד התמיכה במו"פ יישומי, הרלוונטי באופן ישיר למאמץ ההגנה הלאומי.

ישראל מכוונת להרחיב את פעילות מרכזי המצוינות והמעבדות מול האקו-סיסטם, בין היתר בהגדלת מעורבותן של חברות מהמגזר הפרטי במרכזים אלה, ובמאמץ להטמעת הידע והפתרונות שהמעבדות מעמידות לטובת חברות במשק ובעולם.

8.2 יעד שני: אימוץ בטוח של בינה מלאכותית

לטכנולוגית הבינה המלאכותית היוצרת (Generative Artificial Intelligence) פוטנציאל גדול בשיפור ההגנה בסייבר, בין היתר, על-ידי איתור חולשות מהיר יותר, קיצור חקירה פורנזית, עיבוד מקורות מידע מסוגים שונים, יכולת הצלבת נתונים והיתוכם, ועוד.

מול זאת, הבינה המלאכותית עלולה לשמש ככלי בידי היריבים לביצוע התקפות מתוחכמות וממוקדות יותר, בקיצור זמני השמשת חולשות, במבצעי השפעה נרחבים יותר, ב"הרעלת" מודלים במידע שגוי והטיית תוצאות ההחלטה, ועוד.

ישראל תפעל לאימוץ טכנולוגיית הבינה המלאכותית במשק בהתבסס על ארבעה מרכיבים עיקריים:

א. הגנה על מערכות AI מאיומי סייבר - מאמץ זה יכלול, בין היתר, מחקר ופיתוח מתודולוגיה להגנה על מערכות בינה מלאכותית, והנגשת המעבדה הלאומית למחקר יישומי בתחום למשק; תוצאות המחקרים ישמשו לפיתוח מתודולוגיות הגנה עבור כלל המשק.

ב. הגנת סייבר מבוססת בינה מלאכותית לשיפור יכולת ניטור, גילוי וזיהוי של תוקפים ותקיפות, ניתוח דפוסי תקיפה ופיתוח יכולות ניבוי לטובת מאמצי הגנת הסייבר.

ג. הגנה מפני תוקפים המנצלים לרעה את הטכנולוגיה לשם תקיפות סייבר - באמצעות קידום המחקר על יכולות הבינה מלאכותית מנגד (Adversarial AI).

ד. הטמעה מאובטחת של כלי בינה מלאכותית במשרדי הממשלה השונים - מאמץ שמטרתו ייעול תהליכי העבודה ואיכות השירות לאזרח, ודורש יישום כללי זהירות לאימוץ בטוח של הטכנולוגיה, בכדי להבטיח את אמינות וזמינות השירות.

התובנות מהמאמצים הללו, לצד העלאת המודעות, פיתוח פתרונות ייעודיים והסדרת עקרונות ההגנה יאפשרו הטמעה מאובטחת של בינה מלאכותית במערכות הממשלה ובקרב כלל המשק.

8.3 יעד שלישי: פיתוח הון אנושי מיומן

אחד המרכיבים המשמעותיים להצלחת תחום ההייטק בישראל בכלל, ותעשיית הסייבר בפרט, הוא איכות ההון האנושי הטכנולוגי שלה, עליה מתבסס מגזר ההייטק בישראל. הצורך בעובדים מיומנים בתחום הסייבר בעולם בכלל, ובישראל בפרט, הולך וגדל. על מנת להתאים את רמת הגנת הסייבר הדרושה במשק להתמודדות עם האיומים המתחזקים והמפציעים קיים צורך קריטי להמשיך ולהרחיב את היקף ההון האנושי המיומן בסייבר ובתחום הבינה המלאכותית בישראל, תוך מיקוד בשילוב אוכלוסיות הנמצאות בשיעור השתתפות נמוך בתחום.

לשם כך, ישראל תפעל במספר מאמצים:

הרחבת שער הכניסה לעולם הסייבר על-ידי יצירת הזדמנויות לאוכלוסיות ממגזרים בהם שיעור ההשתלבות במקצועות הללו נמוך, תוך שחרור החסמים הייחודיים לאוכלוסיות השונות ורתימת כלל הגורמים המשפיעים (הורים, מורים, מנהלי בתי ספר, גופים ברשויות מקומיות, משרד החינוך, צה"ל ועוד). טכנולוגיות מפציעות, דוגמת בינה מלאכותית, יקבלו ביטוי ספציפי במסגרת התכניות הללו. לפעילות זו ערך מוסף ברמה הלאומית, ובפרט בהיבטים כלכליים וחברתיים, והיא תבוצע באופן מתוכלל ובראייה לאומית רחבה.

בניית רצף הוליסטי ומסונכרן של פעילות הכשרה זאת, באמצעות הרחבת תכניות החינוך וההכשרה כך שיחלו עוד במסגרת לימודי החובה בבתי הספר היסודיים ובחטיבות הביניים; הרחבת תכניות ההתמחות בלימודים מתקדמים בסייבר ובינה המלאכותית; ועידוד בעלי מיומנויות בתחום הסייבר הפונים למחקר אקדמי בתחום הסייבר והבינה המלאכותית.

פריצת חסם הג'וניורים – היעדר ניסיון ראשוני בתעשיית הסייבר מהווה חסם המרתיע מעסיקים. ישראל תפעל לעידוד העסקת פצועי מלחמת "חרבות ברזל" בוגרי לימודי סייבר, בתפקיד ראשון בממשלה ובתעשייה, במטרה לאפשר להם לצבור ניסיון ולהתפתח מקצועית.

האסטרטגיה הישראלית להגנה בסייבר היא אסטרטגיה לאומית. גיבוש המסמך נעשה בשיתוף גופי ממשלה רלוונטיים, מערכת הביטחון ותוך התייעצות עם הציבור. מימושה תלוי אף הוא בפעולה משותפת של גופי הממשלה, המשק בכללותו ואף שותפים בזירה הבין-לאומית.

לנוכח הדינמיות הרבה שמאפיינת את מרחב הסייבר, האסטרטגיה הלאומית להגנה בסייבר דורשת עדכון במקרה של התפתחויות ושינויים משמעותיים במרחב הסייבר, בין היתר בעצמת החישוב, בממשק אדם-מכונה, או במקרה של שינויים גאו-פוליטיים או רגולטוריים משמעותיים.

כדי להביא את האסטרטגיה למימוש, תגובש במשותף תוכנית יישום קונקרטית שתהווה מפת דרכים ליישום האסטרטגיה. על מימוש התוכנית יהיו אמונים גופי הממשלה השונים בתכלול של מערך הסייבר הלאומי.

מימוש מיטבי של המאמצים הללו יאפשרו לבסס מרחב דיגיטאלי לאומי מתקדם, אמין, זמין ובטוח יותר, שיאפשר ויאיץ שגשוג כלכלי למדינת ישראל ורווחה לתושביה.

***

האסטרטגיה הלאומית להגנה בסייבר נכתבה במערך הסייבר הלאומי על ידי צוות אגף אסטרטגיה והתעצמות: ראש מרכז אסטרטגיה, יוסי אבירם; ראש תחום בכירה מדיניות וממשל, מירי זילברשטיין; ראש תחום מדיניות רגולציה, איילת-חן כהן; בהנחיית ראש אגף בכיר אסטרטגיה והתעצמות, רועי פרידמן.

צוות מייעץ במערך הסייבר הלאומי: ראש אגף בכיר חדשנות טכנולוגית, דדי גרטלר; ראש מחלקת הגנה אקטיבית, יובל סיני; מר אבנר בן-אפרים; ראש אגף המודיעין; ראש מרכז הגנת תשתיות תקשורת, גיל אנגל.

סייעו בתהליך בעלי תפקידים רבים במערך הסייבר, משרדי ממשלה, גורמי אקדמיה בכירים וגופי מערכת הביטחון העוסקים בנושא, תוך התייעצות עם גורמים בולטים בתחום הסייבר לרבות מהתעשייה וקהילת המחקר.

מערך
הסייבר
הלאומי