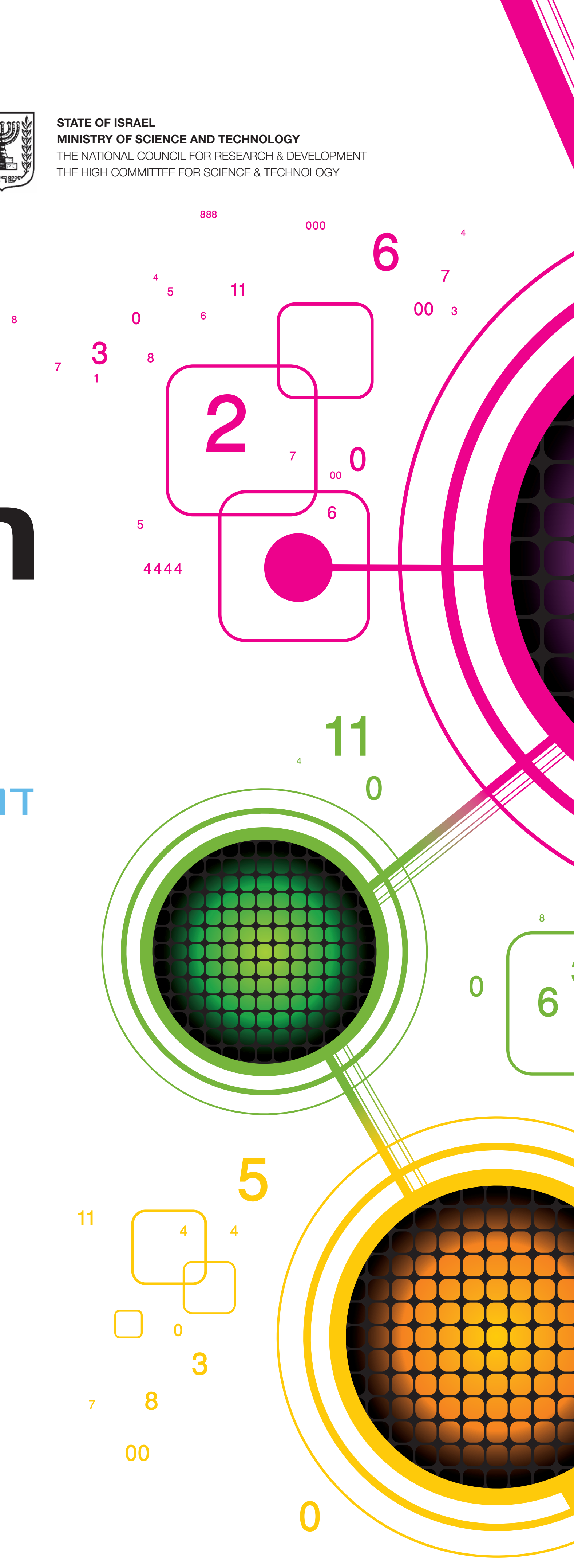
מדינת ישראל
משרד המדע והטכנולוגיה
המועצה הלאומית למחקר ופיתוח
הועדה העליונה למדע וטכנולוגיה

STATE OF ISRAEL
MINISTRY OF SCIENCE AND TECHNOLOGY
THE NATIONAL COUNCIL FOR RESEARCH & DEVELOPMENT
THE HIGH COMMITTEE FOR SCIENCE & TECHNOLOGY

המיזם הקיברנטי הלאומי



דו״ח מיוחד לראש הממשלה

תל אביב, אייר התשע״א, מאי 2011

המיזם הקיברנטי הלאומי

דו״ח מיוחד לראש הממשלה

עורך:
רם לוי

מסמך זה נכתב בשיתוף סדנת יובל נאמן למדע טכנולוגיה וביטחון, אוניברסיטת תל אביב
http://www.sectech.tau.ac.il

עריכה גרפית ועריכת שער: H+H הגר וחגית עיצוב ומיתוג
www.hplush.co.il

הודפס בדפוס ע.ר. תל אביב

©
כל הזכויות שמורות למשרד המדע והטכנולוגיה.
כל הזכויות שמורות. אין להעתיק, לשכפל, לצלם, לתרגם, לאחסן במאגר מידע או להפיץ נייר זה או קטעים ממנו בשום צורה ובשום אמצעי אלקטרוני, אופטי או מכני, ללא אישור בכתב.

המועצה הלאומית למחקר ופיתוח
משרד המדע והטכנולוגיה
משרדי הממשלה,
הקריה המזרחית, בנין ג', ת.ד. 49100, ירושלים 91490
טלפון: 02-5411190 פקס: 02-5825581
כתובתנו באינטרנט: http://www.most.gov.il

יום רביעי, ז' באייר התשע"א
5 מאי, 2011

לכבוד
מר בנימין נתניהו
ראש הממשלה

שלום רב,
ביום 17 בנובמבר 2010 מינה אותנו ראש הממשלה מר בנימין נתניהו כצוות מיוחד לגיבוש תוכנית קיברנטית לאומית.

הצוות עבד במשך מספר חודשים וגיבש דו"ח שכותרתו "המיזם הקיברנטי - דו"ח מיוחד לראש הממשלה". עבודת הצוות נועדה לענות על ההנחיות שניתנו לנו בפגישת הממשלה בנושא. הצוות פעל לאור החזון לפיו יש לשמר את מעמדה של ישראל בעולם כמרכז לפיתוח טכנולוגיות מידע ולהקנות לה יכולות מעצמתיות במרחב הקיברנטי, בכדי להבטיח את חוסנה הכלכלי והלאומי כחברה פתוחה, דמוקרטית ומבוססת ידע.

הדו"ח שלהלן כולל שני חלקים: אחד בלתי מסווג והשני מסווג. הדו"ח הגלוי מכיל מתאר את פעילות הצוות ומכיל המלצות לפעולה לממשלת ישראל . מטרתו לנתח ולהגיש לממשלת ישראל הצעה מעשית כיצד להציב את ישראל בחמישייה הפותחת של מדינות העולם במרחב הקיברנטי עד 2015.

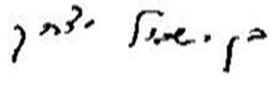
הדו"ח מסתמך ממצאיהן של שמונה תתי ועדות, שבחנו את המרכיבים החיוניים להתמודדות של מדינת ישראל במרחב הקיברנטי, ועל ניתוח התועלות הלאומיות של המלצות הצוותים בהיבטי הכלכלה, האקדמיה והביטחון הלאומי.

אני ממליץ שהדו"ח, בנוסחו המלא, יעמוד לעיון נשיא המדינה, שרי הקבינט, הרמטכ"ל, ראש השב"כ, ראש המוסד למודיעין ולתפקידים מיוחדים וחברי המטה הכללי של צה"ל - כפי שיחליט הרמטכ"ל וגורמים נוספים לפי שיקולך.

אני מודה לכל חברי הצוות על עבודתם החשובה ותרומתם לגיבוש דו"ח זה והמלצותיו.

אנו מעריכים את האמון שניתן בנו, וכן את ההזדמנות לנסות ולתרום לקידומה של מדינת ישראל.

בתודה ובכבוד רב,



פרופ' אלוף (מיל.) יצחק בן ישראל

יו"ר המולמו"פ

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

תקציר מנהלים

החזון:

לשמר את מעמדה של ישראל בעולם כמרכז לפיתוח טכנולוגיות מידע, ולהקנות לה יכולות מעצמתיות במרחב הקיברנטי, בכדי להבטיח את חוסנה הכלכלי והלאומי כחברה פתוחה, דמוקרטית ומבוססת ידע.

המטרה:

להציב את ישראל בחמישייה המובילה של מדינות העולם במרחב הקיברנטי עד 2015.

רקע

למעלה מ- 50% מאוכלוסיית העולם נגישה לשילוב כלשהו של ציוד אלקטרוני, הכולל, ברוב המקרים, מחשבים, טלפונים ניידים ואינטרנט.[1] נתון זה משקף את המגמה המסתמנת **בשנים האחרונות,** לפיה **הפעילות במרחב הקיברנטי**[2] (cyberspace) בעולם כולו, ובכלל זה **במדינות ובארגונים יריבים לישראל, הופכת לבעלת משמעות,** כחלק ממגמת המודרניזציה, המתבטאת בכלכלה, תשתיות אזרחיות, ביטחון אזרחי, ביטחון לאומי, תקשורת בין-ארגונית, חינוך, מחקר ופיתוח ועוד.

גם מדינות משתמשות באופן הולך וגובר במרכיבי המרחב הקיברנטי. מדינות מודרניות ומפותחות נעזרות ברשת האינטרנט, למשל, לניהול מוסדות השלטון, לפעילות התשתיות הלאומיות ולקשר עם האזרחים. **ככל שמדינה מנצלת לתועלתה את המרחב הקיברנטי, והתלות שלה בו גוברת, כך היא חשופה יותר לפגיעה בו ובתשתיות שלו.** ככל שארגונים וגורמים נוספים (מדינות וגופים לא-מדינתיים) מרחיבים את תלותם במערכות ממוחשבות, גדל פוטנציאל הנזק שניתן להסב להם דרך המערכות, שהיו פעם בעלות היקף נפרד ומוגבל, והיום הן מקושרות ומתוחכמות יותר. המתח החדש שנוצר, בין תועלת לסיכון, מאפיין תהליכים שהיו בעבר מנוהלים בידי אדם, ובהדרגה הופכים לממוחשבים.

הפעילות המסועפת במרחב הקיברנטי יצרה תלות רבה בקרב המשתמשים בו, ביניהם יחידים, חברות, ארגונים ומדינות. בשל תלות זו, הפכה הפגיעה בפעילות במרחב הקיברנטי לפעולה אטרקטיבית. פריצות למערכות מחשב, **ניסיונות פריצה והתקפות על רשתות התקשורת ומרכיבי הרשתות האזרחיות והממשלתיות בישראל ובעולם מתרחשות מדי יום ובכמות מטרידה. מגמה זו צפויה להתרחב, ככל שההישענות על פעילות במרחב הקיברנטי תגדל.**

בראייתנו, מתקפות קיברנטיות על תשתיות ממוחשבות במדינת ישראל בכלל, ועל תשתיות לאומיות קריטיות בפרט, עלולות להסב נזק משמעותי בטווח הקצר והארוך לכלכלה, לביטחון ולהיבטים נוספים של החברה.[3] יתרה מזאת, הקו שהפריד בעבר בברור בין לוחמה צבאית, לבין נזקים שמקורם בפעילות פלילית או עסקית מתעמעם כיום.

בהקשר זה, ממשלת ישראל מצויה כעת בצומת החלטה מרכזי. מצד אחד, צריך לוודא שהמדינה תמשיך להוביל בתחומי המדע, הטכנולוגיה והכלכלה, שהם בגדר מרכיבים קריטיים בחוסנה הלאומי (אך טומנים בחובם הישענות רבה על המרחב הקיברנטי); מצד שני, צריך להתמודד עם הפגיעות הנובעת מכך, ולהגן על התשתיות הלאומיות החיוניות לקיומם של חיים תקינים במדינת ישראל ולחסנן מפני התקפה קיברנטית. בכדי להתמודד עם הדילמה הזו, אין די בגישה המסורתית, הממוקדת באיומים הביטחוניים, כיוון שהאיומים הקיברנטיים עלולים לפגוע לא רק בנכסים ביטחוניים,[4] אלא גם ביסודות הכלכלה והחברה.

1 ראו Schmidt and J. Cohen, The Digital Disruption , Foreign Affairs, November/December 2010. בנוסף, על פי נתוני איגוד הבזק הבינלאומי (ה- ITU), החיבור לאינטרנט בפס רחב זמין ל-22.6 % מאוכלוסיית העולם (http://www.itu.int/net/pressoffice/stats/2010/09/index.aspx). בישראל, כ-30% מהאוכלוסייה ו-77% מבתי האב, מחוברים (http://www.websiteoptimization.com/bw/1001). נתונים אלה במגמת עלייה מתמדת, ככל שמחיר החיבור יורד עבור מספר רב יותר של אנשים בעולם, לרבות במדינות מתפתחות (www.itu.int/net).

2 "המרחב הקיברנטי" הינו המתחם הפיזי והווירטואלי ("המימד החמישי") שמורכב מהגורמים הבאים ומכל מצבור שלהם: מחשבים, מערכות ממוכנות ורשתות; תוכנות, מידע ממוחשב; התוכן של אלה האחרונים; נתוני תעבורה ובקרה שלהם; ומשתמשי כל אלה.

3 כפי שנראה בהמשך המסמך, המרחב הקיברנטי כולל מספר מרכיבים מקוונים ופיזיים: הוא מהווה "מערכת של מערכות" (a system of system) בצורה מובהקת - ובכך מחייב מענה מערכתי.

4 ראו: ITU Report on Best Practices for a National Approach to Cybersecurity, ITU-D Doc. 1/249 (Rev. 1), 4 December 2009

המיזם הקיברנטי הלאומי

המיזם הקיברנטי הלאומי היא תוכנית שתכליתה להציב את ישראל בין חמש המדינות המובילות במרחב הקיברנטי עד 2015, בהתאם לחזון לפיו ישראל תשמור על מעמדה בעולם כמרכז לפיתוח טכנולוגיות מידע, ותהיה בעלת יכולות מעצמתיות במרחב הקיברנטי. יכולות אלה, שחלקן מבוסס על הקמה והטמעה של יכולות מחקר ופיתוח חדשות, מנגנוני תיאום והסדרה ושינויי חקיקה (כמפורט בהמשך), יאפשרו לישראל להתמודד בצורה מיטבית עם אתגרים ואיומים במרחב הקיברנטי. הידע והטכנולוגיות הנחוצים, בשילוב עם תעשייה ואקדמיה מפותחות, יספקו גם תנופה לכלכלה הישראלית, שטכנולוגיות מידע הן חלק מרכזי בה.

התועלות של המיזם אינן מסתכמות ברווחים כלכליים בלבד. תוצרי המיזם יקדמו גם את המחקר והחינוך, ויספקו מענה להגנה על המידע ומערכות המידע הנחוצות לניהול חיים תקינים בישראל. בנוסף, תוצרי המיזם ישמשו בסיס חיוני להבטחת תקינות ואיתנות התשתיות הלאומיות ונכסים אסטרטגיים, לרבות חסינות מפני התקפה קיברנטית.

לצורך כך, תפקיד צוות המיזם היה לייצר בסיס ידע רחב, ולהגדיר את המצב הרצוי במדינת ישראל, לקראת התמודדות במרחב הקיברנטי, תוך פיתוח וחיזוק הכלכלה הישראלית. הצוות התמודד עם שלוש שאלות מרכזיות:

- מה הם הצעדים הנחוצים כדי לעודד ולפתח את התחום הקיברנטי בארץ, ולהביא לקפיצת מדרגה שתבטיח את מעמדה של מדינת ישראל בזירה העולמית?
- אילו תשתיות ידע דרושות כדי לטפל בצרכים בתחום חישוב-העל במדינת ישראל?
- אילו שינויי "הסדרה" (ארגון, אחריות, מדיניות ורגולציה) נחוצים כדי לאפשר התמודדות מיטבית עם האתגרים והאיומים במרחב הקיברנטי?

מסמך זה הוא פרי עבודתן של שמונה ועדות שפעלו במסגרת המיזם, ושל ניתוח שערכה חברת שלדור. המטרות של תת הוועדות מפורטות להלן:

- **תת ועדת הגנה, ניטור ובקרה:** לבחון באופן מעמיק את הצרכים בתחום ההגנה הקיברנטית, בכדי לענות על צרכי הביטחון הלאומי במובנו הרחב (כולל כלכלה וחברה) הנוכחיים והעתידיים. הוועדה עסקה, בין היתר, בבחינה של תפיסת ההגנה הקיברנטית של מדינת ישראל.
- **תת ועדת צופן וסימולציה**[5]**:** לבחון באופן מעמיק את הצרכים בתחום הצופן והסימולציה, ולהמליץ על תוכנית פעולה לקידומו.
- **תת ועדת חישוב–על ותשתיות רחבות פס:** לבחון באופן מעמיק את הצרכים בתחום חישוב-העל ותשתית תקשורת רחבת פס, ולהמליץ על תוכנית פעולה לקידומו.
- **תת ועדת פעולה:** לבחון באופן מעמיק את הצעדים הנחוצים לפיתוח יכולת הפעולה במרחב הקיברנטי, ולברר כיצד הם ישתלבו בתפיסה הקיברנטית הכוללת של ישראל.
- **תת הוועדה לבחינת תועלות כלכליות:** לבחון את התועלות הכלכליות של היוזמות שהתגבשו בתתי הוועדות של המיזם הקיברנטי, ואת כדאיותו הכלכלית של הפרוייקט למשק הישראלי ולתעשייה, כספק וכלקוח של הפרוייקטים השונים.
- **הוועדה לבחינת התועלות האקדמיות:** לבחון את הפערים בין המצב הרצוי למצב הנוכחי בהקשר האקדמי, להמליץ על תוכניות פעולה לקידום התחום, ולנתח את התועלות הלאומיות שלהן בהיבט האקדמי, בשני מימדים: (1) מענה לצרכי האקדמיה (בדגש על מהלכים בתחום מחשוב- על ותקשורת); (2) התרומה האפשרית של האקדמיה לבניית יכולות לאומיות (בדגש על קידום מו"פ ויצירת הון אנושי).

[5] במושג סימולציה, כוונתנו לסביבה המאפשרת לדמות, באופן נאמן, את המרחב הקיברנטי, או נתחים ממנו; לבצע מחקר אודות טכניקות הגנה ותקיפה; לערוך ניסויי כלים ולבחון את יעילותם, את הסיכונים שבהפעלתם ואת מגבלותיהם; לבדוק תפיסות הגנה אל מול תוקף, ותפיסות תקיפה אל מול גוף מגן, בכל הרמות.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

- **תת ועדת מדיניות וחקיקה:** מטרתה היתה (1) למפות את המצב הנוכחי במדינות העולם ובארגונים בינלאומיים רלוונטיים, בנוגע למדיניות המו"פ בתחום הקיברנטי; (2) לברר ולמפות את המצב הנוכחי במדינת ישראל בארבע זירות בתחום (מדיניות מו"פ, שיתופי פעולה בפועל, תקינה וחקיקה); (3) לעמוד על הפערים בין שני הסעיפים. כמו כן, הוועדה הצביעה על מספר מודלים לחיקוי (best practices) מן הפעילות של מדינות וארגונים בינלאומיים בתחום המו"פ הקיברנטי, שעשויים לקדם את מטרות המיזם בישראל.
- **תת ועדת הסדרת ההגנה על מערכות ממוחשבות חיוניות במדינת ישראל:** לבחון את המצב הנוכחי בתחום ההגנה על מערכות ממוחשבות, ולהמליץ על תפיסת הגנה כוללת של מערכות ממוחשבות (מדיניות הגנה קיברנטית).

האתגר המרכזי של המיזם הקיברנטי היה לראות כיצד באמצעות החיבור בין אקדמיה, תעשייה וביטחון, תיתכן קפיצת מדרגה שתאפשר למדינת ישראל להתמודד בצורה אופטימלית עם האתגרים הנוכחיים והעתידיים במרחב הקיברנטי.

תהליך הבחינה

את תהליך הבחינה של המיזם הקיברנטי הובילה הוועדה העליונה למדע וטכנולוגיה, ברשות יו"ר המולמו"פ פרופ' אלוף (מיל.) יצחק בן ישראל. הוועדה כללה נציגים מהגופים המרכזיים העוסקים במחקר ופיתוח במדינת ישראל: יו"ר הועדה לתכנון ותקצוב (הות"ת) במועצה להשכלה גבוהה- פרופסור מנואל טרכטנברג, ראש המינהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית (מפא"ת)- מר אופיר שהם, המדען הראשי במשרד התמ"ת- מר אבי חסון, יו"ר המועצה הלאומית לכלכלה- פרופסור יוג'ין קנדל, יו"ר הפורום לתשתיות לאומיות למחקר ולפיתוח (תל"ם)- פרופסור יעקב זיו, יו"ר האקדמיה הלאומית הישראלית למדעים- פרופסור רות ארנון, מנכ"ל משרד האוצר- מר חיים שני, ראש אגף התקציבים במשרד האוצר- ד"ר אודי ניסן. לצורך המיזם הקיברנטי הורחבה הוועדה וצורפו אליה מפקד יחידה 8200 - תא"ל נדב צפריר, מפקד היחידה לתקשוב ולטכנולוגיות המידע באגף התקשוב- תא"ל אילה חכים, ראש מטה לוט"ר במל"ל- תא"ל ניצן אוריאל, ראש הרשות הלאומית לאבטחת מידע בשב"כ- מר ארז קריינר והמדען הראשי בוועדה לאנרגיה אטומית- פרופסור דובי שוורץ. להרכב תתי הוועדות מונו אנשי מקצוע בעלי ניסיון וידע בתחומים השונים, ואליהם צורפו חברים מהגופים הנמנים על הוועדה העליונה לעיל (ראה נספח א'). סה"כ שקדו על המיזם למעלה מ- 80 איש במשך כחצי שנה.

ממצאים עיקריים של תתי הוועדות

בתחום ההגנה, ניטור ובקרה נמצא שהתקפות קיברנטיות הן בגדר פוטנציאל לאיום מהותי על הרצף התפקודי של המדינה, מוסדותיה ואזרחיה. הוועדה זיהתה פער מרכזי בהגנה קיברנטית על המרחב האזרחי הכולל. קיימים אומנם גופים המספקים מענה לתשתיות הביטחון ולמערכות קריטיות, אך יש פער בין רמת המודעות למהות האיום לבין עוצמתו, וחסרה פעילות מו"פ בנושא ההגנה הקיברנטית. הוועדה מצאה שלישראל אכן יש פוטנציאל להציב את עצמה כשחקן מוביל בעולם בתחום ההגנה הקיברנטית.

בתחום הצופן נמצא שהצופן הביטחוני הוא מרכיב מכריע בחוסן של מערכות ביטחוניות במרחב הקיברנטי, היות והצופן נדרש להתמודדות עם תקיפות קיברנטיות (לצד תקיפות צופן מסורתיות). שימור ופיתוח יכולות פעולה בתחום הצופן מהווה אפוא יכולת מדינתית חשובה. נמצא כי העיסוק במחקר צופן בתעשייה דל ביותר, והשוק מתבסס על יכולות מדף ותקנים אזרחיים. עם זאת, באקדמיה יש מספר קטן של חוקרים פורצי דרך בתחום התיאורטי, אך העיסוק במחקר התיאורטי אינו תורם ישירות לצרכי הביטחון. הוועדה הצביעה על מספר אתגרים עיקריים ובעיות בעלות חשיבות עליונה שיש לפתור: שימור ופיתוח היכולות בתחום הצופן בעידן הקיברנטי, הרחבת יכולות הצופן הביטחוני למגזרים נוספים ועיסוק בסוגיות צופן הנוגעות למגזר הפרטי

בתחום הסימולציה נמצא שקיים צורך בסימולציה של המרחב הקיברנטי, או חלק ממנו, במערכת הביטחון, בתעשייה ובאקדמיה לטובת מחקר ופיתוח, בחינת כלים, בחינת תפיסות, אימון טקטי ואימון אסטרטגי. חלק מהחברות האזרחיות, שזקוקות ליכולות סימולציה, כבר מחזיקות ברשותן יכולות סימולציה עצמאיות מתאימות, ומעבדת סימולציה תסייע להם להשלים את יכולותיהן הנוכחיות.

בתחום חישוב–העל נמצא שאין מסה קריטית של ידע ברמה בינלאומית בתחום חישוב עתיר ביצועים (HPC) במדינת ישראל, בדגש על ההיבט המעשי של HPC. קיימים ״איים״ של עיסוק בנושא, אך אין ביניהם סינרגיה, והם מפוזרים באופן שאינו מעודד שיתוף פעולה. הוועדה מצאה שבמקומות שבהם יש מחשבים עתירי ביצועים בישראל, קיימים פערי ידע בנוגע למחשב ולסביבתו, שניתנים לפתרון עם משאבים מתאימים וידע מקצועי ברמה הנחוצה. חלק מהצרכנים אינם מודעים לאפשרויות הרבות לקידום ושיפור הטמונות בשימוש ב- HPC ובסביבה תומכת. הוועדה מצאה שהקמת מרכז מחקר אקדמי, שיתפקד כמרכז ידע לאומי לחישוב-על, הוא תנאי הכרחי לקידום נושא ה- HPC בישראל, אך בחלק מהמגזרים נחוץ גם טיפול בפערים בין הציוד הנדרש לניצול מירבי של יכולותיו, לבין רמת הציוד הקיים.

בתחום הכלכלה נמצא שתעשייה ישראלית חזקה ומובילה היא רכיב מכריע ביצירה ובשימור על היכולות של מדינת ישראל במרחב הקיברנטי. הוועדה הצביעה על כך, שבישראל קיימת כבר כיום פעילות עסקית ענפה בתחום, והמליצה שפיתוח התעשייה הרלוונטית ייעשה סביב צרכי ההגנה הלאומית של מדינת ישראל במרחב הקיברנטי. הוועדה ציינה את הצורך לקדם את התעשייה הקיברנטית האזרחית באמצעות גוף בעל קשרים עם מערכות ההגנה האזרחית ובעל הכרות מעמיקה של טכנולוגיות. לדעת הוועדה, קידום פרוייקטים ממשלתיים משמעותיים בתעשייה, יכול ליצור יתרונות יחסיים חדשים לתעשייה הישראלית ולחוסנה הלאומי של מדינת ישראל.

בתחום האקדמיה נמצא כי לאקדמיה בישראל ישנם צרכים בתחומי ידע, ייעוץ והכשרה מקצועית בחישוב מתקדם. נחוץ שדרוג של יכולות חישוב- על מקומיות ולאו דווקא מתן שירות של חישוב-על מרכזי. הוועדה מצאה, בנוסף, כי דרוש שדרוג משמעותי ברוחב הפס בחיבור לתקשורת באקדמיה. בכל הנוגע לצרכי מערכת הביטחון והתעשייה, תת הוועדה מצאה כי צריך לחזק את המחקר המדעי בארץ בתחום הקיברנטי, ודרוש מרכז ידע ומחקר בתחום חישוב-העל. ממצאי הוועדה מצביעים על כך, שיש צורך להגדיל את שיתופי הפעולה המחקריים בין המגזרים אקדמיה-ביטחון-תעשייה, ולשם מימוש, יש לחזק את ההוראה בתחום, כדי להכשיר כוח אדם מתאים. בנוסף, חשוב להגדיל את שיתוף הפעולה בתחום בין האקדמיה לבין מקבלי ההחלטות וקובעי המדיניות.

בתחום המדיניות והחקיקה נמצא שמדינות וארגונים בעולם גוזרים את מדיניות המו״פ ממדיניות כללית של ביטחון קיברנטי. לעתים קרובות, ראש המדינה בעצמו מוביל את תהליך גיבוש המדיניות, בגלל התפיסה שמדובר בהיבט חשוב של האסטרטגיה הלאומית. במסגרת מדיניות המו״פ הקיברנטי, מספר מדינות מגדירות בצורה מפורשת תחומי מחקר חיוניים לפיתוח יכולות ליבה, ומעניקות תעדוף להשקעת משאבים לאומיים בהם. הוועדה הצביעה על כך, ששיתוף פעולה בינלאומי הוא מרכיב מכריע במדיניות הקיברנטית של ישראל, בגלל האופי הגלובאלי של אתגרי המתחם הקיברנטי ואיומיו. שיתוף הפעולה רלוונטי בארבעה תחומים: גיבוש מדיניות מו״פ, פרוייקטי מו״פ, חקיקה ותקינה. כדי לקדם את המו״פ הקיברנטי בארץ, הוועדה ציינה שקיים צורך במידה רבה יותר של שקיפות בתהליכים הרגולטוריים הקשורים לייצוא טכנולוגיות, ובקיום ״הסברה עסקית״ למשקיעים ישראלים וזרים. יש גם חשיבות רבה לריכוז המידע בצורה זמינה לציבור.

בתחום הסדרת ההגנה על מערכות ממוחשבות נמצא שפוטנציאל הפגיעות של ישראל נובע, בין היתר, ממענה בלתי מספק לתשתיות מדינה (גופים מאובטחים), פער בהסתכלות לאומית רחבה על סוגיית המרחב הקיברנטי בכלל והביטחון הקיברנטי בפרט, קושי לממש את האחריות של ועדת ההיגוי העליונה[6] להגן על מערכות ממוחשבות, וחוסר בתיאום בין מערכת הדינים הישראלית לבין המציאות הקיברנטית החדשה. הוועדה מצביעה על כך, שפגיעה מצומצמת או רחבה בגופים או בחברות יכולה לגרום נזקים כבדים, ובכך לפגוע קשות בתפקוד המדינה ובחוסן האזרחי והחברתי שלה.

[5] ועדה זו, בראשות היועץ לביטחון לאומי, הוגדרה בשנת 2002 ע״י הממשלה (החלטה ב/84) כאחראית על הראייה הלאומית הכוללת.

לנוכח הלקחים מניהול ועדת ההיגוי להגנת מערכות ממוחשבות במטה לוט"ר, ומספר המלצות רוחביות של ועדות המיזם הקיברנטי להקים מטה קיברנטי לאומי, תת הוועדה מצאה שדרוש גוף מטה קיברנטי לאומי להגנה, התוויית מדיניות כוללת להגנה על מערכות ממחשבות בישראל ("מדיניות קיברנטית לאומית"),

פיתוח תפיסת הפעלה מדינתית בשגרה. היערכות ראשונית לחירום קיברנטי (כולל חדר מצב קיברנטי לאומי וכוח תגובה CERT), וגיבוש תוכניות ביצוע הכוללות תוכנית מו"פ קיברנטי אסטרטגי. בנוסף, **חשוב לערוך בדיקה מערכתית של החקיקה הישראלית** הרלוונטית לתחום הקיברנטי, כדי לבחון את מידת התאמתה למציאות הקיברנטית המתפתחת. תת הוועדה סבורה, שחלוקת האחריות בין גופי הביצוע בתחום ההגנה על תשתיות ממחושבות חיוניות בישראל, אינה מצריכה שינוי.

לאור הממצאים שלעיל, צוות המיזם סבור כי היוזמות הבאות נחוצות להתמודדות יעילה וארוכת טווח של מדינת ישראל במרחב הקיברנטי:

המלצות

המלצה 1א – הקמת מטה ורשות סייבר לאומית

הקמת מטה קיברנטי לאומי להגנה שייעודו קידום הגנת המרחב הקיברנטי בישראל.

- במקום ועדת ההיגוי (שהוגדרה בהחלטה ב/84).
  - גיבוש מדיניות להגנת מערכות ממוחשבות
  - ייזום פעולות לחינוך והעלאת המודעות
  - ייזום פיתוח כלים טכנולוגיים לתשתיות מדינה ולמגזר האזרחי
  - פיתוח כלים רגולטוריים וקש"ח מקבילים
  - גיבוש תפיסה לחירום במרחב הקיברנטי
- יש לשמור על המצב הקיים בנוגע לאחריות גופי הביצוע הקיימים בהגנה על מערכות ממוחשבות.

המלצה 1ב – גוף ביצוע לאבטחת המגזר האזרחי

- הקמת גוף ביצוע, או הרחבת סמכויות של גוף ביצוע קיים (לדוגמא רא"מ), לטיפול באבטחת המגזר האזרחי.

המלצה 2 – מדיניות וחקיקה לעידוד תעשיית הסייבר

- שיפור רמת השקיפות בתהליכי הייצוא והייבוא הרלוונטיים למו"פ קיברנטי, ומיסוד תהליך של חוות דעת מוקדמת (pre-ruling), במיוחד במסגרת חוק הפיקוח על ייצוא ביטחוני וצו הצופן, כדי להקל על הליך קבלת רישיונות הייצוא.
- קידום מיקור חוץ במערכת הביטחון ושותפות בין ביטחון לתעשייה, תוך התייחסות לסוגיית הבטחת קווי ייצור של מוצרים ושירותים.
- הצטרפות ישראל בצורה פרו-אקטיבית, מושכלת ושיטתית לתהליכים הבינ"ל המואצים בתחום המו"פ הקיברנטי.
- מעבר לתחום המו"פ, בדיקה מערכתית של חקיקה ישראלית נוספת, רלוונטית לתחום הקיברנטי, כמו חוק התקשורת, חוק העונשין וחקיקת החירום של ישראל.
- הגברת המעורבות של גורמי תקינה (כמו מת"י) בתהליכי התקינה בתחום המו"פ הקיברנטי בעולם, ובפיתוח תקינה מקומית ככלי רגולטורי מעודד תעשייה.
- ריכוז מסמכי מדיניות ממלכתיים, חקיקה, "הסברה עסקית", נתונים כלכליים ועוד מידע רלוונטי לציבור, במקום אחד וזמין כגון אתר אינטרנט מיוחד לנושא.

המלצה 3 – עידוד מו"פ בתחומי סייבר וחישוב–על

המלצה 3א – עידוד המו"פ

- הקמת מרכז ידע אקדמי מחקרי בתחום הקיברנטי ובתחום מחשוב-העל.
- תגבור מענקי מחקר בתחום.
- חיזוק המחקר המדעי בתחום הסייבר בישראל וביסוס מעמדו כגורם מוביל בעולם:
  - גידול במספר חברי הסגל האקדמי בתחומים רלוונטיים באמצעות "השבת מוחות" ועידוד מחקר של חוקרים ותיקים וחדשים.
  - הגדלת תקציבי המחקר המוקצים לתחומים רלוונטיים.
  - שיפור ושדרוג התשתיות המחקריות הרלוונטיות באוניברסיטאות (כגון רוחב הפס וה-clusters הקיימים).
  - יצירת מסה קריטית והעצמת היתרונות היחסיים במחקר בתחום במוסדות האקדמיים השונים.
- גידול במספר הסטודנטים בתחום במסגרת התואר הראשון והשני.
- שינוי מדיניות צה"ל/אמ"ן לגבי פרסום עבודות אקדמיות.
- עידוד שיתופי פעולה מחקריים בתחום הסייבר בין המוסדות להשכלה גבוהה, לבין מערכת הביטחון והתעשייה.
- חיזוק ההוראה בתחום לצורך הכשרת כוח אדם.

המלצה 3ב – מרכז לאומי בתחום חישוב–העל

- הקמה של מרכז לאומי לחישוב-על, כחלק ממוסד אקדמי, שייעודו:
  - הובלת המחקר והפיתוח בתחום חישוב-העל וחישוב עתיר ביצועים.
  - תכנון ומימוש של פרוייקטי מו"פ רלוונטיים.
  - הוראה, הכשרת אנשי מקצוע וחוקרים וייעוץ והכוונה למשתמשים.
- תכנון וניהול תוכנית עבודה במשותף עם מערכת הביטחון והתעשייה.
- הקמת מעבדה עם מחשב-על למחקר ברמה עולמית (200TF).
- הסתכלות מערכתית, ארוכת טווח ומשולבת ורציפות תקציבית לאורך שנים ארוכות (לפחות עשור).
- המרכז ישמש כתשתית למחקר מתקדם, שכיום לא אפשרי במדינת ישראל.
- המרכז מהווה תנאי הכרחי אך לא מספק לצרכי הביטחון.

המלצה 4 – תשתיות פיתוח לטכנולוגיות סייבר

המלצה 4א – יכולות סימולציה

- הקמת מרכז דימות המאפשר את הדברים הבאים: דימוי העולם הקיברנטי, או נתחים ממנו; ביצוע מחקר של טכניקות הגנה ותקיפה; ניסוי כלים ובחינת יעילותם, בדיקת הסיכונים שבהפעלתם ומגבלותיהם; בדיקת תפיסות הגנה מול תוקף, ותפיסות תקיפה מול גוף מגן.
- מרכז הדימות ישמש גם לטובת אימון ותרגול גורמי ההגנה (מנהלי רשת, מנהלי אבטחת מידע, משתמשי קצה וכד'), כדי לקדם את ההגנה בסייבר, לצד רגולציה המחייבת להתאמן.
- פיתוח תשתיות דימות יתבצע באמצעות מערכת הביטחון (מפא"ת, מצו"ב ורא"ם), התעשייה הביטחונית והאקדמיה.

המלצה 4ב – מעבדת הסמכה

- פיתוח מעבדות הסמכה למוצרי צופן והגנה, לצד רגולציה המחייבת להשתמש במוצרים שאושרו עבור תשתיות קריטיות ומערכות ממשלתיות.
- המעבדה תאשר מוצרים בלתי מסווגים, ותעריך את רמת ההגנה שלהם.

- תהליך ההסמכה יוזל, בין היתר, באמצעות התמקדות בצרכי מערכת הביטחון והתשתיות הקריטיות, ולא בכל מרחב הדרישות של התקן.
- תהליך ההסמכה הביטחוני יחפוף לתהליך ההסמכה התקני, ולכן, בהשקעה נוספת, תושלם ההסמכה במעבדות מוסמכות אחרות.
- ההסמכה הביטחונית תתרום למוניטין של המוצרים (פיצוי מסוים על חוסר הסמכה).
- ניתן להמליץ לציבור הרחב על מוצרים שנבדקו, ובכך לשפר את הביטחון של המערכות במרחב האזרחי (בלי תלות בהסמכה פורמאלית).

המלצה 5 – חינוך, השכלה גבוהה והעלאת המודעות הציבורית לסייבר

- העלאת המודעות הציבורית למרחב הקיברנטי בכלל ולאיומים בפרט, מגני ילדים ועד למחקר אקדמי מתקדם, באמצעות פעילויות שונות, כגון:
  - הגברת לימודי מדע וטכנולוגיה, מחשוב והגנה קיברנטית במסגרות החינוך הקדם אקדמיות.
  - מסגרות שעות פנאי: גדנ"ע סייבר, צופי סייבר, נוער מחונן וכו'.
  - הגדלת מכסות הסטודנטים ותוכניות לימודים אקדמיות בנושא.
  - השתלמויות בתחום פיתוח מאובטח של קוד לחברות הזנק וחברות ישראליות.

המלצה 6 – פיתוח כלים לחירום בסייבר

- פיתוח מענה שיאפשר קימום ו"יציאה" ממצבי התקפה, להמשכיות והפעלה מחודשת של יכולות של מערכות חיוניות שנפגעו מאירועי והתקפות מידע. המענה כולל בין היתר:
  - פיתוח יכולות לתפקוד והמשכיות תחת התקפה של מערכות חיוניות.
  - יכולות להעלות מידע מחדש על גבי מערכות שנפגעו עקב אירועי אבטחת מידע.
  - מערכות גיבוי שמופעלות לאחר שאירוע האבטחה הסתיים, או תוך כדי אירוע מתמשך.
  - הגדרת תוכנית פיתוח טכנולוגית ואופרטיבית, אשר תגדיר את המענה והמשאבים הנחוצים לכל תת קבוצת ייחוס, על פי חשיבות ההמשכיות והתפקוד שלה תחת ההתקפה, וכן על פי רמת התפקוד הנדרשת ממנה במצב זה. התוכנית תכלול זיהוי טכנולוגיות קיימות, פיתוח מענה לפערים שאינם בנמצא, פיתוח שיטות אינטגרציה של מערכות, והגדרת תורת פעולה במקרה של התקפה מוצלחת.
  - יישום התוכנית יכלול תרגול עיתי של יכולות הקימום וההתאוששות של גורמי הייחוס, והגדרת צוותי ונהלי בדיקה מתאימים.

המלצה 7 – מעטפת הגנת סייבר לאומית

- מעטפת הגנה לאומית כוללת מערכות ממוחשבות אוטומטיות ומערכות אנושיות, האמורות לספק ביחד הגנה על מערכות מחשב שהוגדרו להן מראש. הפתרון המוצע מיועד להתמודד עם ארבעת הפעילויות הבאות:
  - מערכת איסוף - מערכת מעקב ואיסוף מידע, שתאפשר הגנה על מערכות מחשב שהוגדרו לה מראש מפני תקיפה.
  - המערכת נדרשת לזהות תקיפה בהקדם האפשרי, רצוי עוד בשלבי ההתארגנות של היריב לתקיפה, ולספק התרעה למרכז הבקרה.
  - מרכז תגובה וחירום (CERT) - מרכז התגובה והחירום יספק מענה לטיפול במתקפה מרגע שזוהתה והוחלט כי היא דורשת טיפול.
  - מערכת הסדרה ופיקוח - קיים צורך להסדיר את הפיקוח על מערכת זו תוך שמירה על צנעת הפרט.
  - מרכז בקרה - ימומש בנפרד במטה הקיברנטי הלאומי.

המלצה 8 – פיתוח פתרונות להגנה מקומית / מבוזרת

- חלק מהמענה להעלאת רמת הביטחון יפותח באמצעות שדרוג מבוזר של יכולות בארגונים השונים ובקרב האזרחים. הטכנולוגיות יפותחו ביוזמה ממשלתית, ויינתנו או יימכרו כהטבה לאזרחים ו/או לארגונים במדינה.
- חלק מהפתרונות דורשים עדכוני חקיקה, על מנת שניתן יהיה להפעילם בצורה מבוזרת.
- דוגמאות:
  - חיוב של דיווח תקופתי לדירקטוריון על רציפות תפעולית והגנת תשתיות בכל ארגון משמעותי.
  - עידוד פיתוח מערכות ניטור והתראה.
  - סנסורים תוכנתיים המעבירים אינפורמציית ניטור על מצב הרשת.
  - מלכודות דבש לאיתור פוגענים ממוקדים.
  - עידוד והטמעה של התקנת תוכנות הגנה.
  - קידום הטמעת האיום מהסייבר ופיתוח תפיסת ההתמודדות הארגונית איתו. עידוד פיתוח כלים חדשים להתמודדות עם האיום.

המלצה 9 – פיתוח טכנולוגיות ופתרונות כחול–לבן

- עידוד פיתוח מוצרים ופתרונות אבטחת מידע 'כחול לבן', כדי להפחית את התלות בגורמי חוץ, ולשפר את היכולות הטכנולוגיות של התעשייה הישראלית. הוועדה ממליצה לשקול במסגרת זו תוכנת אנטי וירוס ישראלית, קומפיילר מאובטח, מערכות סינון תוכן והרשאות, ולעודד הקמת עננים מסחריים ישראליים[6], ואולי גם שלוחות של עננים מחו"ל.
- אבני בניין לצופן - יפותחו מראש בשתי גרסאות - גרסה ביטחונית וגרסת יצוא, כך תהליך הפיתוח יבנה מראש את היכולת לייצא (במגבלות הייצוא הביטחוני) תוצרים של התעשייה הצבאית הכוללים יכולות צופן.

המלצה 10– וועדת מעקב של המיזם

- הועמ"ט תעקוב אחר היישום והבקרה על המלצות המיזם הקיברנטי שאושרו בממשלה, ותדווח על ההתקדמות לראש הממשלה

[6] ראו פירוט על נושא מחשוב העננים הישראלי- שהוא בעל חשיבות רבה בעיני הוועדה- בנספח הרלוונטי של ועדת ההגנה

סיכום:

המרכיבים האזרחיים והביטחוניים במרחב הקיברנטי שזורים זה בזה, וחלקם בלתי ניתנים להפרדה. לנוכח זאת, יש צורך בסינרגיה לאומית בין המגזרים, כתנאי להצלחה בהתמודדות עם האתגרים העתידיים. לכן, **ישנה חשיבות לבחינה בינתחומית ורב-תחומית של סוגיית המרחב הקיברנטי, שנובעת מהאופי הייחודי של האתגרים שהוא מציב. לאור זאת, דרושה הסתכלות לאומית רחבה והבנה שהיערכות מדינת ישראל לעידן הדיגיטאלי איננה רק משימה ביטחונית, אלא משימה לאומית. זאת ועוד, בשל היקף הפעילות והמשאבים שיידרשו, תוכנית לאומית היא האפשרות היחידה להגשמת החזון ולהובלה עולמית ישראלית.**

על כן, **כחלק מהתמודדות המדינה עם העתיד הדיגיטאלי והאיומים הקיברנטיים, נחוץ טיפול מערכתי, שינויי רגולציה וחקיקה, תיאום בין הגופים, שיתוף פעולה בין האקדמיה, המגזר העסקי ומערכת הביטחון ותקציב. ככל הנראה, נדרשים גם שינויים בתפיסות הביטחון והמדיניות הציבורית.**

את ההמלצות המובאות במסמך זה, המונחות על שולחן הממשלה, כתבו במשותף גופי המפתח העוסקים בכל ההיבטים של המרחב הקיברנטי במדינת ישראל. בראייתנו, **תוכנית זו, אם תאושר, עשויה לתרום באופן משמעותי לניצול מושכל של הטכנולוגיה המתפתחת, תוך קפיצת מדרגה משמעותית בהיבטים רבים, ובכך תחזק את חוסנה הלאומי של מדינת ישראל.** אנשי המקצוע, החוקרים, הגופים והמוסדות שנטלו חלק בגיבוש נייר זה, הביאו לידי ביטוי את ניסיונם המגוון בתחום הטכנולוגיה, ניהול מו"פ, ניתוח מדיניות ואסטרטגיה, ביטחון לאומי ומשפט, והשילוב ביניהם הוביל לכדי המלצה מאוזנת וכוללת, אשר השלם בה גדול מסך חלקיה.

תוכן העניינים

1. מכתב יו״ר המולמו״פ 3

2. תקציר מנהלים 5
- רקע 6
- המלצות 9
- סיכום 12

3. תוכן העניינים 13

4. המייזם הקיברנטי הלאומי– דו״ח סופי 18

5. הנחיות ראש הממשלה 19

6. הצורך, האיום וההזדמנות 20

7. מטרת הצוות הלאומי ומשימותיו 21

8. תיחום העבודה 22

9. אסטרטגיה כללית 23

10. ממצאים עיקריים ותועלות לאומיות (אקדמיות/ כלכליות/ ביטחוניות) 24

11. המלצות 25

12. התועלות הלאומיות 26

13. דו"ח תת ועדת הגנה, ניטור ובקרה 27

1. מטרת הוועדה ומשימותיה 28
   1.1. הגדרת איומי הסייבר 29
   1.2. קבוצת ייחוס- מערכות מסחריות 29
   1.3. קבוצת ייחוס- אנשים פרטיים 29
2. שיטות העבודה להשגת היכולות 29
3. ממצאים עיקריים 30
   3.1. זיהוי הנכסים והיתרונות היחסיים בישראל 30
   3.2. חולשות עיקריות 31
   3.3. מגמות עולמיות מרכזיות בהגנת הסייבר 31
   3.4. מצב קיים בישראל 32
   3.5. אתגרים עיקריים ובעיות בעלות חשיבות עליונה עליונה שיש לפתור 32
4. המלצות 33
   4.1. כללי 33
   4.2. המלצות ומפת דרכים להכוונת הצורך 36

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4.3. מדדים להצלחה 37
5. נספחים 38
5.1. נספח א. פרוייקטים לאומיים 38
5.2. נספח ב. חינוך ומודעות 38
5.3. נספח ג. פרוייקט מעטפת הגנת סייבר למדינה- פירוט 39
5.4. נספח ד. עידוד המחקר- פירוט 41
5.5. נספח ה. חיסון התשתית 42
5.6. נספח ו. עצמאות טכנולוגית- פירוט 42
5.7. נספח ז. יכולת קימום והתאוששות- פירוט 43
5.8. נספח ח. מחשוב עננים ישראלי 43

14. דו"ח תת ועדת צופן וסימולציה 45

צופן

- תמצית מנהלים 46
- קווי היסוד של ההמלצות המרכזיות בדו"ח 46

1. עולם הצופן- רקע 47
1.1. השלבים העיקריים בפיתוח פתרון צופן 47
1.2. תחומי המחקר, הידע והטכנולוגיה 47
1.3. מגמות חדשות בצופן 48
2. אתגרים 48
2.1. פיתוח תחומי מחקר מרכזיים 48
2.2. היקף כוח אדם מתאים 49
2.3. צופן במרחב האזרחי 49
2.4. קידום הצופן כענף כלכלי 49
2.5. אסטרטגיית צופן 49
3. ניתוח חסמים 49
3.1. כוח אדם לצופן במערכת הביטחון 49
3.2. הגנה על תשתיות קריטיות 50
3.3. תעשיית הצופן כתעשיית יצוא (צו הצופן) 50
4. המלצות 51
4.1. תחומי עדיפות 51
4.2. הכשרת כוח אדם 51
4.3. פיתוח המחקר באקדמיה (בשיתוף התעשייה ומערכת הביטחון) 51
4.4. בניית פלטפורמות לעידוד שיתוף פעולה בין הצבא לאקדמיה לפי רמת סיווג 51
4.5. פיתוח פיתרונות לצופן לתשתיות קריטיות למערכות ממשלתיות ולסביבה עתירת ידע 52
4.6. מעבדת הסמכה למוצרי צופן והגנה 53
4.7. פיתוח מוצרי צופן לתשתיות קריטיות ומערכות ממשלתיות 54
4.8. פרוייקט לאומי- פיתוח אבני בניין לצופן 54
4.9. הצפנה לציבור הרחב 54
5. נספחים
נספח 1 55
נספח 2 55
נספח 3 56

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

סימולציה

1. סימולציה- רקע 57
1.1. מטרות 57
1.2. סימולציה ומרכזיותה 57
1.3. תיחום העבודה 57
1.4. עיקרי ההמלצות 58
2. ממצאים עיקריים 58
2.1 מצב קיים- אקדמיה 58
2.2. מצב קיים- סימולציה במערכת הביטחון 59
2.3. מצב קיים- תעשייה 59
2.4. מצב קיים- יכולות סימולציה בעולם 59
3. דרישות מיכולות הסימולציה 60
3.1. דימוי סביבות גמיש ומהימן 60
3.2. יכולות מחקר 60
3.3. יכולות תקיפה והגנה 61
3.4. יכולות תפעוליות נדרשות 61
3.5. יכולת שו"ב לסימולטור 61
3.6. תפיסת המענה 62
3.7. תוכניות פיתוח לתשתיות סימולציה 62
3.8. נושאי מחקר הנוגעים ליכולות סימולציה 63

15. דו"ח תת ועדת חישוב–על ותשתיות תקשורת רחבת פס 65

1. תקציר מנהלים 66
2. מטרת המסמך ומבנהו 67
3. תהליך העבודה ומתודולוגיית הניתוח 67
4. רקע מקצועי 68
4.1. עולם הבעיה 68
4.2. עיבוד 68
4.3. תקשורת פנימית 69
4.4. תקשורת חיצונית 70
4.5. זיכרון 70
4.6. אחסון עתיר ביצועים 70
4.7. תוכנה 71
4.8. ארכיטקטורה 71
4.9. (Massive Parallel Prossing MPP) 71
4.10. Symmetric Multi-Processing 71
4.11. ארכיטקטורה חישוב היברידית (Hybrid Computing) 71
4.12. אולם המחשב, קירור ואריזה 72
4.13. ביצועים 72
4.14. עולמות בעיה משיקות 72
4.15. מחשוב שריגי (Grid Computing) 73
4.16. מחשב ענן (Cloud Computing) 73
4.17. סקירה בסיסית של השוק 73
4.18. ספקי OEM 73

4.19. חברות מוצרים ל- HPC 74
5. מגמות עולמיות 74
5.1. חישוב-על בעולם 74
5.2. אסטרטגיות ומגמות חישוב-על בארה"ב 74
5.3. אסטרטגיות ומגמות חישוב-על באיחוד האירופאי 75
5.4. אסטרטגיות ומגמות חישוב-על בסין 75
6. תמונת המצב בישראל 76
6.1. המצב בתחום HPC בארץ 76
6.2. מערכת הביטחון 76
6.3. התעשיות 76
6.4. התעשיות הביטחוניות 76
6.5. מחקר מדעי אקדמי 77
6.6. עיקרי הפערים 77
7. הצעה לפעולה 78
7.1. עקרונות הפתרון 78
7.2. פירוט ועלויות 79
7.3. שלב הגיבוש 80
7.4. השלב היציב 80
8. סיכום והמלצות 80

16. דו"ח תת הוועדה לבחינת התועלות הכלכליות בפיתוח תעשיית סייבר ישראלית 81

1. תמצית ועיקרי המלצות 82
2. הקדמה 83
2.1. השפעת תעשיית הסייבר הישראלית על הגנת המדינה במרחב הקיברנטי 83
2.2. השקעה בפיתוח 84
2.3. התערבות הממשלה בפיתוח תעשיית הסייבר 85
3. בחינת תועלות כלכליות ותעדוף בין תחומים ויוזמות 86
3.1. מדיניות תעשייתית ותעדוף בין תחומים ויוזמות 86
3.2. משמעות התועלות הכלכליות בבחינת המיזם והיוזמות השונות 86
3.3. עקרונות כלכליים לבחינת התועלות הכלכליות 87
3.4. מתודולוגית בחינת התועלות הכלכליות- ברמה הכללית והפרטנית 88
4. הקבצי הפעילויות בתחום והערכת פוטנציאל כלכלי-תעשייתי 90
4.1. מעטפת הגנה למדינה במרחב הקיברנטי 90
4.2. תשתית פיתוח לטכנולוגיות המרחב הקיברנטי 91
4.3. עידוד מו"פ בתחומי המרחב הקיברנטי וחישוב-על 92
4.4. פיתוח כילים לחירום במרחב הקיברנטי 93
4.5. פיתוח פתרונות להגנה מקומית / מבוזרת 94
4.6. פיתוח טכנולוגיות / פתרונות כחול-לבן 94
4.7. מטה ורשות קיברנטיים לאומיים 95
4.8. חינוך, השכלה גבוהה והעלאת המודעות למרחב הקיברנטי 96
4.9. מדיניות ורגולציה לעידוד תעשיית הסייבר 98
5. אופי המימון של ההקבצים 98
6. המלצות הועדה 100
6.1. המלצות לארגון התוכניות אל מול השוק הפרטי 100
6.2. המלצות כלליות לקידום תעשיית הסייבר בישראל 100

6.3. המלצות לפעילות מנהלת לפיתוח תעשיית הסייבר הישראלית 101
6.4. בחירת פרוייקטים בתעשייה 103

17. דו"ח תת הוועדה לבחינת התועלות האקדמיות 105

1. תקציר מנהלים ועיקרי ההמלצות 106
2. רקע 107
2.1. מטרת המסמך 107
2.2. תת הוועדה לתועלות באקדמיה 107
2.3. תהליך העבודה והמתודולוגיה 107
3. מיפוי המצב הנוכחי 108
3.1. יכולות ונכסים של האקדמיה הישראלית 108
3.2. מיפוי שיתופי הפעולה בין האקדמיה לבין מערכת הביטחון והתעשייה 110
3.3. מיפוי השקעות נוכחיות בתחום הסייבר באקדמיה הישראלית 110
4. אפיון צרכי האקדמיה 111
5. אפיון צרכים לאומיים שדורשים מענה במסגרת האקדמיה 112
6. אפיון מענים אפשריים של האקדמיה לצרכים שעלו 113
6.1. עקרונות לעיצוב המענים 113
6.2. מענים מוצעים 114
6.3. הערכת תועלות לאקדמיה, לתעשייה ולמערכת הביטחון 116
6.4. הערכת עלויות 116
7. נספחים 117
ניספח א - סיכום של דיון "שולחן עגול" של תת-הוועדה לבחינת התועלות האקדמיות 119
נספח ב - מייל של אשר רוטקופ, אוניברסיטת תל-אביב, 17.2.11 122
נספח ג - מכתבם של נציגי מכון ויצמן, 17.2.11 123
נספח ד - מתוך מכתבו של פרופ' בר יוסף מהטכניון, 10.2.11 127
נספח ה - מכתבו של פרופ' גיא תל צור, אוניברסיטת בן-גוריון, 22.10.10 128
נספח ו - מתוך מכתבו של פרופ' דרור פייטלסון, 1.2.11 130
נספח ז - מכתבו של פרופ' עודד הוד, אוניברסיטת תל-אביב, 8.3.11 130

18. דו"ח תת ועדת מדיניות וחקיקה 131

1. תמצית מנהלים 132
2. ממצאים וניתוח צרכים ופערים 133
3. המלצות מפורטות של תת ועדת הסדרה וחקיקה 134
3.1. כללי 134
4. מבוא 135
5. מיפוי של תהליכי גיבוש מדיניות וחקיקה בתחום הקיברנטי בקרב מדינות וארגונים נבחרים 135
5.1. כללי 135
5.2. תוכניות מו"פ לאומיות של מדינות נבחרות 137
5.3. מדיניות ותכניות מו"פ בארגונים בינלאומיים נבחרים 144
5.4. תקינה בינלאומית 149
5.5. מיפוי המצב הנוכחי בארץ בנוגע למו"פ בתחום הקיברנטי והסדרתו 153
6. הסדרה, חקיקה ותקינה בישראל 156
6.1. חקיקה ישראלית רלבנטית למו"פ בתחום הקיברנטי 156
6.2. תקינה ישראלית ומו"פ קיברנטי 161

7. סיכום 161
8. ביבליוגרפיה נבחרת 162
9. נספחים 163
נספח א - הגדרות ומושגים במיזם הקיברנטי 163
נספח ב - ניתוח דברי חקיקה ישראליים רלבנטיים 165
נספח ג - מאגד סייבר של המדען הראשי ב 166

19. דו"ח תת ועדת ההסדרה על מערכות ממוחשבות חיוניות במדינת ישראל 168

20. נספח א – רשימת חברי הוועדות 169
1. חברי הוועדה העליונה למדע וטכנולוגיה (הועמ"ט) 170
2. חברי תת ועדת הגנה, ניטור ובקרה 171
3. חברי תת ועדת חישוב-על ותשתית תקשורת רחבת פס 172
4. חברי תת ועדת צופן וסימולציה וסימולציה 173
5. חברי תת הוועדה לבחינת התועלות האקדמיות 174
6. חברי תת ועדת מדיניות וחקיקה 175
7. חברי תת הוועדה לבחינת התועלות הכלכליות 176
7. חברי תת ועדת הסדרה וחקיקה 177
9. נציגי חברת שלדור שלקחו חלק במיזם 178

המיזם הקיברנטי הלאומי-
דו"ח סופי

הנחיות ראש הממשלה

5

הצורך, האיום וההזדמנות

2 מטרת הצוות הלאומי ומשימותיו

תיחום העבודה

אסטרטגיה כללית

ממצאים עיקריים ותועלות לאומיות (אקדמיות/ כלכליות/ ביטחוניות)

המלצות

התועלות הלאומיות

דו"ח תת ועדת הגנה, ניטור ובקרה

1. מטרת הוועדה ומשימותיה

הוועדה פעלה במסגרת המיזם הקיברנטי, שמטרתו לבחון את האפשרות להקים תוכנית מחקר ופיתוח לאומית לבניית יכולות במימד הקיברנטי, תוך שילוב היבטים מן האקדמיה, התעשייה, הכלכלה, החינוך, החוסן הלאומי בכלל וצורכי הביטחון הלאומי בפרט. תוכנית המחקר והפיתוח תציב את ישראל בחמישייה הראשונה של המדינות המובילות את המימד הקיברנטי עד 2015, בהתאם לחזון לפיו על מדינת ישראל לשמור על מעמדה בעולם כמרכז לפיתוח טכנולוגיות מידע ולקיים יכולות מעצמתיות במימד זה.

מטרת הוועדה היא להגיש לוועדה העליונה למדע וטכנולוגיה המלצות העוסקות בתחום ההגנה הקיברנטית בארץ, כדי לענות על צרכי הביטחון הנוכחיים והמתהווים בישראל בכל הנוגע להגנה קיברנטית. הוועדה לא עסקה באופן ישיר בשאלה איך מגינים על המדינה מבחינה קיברנטית בטווח הקצר, אלא אילו מרכיבים כדאי לעודד בשביל לפתח את תחום הגנת הסייבר בארץ, אילו תנאים יאפשרו את קפיצת המדרגה במדינת ישראל שתבטיח את חוסנה בתחום בעולם, וכיצד מהלכים אלה ישתלבו בתפיסת הגנת הסייבר של ישראל.

במבט ראשון, טבעי לחשוב על איומים קיברנטיים כאיומים ביטחוניים במובן המסורתי, ולמקד את המו"פ הלאומי בהיבטים הצבאיים של האיום מתוך משאבי מערכת הביטחון. יחד עם זאת, גישה זאת אינה לוקחת בחשבון, מצד אחד, את ריבוי האויבים הפוטנציאלים מכיוונים לא צבאיים, ומצד שני, את ריבוי המטרות הפוטנציאליות במתחם הקיברנטי, כגון: תשתיות חשמל, מים וגז, תשתיות אינטרנט ותקשורת, תשתיות מחשוב אזרחיות, תשתיות תחבורה, מערך הבריאות, תשתיות מזון, בנקאות ומסחר, מערך השרותים הממשלתיים והמוניציפאליים, מאגרים לאומיים, תשתיות החינוך וההוראה, עסקים קטנים וגדולים ואף מחשבים פרטיים וטלפונים סלולאריים. כל אלו, ביחד ולחוד, מהווים מטרות פגיעות, בנוסף למערכות הקיברנטיות הביטחוניות והלאומיות. יתרה מזאת, המרכיבים האזרחיים והביטחוניים במימד הקיברנטי שזורים זה בזה וכמעט אינם ניתנים להפרדה. נחוצה סינרגיה לאומית בין כלל המגזרים כתנאי להצלחה בהתמודדות עם האתגרים.

המדינות והארגונים שמובילים כיום בהיערכותם לקראת אתגרים קיברנטיים, לרבות בתחום המו"פ הקיברנטי, נוקטים בגישה רב-תחומית בפיתוח יכולות ועוצמות של ביטחון קיברנטי (Cyber-Security), המתבססת על ההבנה כי האתגרים במימד הקיברנטי מורכבים מאלמנטים צבאיים, צבאיים-לכאורה, תעשייתיים, כלכליים, ואזרחיים.

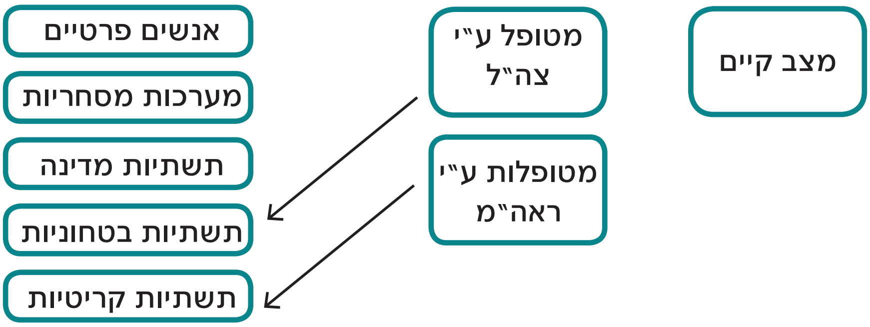
מתוך האמור לעיל נגזרו תפקידי הוועדה והם:

- זיהוי הצרכים[1] הלאומיים, הן הביטחוניים והן האזרחיים, בתחום ההגנה הקיברנטית.
- זיהוי היתרונות היחסיים של ישראל בתחום ההגנה הקיברנטית.
- גיבוש המלצות בחשיבה לאומית רחבה ובין-תחומית, בתכנון ובגיבוש דרכי פעולה מרכזיות, כולל עיקרי המדיניות (כולל ארגון), כדי לגרום לסינרגיה טובה יותר בין הצרכים והגופים בישראל לטובת כולם.

המלצותיה של הוועדה נובעות מעבודה משותפת עם כל הגורמים הרלוונטיים, כדי להמשיך ולהעמיק את ההובלה הישראלית במימד אסטרטגי זה. הוועדה מציגה את הצורך להתמודד בצורה תשתיתית מתמשכת ורחבה עם האתגרים הרבים במימד הקיברנטי, ומחדדת את החשיבות שבהסתכלות הבין-תחומית בסוגיית המימד הקיברנטי, הנובעת מהאופי הייחודי של האתגרים שהוא מציב, תוך דגש על חינוך, מודעות והקמת תשתיות מו"פ מתאימות. אין די בגישה הממוקדת באיומים הביטחוניים במובן המסורתי, כיוון שהאיומים הקיברנטיים מאיימים לפגוע ביסודות החברה הישראלית, לא רק במישור הביטחוני אלא גם הכלכלי והחברתי.

[1] ועדת ההגנה פעלה כדי לזהות את הצרכים הנוכחיים והעתידיים של הגופים השונים העוסקים וצורכים הגנה קיברנטית בישראל, כולל יכולת התמודדות עם תקיפות והגנה על מערכות קריטיות, מניעת מאמצים התקפיים, מזעור נזקים בזמן התקפה והתמודדות באופן אקטיבי, בניית יכולות מניעה וייחוס של התקפות וכד'.

להלן ניתוח הצורך, האיום והזדמנות על פי קבוצות ייחוס:



1.1 הגדרת איומי הסייבר

הוועדה הגדירה את מרחב איומי הייחוס לפי קבוצות הייחוס באופן הבא:

- משילות
- סמלי מדינה ופגיעה בתדמית המדינה
- שירותים שהאזרח מצפה ו/או צריך לקבל
- נזק כלכלי
- כמות נפגעים
- פגיעה בפרטיות
- שמירה על סודות המדינה
- פגיעה בסדר הציבורי

1.2 קבוצת ייחוס – מערכות מסחריות

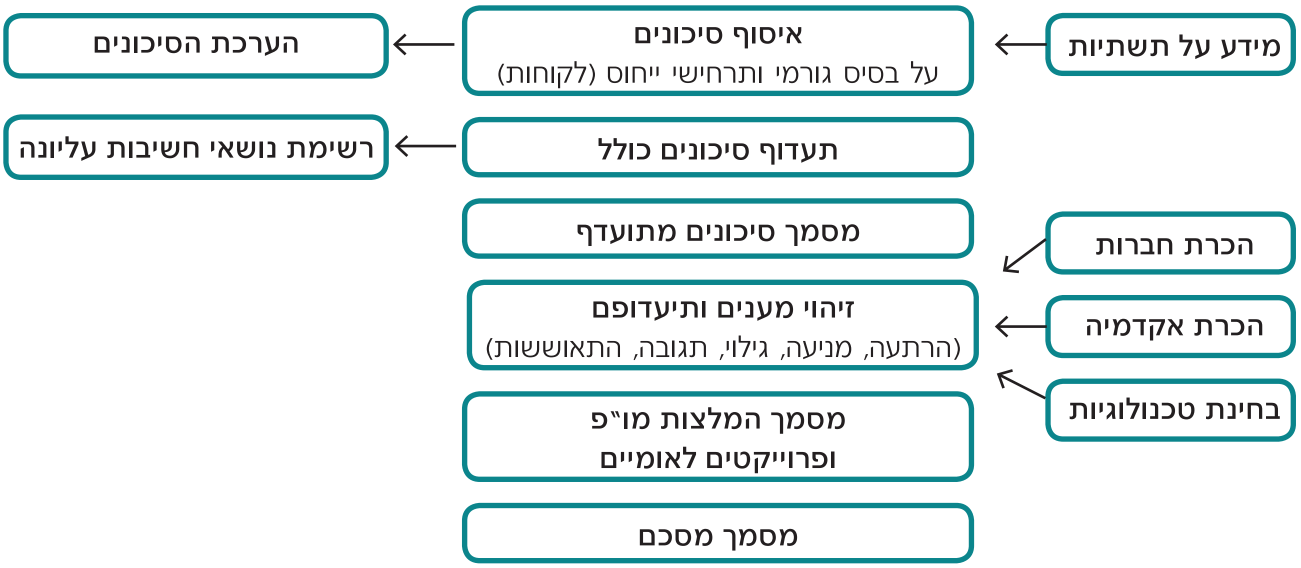
- מניעת שירות לטווחי זמן ארוכים בעיקר
- תקיפה רחבה מאוד - יכולה להפוך להתקפה על המדינה כולה
- פגיעה בחברות בורסאיות
- פגיעה ביכולת הייצור והשיווק
- פגיעה בקניין רוחני

1.3 קבוצת ייחוס – אנשים פרטיים

- פגיעה בקבלת שירותים לאזרח ולבית הפרטי
- פגיעה רוחבית מגדילה את עוצמת ומשמעות האיום
- פגיעה ממוקדת מגדילה את משמעות ואת עוצמת האיום
- קיימים איומים גם על מחשבים "קטנים" ו"סמויים"
  - למשל, מחשבים ברכבים, GPS, מחשבי בקרה על מערכות שונות.
- פגיעה במורל / פגיעה פסיכולוגית
  - על בסיס ובעזרת המערכות הממוחשבות, אמצעי תקשורת המוניים וכיו"ב.

2. שיטת העבודה להשגת היכולות

שיטת העבודה של הוועדה לצורך השגת היכולות הנחוצות לניתוח המידע ובניית תוכנית הפעולה שלה, מבוססת על התהליך שלהלן:



3. ממצאים עיקריים

3.1 זיהוי הנכסים והיתרונות היחסיים של ישראל

3.1.1 אקדמיה ומערכת החינוך

ישראל בורכה במערכת אקדמית מפותחת, המעניקה לה יתרון בתחומי המחקר והטכנולוגיה המשיקים להגנת הסייבר. מערכת החינוך הפכה את לימוד מקצוע המחשוב לפופולרי בקרב בני נוער רבים. אין להקל ראש בחשיבות חיזוק והרחבת היכולות הללו, כפי שיפורט בהמלצות הוועדה בהמשך.

3.1.2 תעשייה

בתחום אבטחת המידע לבדו יש כ 150 חברות מוצר ומערכות הפועלות בישראל (נכון לשנת 2009) מביניהן חברות מובילות בעולם, ובראשן (מבחינת הקדמת ויצירת השוק) חברת "צ'קפוינט", אלביט, ורינט, נייס ורבות אחרות.

בנוסף, פועלות בארץ מספר חברות רב לאומיות בעלות יכולות מחקריות ועומק מדעי יישומי גבוה ביותר, למשל: מרכזי המחקר של IBM בחיפה, מרכזי המחקר של מיקרוסופט, דויטשה טלקום, RSA וכדומה.

3.1.3 החברה בישראל

החברה בישראל בעלת מודעות ביטחונית וטכנולוגית גבוהה, ומהווה מקור לתמיכה, עניין ומעורבות, בשל הבנת האזרחים את חשיבות תחום הביטחון ונגזרותיו. היא גם בשלה להצמיח מתוכה את כוח האדם הנדרש למימוש מטרות המיזם, בהינתן החינוך והמו"פ המתאימים. חשוב להדגיש את החשיבות של הגברת והעמקת החינוך הטכנולוגי ושל טיפוח המצוינות והאקדמיה להיבטי הגנת הסייבר.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

העובדה שישראל מדינה קטנה מאפשרת להטמיע בה שינויים במהירות גדולה, בהתאמה לקצב ההתפתחויות בתחומי הסייבר.

יש בה מספר יחסית קטן של נקודות ממשק במארג התשתיות, ומספר המערכות שיש להתמקד בהן גם כן קטן יחסית למדינות אחרות בעולם. אין ספק שהסברה נאותה יכולה לשנות את סולם הערכים וההעדפות של הנוער ושל הציבור בנוגע לחשיבות תחום הגנת הסייבר.

3.1.4 ביטחון

בארץ קיימים גופים בעלי התמחות בתחום אבטחת מידע במערכת הביטחון:

- צה"ל (מס' יחידות)
- רא"מ
- מלמ"ב
- תעשיות בטחוניות

גופים אלו הם בגדר נכסים המעניקים יתרון יחסי למדינה בתחום אבטחת המידע והגנת הסייבר. ניסיונו של רא"מ בהרחבת התפיסה הביטחונית מעבר לגופי הביטחון, מאפשר הבנייה עתידית רחבה של תפיסת הגנת הסייבר.

3.1.5 ממשלה

המגזר הממשלתי כולל בחובו גופים בעלי התמחות בתחום אבטחת מידע:

- תהילה
- ממוני ביטחון (מנב"ט-ים) במשרדי הממשלה השונים
- משטרת ישראל (לה"ב 433)
- הרשות למשפט, טכנולוגיה ומידע
- משרד האוצר - אגף שוק ההון, ביטוח וחיסכון
- בנק ישראל - המפקח על הבנקים

בנוסף, יש גופי רגולציה היכולים לשתף פעולה להטמעת תפיסת ביטחון הסייבר, ביניהם ועדות הכנסת.

3.2 חולשות עקריות

3.2.1 חולשות כלל עולמיות

- התלות בסייבר בחיי יום יום גוברת מהר
- גבולות הסייבר הורחבו גם לתשתיות שבעבר נחשבו מבודדות ומוגנות
  - למשל, המודעות לאנרגיה ירוקה משנה מהותית את תשתיות רשתות האנרגיה, וחושפת אותן להתקפות סייבר שלא היו אפשריות קודם לכן
- הצורך באופטימזציות ויעילות מביא ארגונים למרכז מערכות שליטה ובקרה (מרחוק) על כלל הפריסה הארגונית, ובשל כך להגיע למצב של "single point of failure
- אוטומטיזציה של מערכי הארגון משביתה את זרימת הייצור במקרה של ארוע סייבר משמעותי.
- אנשים פרטיים וארגונים עוברים לשימוש מסיבי ברשתות חברתיות ללא בקרה על אבדן הפרטיות, יכולות המעקב וגזירת המידע מהפעילות בסביבה החברתית
- התלות ב- GPS גוברת, ובעתיד הלא רחוק, ללא קישור ל- GPS, תשבש יכולת התנועה במערכות שונות.

3.2.2 חולשות ישראליות

- העדר הכוונה לאומית בתחום ההגנה הקיברנטית
- העדר גוף לאומי בעל סמכויות בנושא במגזר האזרחי
- העדר יכולת פעולה ברגיעה ובחרום להשיב על האיום
- פיזור מאמצים ללא אגום שת"פ בין הממסד הביטחוני לאזרחי

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

- מדינה קטנה
- ירידה ברמת החינוך
- החלשות החינוך הטכנולוגי אקדמי, והתמקדות אקדמית בפן התיאורטי בתחומים הרלוונטיים

3.3 מגמות עולמיות מרכזיות בהגנת הסייבר

רשימת מגמות עולמיות בתחום אבטחת מידע, בהסתמך על מחקר של IDC המעודכן לשנת 2009 ומקורות נוספים.

3.3.1 ברמה לאומית

- הקמת גופים מגזריים לקידום מאמצים בתחום ההגנה על הסייבר ולהטמעת המודעות הציבורית
- התחזקות הרגולציה
- הקמת מערכי ISOC לניטור אירועים ברשת
- תוכניות להגברת החינוך המדעי, המתמטי והטכנולוגי
- השקעה מסיבית במו"פ בתחומים הרלוונטיים
- שיתופי פעולה בין לאומיים

3.3.2 ברמה הארגונית

- הגברת ההשקעה בהגנת תשתיות המחשוב והתקשורת
- בנוסף להגנה ב"גבולות" המערכת, התמקדות בהגנה בתוך המערכת
- התכנסות (התחברות, התגבשות, CONVERGENCE) של האבטחה, מערכות התוכנה והאפליקציות, איחסון הנתונים, ומערכות ניהול הרשת
- מעבר לעבודה בממשקי WEB ואבטחת ה- WEB
- ממשל ושליטה ברשת Governance, Risk and Compliance (GRC)
- שירותי אבטחה מנוהלים מחוץ לארגון MANAGED SECURITY SERVICES

3.3.3 ברמת הפרט

- מודעות לצורך באנטי וירוס וזהירות בפתיחת דואר אלקטרוני
- חיבור שוטף לטלפון סלולרי ומכשירי דואר אלקטרוני והעמקת השימוש בגלישה סלולרית
- מגמות של חשיפת מידע אישי באינטרנט ותקשורת כתובה שמחליפה תקשורת מדוברת

3.4 מצב קיים בישראל

סעיף זה מתאר את המצב הקיים בארץ בתחום המחקר והפיתוח של מוצרי, מערכות, ויכולות אבטחת מידע.

3.4.1 מחקר ופיתוח

- בארץ פועלים מספר מכונים למחקר אקדמי של אבטחת המידע, וישראל בורכה בחוקרים מהטובים בעולם בתחומים אלו.
  - באוניברסיטאות עובדות קבוצות מחקר המתמחות במערכות מבוזרות ובפיתוח טכנולוגיות לעמידות פרוטוקולים בפני כל שגיאות אפשריות, ובפיתוח תשתיות החסינות בפני התפשטות תקלות.
  - יש בארץ קבוצות מחקר, מהטובות בעולם, העוסקות בנושאי למידה חישובית ובכריית מידע.
  - ישראל נמצאת בחזית הטכנולוגית העולמית בנושאים שונים הקשורים לתקשורת נתונים.
  - חברות רב לאומיות רבות מחזיקות בארץ גופי מחקר, שרובם רלוונטיים להיבטים שונים של הגנת הסייבר, ביניהם IBM, RSA, דויטשה טלקום, מיקרוסופט, גוגל, צ'ק פוינט, HP.
  - יש בארץ תוכניות מחקריות אקדמיות, בשיתוף התעשייה ומערכת הביטחון ותוכניות רב לאומיות שונות.

3.4.2 תעשייה

יכולות התעשייה נשענות על יכולות האקדמיה ותוצרי מערכות הביטחון, בעיקר בתחום המחקר של אלגוריתמי צופן, וכן על יזמות עסקית בתחום, שנתמכת על ידי קרנות וחממות עסקיות, ומופעלת ויזומה על ידי יוצאי מערכת הביטחון וצה"ל, המיישמים ידע וניסיון טכנולוגי מקיף.

הדוגמה הבולטת היא חברת "צ'קפוינט", אשר פרצה את תחום אבטחת המידע ברמה עולמית והובילה את השוק ואת המוטיבציות לפיתוח של פתרונות אבטחת מידע בהיקף רחב. בנוסף אליה, יש מגוון חברות הפועלות במגזרים שונים של הגנות הסייבר, והיכולות להפנות משאבים לקידום התחום, ביניהן אלביט, נייס ואחרות.

נכון לשנת 2009, רק בתחומי אבטחת המידע קיימות בארץ כ- 150 חברות (מסקר של IDC 2009) העוסקות במגוון רחב של נושאים, ומייצגות את הכיוונים העיקריים של התפתחות התחום בעולם.

במשך השנים (החל מ- 2004 ועד 2009), נרכשו מספר חברות ישראליות וידע על ידי חברות מובילות בתחומן וגדולות יותר בעולם.

3.5 אתגרים עיקריים ובעיות בעלות חשיבות עליונה שיש לפתור

- מספר אתגרים חייבים, לדעת הוועדה, למצוא את פתרונם בעדיפות ראשונה:
- יצירת מוטיבציה לתעשייה הביטחונית לייצר ידע, להשקיע במו"פ, ולפתח טכנולוגיות של יתרון איכותי בתחום הסייבר.
- יצירת מוטיבציה לאקדמיה ולגופים המקבילים לה לבצע מחקרים פורצי דרך בתחום הסייבר, ולהקים מערכי לימוד והכשרה בתחום אבטחת הסייבר.
- הקמת גופים לניטור הסייבר, לפעולה במקרה של איומים בתחום ולמכלול פעילות בשגרה, תוך שמירה על המידור והסיווג של המידע
- ניטרול כל איום על התשתיות מחק (הקריטיות) בהקשר למצבי קיצון
- הקמת גוף מתאם עליון לכלל המדיניות בתחומי הגנת הסייבר האזרחי
- מניעת פאניקה בהקשר של התקפות מידע
- פיתוח יכולות לאבטחת מידע בעלות עליונות ברורה ביחס ליכולות היריב, ופריסתן בצורה מבוקרת ובטוחה
- הקמת יכולת קימום והפעלת מערכות תחת התקפה
- הכנת מערכות חליפיות ברמת המידע, החומרה והתוכנה
- הטמעת הנושא והגברת החינוך בו לקראת העתיד
- הגברה משמעותית של המו"פ בתחומים הרלוונטיים

4. המלצות

4.1 כללי

הוועדה מציגה שש **המלצות ראשיות** בשלב הנוכחי:

1. העלאת **המודעות והחינוך** לסייבר.
2. יצירת **תשתית ידע, מו"פ ותקשוב** המאפשרת את שיפור הגנת המדינה בסייבר.
3. יצירת **מעטפת הגנה למדינה** באמצעות מו"פ ופרוייקט-על
4. פיתוח תפיסת הפעלה מדינתית בשגרה **והערכות ראשוניות לחירום** בסייבר.
5. **שדרוג מבוזר** של רמת המיגון באמצעות פיתוח מרכיבים טכנולוגיים וחקיקה.
6. שדרוג רמת האבטחה באמצעות **טכנולוגיות ישראליות** ורתימת התעשייה המקומית למיזם.

ההמלצות יפורטו בסעיפים הבאים.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4.1.1 העלאת המודעות והחינוך לסייבר

הבסיס לשינוי מהותי בתחום ההגנה בסייבר ברמה הלאומית, נעוץ בהרחבת המודעות לנושא ובחינוך בכל הרמות, החל מגני ילדים ועד למחקר אקדמי מתקדם.

המאמץ יפוצל בין לימוד והנחלת הידע הקיים למסגרות חינוך שונות ומגוונות, לבין הרחבת הידע הקיים באמצעות מחקר בסיסי בנושאי הסייבר בפרט, ובהשלכותיהם על החיים בעידן הנוכחי בכלל. ההשקעה בתחום החינוך מיועדת ליצור אוכלוסיית עוסקים בסייבר, להגביר את הידע בקרב הציבור הרחב ולהעלות מודעות של מקבלי החלטות.

להלן **דוגמאות** לנושאים למימוש בתחום:

- הגברת המודעות הציבורית לנושא בכלל ולאיומים בפרט.
- הטמעת קריטיות הנושא אצל מקבלי ההחלטות בממשל ובתעשייה.
- הגברת לימודי מדע וטכנולוגיה בכלל, ובנושא הגנת הסייבר והמחשוב בפרט, במסגרות החינוך הקדם אקדמיות.
- בניית תוכניות לימודים אקדמיות בנושאי הגנת הסייבר.
- הענקת מלגות ועידוד מחקרי הגנת הסייבר במסגרת תארים מתקדמים.
- מתן השתלמויות בתחום פיתוח מאובטח של קוד (ואולי גם של חומרה ותקני תקשורת) לחברות הזנק ולחברות מוצרי סייבר ישראליים.
- הסמכת מומחים לתחומי הגנת הסייבר.

לסיכום:
הכרה בחשיבות העלאת המודעות לנושא הגנת הסייבר, ופעילות מואצת בכל מסגרות החינוך לשיפור המוכנות להתמודדות עם האתגר.

4.1.2 יצירת תשתית ידע, מו״פ ותקשוב המאפשרת את שיפור הגנת המדינה בסייבר

כדי ליצור יתרון בתחום מקצועי כדוגמת הסייבר, נחוצה השפעה מדינתית למימון של עיסוק מחקרי בנושא. בנוסף, יש להתניע פרוייקטים ותוכניות ליצירת תשתית המאפשרת לשדרג את רמת ביטחון הסייבר במדינה.

בסעיף זה נכללים כדוגמא:

- הקמת מרכזי מחקר יעודיים לתחומי הסייבר וההגנה בו.
- עידוד ביצוע מחקרים בתחום במוסדות הקיימים.
- עידוד פיתוח טכנולוגיות ופרוייקטים בנושאי הגנה בסייבר.
- הקמת מכון לבחינת קוד ומוצרי תוכנה וחיסונם.
- יצירת מאגר אירועים ותעבורת מידע של ניסיונות תקיפה חיצוניים לשם מחקר ופיתוח טכנולוגיות הגנה.
- הקמת סימולטור מבוזר לבחינת עמידות בפני התקפה (בשיתוף ועדת הצופן)

לסיכום:
הוועדה ממליצה להקים מרכזי מצוינות ומרכזי מחקר למטרת הגברת רמת אבטחת המידע בישראל. המרכזים יפעלו לאיפיון פרטני, מעקב מקצועי, ותקצוב ובקרה של פעילויות מחקר בתחומי אבטחת המידע והסייבר לאורך זמן, על פי תוכניות ארוכות טווח, במטרה לסגור את פערי האיומים בתחומים אלו מצד היריב.

4.1.3 מו"פ ופרוייקט–על ליצירת מעטפת הגנת סייבר למדינה

על המדינה לגבש את התפיסה שבה היא מגינה על המרחב הפרוס (ברמה המקוונת) בין הארגונים הביטחוניים המוגנים לבין גבולות המדינה. במרחב פרוסים ארגונים ציבוריים, מסחריים ופרטיים. המרחב, אף כי הגופים שבו אינם מוגדרים כקריטיים, עלול לפגוע ואף להשבית את החיים התקינים במדינה. כושר הייצור של המדינה, התל"ג ורווחת תושביה פרוס בו.

אי לכך, יותנע פרוייקט-על המשלב ניטור של המצב הסייברי במדינה, של פוגענים המנסים לחדור מחוץ לה, של זיהוי תופעות חריגות ואיתור ניסיונות פגיעה חיצוניים או פנימיים. יפותחו גם רכיבים מבוזרים או פתרונות נוספים המשלימים את המענה המלא. קיים מתח מובנה בין הרצון להעלות את רמת ההגנה המדינתית והציבורית בסייבר, לבין החשיבות של שמירה על פרטיות האזרחים והארגונים במדינה, המלווה כל טיפול טכנולוגי ורגולטורי בסוגייה, ומשפיע על בחירת הפתרונות למימוש מעטפת ההגנה.

דוגמאות:

- מערך זיהוי, דיווח ואיסוף ארועים חריגים (בשילוב עם ISOC)
- מערכת ניטור בכניסות למדינה ובנקודות מפתח בתוכה
- מערכת שו"ב לאינטגרציית תקינות שירותים שונים
- ביצוע פטרול מדינתי סייברי בגבולות ובתוכם
- חדר מצב מדינתי להצגת תמונת מצב עדכנית ותיאום מערכי הפעולה בזיהוי התקפה בפועל, או אפשרות להתקפה קרובה
- טכנולוגיות איסוף המידע תוך שמירת פרטיות האזרח / הגוף המסחרי

הערה: ראו פירוט של תכונות המערכת בנספח: "פרוייקט-על ליצירת מעטפת הגנת סייבר למדינה" בסוף המסמך.

לסיכום:
פיתוח, יישום, ותחזוקה של מערכת (מערך) לאומית של סנסורים ומערכות לעיבוד מידע ממקורות שונים, וזיהוי של התקפות על הגורמים במדינה אשר זוהו כ"לקוחות" המיזם.

4.1.4 פיתוח תפיסת הפעלה מדינתית בשגרה והערכות ראשונית לחירום בסייבר

על המדינה להיערך למקרה שאירוע סייבר יתממש חרף נסיונות המיגון. גופי המדינה השונים אינם בשלים כיום להיערך לכך, לפיכך הוועדה ממליצה להקים צוות חשיבה מקצועי, אשר ינתח ויגבש את תפיסת הפעולה בשגרה ובחירום במהלך חצי השנה הקרובה, ובמקביל להתניע מהלכי היערכות אשר אינם דורשים המתנה למסקנות הצוות. כמו כן ממליצה הוועדה להקצות תקציבים עתידיים בטווח של שנה, במהלכה יותנעו צירי פעולה להיערכות בשגרה ובחירום.

דוגמאות:

- יצירת יתירות בעורקי ותשתיות התקשורת הפנים ארצית והבינלאומית.
- פיתוח כלי לאיתור מקור הנזק.
- פיתוח כלי "עזרה ראשונה" לתפעול ושיקום פגיעה.
- פיתוח יכולות התאוששות מהירה ושרידות במקרה חירום Disaster Recovery Plan (DRP).
- התנעת מחשבה על מסגרת "מילואים" בסייבר.
- פיתוח מערכת Business Continuity Planning (BCP) להבטחת רציפות תפקודית בחירום.

לסיכום:
פיתוח ויישום של תפיסת BCP DRP ברמת המדינה וברמת הארגונים, אשר תאפשר לגורמים הרלוונטיים להתאושש / לתפקד באופן סביר גם תחת או לאחר ספיגת התקפות סייבר.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4.1.5 שדרוג מבוזר של רמת המיגון באמצעות פיתוח מרכיבים טכנולוגיים וחקיקה.

רמת הביטחון תעלה באמצעות שדרוג מבוזר של יכולות בארגונים השונים ובקרב האזרחים. הממשלה תיזום פיתוח של טכנולוגיות רלוונטיות, שיחולקו או יימכרו בהטבה לאזרחים ו/או לארגונים במדינה.
חלק מפתרונות אלו דורשים עדכוני חקיקה, כדי להפעילם בצורה מבוזרת.

דוגמאות:

- דיווח תקופתי לדירקטוריון על רציפות תפעולית והגנת תשתיות בכל ארגון "משמעותי"
- פיתוח מערכות ניטור והתראה (אין פתרון בעולם)
- סנסורים תוכנתיים המעבירים אינפורמציית ניטור על מצב הרשת
- מלכודות דבש לאיתור פוגענים ממוקדים
- הטמעת התקנת תוכנות הגנה אחרות

לסיכום:
קידום הטמעת האיום מהסייבר, פיתוח תפיסת התמודדות ארגונית איתו וכן פיתוח כלים חדשים להתמודדות איתו.

4.1.6 עידוד רכש 'כחול לבן', על מנת לאפשר מתן פתרונות אבטחת מידע שאינם תלויים בגורמי חוץ, יחד עם שיפור היכולות הטכנולוגיות של התעשייה הישראלית

להלן הסבר לצורך האבטחתי בפיתוחים טכנולוגיים בתחום הסייבר בארץ:
טכנולוגיית אבטחת המידע היא דינמית, ומבוססת על תשתיות מגוונות: חומרה, תוכנה, קושחה. יריב יכול, ובפועל גם מנסה, לנצל זאת כדי לתקוף את מערכות הסייבר. למשל, כפי שכבר פורסם, באמצעות החדרת קוד עוין דרך חומרות מחשב מטופלות.
לצד קידום סעיפי ההמלצות הקונקרטיים המופיעים לעיל, אפשר להתקדם באמצעות רתימת המדינה לעידוד רכש מתוצרת התעשייה הישראלית לאבטחת מידע, והרחבת כמות המוצרים המפותחים על ידי תעשייה מוכרת, כולל מוצרים שיוחלט כי חשוב שפיתוחם יבוצע בארץ תוך סיוע ברכישתם, כדי לחזק את הכדאיות הכלכלית בייצורם המקומי ובהתבססות טכנולוגית עליהם.

לדוגמא:

- עידוד לרכש תוכנת אנטי וירוס ישראלית
- עידוד לרכש קומפיילר מאובטח
- עידוד לרכש מערכות סינון תוכן והרשאות
- עידוד הקמת עננים מסחריים ישראליים[2], ואולי גם שלוחות של עננים מחו"ל

לסיכום:
תוצרי הפעילויות השונות, אשר מיזם הסייבר הלאומי אמור להקים על פי תוכניות ועדת ההגנה שלעיל, ועל פי הפירוט הטכנולוגי והמקצועי אשר ייכלל בהן בהמשך, וההכוונה המקצועית והמדעית של הוועדה והדרגים המקצועיים, יגבירו את חוסנן של התשתיות האזרחיות במדינה, כגון מערכות הרמזורים, מערכות התקשורת האינטרנטית וכיו"ב, ויחזקו את הפיתוח וההטמעה של פתרונות ומערכות הגנה בקרב המערכות של גורמי הייחוס הנחוצים להגנה.

4.1.7 שדרוג רמת האבטחה דרך התבססות על טכנולוגיות ישראליות ורתימת התעשייה המקומית למיזם

לדוגמא:

- הקמת עננים מסחריים ישראליים, ואולי גם שלוחות של עננים מחו"ל.

הסבר:

1. ניתוק רשתות המידע העולמיות לא תמנע עבודה של הגורמים בארץ
2. המידע הישראלי יהיה נגיש ולא יאבד

[2] ראו פירוט על נושא מחשוב העננים הישראלי - נושא בעל חשיבות רבה בראיית הוועדה - בנספח הרלוונטי בסוף המסמך.

3. ניתן יהיה להפעיל הגנה על המידע
4. המידע והפעילות תהיה ברת ניטור

- מערכות סינון תוכן והרשאות
  הסבר:
  1. תקיפות רבות משתמשות ביכולות ברמת פורמטים של המידע והקבצים
  2. מדיניות סינון צריכה להיות פרטנית ואף פרטית
- תוכנת זיהוי חתימת התקפות ממוקדות
  הסבר:
  1. אנטי וירוס במובן הרחב והבסיסי לצורך זיהוי חתימות
  2. אין כוונה להתחרות בנעשה בעולם - מערכת תוצרת כחול-לבן תאפשר בדיקת חתימות סמויות שלא רוצים לפרסם אותן
  3. קשה להתחרות על בסיס כלכלי גרידא מול הנעשה בעולם

לסיכום:
פיתוח של מערכת לקבלת החלטות, תעדוף, ויישום של פרוייקטים באבטחת מידע, אשר חשוב, לדעת הוועדה, שיהיו מתוצרת ישראלית, במטרה למנוע חדירה של מרכיבים מטופלים אל תוך מערכות האבטחה המטופלות במסגרת המיזם. תיאור של הפרוייקט בנספח בסוף המסמך.

4.1.8 הערות לנושא המלצות הוועדה:

1. בשל התהליך המהיר לגיבוש נושאי הוועדה, ובשל התפתחות ודינמיות התחום, הוועדה ממליצה להקצות משאבים נוספים לתהליכי מו"פ שאינם נכללים בסעיפים שלעיל ויזוהו במהלך השנה הקרובה.
2. הנספח מפרט בהרחבה פעילויות שונות, פרוייקטים לאומיים ונושאי מחקר ופיתוח אשר הוועדה ממליצה עליהם, ושצויינו בסעיפים שלעיל.
3. הנושאים נמצאים ברמת בשלות ראשונית. העיסוק בהם יכלול תחילה ניתוח ספציפי הגדרת הדרישה המדוייקת ומאפייני הפתרון הנחוץ.
4. ועדת ההגנה במיזם תמשיך לשמש באופן מלא או חלקי כוועדת היגוי, המלווה את הפתרונות המתגבשים ומבקרת את מידת המענה לצרכים שלשמם הותנעו.
5. ממשקים לוועדות מקבילות אחרות במיזם הסייבר הלאומי:
   1 ממשק לוועדת צופן -
      1. נושא הסימולציות יטופל על ידי ועדת הצופן, ואנו רואים חשיבות בקידומו.
      2. יצירת מאגר אירועים ותעבורת מידע על נסיונות תקיפה
      3. קידום השימוש במפתחות ואמצעי צופן מסחריים לאבטחה האזרחית
   2 ממשק לוועדת מחשוב-על -
      1. הוועדה רואה חשיבות בקיומם של ענני מחשוב בישראל
   3 ממשק לוועדת תועלות כלכליות -
      1. מוקדם לעסוק בפרוייקטים ספציפיים
      2. אנו רואים חשיבות בעידוד הקמת תשתית טכנולוגית, שתשמש כבסיס לתעשייה משמעותית בתחום הסייבר
   4 ממשק לוועדת רגולציה וחקיקה -
      1. חלק ניכר מההצעות לפיתוחים ולפרוייקטים לאומיים בתחום ההגנה זקוקים לניתוח תחיקתי ואולי לעדכונים בתחום לצורך יישומם בפועל
      2. חובה לעגן את שמירת פרטיות האזרח בכל פעילות שתגזר מהמלצות הוועדה
      3. בדיקת האפשרות לשימוש בחקיקה כדי לקדם את הגנת הסייבר בארגונים גדולים ובשירותים מרכזיים (למשל: חיוב על דיווח תקופתי לדירקטוריון על נושאי הגנת הסייבר ורציפות תפעולית בארגונים וחברות גדולים).

5 ממשק לוועדת תועלות אקדמיות -
1. הקמת מרכזי מצוינות
2. קידום תוכניות הוראה בתחום אבטחת הסייבר והטכנולוגיות הנילוות
3. קידום מגוון מחקרי מו"פ בתחומים השונים

4.2 המלצות ומפת דרכים להכוונת הצורך

הכנת תוכנית לאומית פרטנית, אשר תגדיר את יעדי האיום, פערים ודרכים לטיפול בו, גופים אשר אחראים לטיפול בו, משאבים ולוחות זמנים, ואשר תיצור הזדמנויות והכשרות בכדי להענות לצורך הנחוץ למדינה בתחום אבטחת המידע . התוכנית תכלול מפת דרכים עם מספר אפשרויות להתקדמות בכל אחד מתת תחומי האיומים שבאחריותה.

התוכנית תמנף את פעילותה, תוך שילוב של תוכניות המחקר הקיימות במל"ג, התמ"ת, מפא"ת, ומשרד המדע.

4.2.1 דילמות

- דילמה מרכזית שמצאנו שיש להציף:
  - מורכבות בעיית ההגנה בסייבר איננה מאפשרת טיפול נאות בה בהיקפי הזמן והמשאבים אשר עומדים לרשות הוועדה.
  - כתוצאה מכך, הוועדה ממליצה להקים פורום המשך, אשר יפרוט את הכיוונים המקצועיים שהוועדה מצביעה עליהם לכדי תוכניות אופרטיביות, וילווה את הנושא באופן מתמשך וצמוד.
- דילמה עקרונית שנחוץ להציף ולהתייחס אליה:
  - חלק מן הפרוייקטים הטכנולוגיים מצריכים רמות שונות של טיפול וניתוח של מידע משתמשים, ולכן נמצאים במתח עקרוני עם הדרישה, החשובה גם היא, של שמירה על פרטיות המידע.
  - פתרון חלקי וראשוני שהוצף בוועדה מורכב משני חלקים:
    - לכלול בכל פרוייקט / פעילות / מוצר אבטחה מרכיב של ניתוח פורמלי אובייקטיבי ובלתי תלוי של מידת הפגיעה האפשרית בפרטיות המשתמשים, תוך הקפדה על יישום מלא של החוקים הרלוונטיים, ואף על מזעור זליגת מידע פרטי ככל הניתן.
    - עידוד המחקר בשיטות מתקדמות לשימור הפרטיות (למשל, בתחומים של PRIVACY PRESERVING DATA MINING, חישוב מאובטח משותף וכדומה), ויישומו החדשני בפרוייקטים הלאומיים לאבטחת הסייבר.

4.3 מדדים להצלחה

יוזמות או פרוייקטים מכל סוג בעלי טעם רק במידה שניתן למדוד את השפעתם ולהגדיר את הצלחתם באמצעות קריטריונים מדידים.
מוכר הציטוט הידוע: "you can not manage that which you cannot measure" ולכן:
יש לפתח מערכות וכלי בדיקה, לרבות בסיסי נתונים מתאימים, לצורך בחינת העמידות של המערכות שיפותחו, ושל כלל המערכות הרלוונטיות במדינה כנגד התקפות מידע ממוקדות ורבות עוצמה. חלק זה במיזם יהיה מסווג ומתמשך באופיו, במיוחד לאור הדינמיקה של תחום אבטחת המידע ויכולות היריב המשתנות ומשתכללות בהתמדה.
מדדי הצלחה טכנולוגיים פרטניים יקבעו עבור כל פרוייקט בנפרד.מדדים נוספים שימדדו לאורך זמן כוללים: מידת התעסוקה שהפעילות הכוללת של המיזם הוסיפה למשק, היעילות הכלכלית של הפרוייקט (ישירה ועל בסיס עלות חילופית) וכיו"ב.
הוועדה גם תעודד מחקר ופיתוח בתחומי "אבטחת מידע ברת מדידה" -measurable computer security methods, ובפיתוח שיטות סטנדרטיות לצורך מדידת רמת אבטחה במערכות מחשוב ורשתות מחשבים המיושמות לטובת אבטחת הסייבר הישראלי.

5. נספחים

5.1 נספח א – פרוייקטים לאומיים

סעיף זה עוסק בפעילויות טכנולוגיות שהוועדה הגדירה אותן כ"פרוייקטים לאומיים", בשל חשיבותן הרבה לאבטחת הסייבר הישראלי, וכן בשל היכולת הסבירה ליישמם (אם כי מחקר תמיד כולל היבטים של חוסר ודאות טכנולוגית), ובשל העניין והמעורבות של המדינה במימושם.

יש לציין, כי בשל אופייה הנרחב של הבעיה שטופלה במסגרת הוועדה והגדרת הפתרונות בטווח הזמן שהוקצב לה, חולקו הנושאים למקבצי המלצות מפורטות, כך שפרוייקטים פרטניים מסויימים עלולים להופיע מלבד בבסעיף נספח זה, גם בסעיפי פירוט מרכיבי מקבצי ההמלצות של הוועדה.

5.2 נספח ב – חינוך ומודעות

הוועדה ממליצה להגביר את החינוך והמודעות למושאי אבטחת המידע ולטכנולוגיות הסייבר:

- הגברת המודעות הציבורית לנושא בכלל ולאיומים בפרט
- הטמעת קריטיות הנושא אצל מקבלי ההחלטות בממשל ובתעשייה
- הכנסת מערכי שיעור לתלמידי בתי הספר היסודיים
- לימוד טכנולוגי בכלל, ונושא הסייבר ומחשוב בפרט, בבתי הספר התיכוניים
- לימוד קורסי אבטחת מידע במסגרת תואר ראשון
- הענקת מלגות ועידוד לימוד אבטחת מידע וסייבר במסגרת תארים מתקדמים
- הענקת מלגות ועידוד כתיבת דוקטורטים בתחום אבטחת מידע וסייבר
- שיעורי מודעות למבוגרים
- לימודים בתחום פיתוח מאובטח של קוד (ואולי גם של חומרה ותקני תקשורת) לחברות הזנק ולחברות מוצרי סייבר ישראליים
- עידוד כלכלי לפיתוח ושילוב יכולות אבטחת מידע במוצרים ישראליים
- בניית תקן ישראלי למוצרי אבטחת מידע ואכיפתו
- הקמת מסגרות לתחרויות נוער בנושאי מיומנויות סייבר ועידוד השתתפות בתחרויות דומות בחו"ל

שם היוזמה:	חינוך בנושא סייבר - מגני ילדים ועד מחקר אקדמי.
תיאור היוזמה:	הגדלת העיסוק בתחום הסייבר במערכת החינוך בישראל, החל מטיפוס כיוונים ומחקרים קיימים, ועד למחקר בנושא השפעת מערכת החינוך על מוכנות העם ללוחמת סייבר.
מטרת היוזמה:	שיפור עמידות העם בלוחמת סייבר: החל ממוכנות משופרת מול הנדסה חברתית, באמצעות הקניית "הגיינת סייבר" טובה יותר לאוכלוסיה הכללית; דרך משמר אזרחי פעיל ומקצועי בתחום; ועד יכולת מחקרית טובה יותר בנושאי סייבר. במצב הנוכחי, ויותר מכך בעתיד הבינוני-קרוב, היכולות הנ"ל ישמשו ככלי עזר חיוני בהגנת "שמי הסייבר" של מדינת ישראל.

מכיוון שהתמורה עבור השקעה בתחום החינוך ניכרת רק לאחר שנים רבות (עשרות שנים, במקרה של חינוך הגיל הרך), הרי שמטבע הדברים נחוצה מעורבות ממשלתית בתחום, שכן גורמים מסחריים, בעלי אופק קרוב של שנים בודדות, לא יוכלו לעסוק בו, וכתוצאה מכך הנושא יטופל באופן חלקי בלבד ולטווח הקצר. הוספת הנושא לתוכנית לימודי הליבה ו\או מודל ביטוחי באמצעות רגולציה עשויה לשפר את המצב.

הנהנים העיקריים מהיוזמה הם אזרחי מדינת ישראל. במידה מסוימת גם העוסקים בחינוך (150,000 המורים וכדומה) "יהנו" מתוספת שעות הוראה, שתשפיע באופן חיובי וישיר על מספר המועסקים (בהנחה שתוכנית הלימודים תהיה חדשה ולא תחליף תוכנית קיימת).
הלימוד יכול להתבצע בקלות גם באופן מקוון, ולכן קל יותר לגשר על הפער הדיגיטלי מול הפריפריה. "תעשיות" אזרחיות יכולות לעסוק בתחום החינוך, לשימוש פנימי או לייצוא, כפי שנעשה כבר כיום באופן נרחב במגזר השלישי. חוגי נוער שוחר מדע, מתנ"סים, תפוח פיס, מופ"ת, חמד"ע, מכון דוידזון וגורמים רבים נוספים הם קהל יעד רלוונטי, שישפרו את יכולותיהם גם במגזרים אחרים כתוצר לוואי.

חוסר פעילות עלול לדרדר את מדינת ישראל בתחום. וכשם שהתוצאות במבחני המיצב מעידות מדי שנה על נסיגה - כך גם ללא חינוך נאות ידרדר מצבנו בתחום הגנת הסייבר.

לחינוך אין קוונטה בסיסית - אפשר להשקיע כל סכום החל מפרוטות ועד למיליונים. התוצאה תהיה בהתאם. מכירת תוכניות הלימודים לייצוא עשויה לממן את הפעילות, כמו גם שיתופי פעולה וחלוקת משאבים. תוצאות ראשוניות יתקבלו תוך שנים ספורות, ההשפעה במלואה תבוא לידי ביטוי רק לאחר כמה עשרות שנים.

מכיוון שברשותנו כוח אדם מתאים, הרי שההצלחה כמעט מובטחת. החסמים הם שמרנות מערכת החינוך והתנגדות גורמים פוליטיים. מדד מצוין להצלחה הן תחרויות המוקדשות לנושא.

5.3 נספח ג – פרוייקט מעטפת הגנת סייבר למדינה

5.3.1 תכונות הפתרון הנדרש

הפתרון יורכב ממערכות ממוחשבות אוטומטיות ומערכות אנושיות, האמורות לספק הגנה על מערכות מחשב שיוגדרו עבורן מראש, הפתרון המוצע אמור להתמודד מול ארבע הפעילויות הבאות:

5.3.2 מערכת איסוף

מערכת מעקב ואיסוף מידע אשר תאפשר הגנה על מערכות מחשב שהוגדרו לה מראש מפני תקיפה. המערכת נדרשת לזהות תקיפה בהקדם האפשרי, רצוי עוד בשלבי ההתארגנות של היריב, ולספק התרעה למרכז הבקרה. מערכת האיסוף תורכב קרוב לוודאי מהמרכיבים הבאים:

סנסורים	סנסורים שתפקידם לאסוף מידע רלוונטי, המפוזרים ברשת בנקודות אסטרטגיות. בשלב זה סביר להניח שהסנסורים יתבססו על טכנולוגיות שונות ועל רמות שונות של עצמאות ויכולת עיבוד מקומית. ייתכן שחלק מהסנסורים יהיו ממשקים אל מערכות ניהול אבטחה SIEM קיימות בארגונים, שיקבלו שירות ואבטחה מהמערכת. המערכת צריכה לתמוך במגוון סנסורים ולהיות פתוחה בעתיד לשילוב סנסורים חדשים בתוכה.
מרכז ניתוח	מערכת מחשוב, שתפקידה לייצר את ההתרעות מתוך ניתוח התעבורה שנאספה והועברה אליה, תוך שימוש במגוון טכניקות שונות כולל כריית מידע, מערכות לומדות וכדומה. המערכת מיועדת לפעול בזמן אמת ולהפיק התרעות מיד כשיזוהו בתעבורה. עליה להיות גם פתוחה בעתיד, ולאפשר שילוב אלגוריתמים ומערכות ניתוח עתידיות.

ארכיון	מערכת שתאפשר אחסון וארכוב של מידע במשך תקופה ארוכה, ייתכן תוך צמצומו, ותאפשר להפיק חתכים ממנו לצורך ביצוע ניתוח היסטורי מקיף, ולצורך זיהוי מאפייני מתקפה שהתקבל עליה מידע ממקור חיצוני, אמדן נזקים וכדומה.
סימולטור	מערכת דומה למרכז הניתוח, שתאפשר להריץ מחדש מידע שנגזר מהארכיון לצורך בדיקות, כולל אירועים היסטוריים, אלגוריתמים חדשים וכדומה. המערכת לא מיועדת לפעול בזמן אמת, ולכן ככל הנראה תתבסס על עצמת מחשוב נמוכה משל מרכז העיבוד.
התממה	מערכת שתאפשר לגזור נתונים מהארכיון ולהתמים אותם, תוך השמטת פרטים מזהים / החלפתם במידע ניטרלי, לצורך ייצור סטים לבדיקה עבור גופי מחקר ופיתוח בארץ, כגון אוניברסיטאות, חברות מסחריות השותפות בפרוייקט וכדומה.

5.3.3 מרכז בקרה
מרכז הבקרה הוא חלק ממעטפת ההגנה הקיברנטית אשר ממשש, בשילוב של אמצעים טכנולוגיים ואנושיים, את תפקיד קבלת ההחלטות במערכת. המרכז אמור לתת מענה לצרכים הבאים:

מוקד התרעות	קבלת התרעות מהמערכת הממוחשבת וטיפול בהן, כולל בחינה ראשונית של המידע בהתרעה, והעברת ההתרעה לרמות בכירות של קבלת החלטות.
מוקד שירות	מענה ללקוחות המקבלים הגנה מהמערכת, במסגרת קבלת שיחות נכנסות או בהתקשרות יזומה ללקוחות במקרה של אירוע רחב.
חקירת מתקפות	צוות שתפקידו לחקור מתקפות, לזהות אותן, ולנסות לאתר להן פתרונות בכלים קיימים, או, במידת הצורך, באמצעים חליפיים, כגון פיתוח תוכנה ייעודית, חסימת כתובות תוקפות וכדומה...

5.3.4 מרכז תגובה וחירום
מרכז התגובה והחירום יספק מענה לטיפול במתקפה מרגע שזוהתה והוחלט כי היא דורשת טיפול. בשלב זה, טרם הוגדר היטב מרחב התגובה, אך הוא כולל בין היתר:

- טיפול מרכזי באירוע - **חסימת כתובות תוקפות וכדומה**
- טיפול בשטח - **הזנקת צוותי טיפול לנכסים אסטרטגיים שהותקפו**
- הפצת כלי מגננה
- בדיקות יזומות
- קשר עם מדינות / נותני שירותי רשת - **שמשטחם מגיעה המתקפה**
- טיפול פורנזי ומשפטי

5.3.5 מערכת הסדרה
מערכת אשר תפקידה להסדיר ולפקח על פעילות המעטפת הגנה הקיברנטית בהיבט החוק, ליזום חקיקה ראשית ומשנית מתאימה, ובמקביל לוודא עמידה בעקרונות החקיקה וכללי צנעת הפרט.

5.3.6 מימוש הפתרון
מערכת בסדר גודל כזה, בהתחשב בחוסרים במערכות עבור מרכז הניתוח, תבנה בשלבים, כאשר בתחילה ייעשה שימוש במערכות SIEM מסחריות, ובהמשך ישודכו אליהן מערכות ייעודות שיפותחו עבור הפרוייקט. למעשה, פיתוח מערכות הניתוח יימשך לאורך כל פעילות המעטפת הגנה הקיברנטית.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

5.3.7 עלויות[3]

עלויות משוערות של פרויקט מעטפת ההגנה הקברנטית, על פי מסמך ניתוח תועלות כלכליות שהכינה חברת "שלדור" עבור המיזם[4]:

6.3.7.1 עלויות הפיתוח

- עשרות - מאות מיליונים דולרים עבור הפיתוח.
- כוח אדם איכותי - לשריין לפרוייקט.

6.3.7.2 עלויות מרכז בקרה

עלויות משוערות של מערכות SIEM רב-שכבתיות ותפעולן:

- עלויות הקמה: מיליוני שקלים (ציוד, תשתיות, מיזוג, ציוד משרדי)
- עלויות תחזוקה: שליש עלות הקמה בשנה
- עלויות תפעול: עשרות אלפי שקלים בחודש
- עלויות כוח אדם: (350K ₪ לבעל תפקיד בשנה) > 1.5M ש"ח בחודש

5.3.8 תועלות

תועלות ישירות של הגורמים הנהנים מן היוזמה:

- חברות תשתיות קריטיות - מניעת נזק פוטנציאלי (בהיקף גבוה), חיסכון מסוים בהוצאות הגנת סקיוריטי (בהיקף גבוה).
- חברות מסחריות במשק מניעת נזק פוטנציאלי (בהיקף נמוך), חסכון מסוים בהוצאות הגנת סקיוריטי (בהיקף נמוך).
- חברות המעורבות בפיתוח המערכת - צבירת רווחים ממכירת המערכת בארץ, רווחים ממכירת המערכת בחו"ל (בספק).
- אזרחי המדינה - מניעת השבתת שירותים, מניעת הונאות כספיות.
- חוקרים באקדמיה וגם בחברות בתעשייה - יצירת מאגר מידע מחקרי מעוקר בהיבטי פרטיות - לצורכי מחקר.
- המגזר הביטחוני - מניעת נזק פוטנציאלי (בהיקף גבוה), חיסכון מסוים בהוצאות הגנת סקיוריטי (בהיקף גבוה)

תועלות עקיפות ינבעו בעיקר מהגדלת היקפי התעסוקה והעבודה, שפרוייקט מעטפת ההגנה הקיברנטית ייצור.

5.4 נספח ד – עידוד המחקר – פירוט:

פירוט עיקרי המלצות הוועדה לנושא עידוד המחקר בתחום אבטחת הסייבר בארץ מבוסס על קווי הפעולה הבאים:

1.1. הקמת מרכזי מחקר ייעודיים לנושא אבטחת הסייבר
1.2. עדיפות לכך שמרכזי המחקר יוקמו בתוך האוניברסיטאות
1.3. תמרוץ באמצעות מענקים, ובאמצעות קורסים אקדמים, אשר יגובשו לכדי מסלולים בתואר ראשון ובתארים מתקדמים מחקריים
1.4. הכנת תכנים לקורסים ולמחקרים בשיתוף פעולה בין האקדמיה, גורמים ממשלתיים וגורמי תעשייה, באם יזוהו כבעלי יתרון יחסי מובהק ויוכלו לתרום למיזם
1.5. את המחקרים תנהל בראיית על ועדת היגוי לנושאים האקדמים, בהשתתפות נציגי כל הגורמים שתוארו לעיל, לפי הצורך והנושאים המטופלים
1.6. בשל הבינתחומיות של נושא אבטחת הסייבר, יוזמנו מרצים אורחים וישולבו חוקרים מדיסציפלינות שונות רלוונטיות לטיפול בנושאי אבטחת הסייבר

[3] על פי המסמך שהוכן על ידי "שלדור" לטובת הפרוייקט.
[4] העלויות ראשוניות ומשוערות בלבד, ונכללות במסמך EXCEL של ניתוח תועלות כלכליות, שהכינה חברת "שלדור" עבור הפרוייקט.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

1.7 . היקף פעילות:
1.7.1. הקמת ארבעה מכוני מחקר
1.7.2. יצירת 8-10 קורסים בכל אוניברסיטה במבנה של שרשרת + קורסים מתקדמים וסמינרים בתחום
1.7.3. הקמת 10 מחקרים בשנה (דוקטורנטים)
1.7.4. יצירת גידול של בין 20 ל- 40 אחוז בשנה בהיקפי המחקרים והקורסים, ובמקביל של כוח האדם המבצע את הפעילות למשך כחמש שנים, ולאחר מכן תחזוקה שוטפת של הפעילות

המלצה למערך קורסים בתחום הגנת הסייבר:

1. הנדסת אבטחת מערכות:
א. מבוא לאבטחת מערכות מידע, הכולל סקירה בסיסית של שיטות אבטחה ופעולתן AV, IPS, I\DS, SIEM וכו'.
ב. מבוא לתקיפות ולוחמת מחשבים/מידע
ג. אבטחת מסדי נתונים ומערכי אחסון

2. קריפטולוגיה:
א. מבוא לקריפטולוגיה
ב. קריפטולוגיה מתקדמת - סטנוגרפיה, הצפנה קוונטית, פרוטוקולי הצפנה וכו'

3. מערכות הפעלה (הרחבת הקורסים הקיימים):
א. אבטחת מערכות הפעלה
ב. אבטחת וירטואליזציה

4. הנדסת פיתוח מאובטח:
א. מבוא לתקיפות לוחמת מחשבים/מידע
ב. מבוא לפיתוח מאובטח
ג. שיטות תקיפה מתקדמות, כולל ניתוח פוגענים מתקדמים
ד. פיתוח מאובטח מתקדם ואבטחת יישומים
ה. Reverse Engineering

5. אבטחת רשת תקשורת (הרחבת קורסי התקשורת):
א. תוכן אבטחת רשתות מחשבים
ב. נושאים מתקדמים באבטחת רשתות, IP, אינטרנט, פרוטוקולי רשת
ג. אבטחת רשתות סלולאר

6. שיטות לזיהוי תקיפות:
א. מבוא למערכות לומדות (רשתות בייסניות, גרפים, SVM, רשתות נוירונים וכו')
ב. זיהוי תבניות ובינה מלאכותית
ג. שיטות מתקדמות לכריית מידע וללמידה חישובית
ד. שיטות לשערוך וזיהוי במערכות דינמיות

7. סוגיות משפטיות וכלכליות באבטחת מידע (חוקי הגנת מידע, תקינה בינלאומית, החוק בישראל וכו')

8. סדנאות ומעבדות :
א. סימולציית תוקף/מגן
ב. טכניקות מתקדמות לאבטחת חומרה
ג. שיטות מתקדמות לחישוב מבוזר לזיהוי תקיפות בזמן אמת

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

5.5 נספח ה – חיסון התשתיות האזרחיות הלאומיות – פירוט:

הוועדה ממליצה לפתח תוכניות ליישומן ולהטמעתן של יכולות חדשניות, ולהתבסס על אינטגרציה והצטיידות בהיקף גדול באמצעים טכנולוגיים וביכולות הרתעה ומניעה של התקפות מידע, במקביל לזיהוין של ההתקפות, להגברת רמת אבטחת המידע וההגנה מהתקפות מידע בגופים הנכללים בקבוצות הייחוס שהוועדה הגדירה ושיש לספק להן מענים. הוועדה מדגישה את הצורך בתוכניות פעולה מעשיות שיתורגלו באופן עיתי, ושיונחו על ידי גורמי המדינה בתיאום עמה, כך שבעת התקפת מידע ייקל על המערכות השונות, וגורמי הייחוס המאובטחים בראשם, להתמודד בצורה מוצלחת וראויה. כל זאת למען כלל הגורמים המוגדרים כ"לקוחות" המיזם וקבוצות הייחוס (במידות ובשיטות שונות, ועל בסיס מדיניות ואסטרטגיות שונות, שיפותחו וייקבעו בהמשך באמצעות פעילויות שוועדות ההמשך יפתחו לתוצריהן).

5.6 נספח ו – עצמאות טכנולוגית

במסגרת פעילויות הוועדה זוהו תת- תחומים / פרוייקטים לאומיים שיש יתרון לפתח בארץ, מעבר ובנוסף לפיתוחים נוכחיים, בכדי לשמר "עצמאות טכנולוגית" בתחום אבטחת הסייבר, כדלקמן:

.1	End station security / server security
.2	הקשחות (מערכת הפעלה /אפליקציות /תשתיות)
.3	DLP - דלף מידע
.4	שו"ב לאומי
.5	מחקר פגיעויות וניהול טלאים patches
.6	הגנה על מערכי אחסון נתונים חומרה ותוכנה
.7	אבטחת בסיסי נתונים תוכנה
.8	פיתוח ציוד לאבטחת רציפות ותקינות BCP DRP ברמה הלאומית (בנוסף לאינטגרציה של ציודים מסחריים קיימים ופיתוח לוגיקת תפעול ייעודית)
.9	סינון תוכן וסינון תקשורת
.10	סנסורים לאיתור לו"מ + זיהוי אנומליות והתקפות ברשתות
.11	ענן מחשוב ישראלי / אבטחת מחשוב ענן
.12	מעבדות לטיפול וכלים לאבחון מתקפות לו"מ
.13	תשתיות לתרגול לו"מ cyber range
.14	בסיסי מידע למחקרי לו"מ
.15	מערכות הידור וסביבות פיתוח מאובטח
.16	מעבדות לאומיות לבדיקת ציוד חומרה ותוכנה
.17	anti- virus שכולל content filtering, verification, personal firewall, ect
.18	CERT לאומי
.19	כ"א מסומן - מילואים לסייבר
.20	הלבנת קוד

הערה: מירב הנושאים שתוארו לעיל משולבים, וכלולים גם כתת-נושאים בסעיפי ההמלצות המחולקות למקבצים שלעיל.

5.7 נספח ז – יכולות קימום והתאוששות

הוועדה ממליצה כי המענים החשובים ביותר שיפותחו וייושמו בעתיד בפרישה רחבה ועמוקה, יספקו יכולות של המשכיות לתפעולן של מערכות המחשוב ברמות בסיסיות, לצורך קימום ו"יציאה" ממצבי התקפה. הנחת היסוד בפיתוח, אינטגרציה, והטמעתן של פתרונות אלו היא כי ייתכן מצב, שבו יריב אכן יצליח לעקוף, ולו חלקית, את מערכות ההגנה. במצב כזה, לאור תכונות ציוד המחשוב, נכון יהיה לקיים מערכות גיבוי חזקות ומקיפות ולפרוש אותן על פי מדיניות מוכנה מראש, לכל מיני מקרים שיוגדרו כהתקפות סייבר מוצלחות כנגד המדינה וגורמי הייחוס שזוהו, שיש לספק להם מענה אבטחתי מתאים.

המענה העקרוני לבעיה זו מכונה בעברית "יכולות קימום והתאוששות מאירועי אבטחת מידע", והוא כולל מגוון רחב של צורות להמשכיות ו/או להפעלה מחודשת של יכולות או תת יכולות קריטיות של מערכות שנפגעו מאירועי התקפות מידע. חשוב להדגיש כי יכולות קימום צריכות להניח כישלון בהגנה, או מניע של התקפות מידע, וכוללות גם מערכות גיבוי שמופעלות באופן ייעודי, לאחר שהתקיים אירוע אבטחה, או תוך כדי אירוע מתמשך. תורת עבודה וקימום בחירום חשובים לא פחות, ויתורגלו על ידי המשתמשים ומנהלי המערכות השונות.

בשוק המסחרי מכונה תחום זה BCP - DRP, והוא כולל יכולות לתפקוד והמשכיות תחת התקפה (מהיבטי תפקודיות ויכולות מעטפת הביצועים המבצעית של מערכות), וכן יכולות להעלות מידע מחדש על גבי מערכות שנפגעו עקב אירועי אבטחת מידע.

מחקרים שונים באוניברסיטאות יכולים להיות נקודת פתיחה לפיתוח יכולות להמשכיות תפקודית תחת התקפה, יש תחומי מחקר שפיתחו פרוטוקולים העמידים בפני שגיאות זדוניות ואקראיות, והמבטיחים התכנסות למצב יציב (בהסתברות מאד גבוהה) תוך זמן קצר. יש טכנולוגיות לגילוי קורולציות בין אירועים "מרוחקים", שעל פניהם לא נראים שייכים, ושהמקבץ שלהם יכול לתת התראה מקדמית מספקת לאפשרות התקפה קרובה. טכנולוגיות אלה לא פותחו לתחום הגנת הסייבר, אך אפשרי להסיבן לתחום.

כוונת הוועדה היא שיש להגדיר תוכנית פיתוח טכנולוגית ואופרטיבית, אשר תכלול הגדרת המענה והמשאבים הנחוצים לכל תת קבוצת ייחוס, על פי חשיבות המשכיות התפקוד שלה תחת ההתקפה, וכן על פי רמת התפקוד הנדרשת ממנה. התוכנית תכלול זיהוי של טכנולוגיות קיימות, פיתוח מענים לפערים שאינם בנמצא, פיתוח שיטות אינטגרציה של מערכות, והגדרת תורת פעולה במקרה של התקפה מוצלחת. יישום התכנית יכלול תרגול עיתי של יכולות הקימום וההתאוששות של גורמי הייחוס, והגדרת צוותי ונהלי בדיקה מתאימים.

5.8 נספח ח – מחשוב עננים ישראלי

בעשור האחרון, יש נטייה הולכת וגוברת להחזיק מידע בעננים הממוקמים פיזית ברובם מחוץ למדינה, לדוגמא שימוש בדוא"ל של GMAIL או HOTMAIL, ושימוש במערכות מחשוב אחרות בחו"ל (למשל אמאזון). שימושים אחרים בענן כוללים שירותי אחסון מידע, שירותי חישוב, רשתות חברתיות וכמובן שילובים של כל הסוגים הנ"ל. הצלחתן של כמה ממערכות אלה גדולה, והן נחשבות אטרקטיביות במיוחד לציבור הרחב, ואף לחברות וארגונים ציבוריים ופרטיים.

מערכות מסוג זה מהוות אתגר מבחינת אבטחתן מכמה סיבות:

1. הן נמצאות ברשותם של גופים מחוץ למדינה, ללא יכולת של בעל המידע או של מדינת ישראל להשפיע על כך.
2. אין יכולת להגן על המידע באותו אופן שמגינים על מידע הנמצא ישירות ברשות הגוף בעל המידע, או בדומה לנעשה במדינה (למשל, אין אפשרות להפעיל את ההמלצות האחרות של ועדה זו). וכמובן אין יכולת מעקב אחרי ניסיונות התקפה (כדוגמת מעטפת הגנה הקיברנטית).

3. בעת נפילת חיבור האינטרנט מהמדינה החוצה, או בעת התקפה על הרשת של המדינה, לא ניתן לגשת לענן מרוחק מתוך ישראל ולכן לא ניתן להשתמש בו בזמן חירום.
4. למדינות זרות יש גישה פוטנציאלית למידע, בפרט על פי החוקים שלהן.
5. מידע הנמצא מחוץ למרחב המדינה מקל על גופים זרים לבצע שאילתות מתוחכמות, המאפשרות להם לקבל מידע הנוגע לפרטיותו של האזרח, למשל רשימת מכריו של אדם מתוך דוא"ל, רשימת אנשים שעליהם הוא מתקשר בסקייפ, ואף חתכים המחושבים על סמך כלל המידע שנמצא בענן (שלעיתים ניתן לחשב אותו גם לגבי אדם שלא משתמש בעצמו בשירות). מתוך המסה של המידע, ניתן לחשב חתכים מסוימים הנוגעים לביטחון המדינה, שסודיותם גבוהה מזו של הנתונים הגולמיים.
6. בימינו טלפונים סלולאריים הינם מחשב המשמש גם כטלפון, ולכן כל היבטי אבטחת המידע במחשבים נוגעים אליהם. הדבר בולט במיוחד בטלפונים החכמים המסנכרנים את רשימת אנשי הקשר ומידע אחר הנמצא בטלפון מול הרשת, עם גופים ידועים (למשל GOOGLE במקרה של אנדרואיד או עם APPLE במקרה של IPHONE) ולא ידועים כאחד, כדוגמת מתקיני רוגלות למיניהם.

אי לכך הגנה על מידע בענן הוא אתגר הדורש התמודדות מיוחדת:

1. עידוד חברות ענן גדולות להקים מרכזי מידע בארץ, למשל אחזקת שרת דוא"ל של GMAIL בארץ עבור דואר ישראלי ו/או עידוד התעשייה המקומית להקים מערכות מסוג זה.
2. עידוד אחזקת מערכות ישראליות קריטיות בתוך המדינה ולא מחוצה לה.
3. פיתוח מערכות להצפנת המידע הנמצא בענן והגנה עליו.
4. חינוך הציבור ליתרונותיו וחסרונותיו של הענן, ובפרט לסיכונים הפוטנציאלים הכרוכים בשימוש בו מבחינת סודיות ופרטיות.
5. הגדרת רגולציה שתחייב גופים המחזיקים מידע בענן בחו"ל להגן עליו ולשמור על פרטיות האזרחים, ושתגדיר באילו תנאים גופים יכולים להעביר את שירותיהם לשרתים בחו"ל, ולאילו צרכים מותר להשתמש במידע שנאסף.
6. ייזום והשתתפות בפעילויות חקיקה, תקינה ופיתוחים טכנולוגיים לפרטיות המשתתפים, בפורומים ובזירות בינלאומיים.

דו"ח תת ועדת צופן וסימולציה

תמצית מנהלים

מרבית המערכות הגדולות במדינה (תקשורת, בסיסי נתונים ותשתיות פיסיות) מוגנות, או אמורות להיות מוגנות, ע"י מערכות צופן חדשניות וייחודיות. התחומים המדעיים והטכנולוגיים העוסקים בפיתוח יכולות בעולם הצופן הם, בין השאר, מתמטיקה, מדעי המחשב, הנדסת מחשבים, הנדסת מערכות, פיסיקה ועוד.

מסמך זה, המוגש לוועדת ההיגוי של המיזם הקיברנטי 2011 בידי ועדת הצופן (ראו נספח 1), מנתח את נקודות החולשה והחוזק של מערכות הצופן במדינה, את הצרכים העתידיים ואת האתגרים האקדמיים והטכנולוגיים בתחום. בנוסף, המסמך ממליץ על כיווני הפעולה המתאימים והרלוונטיים למדינת ישראל, שראוי לקדמם במסגרת המיזם הקיברנטי בתחום הצופן, בהתייחס לאקדמיה, לתעשייה, למערכות הממשל ולמערכת הביטחון. כמו כן, חלק מההמלצות רלוונטיות לפיתוח יכולות של מדינת ישראל בתחומי ההגנה בסייבר באופן כללי.

קווי היסוד של ההמלצות המרכזיות בדו"ח

עדיפות למחקר ופתוח בתחומים הבאים:
הבסיס המתמטי של הצופן: קריפטואנליזה, סטגנוגרפיה וקריפטולוגיה (פונקציות חד כווניות, מערכות לא קומוטטיביטות).

חוסן מערכות: שיטות פורמאליות (במדעי המחשב), אומדן חוסן ואיתור חולשות, טכניקות לחיסון מערכות קיימות, מערכות חסונות עתידיות: עיבוד מידע מוצפן, פרוטוקולים, KPD, Obfuscation.

הנדסת אבטחה (פיתוח טכניקות הנדסיות ברמת המוצר או המערכת, חקר חולשות בטכנולוגיות אבטחה וכד') ואבטחה פיסיקאלית (למשל לייזרים כאוטיים).

הצפנה קוונטית ומחשוב קוונטי.

יצירת הון אנושי.

עידוד סטודנטיות וסטודנטים ללמוד מתמטיקה והנדסת חשמל.

תארים אקדמים בתחום הסייבר, ביניהם מסלולי התמחות בתחום הצופן במסגרת לימודי מתמטיקה ומדעי המחשב, או מסלול בין-מחלקתי (מתמטיקה, מדעי המחשב, הנדסת חשמל).

מודלים לקדם שיתוף פעולה בין הצבא לאקדמיה (פתיחות מול ביטחון).

מערכות תשתית לאומיות

הקניית חוסן לצופן לתשתיות קריטיות ומערכות ממשלתיות, על ידי מעבדה להסמכת מוצרים, ו/או על ידי פיתוח פתרונות צופן חסונים ואינטגרלים באמצעות ידע בטחוני.

פיתוח צופן צבאי מהיר

פיתוח אבני בניין גנריות, שיאפשרו סטנדרטיזציה ופיתוח מהיר של מערכות הכוללות צופן למערכת הביטחון, וכן השקעה באפשרויות הייצוא.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

הערה:
חלק מההמלצות אינן מחייבות להגדיל את התקציב לארגונים הרלוונטיים, וחלקן כן. התקציב יחולק בהתאם לנתונים שישולבו בדו"ח הכללי של המיזם.

1. עולם הצופן - רקע

הצופן רלוונטי בתחום ההגנה כמו גם בתחום האיסוף. יכולות גבוהות בתחום הצופן הן נכס חשוב למדינה, המקנה לה יתרון בתחום ההגנה (כלכלית וביטחונית) ובתחום האיסוף.

ללא הגנה על ידע - מערכות תקשורת, ניהול תשתיות ורכוש אינטלקטואלי לא ניתן לשרוד כלכלית וביטחונית, במיוחד בסביבה עוינת[1]. צופן מגן על הסודיות של פריטי מידע, ומשמש כחומה לבידוד רשתות ולתיחום אזורים בעולם הקיברנטי. הצופן של עידן הסייבר שונה מהצופן המסורתי. בעידן הסייבר, הצופן הוא חומה מרכזית באסטרטגיית ההגנה, הנדרש להתמודד עם תקיפות סייבר. יתר על כן, הוא נדרש להשתתף במעגל זיהוי פריצה (בחומה מקוונת קשה יותר לזהות את הפריצה מאשר בחומה פיזית), תקיפות והונאה.

שבירת הצופן של האויב הוא גורם אסטרטגי מכריע, כפי שמעידה ההיסטוריה הצבאית העולמית (במהלכה ידיעת הסודות של היריב היוותה גורם מכריע בסכסוכים ומלחמות).

במדינת ישראל, הנשענת על תעשיות עתירות ידע, ובעלת אויבים ויריבים קרובים מבחינה גאוגרפית, הצורך לשמור על סודיות הידע - תקשורת, מערכות תשתית ורכוש אינטלקטואלי - הוא בעל משמעות לאומית בהקשר ביטחוני וכלכלי כאחד. מסמך זה לא יפרט, מפאת הסיווג, את העיסוק בתחום במדינת ישראל.

1.1 השלבים העקריים בפיתוח פתרון צופן

הנדסת מערכת - גיבוש דרישות האבטחה מהמערכת, ועיצוב פתרון. לפתרונות צופן יש השלכות רבות על הביצועים, התפעול וכמובן הביטחון של המערכת. על מנת לפתח פתרון צופן מספק, בטוח ובר יישום, יש לבצע תהליך מורכב של הנדסת מערכת, מתוך הבנה עמוקה שלה.

פיתוח מרכיבי הצופן - החל מפיתוח הפתרון במרחב המתמטי ועד יישומו ברמת סמך גבוהה במוצרים ובמערכות, כולל פיתוח אמצעים משלימים דוגמת מפתחות צופן. נתח נכבד ממשאבי הפיתוח מושקע ביישום בטוח.

הטמעת הצופן - במובן התפעולי, ברגולציה, בעידוד וחינוך לשימוש נכון בצופן.

1.2 תחומי המחקר, הידע והטכנולוגיה

לפיתוח צופן משמשים מחקרים מתמטיים ומחקרים הנדסיים, הנדסת מערכות, הנדסת מחשבים והנדסת אלקטרוניקה. עולם הצופן (ובעקבותיו המחקר והפיתוח), מגבש שיטות יצירתיות של תקיפה והגנה, העוקפות את מסגרות החשיבה המסורתיות (למשל, תחום ה- TEMPEST, העוסק בביטויים פיסיקאליים של המידע, שללא טיפול מתאים עלולים לעקוף את מנגנוני הצופן ולייתרם). מלבד מחקרים העוסקים ישירות בנושא הצופן, תורמים לתחום גם מחקרים כלליים בהנדסה ומדעי המחשב, שכן מערכות צופן הן מטבען מערכות מחשב המבוססות על חומרה ותוכנה.

[1] בספרו "עולם ללא סודות", מתאר פרופ' אחיטוב מציאות שאין בה סודות בעידן המידע. מציאות כזו, אם נדמיין אותה, קשה ביותר לאדם הפרטי, אך בלתי אפשרית למדינה.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

- מחקר מתמטי - עוסק בבעיות הליבה של הצופן בתחומי הקריפטולוגיה, הקריפטוגרפיה והקריפטואנאליזה (מדע הסתרת הסוד וחשיפתו), והסטגנוגרפיה והסטגואנאליזה (מדע התממת הסוד וחשיפתו), לצד תחומים מתמטיים נוספים: סטטיסטיקה, למידה חישובית וכריית מידע.
מחקר השיטות הפורמאליות במדעי המחשב מזוהה ומתפתח כתחום ליבה, שיוכיח את חוסן של מערכות הצופן ויאתר פגיעות בהן.

- מחקר הנדסי - בתחום התקשורת, החומרה, מערכות התוכנה, הנדסת מערכות ופיסיקה, בוחן כיצד לספק ולממש הגנה באופן בטוח, אמין, ישים ויעיל. תחום המחקר העוסק באבטחה במישור ההנדסי מכונה לעיתים הנדסת אבטחה.

1.3 מגמות חדשות בצופן

הצופן כמעגל הגנה בסיסי בסייבר - הצפנה משולבת להגנה על נתחים מעולם הסייבר באמצעות בידודם, בנוסף לאמצעי הגנה נוספים (לדוגמה זיהוי תקיפות), מעצימה את המוטיבציה לתקיפת הצופן, הנעשית לעיתים גם בשיטות סייבר, לצד תקיפות בשיטות מסורתיות (מהמרחב המתמטי).

הצופן כמרכיב בסיסי בכל מערכת תקשורת - מספר גדל של מערכות הכוללות תקשורת נדרשות לספק פתרון צופן אינטגרלי, במסגרת דרישת תקן (כגון בתקני תקשורת נתונים אלחוטית), או דרישת לקוח (לדוגמה, בעסקת יצוא ביטחוני). העיסוק הגובר בסייבר בעולם באה לידי ביטוי בדרישות מפורטות יותר, בהיכרות עמוקה עם התחום ובביקורותיות של הדורשים.
מספר שכבות הצפנה - מהצפנת תקשורת ועד הצפנה אפליקטיבית: לארגונים המתמודדים עם איומים חיצוניים מספיקה הצפנת תקשורת, ואלה המתמודדים עם מגוון איומים פנימיים זקוקים לפתרונות של הצפנה מותאמת יישום (הצפנת בסיסי נתונים, וידאו ועוד). כמו כן, הצופן הוא אמצעי ל"נעילת תוכן", ומרכיב בסכמות רבות של מידור, מניעת דלף ועוד.

2. אתגרים

כדי לשמר ולשפר את יכולות הצופן של מדינת ישראל (בהקשר ביטחוני, ממשלתי וציבורי, במערכות מקוונות ובתשתיות פיזיות), ולהבטיח את יתרונה בתחום הצופן, לנוכח העובדה שהצופן הוא מטרה מועדפת לתקיפה, ושהאויב מרחיב את השימוש בו, ולנוכח ההתפתחויות המדעיות והמגמות שהוזכרו לעיל, יש צורך לשפר את שיטות ואמצעי ההצפנה, החל בתפיסה המתמטית שבבסיסן (בדגש על קריפטולוגיה ופרוטוקולים), כמו גם בשיטות היישום (במיוחד לנוכח דרישות מורכבות וכביכול סותרות ממערכות הצופן), ועד בניית מערכות צופן חסינות, המותאמות לאיום לאורך שנים, תוך התמודדות עם שינויים טכנולוגיים, ובמיוחד עם התפתחות טכנולוגיות התקשורת. מערכות צופן אלה יאפשרו חופש פעולה למדינת ישראל וקהילת הביטחון הישראלית במרחב הסייבר, יבטיחו את החוסן של מערכות הצופן במרחב הממשלתי והציבורי, ויגדילו את עמידותן של תשתיות קריטיות בפני תקיפות סייבר. ההתמודדות עם צופן הינה יכולת מרכזית, כיוון שהיקף המערכות הלא מוצפנות בעולם ילך ויקטן.

יש צורך מיוחד לעמוד באתגרים ובמטלות, ולספק מענה לשאלות שלהלן.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

2.1 פיתוח תחומי מחקר מרכזיים

יש צורך לחזק ולעודד תחומים מדעיים וטכנולוגיים פורצי דרך ובעלי פוטנציאל לקדם משמעותית את תחום הצופן ממתמטיקה למחשוב והנדסה:

מתמטיקה עיונית: נושאים מתקדמים בתורת המספרים, בתורת החבורות, באלגברה לא אסוציאטיבית, ובגיאומטריה אלגברית, העומדים בבסיס התכנון וההתמודדות עם מנגנוני צופן.

קריפטואנליזה: שיפור יכולות ההצפנה וההתמודדות עם צופן.

קריפטולוגיה: פונקציות מתמטיות חד כיווניות חדשות וחזקות, עיבוד מידע מוצפן והצפנה, הדרושות לטכנולוגיות מתחדשות, פרוטוקולים וסכמות.

פרוטוקולים ומודלים: איתור וחיסון מפני חולשות במערכות צופן: קוד, פרוטוקולים, מודלים.

שטות פורמאליות במדעי המחשב: זיהוי אוטומאטי של תקיפות על צופן, כולל איתור המיקום ומאפייני התקיפה, Obfuscation, מצפין מתפתח דינאמי, שיטות פורמאליות לפיתוח חיסון ולאיתור פגיעויות.

הנדסת אבטחה: היבטים הנדסיים של הגנה על המערכת או תקיפתה - הגנת מערכות בחומרה - ארכיטקטורות ואבני בניין, תקיפות והגנתן, תקיפות על כ"ח, התמודדות עם תקיפה פיסית של מכשיר (Anti-Tampering, Tamper-Detection).

פיסיקה: לייזרים כאוטיים, הפצת מפתחות קוונטית והגנת מידע באמצעים פיסיקאליים כתחליף, או כטכנולוגיה משלימה לתחום הצופן.

חישוב קוונטי: פיתוח אלגוריתמים מתמטים שמתאימים למחשב קוונטי, שפיתוחו עלול לאיים על שיטות צופן קיימות.

2.2 היקף כח אדם מתאים

יש צורך להבטיח עתודות כח אדם מיומן, שיספק את הנדרש בכל תחומי העשייה של הצופן, מהמחקר האקדמי ועד לפיתוח הביטחוני, ממחקר בסיסי רלוונטי ועד לפיתוח טכנולוגיות ומוצרים.

2.3 צופן במרחב האזרחי

האם וכיצד ניתן לספק צופן חסון למערכות תשתית אזרחיות מרכזיות (חשמל, מים, תקשורת ומערכות חירום) ולתעשייה, כדי להגן על ידע בכלל ועל בסיסי נתונים בפרט?[2]

2.4 קידום הצופן כענף כלכלי

האם ניתן לפתח צופן בתעשייה הישראלית (הצבאית והאזרחית), באופן שיאפשר להפוך את מדינת ישראל לגורם מוביל בתחום הצופן בשווקים הבינ"ל, בלי להגדיל באורח משמעותי סיכונים ביטחוניים בטחוניים?

התעשייה במדינת ישראל תעמוד בפני דרישה גוברת לספק פתרונות צופן אינטגרטיביים, ולעמוד בדרישות מחמירות יותר (לדוגמה, בתקני אבטחה והבטחה). האם וכיצד ניתן להשפיע על התקינה הבינ"ל, כך שמוצרי מדף יעניקו מענה מספק, ו/או תשתית למענה ביטחוני?

התעשייה תידרש לפתח מערכות קישוריות (לאור הגידול המתמיד בצרכים לקישוריות), התומכות במגוון קישורים מוצפנים לגורמים שונים.

[2] ראו תקיפת גוגל מהשנה האחרונה.

2.5 אסטרטגיית צופן

יש צורך להפוך את פיתוח הצופן הביטחוני לחלק אינטגרלי וטבעי מפיתוח המערכת, לצמצם את התקורות על הפרוייקטים, ולתת מענה לפיתוח צופן ביטחוני לצד אינטראופרביליות (פיתוח מערכות שמרכיביהן מתקשרים זה עם זה, גם אם אינם מיוצרים על ידי אותו היצרן), תוך יכולת מענה מהיר לצרכים בתחום הצופן.

צריך לפתח תפיסות וארכיטקטורות חדשניות של הצפנה (פרוטוקולים וסכמות הצפנה), המותאמות לדרישות מבצעיות וטכנולוגיות מתקדמות

3. ניתוח חסמים

תחומי והיקף מחקר באקדמיה

העיסוק בקריפטוגרפיה באקדמיה הישראלית מועט, וממוקד בקריפטוגרפיה תיאורטית (כ- 20 חוקרים, לא כתחום יחיד). בתחום הקריפטאנליזה, חוקרים בודדים מגיעים להישגים משמעותיים.
יש חוקרים בתחומים רבים הרלוונטים לצופן, וביניהם: למידה חישובית, שיטות פורמאליות, תקשורת ועוד, אך בתחומים רלוונטים אחרים, דוגמת הנדסת אבטחה, הפעילות מצומצמת (כ- 15 חוקרים), ועוד יותר כך בתחומים כמו Tamper Resistance, Tempest

3.1 כח אדם לצופן במערכת הביטחון

השימוש בצופן במערכת הביטחון מבוסס על מחקר ופיתוח בתוך המערכת ובתעשיות הביטחוניות, המכוון בהתאם למערכות המוגנות, כמו כן מפותחים מוצרי תשתית גנריים, היכולים להשתלב במערכות רבות.

3.1.1 עיקר המחקר והפיתוח המסווג מתבצע במערכת הבטחון, על ידי כח אדם צבאי (בעל נסיון מקצועי קצר יחסית), ובתעשיות הבטחוניות.

כוח אדם צבאי המתאים למחקר ופיתוח, נשען על בוגרי תיכון בעלי חמש יחידות במתמטיקה. זהו תנאי הכרחי לרכישת ההשכלה והמיומנויות הנדרשות כדי להתמחות בצופן על כל מרכיביו בפרט, ולתעשיות עתירות ידע המהוות מרכיב מרכזי בצמיחת המשק בכלל. תנאי זה מגביל, בעיקר בנות. מספר התלמידות הלומדות מתמטיקה ברמת חמש יחידות נמוך מכמות התלמידות שברשותן יכולות גבוהות בתחום. לכן, בנות שמוותרות על לימודי מתמטיקה בהיקף של חמש יחידות נעדרות ממצבת כוח האדם של יחידות צבאיות בתחום הצופן (יחידות אלה נמצאת כיום בחסר שאף יגדל), ובעתיד לא תוכלנה להשתלב בתעשיות עתירות ידע עם אופק בינלאומי.

נשים בעלות תואר שלישי מתקשות להתקדם בעולם האקדמי (למשל, בהשלמת לימודי פוסט-דוקטורט בחו"ל וכד'). ייתכן שדווקא בעקבות הקשיים האלה, נשים יפנו למחקר בזיקה לעולם הביטחוני המסווג.

3.1.2 מערכת הביטחון משקיעה משאבים רבים בפיתוח כוח אדם בתוך המערכת ועבורה. כיום אין מספיק מסלולי קידום אטרקטיביים של שרות מקצועי-טכני ארוך טווח לכוח האדם הדרוש בתחום. לאור הקושי לרתום חוקרים מנוסים לאורך זמן (בנוסף לצורך לעקוב אחרי הפיתוחים בעולם האקדמי והחדשנות ההכרחית בהגנות והתקפות צופן) - צריך להסתייע בחוקרים מהאקדמיה, אך גם חוקרים אקדמים מובילים מתקשים להירתם לאורך זמן, בפרט במחקר מסווג (ובמיוחד בקריפטולוגיה), שכן בשל החסיון על המחקר הם לא יכולים לפרסם כמקובל, לצורך קידום מקצועי בעולם האקדמי (פתיחות מול ביטחון). להלן הערכה של מימדי החסר המיידי בחוקרים בכירים למערכת הביטחון (במיוחד חוקרים באקדמיה שפועלים בשיתוף עם הצבא) בתחומים הבאים:

- קריפטואנליזה, קריפטולוגיה וסטגנוגרפיה- עשרים חוקרים
- שיטות פורמאליות במדעי המחשב (אימות, הוכחות קוד, איתור חולשות וכד') עשרה חוקרים

- הנדסת אבטחת מידע (מחקרים הנדסיים - חולשות טכנולוגיות, פיתוח חיסון, ארכיטקטורות מערכות (Tamper, Tempest עשרה חוקרים.

3.2 הגנה על תשתיות קריטיות

גורמי ממשל וגורמי ביטחון ציבורי, כמו גם הנהלות של תשתיות קריטיות, משתמשות במוצרי צופן מסחריים (כמו התעשייה הישראלית), כל עוד לא מדובר בהגנה על סודות ביטחוניים. רמת האבטחה של המוצרים היא המקובלת בעולם המסחרי, הם נמכרים ליריבים ואויבים ואינם נחשבים חסונים דיים.

3.3 תעשיית הצופן כתעשיית יצוא (צו הצופן)

במדינת ישראל יש תעשיית צופן מפותחת. בכל שנה מוגשות עשרות בקשות פטנט בתחום הצופן (כ-2% מהפטנטים בתחום הצופן בעולם). עשרות חברות ישראליות עוסקות בתחום הצופן, וחברות בינ"ל מפתחות את הצופן שלהן בישראל. מספר חברות בולטות בתחום הצופן בישראל:

Checkpoint - אחת מהחברות המובילות בעולם לפתרונות הגנה באינטרנט, ובכלל זה פתרונות צופן
Discretix - חברה לפתרונות IP המשולבים בטכנולוגיות סלולאריו
NDS - חברה לפתרונות צופן וניהול זכויות למידע (בולטת בתחום הוידאו)
OTI - חברה לכרטיסים חכמים בטוחים
RSA - חברה לפתרונות הזדהות ואימות
Verint - חברה לפתרונות איסוף (לגופי ביטחון), הכוללים לעיתים שבירת צופן או עקיפתו.

הפיקוח על העיסוק בצופן (פיתוח, יבוא, יצוא, שיווק וכד') בעולם ובישראל נובע משתי סיבות:
(I) עמידה באמנת וסנר - לפיה צופן, גם צופן מסחרי, הוא בגדר טכנולוגיה דו שימושית (אזרחית/צבאית), וקיים חשש שיגיע לידיים הלא הנכונות, כגון מדינות המוכרזות כתומכות בטרור, ארגוני טרור וגורמים פליליים שישתמשו בו למטרות פסולות. מדינת ישראל אינה חתומה על אמנת וסנר, אך חותרת להיות תואמת לה. (II) מניעת דליפה של טכנולוגיות צופן צבאיות ישראליות במסגרת היצוא הביטחוני.

הפיקוח מתחשב בעובדה שהצופן המסחרי נפוץ וזמין, וברוב המקרים מעניק אישור כמעט גורף לעסוק בטכנולוגיות הצופן גם ביצוא. התעשיות הביטחוניות מושפעות יותר מהפיקוח. פיתוח צופן ביטחוני, בדומה לפיתוח ביטחוני מסוג בתחומים אחרים, נעשה בכפוף להנחיות הביטחון של מלמ"ב. מדובר בפיתוח ייעודי עבור מדינת ישראל, וסוגיית היצוא מטופלת בהתאם למערכת ולייעד היצוא.

גופים בתעשייה חשים כי אין כללים ברורים לפיקוח על היצוא בתחום הסייבר (כלי תקיפה) - נושא זה חורג מתחום מסמך זה ולא ידון בו.

4. המלצות

4.1 תחומי עדיפות

כדי לפתח כוח אדם ייעודי וחוקרים, דרושים תחומי הידע הבאים שימושי גאומטריה אלגברית ותורת המספרים, קריפטולוגיה, קריפטואנאליזה בסיסית, צופן יישומי, אבטחת מידע ותקיפת מערכות תוכנה.
יש לפתח קורסים בסייבר, ולשלבם בלימודי תואר ראשון במתמטיקה, מדעי המחשב, הנדסת מחשבים והנדסת חשמל.

4.2 הכשרת כח אדם

4.2.1 לעודד תלמידות להתמחות במתמטיקה ברמה של חמש יחידות (כמו כן, לעודד לימודים בתחומים אלו גם ללא קשר למגדר).

4.2.2 ליזום (ע״י האוניברסיטאות ומל״ג) תארים אקדמים בתחום הסייבר ומסלולי התמחות בתחום הצופן

קדימות להעניק עדיפות בחלוקת מלגות לתלמידים לתואר שלישי מחיםבתחומים שלעיל (מלגות אוניברסטאיות, כמו גם מלגות של משרד המדע והטכנולוגיה), בתנאי שישתלבו במחקר באקדמיה ובתעשייה בישראל, מחוייבות ויתחייבו לעבוד תקופות קצרות במערכת הבטחון.

לממן (ע״י מהתעשייה הישראלית) מלגות לתארים מתקדמים (ולתלמידים מצטיינים בשנתונים מתקדמים), בתנאי שישתלבו במחקר בתעשייה בישראל.

ליצור מסלול צבאי מיוחד המיועד לקלוט בוגרים מהתחום בצבא במקביל ללימודים לתואר שלישי. ליצור מסלולים, במימון מערכת הבטחון, לשילוב גורמים מצה״ל בעולם האקדמי כאמצעי לפיתוח המקצועיות ולהעברת ידע.
בניית קורסים יעודיים לתואר ראשון, שישולבו בתוכניות הלימודים ויאפשרו לבוגרים להשתלב במהירות בתחום הסייבר (חלקם כבר קיימים).

פיתוח תואר שני (עם תיזה) בסייבר בתחום הצופן, שיבוסס על תואר ראשון במתמטיקה/מדעי המחשב/הנדסה/פיסיקה, שיתמקד במרחב הידע הנחוץ בתחום הסייבר בכלל, ובתחום הצופן בעידן הסייבר בפרט.

4.3 פיתוח המחקר באקדמיה (בשתוף התעשייה ומערכת היבטחון)

4.3.1 להקים מכוני מחקר/מרכזי מצוינות באקדמיה, שיכללו בשלב הסופי 40 חוקרים בתחומי עדיפות, לפי החסרים שצוינו לעיל.

4.3.2 במכונים ייערך מחקר אקדמי, שיתבסס על תשתיות של המוסד ועל תשתיות חישוב לאומיות, ויוכשרו תלמידים לתואר שלישי, כולל תלמידים ממערכת הביטחון.

4.3.3 המחקר יכוון לשוק הפרטי ולתעשיית הביטחון, ויכלול פרוייקטים שיוצעו ע״י מערכת הביטחון והתעשייה ובמימון ישיר.

נושא הזכויות המסחריות והפטנטים ידון ישירות בין המכון לבין התעשייה הרלוונטית.

מכוני המחקר יהיו שותפים למאמצי תקינה בינ״ל בתחום הצופן והגנת המידע, וכך יקדמו תקינה בטוחה עבור הציבור הרחב.

4.4 בניית פלטפורמות לעידוד שיתוף פעולה בין הצבא לאקדמיה לפי רמות הסיווג הבאות:

- מחקרים בלתי מסווגים - בנייה של תשתית ידע, והתקדמות במחוזות שיש בהם כבר היום יתרון יחסי לעולם האקדמי הרחב, כמו למשל, מרכיבים באבטחת מידע בחומרה, מחקרים כלליים בגיאומטריה אלגברית ובתורת המספרים, בהנדסת אבטחה וכד'.

- מחקרים מסווגים - מחקר הכולל חשיפה למידע מסווג, או שתוצאותיו מוגדרות מראש כמסווגות.

- תוצאות מסווגות - מחקרים אשר תוצאותיהם (באופן צפוי או בלתי צפוי) מהוות פריצת דרך (דוגמה היפותטית): הצלחה מפתיעה בפירוק מספרים לגורמים ראשוניים).

מטבע הדברים, מערכת הביטחון מעוניינת באופן ישיר בעיקר בשתי הקטגוריות האחרונות, ואילו החוקרים בעלי עניין בעיקר בקטגוריה הראשונה, שכן הקידום בעולם האקדמיה תלוי בפרסומים מחקריים. על כן, צריך לפתח מודל שיאפשר לשלב בין מחקר ביטחוני מסווג לבין פרסום.

באמצעות מכוני מחקר חדשים ומשרות נוספות לחוקרים, ניתן לבנות מסגרות שיספקו מענה לצרכים ולסיכונים השונים:

הקטנת סיכונים בטחוניים	כדאיות לחוקר	קושי בבקרה על המחקר
• הגדרה מראש של סיווג המחקר המותר לפרסום	• הגבלת הפרסום על סמך ועדה מקצועית ביטחונית	• ועדת היגוי אקדמית-בטחונית
• ביצוע המרכיב המסווג בזמן מוגבל ובסביבה ביטחונית (סנדאות קיץ, אחוזי משרה בסביבה ביטחונית, שבתונים במערכת הביטחון וכד')	• פטור מהוראה	• סמכות להפסקת הפעילות בידי מערכת הביטחון
• כרטיסיית הגבלות -מערכת הבטחון רשאית לאסור פרסום, אך באופן מוגבל	• קידום בהתחשב במרכיב המסווג	
• פטנט מסווג/שיפוי כלכלי לחוקר אשר הוגבל בפרסום	• שותפות בפעילות ביטחונית	
• וטו ברמה בכירה מאד,המאפשר למערכת הביטחון לפסוק, אך ללא "אצבע קלה על ההדק"		

מודלים אפשריים הנגזרים מהדרישות האלו:
- מודל סדנאות קיץ - החוקר עוסק במחקר בלתי מסווג רוב השנה, אך מחוייב להשתתף בסדנאות בעת החופשה, לדוגמא בפורום מחשבה על בעיות בתחום הצופן והאבטחה.
- מודל לפיו החוקר יוצא לחופשה לפרק זמן רצוף של מספר חודשים, ובמהלכה מקדיש את עיקר זמנו למחקר מסווג במערכת הביטחון. יש לבחון כיצד לתגמל את החוקר כך שימשיך להתקדם בעולם האקדמי, על סמך הישגי המחקר המסווג שיבצע (מודל דומה קיים כיום במספר תחומי עיסוק מסווגים).
- מודל לפיו החוקר מכוון לבעיות תשתית, אך האפשרות לפרסם פריצות דרך בעלות משמעות אבטחתית מוגבלת, ומכילה איזונים ובלמים בין אנשי האקדמיה לגורמי הבטחון. על פי המודל, החוקר הוא, בסופו של דבר, איש מערכת הבטחון מבחינת האחריות המוטלת עליו.
- מודל למחקר במסגרת מרכז המחקר וייעוץ לפרוייקטים מסווגים במשרה חלקית - מחייב להגמיש את

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

המדיניות הביטחונית, ולאפשר חשיפה של החוקרים לפעילויות מסווגות, וכן מחייב פיקוח על פרסומי החוקר, במקרה שיש חשש הוא מתבסס על תוצאות מסווגות.

4.5 פיתוח פתרונות לצופן לתשתיות קריטיות, למערכות ממשלתיות ולסביבה עתירת ידע

על מנת להתאים את פתרונות הצופן בתשתיות קריטיות, במערכות ממשלתיות ובסביבה עתירת ידע, להלן שתי חלופות:

1. פיתוח מעבדות הסמכה למוצרי צופן (והגנה), לצד דרישה מטעם רגולטורים להשתמש במוצרים שאושרו עבור תשתיות קריטיות ומערכות ממשלתיות. על פי מודל זה, כל יצרן יכול לאשר את מוצריו, כשהמניע לאישור הוא השוק והרגולציה.

2. פיתוח מוצרי צופן עבור תשתיות קריטיות ומערכות ממשלתיות. במסגרת זו, יפותח סל מוצרים המספק מענה למרבית הצרכים (עקב דמיון בין מערכות ה-IT), וכן יפותחו מספר מצפינים (על בסיס תשתיות קיימות בעולם הצופן הביטחוני), שיחוייבו בשימוש בקרב עולם התשתיות הקריטיות והמערכות הממשלתיות.

המלצתנו היא להתמקד בחלופה א', אך לא לזנוח את חלופה ב'. יכולת הסמכה היא חשובה עבור מוצרים לא רק בתחום הצופן, והיא מסייעת לפתח ידע בתעשייה, באקדמיה ובמערכת הביטחון. חלופה זו גם פשוטה יותר בהיבט הרגולציה. עם זאת, מומלץ לבחון את חלופה ב' מול צרכים ספציפיים.

4.6 מעבדת הסמכה למוצרי צופן והגנה

באמצעות מודל ההסמכה ניתן לאשר מוצרים בלתי מסווגים, או לכל הפחות להעריך את רמת ההגנה שלהם, וכן להמליץ, ולעיתים אף ליצור רגולציה, שתעודד או תאלץ שימוש במוצרי צופן והגנה חזקים באופן הנכון, בקרב גורמים במדינת ישראל, דוגמת תעשיות עתירות ידע (הגנת ה-IP של מדינת ישראל).

ההמלצה עוסקת בהסמכה של מוצרי הצופן; יש צורך בכלים אחרים כדי להסמיך ולבחון את הארכיטקטורה והיישום של ההגנה על המערכות של הגופים האמורים. לדוגמה, במקרה של תשתיות קריטיות, קיים תהליך לבחינה, בקרה ואישור של תפיסת האבטחה.

ההסמכה הפורמאלית הרלוונטית היא הסמכה כמעבדת Common Criteria (CC). ה-CC הוא תקן לאומדן רמת ההבטחה של מוצרים, במיוחד מוצרי הגנה, כלומר עד כמה אפשר לסמוך על כך שהמוצר אכן מספק את רמת ההגנה שהוא מבטיח.
התקן מגדיר מספר רמות סמך, וככל שעולים ברמה, רמת הראיות וההוכחות לרמת ההגנה גדלה. בנקודת הקיצון - רמת הבטחה שבע - יש צורך בהוכחות פורמאליות.

קיימות מעבדות CC רבות ברחבי העולם, חלקן מספקות שירות על ידי חברות יעוץ גדולות מתחום האבטחה, וחלקן הוקמו בסיוע ממשלתי. המעבדות עצמאיות במידת האפשר, גם מבחינה כלכלית.

כיום, חברות ישראליות המעוניינות בהסמכה פונות למעבדות בחו"ל. מדינת ישראל חתומה על אמנה, לפיה היא מקבלת על עצמה את רמת הסמך שייקבעו מעבדות בינ"ל עד לרמה שלוש כולל (מדובר ברמה נמוכה למדי).

הסמכה היא תהליך יקר, שאורך חודשים רבים. הסמכה לרמה ארבע אורכת בממוצע ארבעה חודשים, ועולה כ-$350K. אנו חותרים לרמות הסמכה גבוהות (שש, שבע), הכרוכות בעלות גבוהה ונמשכות זמן רב.
קיים מתאם בין הסמכה מרמה חמש ומעלה להגבלות יצוא.

בחלופה הזו, יש יתרון גדול לקשר בין המעבדה לעולם האקדמי ולמערכת הבטחון, שכן הוא מפרה את החשיבה המחקרית בתחום הפיתוח ברמת סמך גבוהה, ובונה מיומנויות באיתור חולשות. חיוני שהקשר לא יפגע בזכויות של בעלי הקניין הרוחני של המוצר הנבדק.

לאור האתגרים בהסמכה הפורמאלית בתקן ה-Common Criteria, יש לפתח ולהרחיב את תהליכי ההסמכה הקיימים, באמצעות מעבדה בעלת יכולות דומות ל-Common Criteria; פתרון זה אמנם לא יספק את ההסמכה עצמה (קרי - היתרון השיווקי של ההסמכה הרשמית), אך יש לו מספר יתרונות:

- תהליך ההסמכה יתמקד בצרכים של מערכת הביטחון ושל התשתיות הקריטיות, ולא בכל מרחב הדרישות של התקן, ותהליך ההסמכה יוזל.
- תהליך ההסמכה הביטחוני יחפוף לתהליך ההסמכה התקני, ולכן, בהשקעה נוספת, יהיה ניתן להשלים את ההסמכה במעבדות מוסמכות אחרות.
- ההסמכה הביטחונית תתרום למוניטין של המוצרים (פיצוי מסוים על העדר הסמכה).
- ניתן לשלב גורמי ביטחון במעבדה, סוגייה חשובה במיוחד בכל האמור בהסמכת מוצרי צופן.
- קל יותר לשלב גורמי אקדמיה במעבדה, מאשר בחלופה של מעבדה מוסמכת בהסמכה בינ"ל.
- ניתן להמליץ על מוצרים שנבדקו לציבור הרחב, ובכך לשפר את הביטחון של מערכות במרחב האזרחי (בלי תלות בהסמכה פורמאלית).

במימון התחלתי אפשר להקים את המעבדה, רצוי במסגרת ניהולית הכוללת את רא"ם ואת מצו"ב, ולהחזיקה מספר שנים עד שתתבסס. מומלץ לתקנן חלק מכוח האדם מראש ככוח אדם צבאי, המפותח במצו"ב ומגשר בין מצו"ב לבין מעבדת הבדיקה. במסגרת ההקמה, נכון לבחון אם סמל"א תתאים כמוקד למספר מעבדות ביטחוניות לאומיות. למימוש החלופה, יש צורך ברגולציה שתחייב ותעודד שימוש במוצרים שהוסמכו.

אחד הסיכונים בחלופה הוא שמידע ידלוף, במקרה שהמעבדה אינה מסמיכה את המוצר עקב חולשה מתמטית/הנדסית מסווגת. במקרה כזה, לא יהיה ניתן לספק ליצרן הציוד הסבר על הסיבות לאי אישור המוצר, והוא עשוי לעתור לבג"ץ. רגולציה קיימת מקטינה את הסיכון (כאשר בתי המשפט מקבלים חוות דעת מסווגת של גורם ביטחוני), וכך גם רגולציה שתתווסף (לדוגמה, נהלים שיקבעו להסמכה ללא חובה להסגיר מידע מסוים, או כללים טכניים ומקצועיים שישמשו כדרישות סף ויעקפו בעיות כגון אלה).

ראו פרוט בנספח 3

4.7 פיתוח מוצרי צופן לתשתיות קריטיות ומערכות ממשלתיות

רוב מערכות ה-IT מבוססות על טכנולוגיות תקשורת סטנדרטיות (הצפנת IP), כמו גם מרכיבים גדולים מציוד מנוהל ומבוקר. על כן, ניתן לפתח מספר מצומצם של מערכות הצפנה, שיספקו מענה להיקף גדול מאד של תשתיות קריטיות ומערכות ממשלתיות. מעבר לכך, יתכן שיהיה ניתן לעודד גורמים שונים בשוק האזרחי להשתמש במוצרים אלו.

הישגים המרכזיים בפיתוח של המוצרים, הם אספקת מוצרים ברמת הגנה גבוהה, המתאימים למגוון צרכים רחב, בעלויות (פיתוח והצטיידות) נמוכות. להלן החלופות המרכזיות ליישום ההישגים:

1. לפתח מוצרים המבוססים על טכנולוגיות צבאיות, ולשלב שינויים שיבדילו בינם לבין מוצרים צבאיים, תוך התאמתם לסביבת התפעול הצפויה.
2. לבחור מספר מוצרים ישראליים, ולבצע בהם תהליך של בחינה ושיפור (בדומה למודל המעבדה, אך רק לטובת סל מוצרים מצומצם).

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

לכל מוצר צופן נדרש, יש לבחור את חלופת המימוש הדרושה.

יש לחייב/לעודד, באמצעות רגולציה, שימוש במוצרים, על פי מודל כלכלי שיחזיר חלק מהמימון הממשלתי דרך הרווחים של מכירות המוצרים, כך שבסופו של דבר, עלות הפרוייקט תהיה נמוכה מאד (עלות בסיס + עלויות מימון).

ראו פרוט בנספח 3

4.8 פרויקט לאומי – פיתוח אבני בניין לצופן

כדי שמערכת הביטחון תתבסס על מערכות מתקדמות מוצפנות, התעשייה הביטחונית תבצע במהירות פרוייקט לפיתוח אבני בניין לצופן, שיהוו סטנדרט לצופן באמל"ח ובמערכות.
אבני הבניין יכללו:

- רכיבים (צ'יפ) המותאמים להצפנה צבאית במגוון ישומים (צ'יפ שניתן לשלב במכשיר קשר / אמל"ח)
- רכיבי קושחה (IP Core VHDL) שניתן לשלב ברכיבים מיתכנתים גנריים.
- רכיבי תוכנה דוגמת מערכת הפעלה, מודלים מתמטיים וכד'.
- הנחיות ומערכי בדיקה לאימות ולעמידה בדרישות Tempest

אבני הבניין יפותחו מראש בשתי גרסאות - גרסה בטחונית וגרסת יצוא, כך בתהליך הפיתוח יבנה מראש את היכולת לייצא (במגבלות היצוא הבטחוני) תוצרים של התעשייה הצבאית הכוללים יכולות צופן. מפוי הפרוייקט נמצא בנספח 4

4.9 הצפנה לציבור הרחב

שילוב נושאי צופן בפעילות לקידום הגנת הציבור הרחב:

- הסברה - החל מהסברה כללית על הצורך בהגנה, ועד להמלצות והנחיות לשימוש פרטני בציוד ובמוצרים מומלצים ומוסמכים.
- שותפות במיזמי קוד פתוח ליצירת כלים נוחים לשימוש הציבור הרחב (בדומה להשתתפות בעבר של משרד האוצר בפרוייקט Open Office)
- חיזוק התקינה בתחום האבטחה (אימוץ תקני NIST), הרחבת מכון התקנים (קשור למרכיבי ההסמכה למוצרים)
- גיבוש פתרונות קריפטולוגיים, והמלצות לציבור הרחב (דוגמת תעודת זהות חכמה ותשתית PKI מדינתית, שילוב זהויות ביישומים ברשת, מסחר אלקטרוני וכד')

5. נספחים

נספח 1

במעבדה לאלגוריתמים בקריפטולוגיה ובאבטחה באוניברסיטת לוקסמבורג, חברים שבעה אנשי סגל, ולצידם 16 עוזרי מחקר. ביניהם החוקרים המובילים בתחום הקריפטואנליזה ביריוקוב, קורון וחוברטוביץ'. ארבעה עוזרי מחקר נוספים עוסקים בתחום הקריפטואנליזה. במעבדה לטכנולוגיה קריפטוגרפית ואבטחת מידע באוניברסיטת Shandong, חברים שבעה אנשי סגל וחמישה חוקרים נוספים, לא כולל עוזרי מחקר וסטודנטים. גם כאן רב העיסוק בתחום הקריפטואנליזה. בין החוקרים הבולטים - Xiaoyun Wang, Meiqin Wang, Hongbo Yu.

נספח 2

להלן הערכת עלויות ראשונית ליישום תוכנית מעבדת ההסמכה (4.6 א):

מרכיב	עלות (מש"ח)	הערות
כח אדם ליבה - 3 חוקרים/יועצי אבטחה ל-5 שנים גרעין הקמה - לשנה וחצי + 3.5 שנים של פעילות	10	הקמת המעבדה והכשרת חוקריה תארך קרוב לוודאי כשנתיים. לאחר מכן, שני צוותים בני שלושה חוקרים יפעלו במשך שלוש שנים, צוותים בני שלושה חוקריםבהנחה שבדיקה לרמת סמך גבוהה תארך כשנה (כולל בדיקות חוזרות לאחר תיקונים) ניתן יהיה לבדוק 6 מוצרים. יש מקום לעודד את ההסמכה בכך שמוצרים ישראליים יוכלו לעבור הסמכה במסגרת עלויות הפרוייקט.
כוח אדם - 4 חוקרים נוספים ל - 3.5 שנים	10	
מעבדה (ציוד תקשורת, מחשוב, ציוד בדיקה וכד')	2	
הכשרת והסמכת המעבדה עצמה	3	
סה"כ	25	

להלן תכנון ראשוני לפרוייקט פיתוח מוצרי צופן לתשתיות קריטיות ומערכות ממשלתיות

מרכיב	עלות	יעד עלות למוצר	משך פיתוח / הערות
ניתוח צרכים וחלופות למימוש על ידי חברה שלא תשתתף לאחר מכן בפיתוח/אספקת המוצרים ובהובלת מצו"ב	2	-	שנה
פיתוח מצפין IP רחב סרט לתשתיות נייחות מרכזיות	7	250 אש"ח	2.5
פיתוח מצפין IP צר סרט למתקנים קטנים	5	50 אש"ח	2
פיתוח מצפין למחשבים ניידים (דיסקים) ולמדיות אחסון ניידות	3	1 אש"ח	1
פיתוח מצפין לתקשורת נתונים סלולארית למתקני תקשורת	5	10 אש"ח	2
פיתוח מצפין לתקשורת נתונים סלולארית למחשבים ניידים	7	10 אש"ח	3
סה"כ	29		

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

נספח 3

להלן מיפוי ראשוני של אבני בניין, ועלויות משוערות לפיתוחן:

	אבן בניין	פירוט	הערכת עלות (מש"ח)	משך פיתוח	הערות
1	רכיב חומרה להצפנה צבאית של תקשורת IP לקצבים של עד 100Mbps	רכיב חומרה, המתאים לשילוב בפלטפורמות בתנאי סביבה מגוונים (תעשייתי וצבאי), המטפל בכל הכרוך בהצפנת תקשורת לקצב בינוני. יכלול את מירב חבילת הצופן, כך ששילוב צופן באמצעותו ידרוש מעט מאד תוספות מסביבו.	10	2	חברה ישראלית פוטנציאלית - AltAir
2	רכיב חומרה להצפנה צבאית של תקשורת IP לקצבי 10Gbps	כנ"ל, כתשתית לפתרונות תקשורת למערכות נייחות, בתנאי סביבה אזרחיים/תעשייתיים	10	3	כנ"ל
3	מעבד מאובטח בתוך FPGA	רכיב מעבד מבוסס System on Chip בעל יכולות הגנה גבוהות - Tamper Resistance, הגנות כנגד Hacking ועוד. התוצר הוא ידע המיושם במסמכים ובקוד VHDL (מכונה בתעשייה IP Core) יאפשר גמישות רבה בשילוב תקשורתי ובשילוב במערכות חומרה.	5	2	
4	עיבוד תקשורת ב-FPGA	רכיב לעיבוד הודעות IP בקושחה בסביבת FPGA, העיבוד כולל הצפנה וקטורית, ויישום חוקת FW בסיסית	3	1	
5	רכיב FW ביטחוני בתוכנה	רכיב תוכנה המיישם FW בסיסי (חוקה לסינון תקשורת), וכן יכולות ביטחוניות ייחודיות בתחום סינון הודעות וזיהוי אנומליות בתקשורת	5	3	
6	ליבת מערכת הפעלה מאובטחת-מוכחת	ליבת מערכת הפעלה, אשר הותאמה ליכולות אבטחה מוכחות (התמודדות עם נסיונות תקיפה, הפרדת סביבות וכד'). ניתן לבסס על טכנולוגיה כגון okLinux	7	3	
7	חבילת פרוטוקולי תקשורת מוכחת	חבילת תוכנה למימוש יעיל ומוכח של פרוטוקולי תקשורת מעולם הרשתות. בביטוי מוכח הכוונה היא להוכחה לחוסן האבטחתי של חבילת התוכנה.	4	2	
		סה"כ	44		

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

1. סימולציה- רקע

1.1 מטרות

המסמך מרכז ומסכם את עבודת המטה של תת הוועדה בנושא סימולציה, במסגרת המיזם הקיברנטי. מטרת המסמך להמליץ על כיווני הפעולה המרכזיים, אשר, לדעתנו, נחוצים ומועילים במיוחד למדינת ישראל, ואשר ראוי לקדמם במסגרת המיזם הקיברנטי בתחום הסימולציה.

1.2 סימולציה ומרכזיותה

פיתוח יכולות חדשות (בכל תחום) מחייב תהליכים של בחינה, בדיקה ואימות. לא נשיק מוצר חדש לשוק, לא נפעיל אמצעי לחימה חדישים, ולא ניישם תפיסות אסטרטגיות לפני שייבחנו. העולם הקיברנטי מגוון ומורכב מכמות עצומה של טכנולוגיות ומשתמשים; מחשבים, ציוד תקשורת, מערכות הפעלה ויישומים. שלכל אחד מהם עשויה להיות תצורה (קונפיגורציה) ייחודית. בכדי לפעול בעולם הקיברנטי, בין כמגן ובין כתוקף, נחוצה סביבה שתאפשר לבחון את הפעולה המתוכננת: האם היא אפקטיבית? האם היא יעילה (Cost Effective)? כיצד עשוי להתפתח הקרב ומה יהיו השיקולים במערכה? האם הכלים הקיימים מספקים מענה?

הסימולציה היא יכולת המהווה בסיס למענה לשאלות אלה.

במושג סימולציה, כוונתנו לסביבה המאפשרת את הדברים הבאים: לדמות, באופן נאמן, את עולם הסייבר, או נתחים ממנו; לבצע מחקר אודות טכניקות הגנה ותקיפה; לערוך ניסויי כלים ולבחון את יעילותם, את הסיכונים שבהפעלתם ואת מגבלותיהם; לבדוק תפיסות הגנה אל מול תוקף, ותפיסות תקיפה אל מול גוף מגן, בכל הרמות, החל מהרמה הטקטית - כיצד מתמודד משתמש הקצה או מנהל הרשת עם לוחמת מחשבים, וכיצד לוחם המחשבים פועל בסיטואציות שונות, דרך הרמה המערכתית - כיצד מתמודדים מקבלי החלטות ברמה המערכתית (צה"ל וגופים ביטחוניים, ארגונים המופקדים על תשתיות קריטיות, וארגונים אחרים המעוניינים לבחון ולשפר את תפקודם), ועד הרמה האסטרטגית.

בנוסף, סביבה כזו מאפשרת לא רק לבחון ולאמוד את המצב, אלא גם לאמן ולתרגל את הגורמים השונים. היא עשויה לבוא לידי שימוש גם בעת אירוע לוחמת מחשבים - ניתן, לדוגמה, לחבר מחשב מותקף לסביבה המדמה את הרשת המותקפת, על מנת לבחון את משמעויות התקיפה ולקבל החלטות ביתר בהירות.

סביבה כזו מאפשרת ומניעה מחקר, פיתוח והטמעה מהירה של טכניקות, כלים ותפיסות בכלל, ובפרט קידום משמעותי של העשייה האקדמית בתחום הסייבר, התקשורת והמחשוב.

היא מביאה לפיתוח של היכולות האנושיות של העוסקים בסייבר בכל הרמות - משתמשי מערכות, גופי תפעול, גורמי מחקר ופיתוח, מנהלים, מפקדים ומנהיגים.

גם המגזר האזרחי ירוויח מבדיקה של מוצרים ותפיסות, ממחקר ומפיתוח של היכולות האנושיות - מוצרים ותפיסות שייבחנו כראוי יתאימו יותר ליעודן ויזכו ליתרון תחרותי, קידום המחקר ינביט פיתוח של מוצרים חדשים ופתרונות מקוריים, ופיתוח ההון האנושי יחזק את המגזר האזרחי בהקשרי הסייבר (לדוגמה, בכל הנוגע להתמודדות של המגזר האזרחי עם אירועי לוחמת מחשבים, והגנת ה-IP של המגזר האזרחי).

גורמים שונים בעולם זיהו את הצורך ביכולות הסימולציה, והמיזם הבולט בתחום הוא ה-Cyber Range האמריקני - פרוייקט ענק, עתיר טכנולוגיה, אשר נתפס כחלק מרכזי ויסודי במיזם הקיברנטי האמריקני, שיאפשר לארה"ב להיות הגוף היוזם ובעל השליטה בסייבר.

1.3 תיחום העבודה

המסמך ינתח את הצרכים בתחום הסימולציה, ויציע תוכנית פעולה לפיתוח המענה עבורם.

1.4 עיקרי ההמלצות

הצורך הקיים בסימולציה עבור אימון, בחינת תפיסות וכלים, מחקר אקדמי, וחקר איומים ספציפיים (כחלק מטיפול באירוע), מזוהה בעיקר על ידי מערכת הביטחון והאקדמיה. במערכת הביטחון הדבר מלווה בדרישה חד משמעית ליכולת מידור חזקה, כלומר להבטחה שיכולות הסימולציה לא תהיינה מקור להדלפת מידע.

צורך מרכזי נוסף הוא פיתוח סימולטור לטובת אימון הגורם האנושי בסייבר בתחום ההגנה (מנהלי רשת, מנהלי אבטחת מידע, משתמשי קצה וכד'). פעולה זו, לצד רגולציה שתחייב אימון, לפחות במרחב התשתיות הקריטיות, חשובה לקידום ההגנה בסייבר. תעשיות הסייבר ישתמשו בתשתיות אם יהיו כלכליות עבורן (חסכון בציוד, יצירת מיומנות גבוהה לכוח אדם וכד'), אך הן תמיד תחזקנה ביכולות בסיסיות עצמאיות. לצרכים השונים של הסימולציה יש מכנה משותף טכנולוגי - היכולת להקים סימולציה של רשתות גדולות, בהתבסס על נתונים על רשתות קיימות, היכולת להזריק מידע בסימולציה ויכולות שליטה ובקרה במרכיבי הרשת המסומלצת. על כן, בפרוייקט סימולטור ניתן לפתח את המכנה המשותף הטכנולוגי, ולהתאימו לצרכים שונים.

- פיתוח מדורג של תשתיות לסימולציה, בהובלת מערכת הביטחון (מפא"ת, מצו"ב ורא"ם) ואינטגרטור מרכזי בעל הכשר ביטחוני, ובשיתוף גורם אקדמי. בשלב הראשון תפותח יכולת ראשונית, ויגובשו דרישות ותכנון מפורט של השלבים הבאים. שלב זה יאפשר אימון של גורמי הפעלה בתחום ההגנה.
- בבסיס התשתית שתפותח מצוי ידע - שיטות, כלים וטכנולוגיה (תוכנה וחומרה) - וכן הון אנושי מהתעשייה, ממערכת הבטחון ומהאקדמיה, המסוגל ליישם אותה על מנת שתספק את השרותים הדרושים.
- התשתית תיושם במספר מופעים עבור מערכת הביטחון, האקדמיה, והתעשייה. האינטגרטור יבצע את היישום בתעשייה, ויאפשר אימון של גורמי הפעלה, על ידי רגולציה, שתחייב את גורמי התשתיות הקריטיות לקיים את האימון, וכן על ידי מערכת הביטחון.
- הפיתוח ישען באופן מירבי על טכנולוגיות מדף, ויתמקד ביכולות היחודיות הדרושות - בדגש על יכולות הניהול, השליטה והבקרה על סביבת הסימולציה ועל המתרחש בה.

הפיתוח ילווה במחקר אקדמי, שעניינו פיתוח יכולות הסימולציה העתידיות, הבנתה ומגבלותיה. להערכתנו, יישום השלב הראשון (המפורט לעיל) דורש כ-10 מש"ח. היקף התקציב כולו ייאמד במסגרת השלב הראשון. להערכתנו, 70 מש"ח על פני כ-5 שנים יאפשרו הקמת יכולות בסיסיות.

2. ממצאים עיקריים

2.1 מצב קיים – אקדמיה

כיום, אין יכולות סימולציה מרכזיות בתחום הסייבר באקדמיה הישראלית. במקרה הצורך, נעזרים בחלופות הבאות:
- יכולות סימולציה בחו"ל - בפרט יכולות אקדמיות מארה"ב.
- מפתחים יכולות סימולציה לפתרון בעיה ספציפית, לדוגמה, כדי ללמוד על מודל התפשטות של וירוס, מפתחים סימולטור המדמה רק את ההידבקות וההדבקה, בלי לכלול פרמטרים רבים נוספים.

על פי גורמים בתחום הסייבר באקדמיה הישראלית, יכולת סימולציה תקדם באופן משמעותי את המחקר האקדמי:

- מחקר פורץ דרך של טכניקות הגנה ותקיפה חדישות - יתפתח בזכות הבנה עמוקה של עולם הסייבר, כתוצאה מהתחככות בעולם הדומה לו ככל האפשר.
- מחקר שתוצריו ניתנים ליישום ברמה גבוהה - ניסויים בסביבה מהימנה יהפכו את המחקר לבר יישום (העברת הטכנולוגיה מאקדמיה לתעשיה) בסיכונים נמוכים יותר ובזמן קצר יותר מהמקובל היום.

בנוסף, יכולות הסימולציה לתחום הסייבר ישמשו למחקר בתחומים אחרים - הנדסת רשתות, הנדסת תקשורת, הנדסת מחשבים ועוד.

2.2 מצב קיים – סימולציה במערכת הביטחון

מערכת הביטחון, ובפרט צה"ל, מבססים רבים מיכולותיהם על אימון וסימולציה. עקב כך, פיתחה מערכת הביטחון, בשיתוף התעשיות הביטחוניות, יכולות סימולציה בתחומים רבים, כגון מאמנים לטכנולוגיות צבאיות רבות (טייס, שריון, שייט ועוד) וסביבות סימולציה לתרגילים מהרמה הטקטית ועד לרמה האסטרטגית

עם זאת, תחום סימולציית הסייבר במערכת הביטחון נמצא בחיתוליו. בעקבות השקעות מצומצמות ביותר, נוצרו תוצרים שגופים מעטים במערכת הביטחון משתמשים בהם לשיפור היעילות של בדיקת כלים בטכנולוגיות מוגבלות. כיום, אין כלים לתרגול ואימון של הגורמים השונים השותפים למערכה בסייבר.

העיסוק המתרחב של צה"ל בסייבר, כפי שבא לידי ביטוי בשנה האחרונה בפן הארגוני, מעורר את ההכרה בצורך ביכולות סימולציה בכל המישורים: מחקר, פיתוח ובדיקה של כלים, אימון ותרגול גורמים רבים (מפקדים ברמות זוטרות ובכירות, גורמי תפעול, ועוד) ובחינת תפיסות.

בעולם התשתיות הקריטיות, מורגש פער ביכולות הסימולציה: התפיסות ומענה ההגנה לגופים מתגבש על בסיס ניתוח איומים על הנייר, ונבחן לכל היותר בבדיקות של צוותים אדומים ובביקורות של עמידה בנהלים. כיום, אין יכולת לאמן ולתרגל את הגופים המונחים בתרגול חי ואפקטיבי, בסביבה המדמה את המערכות עצמן.

2.3 מצב קיים – תעשייה

התעשייה הביטחונית הישראלית בעלת יכולות רבות בתחום הסימולציה שאינו סייבר; הן אלה שביצעו את עיקר הפיתוח הטכנולוגי של מערכות סימולציה לשדה הקרב מהרמה האסטרטגית ועד לרמה הטקטית. כיום, התעשייה הביטחונית הישראלית מתעניינת בפיתוח יכולות סימולציה לסייבר, אך טרם החלו פרוייקטים בתחום.

תעשיות ישראליות, ותעשיות שמקורן בישראל, פיתחו ומפתחות יכולות תשתית לתחום הסימולציה: יכולות וירטואליזציה, יכולות מפוי רשתות לאומדן חולשות ופגיעויות ועוד. לתעשיית הסייבר הישראלית אין יכולות סימולציה מרכזיות בהיקף רחב. כיום, כל חברה בונה לעצמה יכולות סימולציה בהתאם לסביבה ולמוצרים שהיא מפתחת. יחד עם זאת, סביבת סימולציה לתעשיית הסייבר, שלא תסכן את הידע והטכנולוגיה של החברה, תהיה שימושית לצרכים שונים (בדגש על סימולציה לתרחישים מורכבים, בהיקפים גדולים ובתלות בטכנולוגיות מורכבות).

2.4 מצב קיים – יכולות סימולציה בעולם

גורמים שונים בעולם זיהו את הצורך ביכולות סימולציה, ויש פעילויות ומיזמים בתחום. להלן כמה מהם:

2.4.1 Cyber Range

מיזם אמריקני גדול, בהובלת DARPA, ליצירת מעבדת סייבר לאומית, שתאפשר לבחון תפיסות ומוצרים. מספר אינטגרטורים מרכזיים בתעשייה הצבאית האמריקנית מובילים את המיזם, המשלב בין עשרות טכנולוגיות של תעשיות שונות בתחומי הסימולציה, מאמנים, טכנולוגיות תקשורת ומחשוב וטכנולוגיות הגנה ותקיפה.

המיזם, שעל פי DARPA ייארך מספר עשורים, נמצא כעת בתחילת שלב היישום שלו (לאחר שלבים מקדימים של תכנון). עד כה הושקעו בו כ-$70M.

2.4.2 National Scada Testbed – ארה"ב

שיתוף פעולה בין מספר מעבדות לאומיות בארה"ב, שמטרתו לפתח את האבטחה של מערכות קריטיות (בעיקר של תחומי האנרגיה והחומ"ס).

המעבדות משתפות פעולה עם התעשייה האזרחית, שכן היא מספקת את המערכות שנבדקות במעבדות. בזכות הבדיקות במעבדה, המוצרים נהנים משיפור מתמיד. יש לציין, כי משרד ההגנה האמריקאי מאפשר לנציגי מדינות זרות להתנסות במעבדות. במאי 2010 יצאה משלחת ישראלית למעבדה באיידהו, וקיימה הכשרה ששיאה היה במשחק מלחמה בין מגן ותוקף. בסביבת המעבדה אפשר לנהל את משחק המלחמה, לאסוף מידע ונתונים אודות המגן והתוקף והתנהגותם, ולעבד אותם במהירות לצורך הפקת לקחים.

2.4.3 Northorp Cyber-Space solution center - אנגליה

סימולטור, שהוקם במקור על ידי החברה הפרטית נורת'ורפ, במטרה להכשיר עובדים לבדוק מוצרים בהקשר של אבטחת מידע. החברה עושה בו שימוש, בשיתוף אוניברסיטאות ברחבי אנגליה, כדי לבחון את מידת העמידות של רשתות מידע גדולות, בעיקר אלו שהן בגדר תשתיות קריטיות באנגליה (מים, חשמל וכד').

2.4.4 VIKING – האיחוד האירופי וארה"ב

שיתוף פעולה של מספר גופי תעשייה ואקדמיה, שמטרתו לנתח את הקושי בביצוע התקפות וירטואליות על רכיבי שליטה תעשייתיים, ולהעריך את ההשלכות של התקפות מסוג זה.

2.4.5 ETOMIC – Onelab – האיחוד האירופאי

תשתית מדידה מסיבית, שמיועדת לנתח כמות תעבורה גדולה, ולרשת 38 תחנות ניטור מסונכרנות, המנתחות תעבורה בזמן אמת ברחבי אירופה.

3. דרישות מיכולות הסימולציה

3.1 דימוי סביבות גמיש ומהימן

על הסימולטור להיות גמיש באופן מירבי, על מנת שיוכל לדמות מספר רב של סביבות שונות מאד זו מזו (הן בנפרד והן בו זמנית).

דוגמאות:

- דימוי רשתות שונות: רשתות פנימיות של גופי הביטחון, רשתות קריטיות החשופות לרשת האינטרנט כגון תהיל"ה, רשת אינטרנט בלמ"סית לחלוטין ורשתות תעשייתיות קריטיות (מערכות שליטה על תשתית). כמו כן, יש צורך בדימוי הממשקים בין הרשתות (Online\Offline).
- דימוי טכנולוגיות רשת מגוונות - רשתות קוויות, רשתות אלחוטיות, רשתות סלולאר ועוד.
- דימוי תחנות קצה שונות -אלפי צירופים של תצורות של תחנות קצה (מערכות הפעלה, כלי אבטחה, יישומים).
- דימוי התנהגות מגוונת של משתמשים.

לצורך כך, דרושה יכולת לחולל תעבורה בהיקפים עצומים, ולחולל רשתות והתנהגות של משתמשים ומערכות, וכן דרושה יכולת לדמות את הסביבות ברמות הפשטה שונות (ברמת התפיסה אסטרטגית, אנו מעוניינים להמנע מהעיסוק ברמה הטקטית).

3.2 יכולות מחקר

3.2.1 תשתית מחקר

תשתית לביצוע ניסויים רחבי היקף ומבוקרים.
לצורך תשתית המחקר, נדרשות יכולות לאיסוף מידע בהיקף עצום ובקצב מהיר מרחבי הסימולטור. השאלות כיצד לבצע את האיסוף (כלומר, איך לתעדף את נקודות איסוף המידע ואת המידע עצמו), וכיצד לנתחו על מנת שיהיה בגדר מידע שימושי, הן נושא למחקר בפני עצמן

בנוסף, נדרשות יכולות להזרקת אירועים, וליצירה מהירה של סביבת סימולציה של רשתות במבנים שונים.

כמו כן, נדרשת יכולת לחזור על ניסויים באופן מהימן (כלומר, לחזור על תהליכים מאד מורכבים, עם אותם נתונים).

3.2.2 מחקר מוצרי מדף ומערכות

נדרשת יכולת לחבר כל מוצר מדף וכל מערכת, על מנת לבדוק אותם בתרחישי לוחמת מחשבים.
העתקת נתחים מעולם הסייבר לתוך הסימולטור:
נדרשת יכולת להתחבר לעולם הסייבר, ולהעתיק נתחים מתוכו לתוך הסימולטור. לדוגמה, להקים רשת הדומה לרשת אמיתית, להתחבר למחשב אמיתי של משתמש על מנת ללמוד ממנו, ולבנות, באופן אוטומאטי, יכולת דימוי למחשב זה. נדרשת יכולת לייבא נתונים מהעולם האמיתי, ולשלב אותם כחלק מתרחישי סימולציה.

3.3 יכולות תקיפה והגנה

יכולת לדמות פעולות של מגן ושל תוקף במאפיינים שונים. להלן תיאור מנקודת מבטו של התוקף:

תוקף שחור - תוקף המגיע מחוץ לארגון, ומנסה לתקוף את הרשת המוצר ללא ידע מוקדם ובאמצעות ממשקים סטנדרטיים חשופים.
תוקף אדום - תוקף המגיע מתוך הארגון. יש צורך ביכולת לדמות מספר תוקפים אדומים, בעלי הרשאות ורמות מומחיות שונות.
תוקף פיזי - תוקף בעל גישה פיזית למתקן או למתחם המקיף אותו.
תוקף מרוחק - תוקף המנסה לנצל ממשקים חיצוניים המרוחקים מן המערכת הנבדקת.
תוקף אקטיבי - תוקף באופן אקטיבי - מבצע פעולות, מקבל משוב, ומבצע פעולות נוספות.
תוקף פסיבי - מבצע פעולות בהיקף מצומצם, ומנסה להשיג את יעדיו באמצעות עיבוד מתוחכם של מידע שאסף מהמערכות.

3.4 יכולות תפעוליות נדרשות

3.4.1 הפרדת סביבות וסניטציה

פתרון הסימולציה נועד עבור מערכת הביטחון של מדינת ישראל, התעשיות הביטחוניות, גופי האקדמיה וכן גורמי תעשייה. חשוב ליצור יכולת הפריד בין הסביבות על פי רמות סיווג ומידור, ולטהר את הסביבה לאחר ניסוי, כך שהסימולטור עצמו לא יותקף ולא ישמש כבסיס לתקיפות המשך, ונכסי המידע של המשתמשים בו יהיו מוגנים.

3.4.2 סקלביליות

יכולות הסימולציה צריכות לפעול בהיקף רחב - דימוי הסייבר כפי שנראה ממדינת ישראל, או כיצד מדינת ישראל נראית מעולם הסייבר - אך גם בהיקף קטן, המאפשר לבחון כלי או יכולת מסויימים. העלות של היכולת צריכה להתאים למימדיה.

3.4.3 יכולות פיסיות

יכולות לאחסן מידע רב.

יכולת ניטור של נקודות רבות ברשת.

שילוב בין מערכות אמיתיות לבין יכולות סימולטיביות.

3.5 יכולת שו"ב לסימולטור

3.5.1 יכולת לשנות את הסביבה בזמן אמת

על מנת לדמות מצבי אמת, צריך לשנות את הסביבה הפעילה בזמן אמת, לדוגמא: בעת תרגול של הגנה מפני אויב שחור, לדמות שהאויב השחור הופך לאויב אדום, ולדמות שינויים בתצורה ושילוב של טכנולוגיות חדשות במערכות, והטמעה של נהלים חדשים אצל המשתמשים.

3.5.2 יכולת ניהול המציאות

יכולת להזריק אירועים ולהגביל את פעילות המגן/תוקף באופן שייראה למתרגלים מהימן ומציאותי.

יכולת להאיץ זמן - לדמות בפרק זמן קצר תהליך שבמציאות מתרחש במשך זמן רב.

יכולת להפתיע את המגן ואת התוקף (לדוגמה, ליצור אירועים באופן אוטומאטי על פי מודלים הסתברותיים).

3.5.1 ניטור וניתוח

נדרשות יכולות לנטר ולנתח מידע בהיקפים עצומים:
טרום הפעלה - על מנת לגבש שיטות הפעלה יעילות לסימולטור. זמן אמת - על מנת להבין את כל המתרחש, ולאפשר לגוף המתרגל שליטה מלאה על התרגיל בזמן אמת. בדיעבד - יכולת לתחקר את מה שהתרחש בזמן הפעלת הסימולטור ובזמן שקדם לה, על מנת לנתח ולהסיק מסקנות. צריך להבטיח, ולכל הפחות להבין, את ההשפעה של המדידה על הניסויים.

3.6 תפיסת המענה

- פיתוח מדורג של תשתיות לסימולציה, בהובלת מערכת הביטחון (מפא"ת בשיתוף מצו"ב ורא"ם) ואינטגרטור מרכזי בעל הכשר ביטחוני, ובשיתוף גורם אקדמי (כצרכן מייצג).
- הפיתוח ישען, באופן מירבי, על טכנולוגיות מדף, ויתמקד ביכולות הייחודיות הדרושות - בעיקר על יכולות הניהול, השליטה והבקרה על סביבת הסימולציה ועל המתרחש בה.

- הפיתוח ילווה במחקר אקדמי, שיעסוק בפיתוח ובהעמקת ההבנה ביכולות הסימולציה העתידיות ובמגבלותיהן.
- התשתית שתפותח היא במהותה ידע, כלומר שיטות, כלים, טכנולוגיה (תוכנה וחומרה), והון אנושי בתעשייה, במערכת הביטחון ובאקדמיה, המסוגל ליישם אותה, על מנת שתספק את השירותים הדרושים.
- יישום התשתית במספר מופעים:
  - סביבת סימולציה שתשרת את מחקר הסייבר באקדמיה הישראלית - תשתית שעיקרה היכולת לדמות סביבות (רחבות היקף, גנריות), והיכולת לבצע בהן ניסויים ומדידות באופן מהימן.
  - סביבת סימולציה שתשרת את התעשייה הישראלית - שרות שהאינטגרטור יספק לתעשייה הישראלית בתחום הסייבר. בסמכות רא"ם לקבוע רגולציה לאימון גורמי הגנה בתשתיות קריטיות, שתיצור ביקוש בסיסי, ותשרת גם אימון גורמי הגנה במערכת הביטחון.
  - מספר סביבות סימולציה ביטחוניות - סביבות מחקר ממודרות, וסביבת אימונים ותרגול מרכזית, אשר במסגרתן תיבחן גם אפשרות להקים יכולת דומה במעבדות סמל"א, שהן מרכז של מספר מעבדות לאומיות, אשר בשילוב עם מעבדת סייבר יוכלו לספק שלם הגדול מסך חלקיו.

3.7 תכנית פיתוח לתשתיות סימולציה

הפעילות	עלות משוערת (מש"ח)	הערות

פיתוח תכנית פעולה מפורטת:
• גיבוש דרישות מפורטות ואפיון ראשוני
• מיפוי טכנולוגיות ותשתיות קיימות בשוק האזרחי ובמדינת ישראל
• פיתוח דגם להתנסות ולהעמקת ההבנה הטכנולוגית, הביטחונית, התפעולית והניהולית.
  • הדגם יאפשר אימון טקטי ברמות נמוכות ומחקר בסיסי.
  • הדגם ישולב במעבדה אחת באקדמיה הישראלית ובסביבה ביטחונית אחת.
סיכום תוכנית פעולה רב שנתית למחקר ולפיתוח.
הפעילות תבוצע בהובלת מערכת הביטחון, בשיתוף גורמים מהאקדמיה הישראלית ו- 2-3 אינטגרטורים מרכזיים, ותלווה בבניית שיתוף פעולה עם DARPA.
	10	פעילות במשך כשנתיים, בהיקף כולל של כ-15 שנות אדם

פיתוח שלב א' - יכולת סימולציה בסיסית בטכנולוגיות IT סטנדרטיות • פיתוח יכולת אימון ומשחקי מלחמה למערכת הביטחון • פיתוח יכולת מחקר לרשתות מגוונות בהיקף רחב לאקדמיה • ביצוע מחקר ליכולות הסימולציה העתידיות		
פיתוח שלב ב'- הרחבת יכולות סימולציה לטכנולוגיות נוספות, חיבור מערכות אמת לסימולטור		
פיתוח שלב ג' - הרחבת יכולת הסימולציה לרמה הלאומית		

בשלב הנוכחי, קשה לאמוד את היקף התקציב הדרוש לפיתוח יכולות סימולציה מלאות. אנו ממליצים על תקציב של כ-70 מש״ח במשך כ-5 שנים, שלהערכתנו יאפשר פיתוח יכולות סימולציה בסיסיות (הערכה מדויקת תיקבע לאחר ביצוע השלב הראשון דלעיל).

3.8 נושאי מחקר הנוגעים ליכולות סימולציה

- מה בין סימולציה למציאות - כיצד לבצע סימולציה, וכיצד נדע את מגבלותיה
- אבטחת מערכות סימולציה
- כיצד אוספים ומנתחים בזמן אמת, או שלא בזמן אמת, מידע בהיקף עצום, בהקשר לבעיות הנוגעות לסייבר.
- פתרונות סניטיזציה בסימולטור - איך ״לטהר״ את הסימולטור לאחר פעילות של גורם ממודר, ולאפשר לגורם אחר, בלתי ממודר, להשתמש בפלטפורמה מבלי להחשף למידע רגיש (ביטחוני או עסקי).

דו"ח תת ועדת חישוב-על ותשתיות תקשורת רחבות פס

1. תקציר מנהלים

במהלך 30 השנים האחרונות, חישוב עתיר ביצועים (HPC), הידוע גם בשמות חישוב-מדעי (Scientific Computing) וחישוב-על (Supercomputing) תרם תרומה מכרעת לקהילות המדעיות והמסחריות, לחוסנן הלאומי של מדינות ולאיכות חיי האדם. מידול וסימולציה המבוססים על חישוב עתיר ביצועים ביססו את עצמם כענף השלישי של החקר המדעי, ומשלימים את ענפי התיאוריה והניסויים המעבדתיים על מנת לספק ספקטרום רחב ומקיף של כלי עבודה לחוקר. החדירה של פתרונות חישוב-על לחיי היומיום שלנו גבוהה מכפי שניתן לשער - החל מתכנון ופיתוח של כלי הרכב שאנו נוסעים בהם, דרך איתור שדות הנפט והגז אשר מניעים את כלי הרכב הללו, עבור בפיתוח של תרופות מצילות חיים וחיזוי מזג האוויר, ועד להגנה היומיומית על חיינו מפני איומים שונים במימד הפיזי ובמימד הקיברנטי.

חשיבות התחום ומרכזיותו בכלכלה ובחוסן הלאומי מובילות מדינות רבות לגבש מדיניות ואסטרטגיה ולהפעיל תוכניות עתירות משאבים במטרה לקדם את יכולותיהן, ביניהן ארה"ב, (המשקיעה למעלה מ-100 מיליארד דולר לשנה בתחום, ואימצה לאחרונה אסטרטגיה על בסיס דו"ח של יועצי הנשיא לנושא מידע וטכנולוגיה לקידום חישוב-על), האיחוד האירופי (אשר זיהה פער בתחום ומתחיל במימוש אסטרטגיה חדשה להובלה עולמית בתחום עד 2020) וסין (אשר משקיעה משאבים אדירים בהקמת מרכזי המחשוב החזקים בעולם).

בנובמבר 2010, במסגרת "המיזם הקיברנטי" הוחלט גם במדינת ישראל להקים ועדה אשר תבחן את הפערים בארץ בתחום חישוב-על ותשתיות התקשורת רחבות הפס הדרושות לכך, ותמליץ על תוכנית פעולה לקידום הנושא. לראשות הוועדה מונה תא"ל (מיל.) יעקב נגל, הסגן המדעי לראש מפא"ת. הוועדה, אשר כללה נציגים ומומחי תוכן בתחום חישוב-על משלושת המגזרים הרלוונטים (תעשייה, ביטחון ואקדמיה), למדה לעומק את המגמות העולמיות בתחום ואת הפערים של מדינת ישראל, בחנה חלופות שונות לפתרון ולבסוף גיבשה המלצה לתוכנית פעולה.

מתוך עבודת הוועדה עולה כי במדינת ישראל קיימים מספר "איים" של עיסוק בחישוב-על. איים אלה, הנמצאים במערכת הביטחון, באקדמיה ובתעשיות, עובדים כמעט בכל המקרים באופן עצמאי, ועל כן לא נוצרת סינרגיה ביניהם. העדר הסינרגיה גורם לקושי ביכולת של כל אחד מהצרכנים להתמודד עם אתגרי חישוב-העל שלו. מהמחקר עולה, כי לכל הגופים אתגר משמעותי משותף והוא פערי ידע בתחומים המתקדמים של חישוב-על וקושי באיתור, הכשרה והעסקה של אנשי מקצוע מובילים בתחום. עוד עולה מהמחקר כי ציוד חישוב-על הוא בחלק מהמקרים פער, אך תמיד משני בחשיבותו ובקדימותו לפערי הידע והמומחיות.

לאור הממצאים, הוועדה מצאה לנכון להמליץ על הקמת מרכז לאומי לחישוב-על, כחלק ממוסד אקדמי, שייעודו העיקרי יהיה הובלת המחקר והפיתוח בתחום חישוב-על וחישוב עתיר ביצועים בארץ. מרכז זה יעסוק בביצוע מחקרים אקדמיים, בתכנון ומימוש של פרוייקטי מו"פ, בהוראה והכשרה של אנשי מקצוע וחוקרים ובייעוץ והכוונה למשתמשים. תוכנית העבודה והמחקר במרכז זה תבנה במשותף עם הצרכנים המרכזיים (ביטחון ותעשייה) ונציגים מתאימים מגופים אלו יהיו חברים מלאים בגוף המנהל, וכן יהיו חלק בלתי נפרד מגופי המחקר. על מנת לעמוד ביעדים אלה, תעמוד לרשות המרכז מעבדה ובה מערכות חישוב המתאימות למחקר ברמה עולמית.

להערכת הוועדה, לצורך מימוש המלצותיה, ניתן לבנות את המרכז הלאומי בשלושה שלבים, אשר לכל אחד מהם ידרשו ההשקעות הבאות (הערכה ראשונית):

השלב	השקעה נדרשת שנתית (בממוצע)
שלב ההקמה	34 מיליון ₪
שלב הגיבוש	33 מיליון ₪
השלב היציב	44 מיליון ₪

על מנת לאפשר קבלת תוצרים בטווח הקצר ובטווח הביניים, הוועדה ממליצה לבחון את האפשרות שהצרכנים המרכזיים יתוגברו בכוח אדם מתאים אשר חלקו יופנה לפעילות המרכז. הוועדה מדגישה את הצורך בהסתכלות מערכתית, ארוכת טווח ומשולבת, וממליצה שההשקעות בשלב היציב תהיינה רציפות לאורך שנים ארוכות. החלטה על פתרון בשיטת "זבנג וגמרנו" אינה נכונה ואינה מתאימה למאמץ מסוג זה, ועדיף שלא לקבלה.

2. מטרת המסמך ומבנהו

מטרת מסמך זה היא לסכם את עבודת תת ועדת חישוב-על ותשתיות תקשורת רחבת פס במסגרת "המיזם הקיברנטי". הוועדה קיבלה כמנדט לבחון את צרכי מדינת ישראל בתחום חישוב-העל ותשתיות תקשורת רחבת פס הנדרשות לחישוב-על, ולהמליץ על תוכנית פעולה בנושא.

במהלך החודשים האחרונים בוצע תהליך למידה, ניתוח צרכים, בחינת חלופות, ולבסוף גיבוש המלצה לפתרון. עיקרי הדברים מסוכמים במסמך זה.

במסמך מופיע מבוא מקוצר לעולם חישוב-העל ופירוט קצר של המרכיבים השונים במערכת חישוב עתירת ביצועים. לאחר מכן, מוצגת סקירה של תמונת המצב הנוכחית בתחום חישוב-על בעולם ובארץ, וכמו כן הפערים של מדינת ישראל בתחום החישוב-על ותשתיות תקשורת רחבות פס כפי שנותחו בעבודה הצוות. לסיום, מובאת הצעה אפשרית, כולל התייחסות למרכיביו השונים.

3. תהליך העבודה ומתודולוגיית הניתוח

ביציאה לדרך, גיבשה הוועדה תוכנית פעולה המורכבת ממספר שלבים הנבנים זה על גבי זה. על בסיס תוכנית פעולה זו קיימה הוועדה דיונים שבועיים של הועדה, לעיתים בהרכב פנימי ולעיתים עם אורחים מן החוץ. שלבי העבודה היו:

1. יישור קו מקצועי: יצירת שפה מקצועית אחת משותפת בין כל אנשי הוועדה בתחומי העיסוק הרלוונטים.
2. היכרות עם השוק: סקירה של מגמות מרכזיות בשוק החישוב-על והתקשורת רחבת הפס, כולל מפגשים עם נציגי חברות עולמיות וישראליות.
3. תוכניות ומגמות בעולם: סקירה של תוכניות ומגמות עולמיות בתחומי חישוב-העל.
4. תמונת מצב ופערים: במהלך שלב זה התבצעה סקירה רחבה של תמונת המצב בארץ בתחומי חישוב-על ותשתיות תקשורת (אקדמיה, תעשייה וביטחון) ואותרו הפערים המרכזיים בתחום.
5. בחינת חלופות לצמצום הפערים: בחינת חלופות שונות לפעולה.
6. בחירת חלופה מועדפת.
7. ניתוח החלופה: בשלב מסכם זה בוצע ניתוח מעמיק של יתרונות וחסרונות, עלויות, סיכונים והזדמנויות בחלופה המוצעת.

4. רקע מקצועי

4.1 עולם הבעיה

במהלך 30 השנים האחרונות, חישוב עתיר ביצועים (HPC), הידוע גם בשמות חישוב-מדעי (Scientific Computing) וחישוב-על (Supercomputing [1]) תרם תרומה מכרעת לקהילות המדעיות והמסחריות, לחוסנן הלאומי של מדינות ולאיכות חיי האדם. מידול וסימולציה המבוססים על חישוב עתיר ביצועים ביססו עצמם כענף השלישי של החקר המדעי, ומשלימים את ענפי התיאוריה והניסויים המעבדתיים על מנת לספק ספקטרום רחב ומקיף של כלי עבודה לחוקר. יחד עם זאת, לא אנשים רבים מודעים לעומק החדירה של פתרונות חישוב מסוג זה לחיי היום יום.

עד כמה אנשים מודעים לכך כי חישוב עתיר ביצועים מהווה חלק אינטגראלי מתכנון ופיתוח כלי הרכב שהם נוסעים בהם והמטוסים שהם טסים בהם? באיתור שדות הנפט והגז אשר מניעים את כלי הרכב הללו ומספקים חשמל לבתיהם? בפיתוח של תרופות מצילות חיים חדשות? בחיזוי מזג האוויר עליו הם מתבססים לתכנון חייהם? ובהגנה היום יומית על חייהם מפני איומים שונים ומשונים במימד הפיזי ובמימד הקיברנטי?

יכולות חישוב כאלו ואחרות הפכו לחשובות ביותר לא רק עבור טובת הפרט, אלא אף לטובת הכלל - היכולת של חברה מודרנית להתחרות בשוק הגלובלי מושפעת מאוד מהיכולת של החברה להציב ולהשתמש בפתרונות חישוב עתיר ביצועים. ניתן למצוא לכך עדויות רבות, אשר חלקן הגדול מפורט בדו"ח [2]אשר פורסם ע"י חברת המחקר IDC תחת הכותרת "A Strategic Agenda for European Leadership in Supercomputing" ובהן:

- הישענות הולכת וגוברת של חתני פרס נובל על יכולות חישוב עתיר ביצועים במחקריהם.
- 97% מהחברות התעשייתיות הגדולות אשר אימצו טכנולוגיות חישוב עתיר ביצועים מחשיבות אותו כחלק בלתי נפרד מהיכולות שלהן להמציא, להתחרות ולשרוד.
- השקעות חסרות תקדים ביפן, סין, ארה"ב ורוסיה בתוכניות להעצמת היכולות החישוביות, וכל זאת בעת משבר כלכלי עולמי.

חשוב לציין כי יכולות חישוב עתיר ביצועים הן יכולות חישוב רב-ממדיות, כאשר ממדי הפתרון מותאמים לבעיה הספציפית אשר יש לפתור. כעת, נפרט את הממדים העיקריים השונים.

4.2 עיבוד

האטום הבסיסי ביותר בכל פתרון חישובי הוא המעבד. מדובר ברכיב האלקטרוני אשר מבצע את הפעולות החישוביות עצמן. רכיבי העיבוד השונים נמדדים במספר הפעולות אשר הם מבצעים בשנייה בודדת, כאשר בדרך כלל יש הבדלה בין מספר פעולות לשנייה על מספרים שבורים (FLOPS[3]) ומספר הפעולות לשנייה על מספרים שלמים (MIPS[4]). ישנם מספר סוגים של רכיבי עיבוד, כאשר לכל אחד יתרונות וחסרונות שונים.

מעבד כללי

יחידת העיבוד המרכזית (CPU) במחשבים הביתיים וברוב השרתים היא יחידת עיבוד כללית המסוגלת לבצע שלל פעולות (בימים אלו בד"כ מדובר ביחידה ממשפחת x86 של חברת Intel או של חברת AMD). החוזק של יחידת עיבוד זו הוא בכלליות שלה, כאשר חוזק זה מהווה גם את נקודת התורפה העיקרית של היחידה. מאחר ומדובר ביחידת עיבוד כללית, במקרים רבים משאבים רבים מתבזבזים לשווא ולכן המעבד פחות יעיל לכל שימוש ספציפי. יחד עם זאת, הכלליות מאפשרת שימוש קל ונוח, יחסית לכל פתרון עיבוד אחר.

1 לאורך העבודה ייעשה שימוש במונח "חישוב-על" במובן ברחב, קרי במובן הכולל את המובנים של המונחים האחרים המצוינים, למעט אם יצוין במפורש אחרת.
2 http://www.hpcuserforum.com/EU/downloads/SR03S10.15.2010.pdf
3 FLoating point OPerations per Second – נמדד כיום בד"כ ב GigaFLOPS, TeraFLOPS ו PetaFLOPS. רלוונטי לדוגמה לסימולציות מדעיות, עיבוד אות דיגיטאלי, תנועת רובוטים ועוד.
4 Million Instructions Per Second - רלוונטי לדוגמה לעיבוד שפה טבעית, בסיסי נתונים, הרצת מערכות וירטואליות ושימושים ביטחוניים שונים.

המעבדים הכלליים בד"כ (בהכללה גסה) מבצעים בכל יחידת זמן פעולה יחידה, ולכן הם זכו גם לכינוי "מעבדים סקאלרים". יחד עם זאת, בשנים האחרונות אנו עדים למעבדים מדור חדש - מעבדים כלליים מרובי ליבה (-Multi core processors), כאשר למעשה מדובר במספר מעבדים בלתי תלויים הארוזים ונמכרים יחדיו. על מנת לנצל כיאות מעבדים אלו, יש לפתח טכניקות של תכנות מקבילי.

מעבד מקבילי

מעבד מקבילי הוא מעבד המבצע בכל נקודת זמן מספר רב של פעולות במקביל.ישנם סוגים שונים של מקביליות, לדוגמה מעבדי SIMD[5] ומעבדי MIMD[6].

מעבד שכזה מורכב ממספר (יכול להיות רב) של ליבות חישוב, עם יחסי גומלין אפשריים בין הליבות הללו. בד"כ כל ליבה שכזאת לחוד היא ליבה חלשה יחסית, אך היתרון הוא במספר הרב של הליבות. המעבד המקבילי הנפוץ ביותר כיום הוא רכיב העיבוד הגרפי (GPU) המצוי כמעט בכל מחשב ביתי. רכיב זה התחיל כרכיב עיבוד ייעודי, אך הפך בשנים האחרונות למעבד מקבילי חזק ביותר (לעיתים בן מאות ליבות חישוב). שתי חברות עיקריות מייצרות כיום רכיבי עיבוד גרפי - חברת Nvidia האמריקאית וחברת AMD האמריקאית גם כן. ישנם מעבדים מקבילים נוספים כדוגמת מעבדים מתוצרת חברת Tiler[7], מעבדי הוכחת התכנות מתוצרת חברת Intel[8] ועוד.

רכיבי עיבוד ייעודיים

במקרים רבים, כאשר אנו נדרשים לבצע פעולות חישוב מסוג מסוים, יש הגיון רב בתכנון וייצור מעבד ייעודי לטובת אוסף מצומצם של פעולות. דוגמה למעבד שכזה הוא מעבד DSP) Digital Signal Processing) המתוכנן באופן אופטימאלי לביצוע פעולות הנדרשות לטובת עיבוד אות דיגיטאלי (לדוגמה - התחשבות בתכנון הארכיטקטורה של המעבד לטובת יעילות ביצוע פעולות כגון FFT[9] וקונבולוציה). למעשה, ניתן לקחת גישה זו עד לקצה, ובמידת הצורך לייצר מעבד ייעודי (למשל באמצעות טכנולוגיית ASIC[10]) המיועד ספציפית לפתרון בעיה מסוימת. בעוד שגישה זו תספק ככל הנראה את הפתרון היעיל ביותר מבחינת ביצועים, עלות הפיתוח ועלות הייצור של מעבדים מסוג זה גבוהה מאוד.

רכיבי עיבוד מתכנתים

רכיב עיבוד מתכנת (FPGA[11]) הוא מעגל חשמלי המאפשר למהנדס לשנות את התצורה שלו לאחר ייצורו ולממש באמצעותו אלגוריתמים כרצונו. למעשה, ניתן לחשוב באופן אבסטרקטי על רכיב שכזה כעל דף שרטוט ריק אשר מהנדס החשמל מצייר עליו את המעגלים החשמליים אשר הוא מעוניין לממש. רכיבים אלו מהווים פשרה נוחה בין רכיבי עיבוד ייעודים (לדוגמה בטכנולוגיית ASIC) לבין מעבדים כלליים או מעבדים מקבילים, שכן הם מספקים ביצועים טובים, מבלי לשלם את העלויות הכבדות של פיתוח ASIC. כיום בעולם קיימות שתי חברות עיקריות המייצרות רכיבי FPGA - חברת Xilinx וחברת Altera (שתיהן חברות אמריקאיות).

4.3 תקשורת פנימית

ברוב המקרים לא ניתן להכיל את הבעיה החישובית אשר אנו מנסים לפתור ברכיב חישוב יחיד (גם אם מדובר ברכיב מקבילי). כאשר הבעיה החישובית מתחלקת על פני מספר רב של רכיבי עיבוד, ישנם מקרים רבים בהם יש צורך לתקשורת בין הרכיבים הללו, על מנת שהרכיבים השונים יוכלו לעבוד יחדיו באופן סינכרוני לטובת פתרון הבעיה.

5 Single Instruction Multiple Data – מעבד מקבילי המבצע פעולת חישוב אחת על הרבה מידע באופן מקבילי. כלומר מעבד זה מנצל מקביליות ברמת המידע.
6 Multiple Instruction Multiple Data – מעבד מקבילי המבצע מספר פעולות חישוב שונות על מידע שונה באופן מקבילי. כלומר בכל נקודת זמן כל רכיב חישוב במעבד יכול לבצע פעולה אחרת במקביל לאחרים.
7 http://www.tilera.com
8 techresearch.intel.com/ProjectDetails.aspx – תיאור מעבד ניסיוני של חברת Intel המכיל 48 ליבות חישוב
9 Fast Fourier Transform - פעולה נפוצה ביותר בתחום עיבוד האות
10 Application specific Integrated Circuit - מעגל מודפס המיועד לצורך ספציפי ולא לטובת שימוש כללי. לדוגמה, שבב המיועד לבצע תקשורת סלולארית במכשיר נייד.
11 Field Programmable Gate Array

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

מעניין לציין, כי ניתן לסווג בעיות חישוביות לפי מידת התקשורת אשר נדרשת בהן - מבעיות אשר לא דורשות תקשורת כמעט כלל (Embarrassingly Parallel problems) בהן ניתן לחלק בעיה לאוסף של תתי בעיות בלתי תלויות, ועד לבעיות אשר דורשות תקשורת רבה מאוד (Communication-intensive problems). למרבה הצער, מרבית הבעיות החשובות והקשות נוטות להיות בעיות אשר דורשות תקשורת רבה.

לכן, רוב פתרונות המחשוב עתיר הביצועים מכילים רשתות תקשורת מהירות ביותר (Interconnect). הביצועים של רשתות התקשורת הנ"ל נמדדים בכלליות בשני פרמטרים: השיהוי של הרשת (latency) אשר מודד את פרק הזמן בו לוקח להעביר הודעה בודדת מנקודה לנקודה והספיקה (throughput) של המערכת אשר מודדת את כמות המידע אשר ניתן להעביר ברשת בשנייה ממוצע לאורך הזמן. בעבר היו מימושים שונים של רשתות תקשורת מהירות לטובת חישוב עתיר ביצועים (לדוגמה מייצור החברות Myricom, Quadrics ועוד), אך כיום ניתן לסווג את רשתות התקשורת המהירה לטובת חישוב עתיר ביצועים למספר מצומצם של סוגים.

תקשורת מבוססת Infiniband

Infiniband הוא סטנדרט תקשורת ייעודי המיועד לתקשורת בפתרונות חישוב עתיר ביצועים ופתרונות חישוביים אחרים מבוססי שרתים. הסטנדרט מאפשר הגעה לקצבי תקשורת גבוהים עם שיהוי נמוך. בעולם מספר מצומצם של חברות המובילות את שוק ה-Infiniband, כאשר החברה המובילה היא חברת Mellanox הישראלית. פתרונות חישוב עתיר ביצועים המשתמשים ב-Infiniband מהווים כיום 42.60% מכלל הפתרונות המופיעים ברשימת ה [12]Top 500 Supercomputing Sites.

תקשורת מבוססת Ethernet

Ethernet היא משפחה של טכנולוגיות רשתות לרשתות מקומיות, בקצבים שונים. כיום ניתן להשיג פתרונות תקשורת מבוססי Ethernet ב-Throughput של 1gbit/sec ו- 10gbit/sec, ובעתיד הקרוב גם בקצבים של 40gbit/sec ואף 100gbit/sec. יחד עם זאת, השיהוי בטכנולוגיה זאת הוא יחסית גבוה ולא ניתן להגיע בה לביצועים גבוהים ביותר. כמו כן, יכולת הגידול של טכנולוגיה זאת לקישור של מספר רב מאוד של רכיבי עיבוד בעייתי גם כן. למרות זאת, טכנולוגיה זו מהווה כיום חלק נרחב מהמערכות ברשימת ה-Top 500, ונכון לכתיבת שורות אלו 45.60% מהמערכות ברשימה משתמשות בתקשורת Gigabit Ethernet.

תקשורת קניינית (Proprietary)

במספר מצומצם של מקרים, ניתן לראות שימוש בפתרונות תקשורת ייחודיים אשר פותחו ויוצרו במיוחד עבור פתרון חישובי ספציפי. ניתן לראות פתרונות כאלו במחשבי-על מתוצרת החברות Cray, SGI וחלק מהמחשבים מתוצרת חברת IBM, כמו גם במספר מצומצם מאוד של מחשבים נוספים. בד"כ פתרונות אלו מתאפיינים בביצועים גבוהים מאוד, אך בעלות גבוהה גם כן.

4.4 תקשורת חיצונית

במידה והמשתמש של משאבי חישוב-על נמצא קרוב אליו (באותה רשת פנימית, לדוגמא באותו מתקן או באותו קמפוס), תקשורת פנימית מספיקה לצורך שימוש במחשב. אך בהרבה מקרים, משתמשי חישוב-על מבקשים להשתמש במשאבים מרוחקים, או מפני שאין בקרבתם מחשב על גדול דיו או על מנת ביצוע אגרגציה לצורך עבודה עם שותפים רחוקים.

במקרים כאלה, במידה והבעיה החישובית מכילה מידע רב, נדרשת תקשורת רחבת פס (Broadband access) החוצה, לרשתות של משתמשים. בשונה מתקשורת פנימית, המדד הרלוונטי לבחינה הוא ספיקה (ולא שיהוי). בפרסום משנת [13]2010, הנציבות הפדרלית לתקשורת (Federal Communications Commissions – FCC) מגדירה תקשורת רחבת פס כ-4Mbps להורדה, ו-1 Mbps להעלאה (Mbps - מיליון ביטים לשנייה - ולא 220 ביטים).

[12] רשימה המכילה את 500 פתרונות החישוב עתירי הביצועים (הגלויים) המהירים בעולם. ניתן להתרשם מהרשימה ב www.top500.org
[13] www.fcc.gov/Daily_Releases/Daily_Business/2010/db0720/FCC-10-129A1.pdf

4.5 זיכרון

בעיות רבות דורשות את הצורך לגשת לזיכרון רב במהירות רבה ביותר. זיכרון בפתרונות מחשוב מתחלק בד"כ לזיכרון ראשי (זיכרון נדיף ומהיר, בד"כ זיכרון RAM) ולזיכרון משני (זיכרון בלתי נדיף ואיטי יותר, בד"כ מבוסס מדיה מגנטית או Flash). בסעיף זה נתרכז בזיכרון הראשי, בעוד ובסעיף הבא נדון בזיכרון המשני.
במקרים שבהם צריך לגשת במהירות רבה מאוד (הן מבחינת שיהוי והן ומבחינת ספיקה לכמויות מידע גדולות, עולה הצורך בגישה לזיכרון גדול) דוגמה לבעיה שכזו היא פעולת עיבוד על פני גרפים גדולים, לדוגמה על מנת לנתח התקשרויות בין גורמים רבים. בפעולות מסוג זה יש צורך בטיול אקראי על פני הגרף, כאשר הגרף יכול להיות גדול מאוד.

מאחר ובדרך כלל אנו מדברים על פתרונות המכילים מספר רב של מעבדים, גישה זו צריכה להתבצע משלל המעבדים במקביל. כיום קיימים פתרונות המאפשרים לאכלס מספר רב של מעבדים במכונה יחידה עם מרחב זיכרון גדול אחיד משותף (פתרונות כאלו מכונים Single System Image או Symmetric Multi-Processing), כמו גם פתרונות אשר מבזרים את הזיכרון על פני מרחבי זיכרון עצמאיים, ומאפשרים גישה לזיכרון מרוחק מעל פתרון תקשורת מהירה. בעוד שפתרונות מהסוג השני ניתן למצוא באופן נרחב יחסית (או לדמות זיכרון משותף באמצעות תקשורת מהירה), הרי שפתרונות מהסוג הראשון (אשר קלים בהרבה לתכנות ולשימוש) נחשבים ליחסית אקזוטיים ויקרים. פתרונות מהסוג הראשון (SMP) כיום מוגבלים אך ורק למוצרים של חברות המתמחות בכך (לדוגמה חברת Cray, חברת SGI וחברת IBM) והם יקרים באופן משמעותי מהפתרונות מהסוג השני.

4.6 אחסון עתיר ביצועים

כפי שצוין בסעיף הקודם, במקרים רבים יש צורך בגישה לכמות גדולה מאוד של נתונים. במקרים שבהם כמות הנתונים גדולה מאד, לא ניתן לאחסן אותה בפתרונות נדיפים, ויש חובה לאחסנה בטכנולוגיות אחרות כדוגמת דיסקים מגנטיים. לפתרונות אחסון משני יש מספר חסרונות בולטים, כאשר העיקרי שבהם הוא בעיית ביצועים אינהרנטית (הנובעת מכך שפתרונות אחסון משני בד"כ מבוססים על מדיה מגנטית המכילה בתוכה גם רכיבים מכניים). בשנים האחרונות נולדו מספר רב של פתרונות אחסון עתירי ביצועים, המאפשרים גישה לכמויות עצומות של מידע (PetaBytes) ממספר רב מאוד של מעבדים במקביל. פתרונות אלו מורכבים בדרך כלל ממערכת קבצים ייחודית המיועדת לאחסון עתיר ביצועים, מאריזות חומרה ייעודיות למארזי הדיסקים ומחיבור תקשורת מהיר לרשת התקשורת המהירה של פתרון החישוב עתיר הביצועים. בעיות לדוגמה הדורשות גישה לכמות גדולה מאוד של מידע הן בעיות מעולם עיבוד הוידיאו, בעיות הדורשות עיבוד של מידע רב מאוד הנמצא ברשת האינטרנט, ספריות דיגיטאליות ועוד.

כיום ישנן בעולם מספר חברות המתמחות באחסון עתיר ביצועים, לדוגמה חברת Data Direct Networks האמריקאית הנפוצה ביותר במכונות חישוב בעלות ביצועים גבוהים במיוחד (15 מתוך 20 המחשבים הראשונים ברשימת ה-Top 500 מכילים פתרונות אחסון עתיר ביצועים של חברת Data Direct Networks), וחברת Panasas האמריקאית.

4.7 תוכנה

בעוד שחומרה מתקדמת בממדים הקודמים הכרחית על מנת לפתור את הבעיות החישוביות הרלוונטיות, לא ניתן לעשות זאת ללא הכלים המתאימים לפיתוח תוכנה ולניהול סביבת הריצה של הפתרון החישובי. כלים אלו מכילים חבילות תוכנה יעילות המאפשרות לנצל באופן יעיל את רכיבי העיבוד השונים וספריות תוכנה לביצוע תקשורת מהירה (כדוגמת מימוש יעיל של הסטנדרט MPI[14] לטובת תקשורת ברשתות מהירות).

[14] Message Passing Interface - סטנדרט תקשורת להעברת הודעות ברשתות תקשורת מהירות. נפוץ במיוחד בעולם החישוב עתיר הביצועים. כל יצרן של רשת תקשורת מהירה בד"כ מספק מימוש משלו של הסטנדרט אשר מספק ביצועים מיטביים עבור החומרה הרלוונטית.

כמו כן, מדובר בכלים לבדיקות, אבחון ביצועים וניפוי שגיאות בסביבות החישוביות המורכבות הנ"ל. לאחר שנכתבה תוכנית עובדת, יש צורך לנהל סביבת הרצה ולהקצות משאבים מתאימים לתוכניות המתאימות. פעולות אלו מתבצעות בד"כ ע"י כלים מסחריים להקצאת ותזמון משאבים (Resource Scheduling and Allocation). יש לציין כי בעולם של מעבדים מקבילים מורכבים, חשיבות כלי התוכנה וסביבות הפיתוח הולכת וגוברת, שכן היכולת לנצל באופן טריוויאלי את רכיבי העיבוד הולכת ופוחתת.

4.8 ארכיטקטורה

פתרונות חישוב-על מגיעים כיום במספר ארכיטקטורות שונות, כל אחת עם היתרונות והחסרונות שלה.

צביר חישוב (Compute Cluster)

הארכיטקטורה הנפוצה ביותר של פתרונות חישוב עתיר ביצועים בעולם (מהווה 82.80% מהמחשבים ברשימת ה Top500). בארכיטקטורה זו הפתרון מבוסס על אוסף גדול של שרתים סטנדרטיים (עם רכיבי עיבוד מכל סוג) המחוברים ביניהם באמצעות רשת תקשורת מהירה. בחלק גדול מהמקרים השרתים הללו מחוברים גם לפתרון אחסון עתיר ביצועים. כל אחד מהשרתים הללו יכול לתפקד באופן עצמאי, אך החוזק האמיתי של הפתרון החישובי מתקבל באמצעות כתיבת תוכנה המנצלת את כל רכיבי העיבוד במקביל, תוך כדי העברת מסרי תקשורת בין הרכיבים השונים. כמו כן, כמובן שיש צורך ברכיבי תוכנה המנהלים את המערכת כולה. יצרניות בולטות של צבירי חישוב הן החברות האמריקאיות HP ו-IBM אשר יחדיו מחזיקות בכ-70% משוק צבירי החישוב עתירי הביצועים.

4.9 Massive Parallel Processing (MPP)

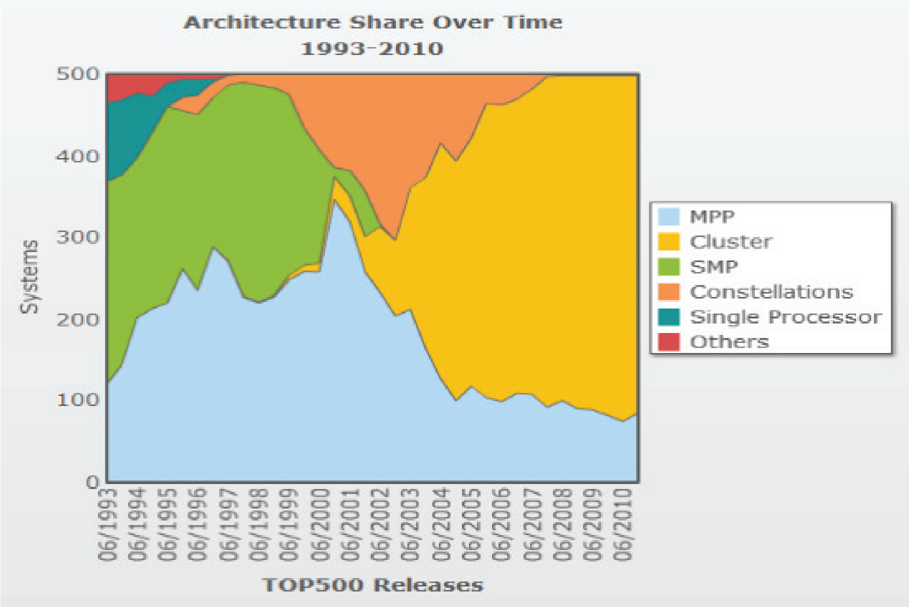
ארכיטקטורה זו דומה לצבירי חישוב, רק שבה רכיבי התקשורת ורכיבי העיבוד מודעים אחד לשני באופן אינטימי ולעיתים קרובות אף מיוצרים יחדיו. בעבר הלא רחוק ארכיטקטורה זו שלטה בשוק חישוב-העל העולמי, ולמעשה מחשבים מסוג זה זכו בשם "מחשבי-על". חברות אשר עדיין מייצרות מחשבים מסוג זה הן Cray (עם קו מחשבי העל XT) וחברת IBM (עם מחשבי העל מסדרת BlueGene). כיום ארכיטקטורה זו מוגבלת לביצועים הגבוהים ביותר, שכן היא נוטה להיות יקרה יותר מאשר צבירי חישוב כלליים, והיא מהווה 16.80% מהמחשבים ברשימת ה-Top 500.

4.10 Symmetric Multi-Processing (SMP)

כאמור, ארכיטקטורה זו מאופיינת באוסף גדול של מעבדים וכמות זיכרון גדולה, אשר נגישה למעבדים באופן סימטרי. כיום, ארכיטקטורה זו הולכת ומאבדת את נתח השוק שלה, שכן היא לא קוסט-אפקטיבית ביחס לפתרונות תוכנה אחרים מעל מכונות MPP או מעל צבירי חישוב. החברה הבולטת ביותר אשר מייצרת כיום פתרונות SMP היא חברת SGI. כיום ארכיטקטורה זו מהווה רק 0.40% מהמחשבים ברשימת ה-Top 500.

4.11 ארכיטקטורת חישוב היברידית (Hybrid Computing)

ארכיטקטורה זו רלוונטית תחת כל אחת משלושת האכיטקטורות אשר תוארו לעיל, והיא מערבת מספר סוגים שונים של רכיבי עיבוד תחת אותה המכונה. הרעיון הבסיסי מדבר על סינרגיה חישובית, שבה כל מעבד מבצע את הפעולות אשר הוא טוב בהן יותר, ובצורה כזו ניתן להגיע למכונות חישוב חזקות במיוחד. לדוגמה, ניתן לחשוב על צביר גדול, אשר מכיל מעבדים כלליים ומעבדים מקביליים (לדוגמה מאיצים גרפיים) אשר נהנה הן מקלות התכנות של המעבדים הכלליים והן מהחוזק היחסי של המעבדים המקביליים. כיום ארכיטקטורה זו נפוצה ביותר, ולמעשה שלוש מתוך ארבעת המכונות הראשונות (כולל המקום הראשון) ברשימת ה-Top 500 הן מכונות חישוב עתיר ביצועים היברידיות המכילות מאיצים גרפים בנוסף למעבדים כלליים.



4.12 אולם המחשב, קירור ואריזה

בעוד קיום של שלל הממדים אשר מפורטים בסעיף הקודם הכרחי לקיום של פתרון חישוב עתיר ביצועים, הרי שהם חסרי משמעות ללא היכולת להפעיל אותם לאורך זמן. על מנת להפעיל אותם, יש לבנות ולתפעל אולם מחשב אשר מסוגל להכיל ציוד בהספקי חשמל גבוהים, לקרר את הציוד ברמה מספקת, ולספק את רמת האמינות והגיבוי הנדרשת. חשוב לציין כי מערכות החישוב המדוברות הן מערכות לא קטנות, התופסות שטח רצפה לא זניח וצורכות הספקי אנרגיה רבים (יכול לנוע מעשרות KWs ועד למספר בודד של MWs), ולכן עלות הקמת האולם, מערכות הקירור ומערכות החשמל, כמו גם עלות מחזור החיים של המערכת גבוהות מאוד, ובד"כ אף עולות על עלות רכישת המערכת. גם קירור של מערכות הצורכות הספקים גבוהים שכאלו (לעיתים אף מספר עשרות KW-ים בארון חישוב בודד) אינה פעולה פשוטה, והחברות השונות משקיעות משאבים רבים על מנת לייעל ולשכלל את פתרונות הקירור אשר הן מציעות. לאורך השנים הוצעו פתרונות רבים ובהם פתרונות קירור אוויר, ארונות מקוררי מים, קירור נוזלי ברמת המעבד, טבילת המעבד בנוזל קירור ועוד.
המודלים כיום מתייחסים לתקופה של בין שלוש לארבע שנים כאורך החיים של טכנולוגית חישוב על. אחרי תקופה זו משתלם יותר לרכוש ציוד חדש ויעיל יותר מבחינה אנרגטית על פני המשך האחזקה של הציוד הקיים. מודלים דומים מראים כי משך החיים של אולם מחשב הוא בין 10 ל-12 שנים, על פי אותם שיקולי כדאיות כלכלית.

4.13 ביצועים

אחת השאלות הבסיסיות ביותר אשר עליהן יש לענות כאשר מתכננים מערכת חישוב עתירת ביצועים היא כיצד נכון וניתן למדוד את ביצועי המערכת. מאחר ומדובר במערכת המכילה מספר רב של רכיבים, המספקים יכולות שונות בווקטורי ביצועים שונים, פעולה זאת נהיית מורכבת עוד יותר. בהכללה גסה, קיימות שתי גישות למדידת ביצועי המערכת - מדידת ביצועים מונחית בוחן ביצועים (benchmark) קבוע, ומדידת ביצועים אל מול בעיית ייחוס. בגישה הראשונה, משתמשים באחד מבין בוחני ביצועים ידועים ונפוצים (לדוגמה, בוחן הביצועים הנפוץ ביותר למדידת מערכות חישוב עתירות ביצועים הוא LINPACK, בו משתמשים לדוגמה בבחינת הביצועים ברשימת ה-Top 500). היתרונות של גישה זו נעוצים ביכולת להשוות בין מערכות שונות (בפרמטרים אותם בוחן הביצועים מודד) ובקלות מדידת הביצועים. הגישה השנייה נפוצה יותר כאשר מתכננים ובונים מערכת לטובת בעיה ספציפית. במקרה זה, ניתן להגדיר ביצועים נדרשים עבור הבעיה אותה מנסים לפתור ולבחון את המערכת מולם.

גם לאחר שסוגיית מדידת הביצועים ברורה, נשאלת השאלה איזה מדד ביצועים נבחן? בעוד ובעבר הלא מאוד רחוק, מדד הביצועים העיקרי היה היכולת החישובית נטו של המכונה (למשל ביחידות FLOPS), הרי שכיום נהוג למדוד את הקוסט-אפקטיביות של המכונה. זאת ניתן למדוד גם כן בדרכים שונות: לדוגמה - ביצועים/עלות רכישה, ביצועים/צריכת חשמל, ביצועים/שטח רצפה ועוד.

4.14 עולמות בעיה משיקים

על בעיות חישוביות קשות ניתן לענות במספר דרכים. הדרך המקובלת ביותר היא זאת שמציעות מערכות חישוב עתיר ביצועים, ותיאור כללי של מערכות כאלו מסופק בסעיף הקודם. יחד עם זאת, ישנן שתי גישות נוספות, אשר במובנים רבים משיקות לעולם החישוב עתיר הביצועים, ויש מקום להציג ביתר פירוט בסעיף זה.

4.15 מחשוב שריגי (Grid Computing)

מחשוב שריגי (Grid Computing) מתייחס למודל אשר מטרתו לענות על פערים חישוביים באמצעות ניצול כוח עיבוד ממספר רב של מחשבים שונים שמחוברים יחד ברשת. בשונה ממודל הצביר, המודל השריגי אינו מחייב המצאות של כלל מרכיבי המחשב באותה רשת מקומית. כמו כן, הוא אינו חייב להיות מורכב ממרכיבים הומוגניים. המודל התפתח עם התפתחות עולם האינטרנט, שהפך דה-פקטו את משתמשי המחשבים בעולם ל"שריג" תיאורטי פוטנציאלי.

מודל אשר התפתח על בסיס המחשוב השריגי הוא מודל ה-"CPU scavenging". במודל הזה, משתמשים מנדבים את זמן העיבוד הפנוי של המחשבים שלהם (בחינם או בתשלום), לצורך ביצוע חישובים ייעודיים אחרים. דוגמא לקונצפט זה היא מערכת SETI@home (Search for Extra-Terrestial Intelligence at Home) של UC Berkeley, שמריצה ניתוחים של אותות חלל על צביר המורכב ממחשבים של משתמשים ברחבי העולם אשר בוחרים להיות חלק מהפרוייקט[15].

מחשוב שריגי מציב אתגרים שונים, ובראשם אבטחת מידע, התמודדות עם בעיות אמינות וזמינות משאבים והתמודדות עם הטרוגניות הפלטפורמות.
מחשוב שריגי יכול להיות פיתרון HPC עבור סוג מסוים של בעיות - בעיקר בעיות שניתנות למקבול מלא (Embarrassingly Parallel). כמו כן, מחשב שריגי יכול להיות מורכב ממספר מחשבי על (מכונה HPC Consortia).

4.16 מחשוב ענן (Cloud Computing)

מחשוב ענן (Cloud Computing) הוא הרעיון לפיו משאבי מחשב מצויים במקום מרכזי ונגיש מעל רשת האינטרנט (או רשת אחרת), באופן המאפשר שימוש של צרכנים באותם משאבי מחשב עפ"י הצורך בלבד (Pay Per Use). בצורה זו נחסך מהצרכנים הצורך להחזיק משאבים משל עצמם. ניתן לדמות את הרעיון של מחשוב ענן לרשת חשמל: העולם שבו למשתמשים יש משאבי מחשוב עצמאיים דומה לעולם שבו לכל צרכן יש תחנת כוח עצמאית. מחשוב ענן דומה לתצורה לפיה צרכנים עושים שימוש בחשמל המיוצר בתחנת חשמל מרכזית ונצרך, לפי הצורך, ע"י חיבור לרשת.

מחשוב ענן מסופק כיום על בסיס שלושה מודלים שונים:
- IaaS (Infrastructure as a Service), - הקצאה של שרתים בענן ושימוש בהם מעל הרשת. משתמש של שירותים אלה אחראי על התקנת השרתים (הוירטואלים) ועל התוכנה שמופעלת בהם.
- PaaS (Platform as a Service) - הקצאה של פלטפורמה שלמה בענן (שרתים ותוכנה) ושימוש דרך הרשת.
- SaaS (Software/Application as a Service) - הקצאה של תוכנה או כלי בענן ושימוש בו דרך הרשת.

[15] www.fcc.gov/Daily_Releases/Daily_Business/2010/db0720/FCC-10-129A1.pdf

רעיון הענן תופס תאוצה בשנים האחרונות, וכבר יש לו אחיזה רבה בעולם הIT. חברות רבות כבר צורכות משאבי מחשוב דרך מחשוב ענן היום. דוגמאות לחברות כאלה הן NASDAQ, NY Times, ESPN ועוד.

בהקשרים של חישוב-על ראוי לציין כי כבר היום ניתן למצוא שירותי חישוב-על מעל לענן - HPCaaS[16]. בשירותים מסוג זה ניתן היום (וביתר שאת בעתיד) לקבל הקצאת חישוב-על עפ"י צורך, בפלטפורמות שונות בענן. בין החברות הראשונות המספקות שירות HPCaaS נמצאת Amazon - אשר השיקה לאחרונה את שירותי HPC שלה[17], והיא מאפשרת לשכור מספר שרתים לצורך חישוב-על, כולל גם שרתים עם מעבדי GPU.

4.17 סקירה בסיסית של השוק

בפרק זה מוצגת סקירה בסיסית של שוק הספקים בתחום ה-HPC. ופירוט מלא של רשימת החברות ניתן לראות בנספח.[18]

4.18 ספקי OEM

חברות הOEM הן חברות המספקות "מוצר שלם" למשתמשים. חברות ה-OEM המובילות היום בתחום ה-HPC בעולם הן:

1. IBM - המחזיקה בכ-40% מהמחשבים (ברשימת ה28% - Top-500 מכוח החישוב הכולל ברשימה זו) ומספקת מגוון פתרונות בסדרי גודל קטנים עד גדולים מאוד.
2. HP - המחזיקה בכ-32% מהמחשבים (ברשימת ה16% - Top-500 מכוח החישוב הכולל ברשימה זו). עוסקת בעיקר בפתרונות בסדרי גודל קטן ובינוני מתצורת צבירים סטנדרטים.
3. Cray - המחזיקה בכ-6% מהמחשבים (ברשימת ה-19% - Top-500 מכוח החישוב הכולל ברשימה). החברה מתמקדת בעיקר בפתרונות בסדרי גודל גדול.
4. SGI - המחזיקה בכ-4% מהמחשבים (ברשימת ה6% - Top-500 מכוח החישוב הכולל ברשימה), משלבת הן פתרונות יחודיים והן מערכות סטנדרטיות.
5. חברות נוספות בתחום - Dell, Oracle (Sun), Fujitsu, Appro.

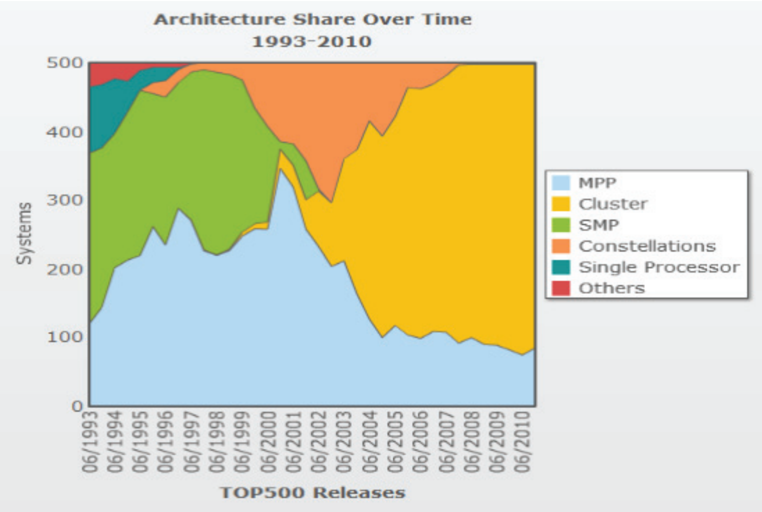
4.19 חברות מוצרים ל-HPC

רשימת החברות כוללת את כל החברות אשר מספקות מוצרים שונים הרלוונטיים לשוק ה-HPC, וביניהם:

1. מעבדים - השוק נשלט כמעט בלעדית על ידי חברות מעבדי x86 – Intelה ו-AMD.
2. תקשורת פנימית - השוק נשלט כיום על ידי תקן 10GigE ו-Infiniband- בעוד שלתקן הראשון יש מגוון חברות המספקות פתרונות, בתקן האחרון החברה המובילה היא חברת Mellanox הישראלית, ואחריה Qlogic.
3. מאיצים גרפים - בתחום זה שתי חברות מובילות - Nvidia ו-AMD.
4. רכיבי FPGA ומאיצים מבוססי FPGA - בתחום רכיבי הFPGA קיימות שתי חברות - Xilinx וAltera-. על בסיס רכיבים אלה מספקות חברות כגון Dini, Pico, XtremeData, Nallatech ו-Gidel הישראלית מאיצי חישוב.
5. HPC Storage - בתחום החומרה מובילות בשוק Data Direct Networks ו-Panasas, לצד חברות OEM המספקות פתרונות משלהן. בתחום התוכנה מובילות IBM ו-Oracle לצד Panasas.

[16] en.wikipedia.org/wiki/SETI@home
[17] למשל blog.cyclecomputing.com/2011/04/single-click-starts-a-10000-core-cyclecloud-cluster-for-1060-hr.html
[18] aws.amazon.com/hpc-applications/#HPCEC2

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות



5. מגמות עולמיות

5.1 חישוב– על בעולם

תחום חישוב-העל וחישוב עתיר ביצועים נתפס בעולם כיכולת אסטרטגית הנדרשת כבסיס להתפתחות כלכלית, מדעית וביטחונית[19]. יותר ויותר מדינות רואות ביכולות חישוב-על סמל לעוצמה וחוסן. הבנות אלה מובילות מדינות רבות למהלכי השקעה משמעותיים לפיתוח יכולות חישוב-על[20], אשר מניעות את התעשייה ואת הכלכלה[21]. בפרק זה נסקור את הכיוונים האסטרטגיים של חלק מהמדינות המובילות בעולם.[22]

5.2 אסטרטגיות ומגמות חישוב– על בארה"ב

ארה"ב עוסקת בתחום חישוב-על כבר שנים רבות, ומתייחסת ליכולות חישוב-על שלה כיכולות אסטרטגיות ומפגן עוצמה. בארה"ב קיימים מעל 700 מעבדות ומרכזי חישוב על, מעל 1500 מרכזי מו"פ בתחום והשקעה של מעל 100 מיליארד דולר לשנה למו"פ חישוב-על. הנשיא אובאמה הצהיר ב-2009[23], כי הממשל מחויב לתמיכה במחקר אשר יפתח את הגל הבא בתחום טכנולוגיות המידע ביניהן חישוב קוונטי, חישוב מקבילי יעיל, וחישוב עתיר ביצועים. בפרט הממשל מאמץ את ההמלצה להציב כיעד בנייה של מחשב Exascale[24] וזאת במטרה לשפר את ההבנה של העולם הסובב אותנו באמצעות סימולציה, וקיצור משמעותי של הזמן הדרוש לעיצוב של מוצרים מורכבים כגון תרופות, חומרים מתקדמים, רכבים יעילים ומטוסים. בשנת 2010

19 בתחום הביטחוני למשל, יכולת חישוב נתפסת בארה'ב כיכולת אסטרטגית: "If one were to choose a metrics that represents the best national military capacity, the high performance computing power of a nation would win as the most comprehensive measure. More and more countries view supercomputing technology as a symbol of national military power." (Worldwide Defense High Performance Computing Market Forcast 2010-2015)

20 ראה למשל "A Strategic Agenda for European Leadership in Supercomputing"

21 עפ"י תחזית אמריקאית גודל שוק ה-HPC לצרכי ביטחון לשנים 2010-2015 נאמד ב-18 מיליארד דולר (Worldwide Defense High Performance Computing Market Forcast 2010-2015)

22 על בסיס עבודת איסוף של חב' "שלדור", ראה נספח

23 "Strategy for American Innovation" (2009)

24 אתגר ה-Exascale הוא האתגר של המאה ה21 להגיע ליכולות חישוב פי אלף יותר גבוהות מהיכולות הקיימות כיום. התחזית להשגת היעד היא 2018.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

הוגש דו"ח לממשל ע"י יועצי הנשיא לנושא מידע וטכנולוגיה[25] ובו ההמלצות הבאות:

Hardware	Novel IC designs incorporating a large number of on-chip processor cores
	Novel intra-chip communication architectures
	System-level interconnection networks with high bandwidth and low latency
	IC and chip packaging technologies offering high input/output (I/O) bandwidth
Hardware/Software Systems	Design of reliable massively parallel computer systems
	Design aspects of HPC systems in which hardware design choices and the ability to write software that takes full advantage of the hardware are interdependent
	Special purpose" machines designed to" achieve high performance on specific classes of algorithms, applications, and data structures
Systems/Applications Software	Latency-tolerant architectures and algorithms
	Programming models and languages for massively parallel machines
	Systems software for massively parallel systems, including OSs, file systems and data stores
	Performance and correctness debuggers
	System management tools
	Development environments
	Tools and techniques for modeling and tuning the performance of large-scale systems and software architectures

5.3 אסטרטגיות ומגמות חישוב–על באיחוד האירופי

ועדה מטעם האיחוד האירופי הגישה בספטמבר 2010 דו"ח לקביעת האסטרטגיה של האיחוד להובלה בתחום חישוב-על[26]. החזון של האיחוד לשנת 2020 הוא "לספק משאבי חישוב-על ומומחיות חישוב-על ברמה עולמית, על מנת להפוך את המדענים, המהנדסים והאנליסטים האירופים לפרודוקטיבים ולחדשנים ביותר בעולם בשימוש ב-HPC לקידום המחקר שלהם". תוכנית הפעולה האירופית כוללת את הצעדים הבאים:

1. להגדיל את מספר משאבי -HPC, גודלם ונגישותם ברחבי האיחוד האירופי.
2. לספק גישה לחישוב-על לצורכי פרוייקטי פיתוח תעשיתיים.
3. להקים מספר מרכזי מו"פ בתחום HPC להתמודדות עם אתגר הExascale- לצורך פיתוח, מחקר והכשרה בתחום.

[25] Report: Designing a Digital Future 2010
[26] A Strategic Agenda for European Leadership in Supercomputing: HPC 2020 – IDC Final Report of the HPC Study for the DG Information Society of the European Commissio

4. למשוך סטודנטים לתחומי ההנדסה והחישוב-על ברחבי האיחוד האירופי.
5. להגדיל את ההשקעות במו"פ להתמודדות עם אתגר ה-Exascale.
6. לכוון להובלה עולמית במספר תחומי אפליקציה לחישוב-על.

5.4 אסטרטגיות ומגמות חישוב–על בסין

סין נכנסה בשנים האחרונות למירוץ חישוב-על מול המערב, ומפנה השקעות עצומות בהקמת תשתית ומחשבי על ובהתמודדות על המקום הראשון ברשימת Top-500. סין בנתה בשנים האחרונות 14 מחשבי על בסדרי גודל של Petascale, ולהערכת מומחים יובילו את התחום לפני סוף העשור הנוכחי. בשנת 2010 זכתה סין לעמוד בראש רשימת Top-500 באמצעות המחשב Tihane-1A. בימים אלה משקיעה סין משאבים גדולים להקמת מרכז חישוב-על בקנה מידה עולמי (National Supercomputing Center). בגרף שלהלן ניתן לראות את הצמיחה של סין בתחום ה-HPC כפי שמתבטא בנוכחות ברשימת ה-Top-500.

6. תמונת המצב בישראל

6.1 המצב בתחום HPC בארץ

במסגרת עבודת הוועדה בוצע תהליך של איסוף נתונים ומיפוי צרכים בתחום חישוב-על ותשתיות תקשורת רחבות פס הדרושות לכך. על מנת לבצע את המיפוי, חילקה הוועדה את כלל הצרכים והצרכנים לארבעה מגזרים: מערכת הביטחון, התעשיות הביטחוניות, התעשיות הלא ביטחוניות, והאקדמיה.

6.2 מערכת הביטחון

הפער המרכזי אשר אותר במהלך הסקירה של צרכי מערכת הביטחון הוא בראש ובראשונה ידע מקצועי מוביל ברמה העולמית. פערי הידע מתבטאים במחסור בהכשרה מתקדמת של מומחים בתחום, העדר עיסוק משמעותי במחקר ופיתוח בתחום באקדמיה ובתעשייה, והעדר מוקד ידע ושיתוף פעולה בין כלל העוסקים בתחום במגזרים השונים. ברור כי לצורך סגירת פער זה נדרשת גם השקעה בתשתית ובמחשבי על, אך הוועדה זיהתה שזהו אינו פער טכנולוגי אלא פער תקציבי בלבד.

6.3 התעשיות[27]

על מנת לבצע סקר צרכים בתעשיות הרלוונטיות, נעשה שימוש במיפוי אפליקציות מרכזיות בחישוב-על אשר בוצע ע"י האיחוד האירופי[28]. האפליקציות המרכזיות מוצגות להלן:
הטבלה הבאה מתארת בקצרה את מאפייני האפליקציות השונות:
במהלך העבודה של הוועדה, התקיימו מפגשים וראיונות עם החברות המובילות בארץ המייצגות את תחומי העשייה הנ"ל:
על פי ממצאי הסקירה והראיונות, נמצא כי ניתן לחלק את החברות הרלוונטיות בארץ לשלוש קבוצות מרכזיות: קבוצה אחת של חברות מגדירה עצמה כמי שיש לה צורך נמוך ומודעות נמוכה לחישוב-על, ובה נמצאות בעיקר חברות הפיננסים, פרמצבטיקה, מזון, ייצור ולוגיסטיקה. קבוצה שנייה של חברות, הכוללת חברות לייצור אלקטרוני וחברות העושות שימוש במודלי CFD רואה בחישוב על כלי תומך בלבד. הקבוצה השלישית, אשר כוללת בעיקר חברות העוסקות בביו אינפורמטיקה, מטאורולוגיה, חיפושי נפט מסחר פיננסי מתקדם, עיבוד תמונה וגרפיקה ממוחשבת מתייחסת לחישוב על כאל כלי מרכזי בעשייה. המשך הסקירה מתייחס בעיקר לחברות מהקבוצה הזו.

27 מקור - דו"ח IDC, עיבוד שלדור
28 כל החומר בפרק זה מבוסס על סקירה אשר בוצעה עבור הועדה ע"י חברת "שלדור" בתיאום עם נציגות המדען הראשי

ברוב החברות אשר נסקרו קיים פתרון בדמות צביר מקומי בגודל קטן עד בינוני (עד אלף ליבות חישוב), בחלק מהמקרים מואץ ע"י כרטיסי GPU. ברוב המקרים נמצא כי **סוגיית הפתרון המקומי היא עקרונית**, ונובעת הן מהצורך והרצון של החברות להגן על ה-Intellectual Property אשר מפותח בהן והן מתרבות עבודה התומכת בפתרונות in-house.

במהלך הסקירה נמצא כי לחברות אלו, ברוב המקרים, לא קיים פער משמעותי בציוד חישוב-על (או שניתן לצמצם את הפער בהשקעה כספית סבירה). לעומת זאת, הפער המרכזי אשר עלה לאורך המפגשים היה פער ידע המתבטא בכמות מצומצמת של אנשי מקצוע בארץ אשר יכולים ויודעים לעסוק בתחום, מחסור במסלול הכשרה לכ"א בתחום, העדר מוקדי ידע המאפשרים מו"פ חישוב-על, פערים בשיתוף פעולה עם האקדמיה, ופערי תקשורת בין כלל העוסקים בתחום בארץ.

6.4 התעשיות הביטחוניות[29]

על סמך סקר האפליקציות הנ"ל מופו החברות המרכזיות בתעשייה הביטחונית אשר עושות שימוש בחישוב-על. בתחומי אפליקציות CFD נסקרו רפא"ל[30], הקמ"ג, והתעשייה האווירית[31], ובתחומי אפליקציות Rendering ועיבוד תמונה נסקרו אלביט[32] ואלאו"פ[33]. הגופים הנ"ל עושים שימוש בחישוב-על ככלי מרכזי לעבודה. לגופים יש פתרונות מקומיים בתצורת צביר בסדרי גודל של 1000 ליבות ברוב המקרים (למעט מקרה חריג של פתרונות מבוססי FPGA). גם כאן, כמו בחברות הלא ביטחוניות, הפתרון המקומי הוא תוצאה של רצון להגן על מידע ושל תפיסת עבודה. בדומה לתוצאות הסקירה של החברות הלא ביטחוניות, נמצא כי גם בחברות הביטחוניות הפער המרכזי איננו בציוד. לעומת זאת נמצא כי קיימים פערים הקשורים בפיתוח אפליקציות חישוב-על "כחול לבן", כלי פיתוח, וידע מקצועי מתקדם בתחום.

6.5 מחקר מדעי אקדמי[34]

במהלך איסוף הנתונים של הוועדה נמצא כי קיים במחקר המדעי בישראל שימוש בחישוב-על. בין הענפים המרכזיים העושים שימוש בחישוב-על בתצורות שונות: חקר המוח ורשתות נוירונים, ביו אינפורמטיקה, ביולוגיה חישובית, כימיה, אסטרופיזיקה, ענפי פיזיקה שונים, חיזוי מזג אוויר, אקוסטיקה מתקדמת, וחקר מדעי המחשב וחישוב-על. להלן נתונים מדגמיים של תמונת המצב הקיימת והצרכים העתידיים של הקבוצות השונות:

Discipline	Institution	Current Platform
Brain research Neural nets	HUJI, BIU, Weizmann	core cluster +GPU 160
Bioinformatics	BIU, BGU, HUJI, TAU Weizmann	(core cluster (BIU 160
Computational Biology	BIU, BGU, Weizmann	Amazon cloud
Chemistry	Weizmann, HUJI Technion	core cluster 300
Astrophysics	HUJI, Weizmann, Technion	core cluster at WIS 1000 Smaller 12-24 at Technion
Fluid Physics / Turbulence/ Reactions	HUJI, TAU, BGU, Technion, Weizmann	cores cluster 1,000

29 כל החומר בפרק זה מבוסס על סקר של פר' דורון חבצלת במסגרת עבודת הוועדה
30 http://www.rafael.co.il/
31 http://www.iai.co.il
32 http://www.elbitsystems.com
33 http://www.el-op.com
34 כל החומר בפרק זה מבוסס על עבודה של "תת וועדה לתועלות אקדמיות" של המיזם הקיברנטי" וכן על סקירה של פר' דורון חבצלת אשר בוצעה במסגרת עבודות הוועדה

Advanced acoustics	TAU	cores cluster 300
Climate	BIU, TAU, HUJI	cores cluster 500
Particle physics	Weizmann, HUJI, TAU	Few hundred cores for post-processing of experiments
Web Simulation, HPC research	TAU, BGU, Technion	Few hundred cores, GPU

כפי שניתן ללמוד, ברוב המוחלט של המקרים פתרונות החישוב הם פתרונות מקומיים. בחלק מצומצם מהמקרים, כאשר הפתרון המקומי אינו מספק, נעשה שימוש בשותפויות עם חוקרים בחו"ל או בשירותי מחשוב על מעל ענן.

במסגרת הניתוח נמצא כי במספר תחומים יכולות חישוב-על מתקדמות יותר מהקיימות יאפשרו מחקר חדשני, ובחלק מהמקרים אף פורץ דרך (למשל בכימיה חישוביות או בביואינפורמטיקה).

לאקדמיה בישראל שלושה פערים מרכזיים בתחומי חישוב-על:
- פער בציוד: בחלק מהמקומות נדרשת יכולת עיבוד חזקה מהקיימת - בד"כ מדובר בצורך בציברים בסדרי גודל של 10,000 ליבות, אחסון גדול או מחשבי על מקביליים (SMP).
- פער בתקשורת רחבת פס: במקרים שבהם ניתן לעשות שימוש בציוד חישוב-על מרוחק (במרכזי חישוב בחו"ל או מעל לענן) קיים פער מהותי הנובע מרוחב פס מקשה ובחלק מהמקרים אף מונע את השימוש בפתרונות אלה[35].
- פער בידע, תמיכה וייעוץ: הפער המרכזי הנובע מהעובדה שברוב המקרים על מנת לעשות שימוש אופטימאלי בחישוב-על במחקר נדרש ידע מדעי, טכנולוגי וטכני מעמיק. ידע זה לא קיים בד"כ בקבוצות המחקר (למעט בקבוצות המחקר אשר עוסקות במחקר חישוב-על). על מנת לנסות לצמצם את הפער חוקרים מפנים סטודנטים או פוסט דוקטורנטים בקבוצות המחקר לעיסוק בתחום. מהלך זה נותן פתרון חלקי בלבד, שכן המומחיות הנדרשת לא מפותחת במלואה ולא נשמרת לאורך זמן.

6.6 עיקרי הפערים

מתוך עבודת הוועדה עולה אם כן כי במדינת ישראל קיימים מספר "איים" של עיסוק בחישוב-על. איים אלה, הנמצאים במערכת הביטחון, באקדמיה ובתעשיות, עובדים כמעט בכל המקרים באופן עצמאי, ועל כן לא נוצרת סינרגיה ביניהם. העדר הסינרגיה גורם לקושי ביכולת של כל אחד מהצרכנים להתמודד עם אתגרי חישוב-העל שלו. מהמחקר עולה, כי לכל הגופים אתגר משמעותי משותף והוא פערי ידע בתחומים המתקדמים של חישוב-על וקושי באיתור, הכשרה והעסקה של אנשי מקצוע מובילים בתחום. עוד עולה מהמחקר כי ציוד חישוב-על הוא בחלק מהמקרים פער, אך תמיד משני בחשיבותו ובקדימותו לפערי הידע והמומחיות. כאשר קיים צורך במחשבי על "סטנדרטיים" - ניתן כיום לרכוש את הציוד הנדרש בעלויות סבירות ברוב המקרים, ואם קיים פער אזי מדובר בפער תקציבי (למשל בחלקים מהאקדמיה ובמערכת הביטחון בישראל). כאשר קיים צורך בציוד לא סטנדרטי, הפער המרכזי הוא במחקר ופיתוח של ציוד כזה או ביכולת ובידע לנצל ציוד כזה בצורה אופטימאלית. האפשרות הנוספת בקשת האפשרויות היא המקרה שבו "לא קיים צורך" בחישוב-על. אפשרות זו יכולה אף היא להצביע, ולו בחלק מהמקרים, על פער ביכולת לזהות את הצורך - הנובע מפערי ידע בתחום. להערכתינו, במקרים רבים לא מודע הצרכן הפוטנציאלי ליכולת שהוא יכול להפיק משימוש בחישוב על - ועד אשר לא יהיו בידיו יכולות אלה והוא לא יתחיל לעשות בהן שימוש, אין כל סיכוי שהוא יזהה חוסר זה כפער.

[35] www.el-op.com

7. הצעה לפעולה

7.1 עקרונות הפתרון

מתוך כלל החומר שנצבר ונחקר ע"י חברי הוועדה, מצאנו לנכון לציין מספר עקרונות יסוד בכל פתרון רלוונטי לפערים של מדינת ישראל בתחום חישוב-על:

עקרון ההשקעה הרב שנתית

פתרון בר קיימא לפערי מדינת ישראל בתחום חישוב-על חייב להיות פתרון ארוך טווח של השקעה מתמשכת. ההתקדמות הטכנולוגית (כפי שמתבטאת בחוק Moore[36]) גורמת לכך שציוד חישוב-על הופך להיות לא יעיל תוך שלוש עד ארבע שנים, ותוך מעט יותר מזה הופך להיות לא רלוונטי לבעיות חישוב-על עדכניות. מסיבות דומות אולמות מחשב הופכים להיות לא כדאיים כלכלית תוך כ-10 עד 12 שנים. ההתקדמות המדעית מאידך מייצרת אתגרים תמידיים במגוון התחומים של חישוב, ובפרט בחישוב על. על כן, כמו בציטוט המפורסם מהספר "עליסה בארץ הפלאות"[37] - על מנת לעמוד במקום (קרי, לשמור על יכולות התמודדות קבועות) אנו נדרשים לרוץ כל הזמן (קרי, להשקיע בהצטיידות ומו"פ). ההיסטוריה מלמדת שהשקעות חד פעמיות בתחום[38] השיגו יתרון יחסי לזמן קצר, אשר הצטמצם במהרה והפך ללא קיים תוך שנים בודדות.

עקרון ההשקעה המערכתית

העיסוק בחישוב-על הוא עיסוק מערכתי, במובן זה שהוא מציב אתגרים **במכלול שלם של תחומים** - החל מאתגרי אנרגיה וקירור, עבור באתגרי כוח עיבוד, תקשורת, אחסון, דרך אתגרי ניהול מערכת ופיתוח אפליקציות, ועד לאתגרי פיתוח מתודולוגיה והכשרת כ"א. האתגר ה-Exascale אשר הציב לעצמו העולם[39] מדגים זאת היטב - לא ניתן להגיע ליכולות חישוב אלה בלי לפתור אתגרים **בכל אחד** מהתחומים האלה. מתוך כך אנו למדים שפתרון לפערי מדינת ישראל חייב להתייחס לכל אחד ממימדי העיסוק ברמה כזו או אחרת.

עקרון ההשקעה המשולבת

עקרון זה מתייחס לעובדה שעיסוק בחישוב-על במדינת ישראל מצוי בשלושת המגזרים המרכזיים העוסקים במו"פ הרלוונטים לתחום - תעשייה, אקדמיה ומערכת הביטחון. מחד - **אף אחד מהמגזרים לא יכול להשיג את כל צרכיו במלואם ללא אחד או שניים מהמגזרים האחרים**. מאידך - לחיבור בין המגזרים יש פוטנציאל סינרגטי משמעותי שיכול לאפשר קפיצות מדרגה משמעותיות לכל אחד מהשותפים. מתוך כל האמור לעיל אנו למדים שכל פתרון שייבחן חייב להתייחס ליצירת השותפות בין התעשייה, האקדמיה ומערכת הביטחון.

36 חוק מור הוא תחזית או ניבוי משנת 1965 של גורדון מור לפיה צפיפות הטרנזיסטורים במעגלים משולבים במחיר מינימלי תוכפל כל עשרה חודשים. בפועל, התחזית הגשימה את עצמה בקצב שונה, אך משמעות התחזית דומה - בכל פרק זמן של בין שנה לשנתיים עוצמת המעבד מכפילה את עצמה.

37 Through The Looking Glass And What Alice Found There (Lewis Carroll) – "Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!

38 במסגרת מרכז החישובים הבינאוניברסיטאי (מחב"א) נרכשו בעבר מחשבי על לשימוש האקדמיה. בעקבות העדר השקעה ממושכת מחשבים אלה הפכו מיושנים תוך זמן קצר.

39 Through The Looking Glass And What Alice Found There (Lewis Carroll) – "Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!

הצעה לפתרון

על בסיס הלמידה והניתוח כפי שמסוכמים במסמך זה, חברי הועדה מוצאים לנכון להמליץ על הקמת "מרכז לאומי לחישוב-על" כחלק ממוסד אקדמי, שייעודו יהיה הובלת מחקר ופיתוח בתחום חישוב על וחישוב עתיר ביצועים. משימותיו של מרכז כזה יהיו:

1. **ביצוע מחקר אקדמי** (כגון מחקרים בתחומי GPU[40])
2. **תכנון ומימוש של פרוייקטי מו"פ** רלוונטים (כגון פיתוח וייצור מאיצים מבוססי FPGA או פיתוח אפליקציות מקביליות)
3. **הוראה והכשרת אנשי מקצוע וחוקרים** (הכשרה מקצועית, קורסים אקדמים, תארים מתקדמים)
4. **ייעוץ והכוונה למשתמשים** (כגון ייעוץ לחוקרים בתחומי מדע אשר עושים שימוש בחישוב למחקר)

המרכז ישלב בתוכו חוקרים מהאקדמיה בתחומי מדעי המחשב וההנדסה, אנשי מחקר ופיתוח מהתעשייה וממערכת הביטחון, וכן אנשי מקצוע ותמיכה מהתעשייה. תוכנית העבודה והמחקר של המרכז תקבע במשותף עם הצרכנים המרכזיים משלושת המגזרים (ביטחון, תעשיה ואקדמיה), ונציגים מתאימים מהמגזרים הללו יהיו חברים בגוף המנהל. למרכז תהיה מעבדת מחקר ובה ציוד חישוב-על מתקדם בהתאם לצורך (ראו פירוט בהמשך). יש להדגיש כי עיקר תפקודו של המרכז, **בשונה מצעדים שבוצעו בעבר בתחום,** איננו להוות ספק שירותי חישוב-על ("זמן מחשב"). כמו כן חשוב לציין, כי הצורך בקיומה של מעבדה כזו איננו מחייב בהכרח הקמת המעבדה במסגרת המרכז - מודל אפשרי אחר הוא הקמת המעבדה וניהולה ע"י ספק חיצוני, והדבר דורש בחינה ע"י צוות ההקמה של המרכז.

בכל מקרה **נדרשת מעבדה כזו** מכיון שברור שמרכז לאומי לחישוב-על, ללא יכולות חישוב-על משמעותיות, יהיה מעוקר וחוסר השפעה משמעותיות. הוועדה מוצאת לנכון לציין כי על מנת לחזק את עתודת החוקרים, אשר תהיה חלק מהמרכז בטווח הארוך, מומלץ לוודא כי הצרכנים המרכזיים במדינת ישראל כיום אשר עוסקים במו"פ מתקדם בתחום יתוגברו בכ"א מתאים, אשר חלקו הגדול יופנה בטווח הביניים ובטווח הארוך לפעילות המרכז.

7.2 פירוט ועלויות

תצורה

לצורך קביעת עלויות הוגדרה תצורה עקרונית למעבדה. התצורה כוללת שתי מערכות חישוב-על בעלות ארכיטקטורה שונה - צביר היברידי (צביר המשלב כרטיסי האצה) לחישוב מבוזר ומערכת SMP (Symmetric Multi Processing) לחישוב מקבילי. התצורה נקבעה עפ"י הערכות מומחים על מנת לאפשר מחקר מתקדם ומוביל ברמה עולמית, אך לא מתוך כוונה להתחרות ברשימת המחשבים החזקים בעולם. כמו כן, מודגש כי מדובר בתצורה כללית לצורך אומדן עלויות בלבד. צביר היברידי:

שרתי חישוב	כ2000 שרתים
מעבדים	x86 מרובי ליבות (6-12)
תקשורת פנימית	תקן Infiniband
מאיצים	כ1000 מאיצי GPU
מערכת אחסון	כפטה-בייט נפח

מערכת SMP:

ליבות חישוב	2048 ליבות x86
זיכרון	16TB

[40] מחקר אקדמי לדוגמה בתחום: http://portal.acm.org/citation.cfm?doid=1654059.1654091

עלויות

הקמת מרכז ידע מהסוג המתואר יעשה לדעת הוועדה בשלושה שלבים מרכזיים:

1. שלב ההקמה

בשלב זה, שאמור להימשך כשנה, ימונה צוות מוביל של אנשי מקצוע - מהתעשייה, האקדמיה ומערכת הביטחון, אשר יהוו גרעין הקמה. הצוות יעסוק באפיון מפורט של המכון והמעבדה, איתור וגיוס חוקרים מובילים, יצירת המנגנונים הדרושים וכדומה. להערכת הוועדה צוות ההקמה צריך להכיל בין שלושה לחמישה אנשי מקצוע מעולים. הוועדה ממליצה לחבור לספקית פתרונות חישוב-על מהמובילות בישראל לצורך הקמת המעבדה.

פירוט העלויות לשנת ההקמה

5 אנשי מקצוע/חוקרים למשך שנה	3 מיליון ₪
עלות מבנה המרכז הלאומי	1 מיליון ₪
עלות מעבדה: רכש ואחזקה למחשב על בתצורת קלאסטר כולל מבנה לפי הפירוט לעיל	25 מיליון ₪
עלות רכש ואחזקה למחשב מקבילי בתצורת SMP לפי הפירוט לעיל	5 מיליון ₪
סה"כ לשנה ראשונה (כולל מחויבות לשנים הבאות)	34 מיליון ₪

7.3 שלב הגיבוש

שלב זה, אשר צפוי להימשך כשלוש שנים, מתחיל עם תחילת ההפעלה של המרכז. בשלב זה יגובש צוות החוקרים והעובדים במרכז, מודל העבודה שלו, תחומי המחקר, ההוראה, שיתופי הפעולה השונים. במהלך תקופה זו יצטרפו למכון חוקרים ואנשי מקצוע נוספים, באופן הדרגתי, עד לשלב הבשלות, וכן יתרחבו וישודרגו תשתיות חישוב-העל (המעבדות) על-פי הצורך.

פירוט העליות לתקופת ההתגבשות

8 אנשי מקצוע/חוקרים לשנה ראשונה	5 מיליון ₪
12 אנשי מקצוע/חוקרים לשנה שנייה	7 מיליון ₪
15 אנשי מקצוע/חוקרים לשנה שלישית	9 מיליון ₪
עלות רכש ואחזקה (לשלוש שנים) למעבדה (הערכה עפ"י הפירוט לעיל)	80 מיליון ₪
תמיכה במחקרים מוזמנים	תקציב חיצוני מהצרכנים השונים
סה"כ לשנה (משוקללת) בשלב הגיבוש	33 מיליון ₪

7.4 השלב היציב

הוועדה מצאה כי על מנת להגיע להישג הנדרש, מכון המחקר צריך להתייצב על כ-20 חוקרים מעולים ועוד כחמישה אנשי מקצוע לתמיכה ושירות במעבדה, וכן לשמור על מעבדה עדכנית אשר תכלול ארכיטקטורות חישוב על בנות שלוש שנים לכל היותר (מעבר לכך הטכנולוגיות לא רלוונטיות ולא כלכליות). פירוט העלות השנתית בשלב היציב

20 חוקרים לשנה	12 מיליון ₪
5 אנשי צוות לשנה	2 מיליון ₪
עלות מעבדה לשנה (משוקלל, כולל החלפה לשלוש שנים)	30 מיליון ₪
תמיכה במחקרים מוזמנים	תקציב חיצוני מהצרכנים השונים
סה"כ לשנה (משוקללת) בשלב היציב	44 מיליון ₪

8. סיכום והמלצות

תת הועדה לחישוב-על ותשתיות תקשורת רחבות פס מונתה לבחון את הפערים והצרכים בחישוב-על במדינת ישראל, תוך בחינת הסינרגיה הנדרשת והמומלצת בין שלושת המגזרים הרלוונטים: תעשייה, אקדמיה וביטחון. הוועדה מצאה לנכון להמליץ על הקמת מרכז לאומי לחישוב-על כחלק ממוסד אקדמי, שייעודו העיקרי יהיה הובלת מחקר ופיתוח בתחום חישוב-על וחישוב עתיר ביצועים ומשימותיו מפורטות במסמך זה. תוכנית העבודה והמחקר של המרכז הלאומי תקבע במשותף עם הצרכנים המרכזיים (ביטחון ותעשייה) ונציגים מתאימים מגופים אלו יהיו חברים מלאים בגוף המנהל, וכן יהוו חלק בלתי נפרד מצוות המחקר במרכז, כחלק מעבודתם. להערכת הוועדה, לצורך מימוש המלצותיה, ניתן לבנות את המרכז הלאומי בשלושה שלבים, אשר לכל אחד מהם ידרשו ההשקעות הבאות (הערכה ראשונית):

השלב	השקעה נדרשת שנתית (בממוצע)
שלב ההקמה	34 מיליון ₪
שלב הגיבוש	33 מיליון ₪
השלב היציב	44 מיליון ₪

על מנת לראות תוצרים למרכז החל מהשלב השני, מומלץ לבחון את האפשרות כי הצרכנים יתוגברו בכ"א מתאים שחלקו הגדול יופנה לפעילות המרכז.

הוועדה מדגישה את הצורך בהסתכלות מערכתית, ארוכת טווח ומשולבת, וממליצה שההשקעות בשלב היציב תהיינה **רציפות לאורך שנים ארוכות.** החלטה על פתרון בשיטת "זבנג וגמרנו" אינה נכונה ואינה מתאימה למאמץ מסוג זה, ועדיף שלא לקבלה.

הוועדה מודה לכל מי שתרם מזמנו היקר על מנת לגבש את ההמלצות המרוכזות במסמך זה.

דו"ח תת הוועדה לבחינת התועלות הכלכליות בפיתוח תעשיית סייבר ישראלית

1. תמצית ועיקרי ההמלצות

תמצית

תעשיית סייבר ישראלית חזקה ומובילה היא רכיב מכריע ביצירה ובשימור על היכולות של מדינת ישראל במרחב הקיברנטי. המשך חיזוקה, לצד הובלה ביכולות ההגנה של המדינה במרחב הקיברנטי, יוצרים "יתרונות לגודל", שמגדילים את היעילות הכלכלית של מערכות ההגנה האזרחיות ומערכות הביטחון, ומגבירים באופן משמעותי את מידת התחרותיות של התעשייה הישראלית בעולם. בישראל קיימת כבר כיום פעילות עסקית ענפה במרחב הקיברנטי, ולכן אנו ממליצים כי המשך **פיתוח תעשיית הסייבר הישראלית ייעשה סביב קידום צרכי ההגנה הלאומית של מדינת ישראל במרחב הקיברנטי.**

המשך פיתוח התעשייה המקומית צריך להתבסס על האתגרים החדשים שהמרחב הקיברנטי מציב להגנה על המדינה, אשר דורשים יכולות טכנולוגיות ומדינתיות חדשות. מינופן של יכולות אלה לקידום מנוע צמיחה משמעותי בתחום בישראל כרוך בעלות נמוכה ביותר, ואנו ממליצים לקדם את תעשיית הסייבר האזרחית בישראל כרובד נוסף של יצירת יכולות כלליות, המתווסף לסל פעילויות ההגנה האזרחיות. בהנחה שהתשתית לקיומה של תעשיית סייבר ישראלית מובטחת, בשל צרכי הגנת המדינה ויכולות מערכת הביטחון, אנו ממליצים כי את **הפעילות להמשך קידום תעשיית הסייבר האזרחית יוביל גוף בעל קשרים עם מערכות ההגנה האזרחית והכרות מעמיקה של טכנולוגיות.**

בחינה מעמיקה של התועלות הכלכליות שתפיק התעשייה הישראלית מהפרוייקטים המוצעים במיזם, הצביעה על כך שחלק ניכר מהפרוייקטים כוללים יצירת מערך יכולות חדש בתעשייה ובמערכת הביטחון. **קידום פרוייקטים ממשלתיים משמעותיים בתעשייה יכול ליצור יתרונות יחסיים חדשים** לתעשיית הסייבר הישראלית ולחוסנה הלאומי של מדינת ישראל.

עיקרי ההמלצות

המלצות לארגון התוכנית מול השוק הפרטי:

1. **הקמת מנהלת לפיתוח תעשיית הסייבר הישראלית, כחלק מבניית היכולות הלאומיות במרחב הקיברנטי.**
2. **כינון מסגרת סייבר בין מגזרית ומינוי של שר בכיר בראשותה, וגיבוש מדיניות לאומית במרחב הקיברנטי, הכוללת את קידום התעשייה הישראלית.**

המלצות כלליות לקידום תעשיית הסייבר בישראל:

3. **הגדלת היקפי המחקר והפיתוח הביטחוניים המבוצעים בתעשייה, תוך שיפור ההסדרה של יצוא טכנולוגיות.**
4. **הגדלת השקיפות בתוכניות העבודה והפיתוח במערכת הביטחון ובמערכת ההגנה האזרחית, וחיזוק הממשקים בין הגופים הצבאיים לתעשייה ולאקדמיה.**
5. **כינון רגולציה המעודדת שוק ראשוני להטמעת טכנולוגיות ומוצרים חדשים.**
6. **יצירת דירוג של רמת ההגנה עבור גופים חברות, שישמש בסיס לבניית כלי מדיניות, ולניהול סיכונים פיננסיים וביטוחיים.**

המלצות לפעילויות מנהלת לפיתוח תעשיית הסייבר הישראלית:

7. **פעילויות ארגוניות של המנהלת**
יצירת מוקד ניהול וידע; קידום תיאום ושיתופי פעולה בין גופים שונים העוסקים בתחום; ריכוז והפצת המידע על הפעילויות המתקיימות בישראל בתחום; הובלת הפעילות הבינלאומית.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

8. **שותפות המנהלת בהרחבת פעילויות למימון מחקר**
שותפות בהקמת מרכז מחקר וידע בתחום; שותפות בהזמנת מחקרים מהאקדמיה ובתוכניות מחקר יישומי באקדמיה.

9. **הרחבת פעילויות למימון יזמות ולקידום התעשייה על ידי המנהלת**
שותפות במימון מחקר ופיתוח תעשייתיים, חדשנות ויזמות בתחום; קידום ניסויים ובדיקות של טכנולוגיות ישראליות; קידום פעילות עסקית, תוך מיצוב ישראל כיעד מועדף להשקעות בתחום.

10. **הרחבת פעילויות למימון פרויקטים בתעשייה על ידי המנהלת**
הובלת פרוייקטים בתעשייה תוך שיתוף פעולה עם גורמים אחרים; השתתפות בפרוייקטים תעשייתיים גדולים או משמעותיים במרחב הקיברנטי ובמימונם.

בחירת פרוייקטים בתעשייה:

11. **בחירת פרוייקטים בתעשייה על פי הצרכים הלאומיים להגנת המדינה במרחב הקיברנטי**
תעדוף בין יוזמות על פי צורך לאומי להגנת המדינה ומשאבי המדינה המוגבלים; אפיון הפרוייקטים השונים באופן שיקדם את התעשייה הישראלית.

2. הקדמה

2.1 השפעת תעשיית הסייבר הישראלית על הגנת המדינה במרחב הקיברנטי

תעשיית סייבר ישראלית חזקה היא רכיב מכריע ביצירה ובשימור על המובילות של מדינת ישראל במרחב הקיברנטי, הן בתחום ההגנה על תשתיות הכלכלה הישראלית, והן בהגנה על המדינה בזירה הביטחונית.
תעשייה חזקה יוצרת:

- מאגר של הון אנושי בתחומים הקיברנטיים, המאפשר גמישות בפיתוח טכנולוגיות חדשות ובהטמעתן בשוק המקומי והעולמי.
- תשתית תעשייתית מקומית לפיתוח מהיר, איכותי וזול של יישומים לצרכים אזרחיים וביטחוניים.
- הגדלת התשואה המשקית למחקר האקדמי בתחום, בשל אפשרויות רבות של מעבר ידע והון אנושי מהמערכת האקדמית לתעשייתית.
- מיתוג המדינה כמוקד עולמי בעל יכולות כלכליות וקשרים גלובליים ענפים במרחב הקיברנטי, שיגביר את ההרתעה מול גורמים עוינים בזירות אחרות, ויחזק את מעמדה של ישראל בזירה הבינלאומית.

הובלה עולמית של מדינת ישראל במרחב הקיברנטי היא רכיב קריטי ביצירת מובילות עולמית עתידית של תעשיית הסייבר הישראלית. שימור המעגל של חיזוק התעשייה על ידי פעילות להגנת המדינה, וחיזוק הגנת המדינה על ידי תעשייה מקומית חזקה, מאפשר שיתוף של שתי המערכות בחלק ניכר מהעלויות הכרוכות בהכשרת הון אנושי, יצירת חדשנות והעמדת תשתיות פיזיות ובסיס יכולות.

תעשיית סייבר ישראלית מובילה, לצד הובלה ביכולות ההגנה על ביטחון המדינה במרחב הקיברנטי, יוצרת ״יתרונות לגודל״, שמגדילים את היעילות הכלכלית של מערכות ההגנה האזרחיות והביטחוניות, ומגבירים באורח משמעותי את מידת התחרותיות של התעשייה הישראלית בעולם.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

תרשים 1 –
קשרי הגומלין בין תעשיית הסייבר בישראל לתשתית היכולות המקומיות במרחב הקיברנטי

2.2 השקעה בפיתוח תעשיית סייבר ישראלית

תעשיית הסייבר הישראלית: בישראל קיימת פעילות עסקית ענפה של חברות טכנולוגיות ישראליות ובינלאומיות, הכוללת מגוון רחב וגדול של חברות הזנק ומשקיעים מקומיים וזרים. בפני המיזם הוצגו נתונים אודות היקפי ההשקעה של לשכת המדען הראשי במשרד התמ״ת בתחומי סייבר (cyber security), או בתחומים ומיזמים משולבי סייבר, וכן אודות היקפי ההשקעה של מערכת ההשכלה הגבוהה בתחומי מדעי המחשב והנדסת אלקטרוניקה. בפני חלק מחברי הוועדה והמיזם הוצגו נתונים מסווגים על היקפי ההשקעה במחקר, פיתוח ויישום של טכנולוגיות ויכולות סייבר בגופי הביטחון. בפני הועמ״ט והמיזם הוצגו סכומים בסדר גודל של מאות מיליוני שקלים שהושקעו בסבסוד של מחקר ופיתוח תעשייתיים במהלך השנים האחרונות, וכן מאות מיליוני שקלים בשנה שהוקצו בהשכלה גבוהה בתחומים רלוונטיים. נתוני מערכת הביטחון מסווגים, ולכן לא הוצגו במלואם לכלל חברי הוועדה, אבל גם בהם מדובר בהיקפים משמעותיים מאוד. על פי נתונים של חברות ציבוריות ושל השקעות הון סיכון, והערכות של מומחים שרואיינו על ידי חברת שלדור, היקף ההשקעה הפרטית בתחומי סייבר ובמערכות ומוצרים משולבי טכנולוגיות סייבר נמדד במיליארדי שקלים בשנים האחרונות. כבר כיום פתרונות סייבר רבים המוצעים בשוק העולמי מבוססים על טכנולוגיה ישראלית, וחברות ישראליות מעורבות בפרוייקטי סייבר רבים בשוק העולמי.

הוועדה אבחנה שתעשיית הסייבר הישראלית היא מהמובילות בשוק העולמי, וכי קיים בסיס פעילות רחב בתחומים קרובים ומשיקים, אשר יכול להוסיף לקידום ולמינוף של מאמצים ביטחוניים לטובת תעשייה זו. חברי הוועדה העריכו כי אין מחסור בהשקעות הון פרטיות בתחום, או בידע לביצוע השקעות נוספות.

הגדרת רכיב הסייבר בהשקעה: רכיב הסייבר (cyber security) קיים בחלק גדול מההשקעות במערכות ובמוצרי תוכנה ותקשורת, ולכן קשה להגדיר מהו ״מוצר סייבר״ בתעשייה - מוצר משולב רכיבי סייבר, או מוצר שכל מטרתו לשמש במרחב הקיברנטי לצרכי הגנה - וקשה להפריד את נתוני ההשקעה בסייבר על ידי המדען הראשי במשרד התמ״ת מכלל ההשקעה בתחומי תוכנה ותקשורת. בדומה, לא ניתן להפריד את הנתונים הגולמיים של המועצה להשכלה גבוהה ולבדלם לתחום הסייבר, המעוגן בתחומי מדעי המחשב והתקשורת.

הצלחת תעשיית הסייבר הישראלית: הצלחת הפעילות העסקית נובעת מהשקעות רבות שנים במחקר, פיתוח ויישום של טכנולוגיות ויכולות במרחב הקיברנטי, או של טכנולוגיות ויכולות בעלות זיקה וממשק אליו:

- תשתית מחקר אקדמית מתקדמת ומובילה בתחומים טכנולוגיים רלוונטיים, והכשרת הון אנושי מתאים במוסדות להשכלה הגבוהה.
- מערך הכשרת כוח אדם במערכת הביטחון, ובסיס לצבירת יכולות מעשיות בתחום.
- מימון פרוייקטים טכנולוגיים ומחקר יישומי במסגרות הביטחוניות הישראליות, ויצירת שוק ראשוני לניסוי ולהטמעת טכנולוגיות חדשניות.
- קהילת יזמים ותעשיינים, המקדמים פעילות עסקית ופיתוח של מוצרים ושירותים בתחום, תוך חתירה להובלה טכנולוגית ויצירת קשרים עסקיים ענפים בעולם.
- שוק פרטי תוסס להשקעות הון סיכון ולהשקעות טכנולוגיות, ופעילות ענפה של חברות רב לאומיות מובילות בישראל.
- סבסוד מחקר ופיתוח תעשייתיים בתחום, באמצעות כלי עידוד המחקר והפיתוח במשרד התעשייה והמסחר לאורך שנים רבות.

לאור כל זאת, נראה כי פיתוח ממוקד נוסף של תעשיית הסייבר הישראלית צריך להיעשות סביב קידום צרכי ההגנה הלאומית של מדינת ישראל במרחב הקיברנטי, ומינופו למען קידום התעשייה בישראל.

המשך פיתוח עתידי של תעשיית הסייבר בישראל: המשך פיתוח התעשייה המקומית צריך להתבסס על העובדה כי האתגרים החדשים שהמרחב הקיברנטי מציב להגנה על המדינה ועל הכלכלה המקומית ידרשו יכולות טכנולוגיות ומדיניתיות חדשות:

- על מנת להיות בחזית המוכנות לאתגרים החדשים יהיה צורך לפתח תשתית של יכולות מקומיות באופן קבוע.
- התשתית הקריטית של היכולות המקומיות משמשת גם כתשתית קריטית להמשך הפיתוח העתידי של התעשייה הישראלית בתחום הסייבר.
- לנוכח המובילות העולמית של התעשייה הישראלית ושל התשתית האקדמית בתחום כיום, זול יותר לשמר את המובילות ולבצע פיתוח מקומי בישראל, מאשר לרכוש מערכות מחו״ל (בתרחיש שבו מגבלות ביטחוניות היו מאפשרות זאת).
- קוטנה של המדינה, הקרבה הפיזית בין המערכות והגורמים בתחום והרישות (Networking) הנרחב ביניהם, יוצרים חזית אזרחית, ממשלתית, ביטחונית אחידה שתתרום רבות להמשך קידום התחום ולהגדלת הביטחון במרחב הקיברנטי, ותהווה קרקע פורייה לפיתוח מערכות הגנה משולבות חדשניות ומתקדמות.

מינופן של הפעילויות לעיל, המהוות תשתית קריטית ואיכותית לתעשייה הישראלית בתחום, לצורך קידום מנוע צמיחה משמעותי כרוך בעלות נמוכה ביותר. קידום תעשיית הסייבר האזרחית בישראל צריך להיעשות כרובד נוסף מעל סל פעילויות ההגנה האזרחיות, שמטרתו היא יצירת יכולות כלליות של התעשייה הישראלית בתחום

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

קידום תעשיית הסייבר האזרחית בישראל: בהינתן שהתשתית לקיומה של תעשיית סייבר ישראלית ולפיתוחן של יכולות חדשות מובטחת בשל צרכי הגנת המדינה והביטחון, קידום התעשייה אל עבר הובלה בשווקים הגלובאליים מצריך:

- **אינטגרציה** בין כלל הפעילויות המתקיימות בזירות ההגנה האזרחיות והביטחוניות, באקדמיה ובתעשייה.
- **פיתוח ממשקים חדשים** לשיתופי פעולה בין הגורמים השונים במערכות ההגנה האזרחית, מערכות הביטחון והאקדמיה ובין שחקני השוק הפרטי (יזמים, תעשייה, משקיעים ולקוחות).
- **יצירת תנאי סביבה תומכים** לפיתוח טכנולוגיות ויכולות חדשות והטמעתן, באמצעות הרגולציה על השוק המקומי ועל הייצוא, והמיקום בזירות הבינלאומיות.

את הפעילות לקידום תעשיית הסייבר האזרחית צריך לבצע גוף בעל קשרים ענפים עם מערכות ההגנה האזרחית ומערכות הביטחון מחד, ובעל הכרות מעמיקה עם פיתוח הטכנולוגיות הרלוונטיות והתפתחות האיומים מאידך, בשל החשיבות הגבוהה לאינטגרציה מול מערכות ההגנה האזרחיות והמערכות הביטחוניות, וליצירת ממשקים חדשים עימן לאורך זמן

רובד נוסף זה של קידום פיתוח התעשייה, במקביל לפעילויות ההגנה, יהיה זול יחסית לסך כל ההשקעות בתחום, והתשואה המערכתית והכלכלית שלו עשויה להיות גבוהה מאוד, כפי שיתואר בחלק העוסק בהערכת הפוטנציאל הכלכלי-תעשייתי של הפעילות התעשייתית הנלווית לפרוייקטים בתחום.

2.3 התערבות הממשלה בפיתוח תעשיית הסייבר

פעילות הממשלה במרחב הקיברנטי: במהלך עבודת הוועדה, התוודעו חבריה לפעילות של גופי הממשלה השונים עם השוק הפרטי, ובפרט עם התעשייה, בתחום הסייבר. במובן זה, לפעילות הממשלה בזירת המרחב הקיברנטי ולהשפעותיה עליו יש משקל רב, וכן תפקידים רבים:

- רגולטור, הקובע את כללי הפעילות בשוק המקומי (פיקוח על פעילות עסקית) ומול השוק העולמי (פיקוח יצוא, אמנות והסכמים לשיתוף פעולה ועוד).
- צרכן, האחראי לחלק ניכר מהביקוש המקומי לשירותים, מערכות ומוצרים.
- יצרן, הן של פיתוחים עצמיים והן של מימון פיתוח במיקור חוץ.
- מעורבות ישירה: מימון (סבסוד) מחקר אקדמי והשכלה גבוהה, שותפות במימון (סבסוד) מו"פ תעשייתי ומיסוי.

התערבות ממשלתית ו"כשלי שוק": המונח "כשל שוק" מתייחס לחוסר יכולתו של שוק פרטי להביא להקצאה תחרותית של משאבים למיקסום תועלת הכלל. לחברי הוועדה היה חשוב להבליט את הנושאים שעלו, ולפרט את אופן ההתערבות הממשלתית ואת "כשלי השוק", כמו גם את השפעתה של פעילות הממשלה על השוק הפרטי:

- הגנה על המדינה היא **מוצר ציבורי** מובהק, ולכן הממשלה תמשיך להיות מעורבת בהגנה במרחב הקיברנטי.
- יש **יתרונות לגודל** בקיום תעשייה אזרחית וביטחונית לצד יכולות מערכת הביטחון.
- מתחוללת **זליגת ידע והשפעות חיצוניות** (Externalities) מפעילות מחקר ופיתוח ומביסוס תעשייה עתירת ידע.
- הממשלה קובעת את **רמת ההפרטה** של פעילות פיתוח שימושים ביטחוניים, ובכך משפיעה על גובה זליגת הידע ועל היקף הפעילות בתעשייה. הגדלת היקפי המו"פ בתעשייה באמצעות הוצאת פיתוח יכולות סייבר מתוך מערכת הביטחון אל התעשייה הביטחונית, היא מהלך הממשיך את ההפרטה המוצלחת של התעשיות הביטחוניות (לפעילות במסגרת חברות, בין אם בבעלות ממשלתית או פרטית) שהואצה מאז סוף שנות השמונים ותחילת שנות התשעים.
- **הממשלה כרגולטור** קובעת רבים מכללי השוק, ולכן הקלה או הקשחה של רגולציה (כמו גם של המבנה שלה) משפיעות באופן מהותי על פיתוח התעשייה.
- **רמת הסיכון** של משקיע ויזם במיזם בודד גבוהה באופן משמעותי מהסיכון המשקי, בשל הפיזור הרב של המשק על פני מגוון של השקעות. אופי פעילות הממשלה והתערבותה קובע, בין השאר, את רמת הסיכון

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

למיזם בודד, כפי שמשתקפת בעיני המשקיע והיזם.

- פעילות ממשלתית יכולה **ליצור שוק** באמצעות קביעת בנצ'מרק וכללים חדשים, למשל לשווקים פיננסיים מפוקחי רגולציה (כגון ביטוח ובנקאות).
- פעילות ממשלתית יכולה **ליצור תזמון** בין שחקנים פרטיים, שללא כניסה ברורה של הממשלה למתווה פעילות לא יוכלו לאמוד את הסיכון ואת המהלכים (הן הממשלתיים והן העסקיים) בתחום.
- פעילות עידוד תעשייה יכולה להתבצע על ידי **חיזוק הרישות** בין השחקנים (networking) **והגברת זרימת המידע** אודות הפעילויות הממשלתיות והעסקיות בשוק (information flow). במקרה זה, השחקנים הפרטיים הם לעיתים קטנים מכדי ליהנות מ"מוצר ציבורי", ולעיתים שחקנים בודדים אף אינם מרוויחים (אלא רק כלל המשק).

לנוכח המעורבות הממשלתית הכבדה השאלה המרכזית העומדת בפני קובעי המדיניות הממשלתית היא לא אם הממשלה צריכה להתערב בשוק, אלא באיזה אופן ועוצמה, ומהי הדרך המיטבית להשפיע על פעילות התעשייה המקומית באמצעות ההתערבות.

3. בחינת תועלות כלכליות ותעדוף בין יוזמות

3.1 מדיניות תעשייתית ותעדוף בין תחומים ויוזמות

בדיוני הוועדה עלתה שאלה מרכזית, המעוררת התחבטות משמעותית בכל הדרגים המקצועיים הגבוהים, בנוגע למדיניות מחקר ופיתוח תעשייתי ממוקדת אל מול מדיניות מחקר ופיתוח ניטראלית, בפרט בתחומי פעילות המדען הראשי במשרד התמ"ת. בארבעת העשורים האחרונים נהוגה במדינת ישראל מדיניות מחקר ופיתוח תעשייתי ניטראלית, ושאלת המיקוד בתחומי מחקר ופיתוח תעשייתיים, וכן אופן בחירתם, עדיין לא מוסדרת ברמת קבלת החלטות, קביעת מדיניות והפעלתה.

הוועדה לא דנה בשאלה זו, ולא בחנה את ההשקעה בתחום הסייבר אל מול תחומים אחרים, אולם עלו בה מספר תובנות לגבי תעשיית הסייבר, שיכולות להשפיע על אופן הפעלת המדיניות בנוגע לתעשייה זו:

- ברובד הבסיסי של **תשתית לפעילות תעשייתית, וגיבוש מסה קריטית** להתנעת פעילות בתחום, לא אובחן מחסור משמעותי בפעילות ובתשתיות מחקר ופיתוח, אשר חוסם את הצמיחה בתחום. חשוב לציין, כי עלו בעיות רבות ואתגרים רבים, חלקם משותפים לכלל טכנולוגיות המידע, וחלקם פרטניים לתחום הסייבר.
- **בישראל קיימת כבר כיום פעילות עסקית ענפה במרחב הקיברנטי**, של חברות טכנולוגיות ישראליות ובינלאומיות, של מגוון רחב וגדול של חברות הזנק ושל משקיעים מקומיים ובינלאומיים, הנובעת מהשקעות רבות ולאורך שנים במחקר, פיתוח ויישום של טכנולוגיות קיברנטיות או בעלות זיקה וממשק לתחום. לאור זאת, הוועדה צופה כי גם ללא התערבות ממוקדת, או הסטה מוגדרת, של משאבים, יגדל הנתח של התעשייה בסך כל חלוקת התמיכה של המדען הראשי, הן בשל השגת יתרונות יחסיים בתחום, והן בשל גידול בהיקף התעשייה. עם זאת, חשוב לציין, כי פעילות עסקית זו היא תוצר של פעילות ממשלתית משמעותית, ולכן גם התפתחותה העתידית תלויה רבות בעתיד הפעילות הממשלתית.
- מבחינה ניהולית, **אין כיום גוף מרכזי המנהל בצורה ממוקדת את קידום תחום הסייבר.** הוועדה מצביעה על כך שהמעורבות הממשלתית הכבדה בתחום, ורמת מורכבותו הגבוהה, דורשים מומחיות ייחודית ותשומת לב לפיתוח התעשייה, וכן טיפול פרטני בסוגיות עקרוניות העשויות לחסום באופן משמעותי את צמיחתו העתידית.

לגבי המלצה על יוזמות שהוצעו במיזם הקיברנטי, **החליטה הוועדה שלא לתעדף בין היוזמות השונות**, כיוון שחברי הוועדה מסכימים על כך שהתעדוף צריך להיעשות לפי הצורך הלאומי ביוזמות להגנת המדינה, ועל פי מגבלת המשאבים הכוללת העומדת בפני המיזם. למשל, יוזמות שאינן מעניקות יתרונות יחסיים לתעשייה הישראלית, או תשתית לבנייתם העתידית, יכולות להיות מתועדפות בשל חשיבותן להגנת המדינה.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

3.2 משמעות התועלות הכלכליות בבחינת המיזם והיוזמות השונות

הוועדה, באמצעות חברת ייעוץ חיצונית (שלדור), ובסיוע של המכון הישראלי למדיניות מדע, טכנולוגיה וחדשנות, בחנה את התועלות הכלכליות של הפרוייקטים השונים שהציעו הוועדות במיזם, ומצאה לנכון להאיר מספר סוגיות עקרוניות הנוגעות לאופן הבחירה בין מיזמים, ולהערכת התועלת המשקית המופחתת בעקבות הסטת משאבים מוגבלים במשק מתחום אחר:

- הפרוייקטים השונים במיזם אינם נבחנים מול אלטרנטיבות אחרות למחקר ופיתוח בתחומים אחרים, שכן מטרתם היא לקדם את הגנת המדינה במרחב הקיברנטי. בשל כך, ממליצה הוועדה לראות את התועלת הכלכלית כרכיב משלים לקבלת החלטה, ולא כרכיב בודד לבחירת מימון פרוייקטים.
- יש להביא בחשבון את המגבלה המשקית של הון אנושי מיומן הזמין לתחומי טכנולוגיות המידע והתקשורת (שיעור אבטלה אפסי), ואת העובדה שכיוון שחלק ניכר מההשקעות בתחום יתורגמו להעסקת כוח אדם, תהיה הסטת משאבים (עובדים) מתחומים אחרים. עובדה זו מפחיתה באופן ניכר את הערכת התועלת המשקית הכלכלית, הנובעת מהעסקת כוח אדם חדש בתחום, שכן יש לנקות ממנה את הירידה בתוצר המשקי עקב עזיבתו את מקום העבודה הקודם. מעבר לכך, הדבר גם עלול להביא לעליית שכר רוחבית נוספת ולירידה בתחרותיות של ענפי טכנולוגיות מידע ותקשורת אחרים.
- חשוב מאד להבין אם צברי היוזמות והפרוייקטים בהקבצים השונים יקדמו גם את התעשייה המקומית ומובילותה העולמית. במקביל, חשוב גם לבחון את תמונת הראי המשלימה, כלומר עד כמה תעשייה חזקה בתת-תחום משפיעה על רמת המוכנות של המדינה.

3.3 עקרונות כלליים לבחינת התועלות הכלכליות

במהלך עבודת הוועדה, סוכמו פרמטרים לניתוח התועלות הכלכליות מהפרוייקטים ומהיוזמות שהציעו תתי הוועדות. הפרמטרים תורגמו לסט של שאלות, שהוצגו לתתי הוועדות בתהליך של שילוב בין תוצריהן לבין הוועדה הכלכלית ויועצי חברת שלדור.

ניתוח התועלות הכלכליות נעשה לגבי הקבצי יוזמות, והתמקד בארבעה תחומים, שיוצרים יחדיו תמונה של תועלת מקרו כלכלית למשק: זיהוי מקור ליתרון תחרותי למדינת ישראל; בחינת הצורך והאופן להתערבות ממשלתית; הערכת היקף הפוטנציאל הכלכלי; הערכת העלויות למימוש הפוטנציאל הכלכלי.
להלן השאלות על היוזמות והפרוייקטים, מחולקות לארבעת תחומי הניתוח:

1. זיהוי מקור ליתרון תחרותי למדינת ישראל

- **מהם הנכסים התחרותיים של ישראל בתחומים המזוהים?**
  - יכולות מוכחות בתחום/ים משיקים
  - הון אנושי איכותי ומוכשר לתחום
  - תדמית / ׳מותג׳ של מדינת ישראל
  - חברות ישראליות מובילות בתחומן
  - פטנטים/ידע ייחודי שפותח בישראל
  - היקפי השקעות מו״פ
  - מצבורי ידע בצה״ל
  - יחסי סחר עם מדינות שיש להן פוטנציאל להפוך לצרכנים

- **מהו מצב השוק והתחרות בעולם ומהן ההשלכות על היכולת התחרותית של מדינת ישראל?**
  - גדלי השוק העולמי למוצר הישיר / מוצרים דומים נגזרים
  - שוק בתולי או בשל / mature?
  - צמיחה / ביקוש הולך וגובר?
  - מאפייני החברות הפעילות
  - יוזמות רלוונטיות המותנעות בקרב מדינות בתחום
  - האם יש סחר בינ"ל בתחום, או שרוב העסקאות מתבצעות בתוך המדינות?
  - תרומה ל-GDP, ליצוא ולתעסוקה
  - פעילות רגולטורית מזוהה (האם קיימות מגמות רגולטוריות בעולם העשויות להשפיע על הביקוש?)

2. בחינת הצורך להתערבות ממשלתית

- **האם קיים כשל שוק / חסמים שדורש התערבות ממשלתית?**
  - חלופת השקעה פרטית
  - האם ללא התערבות עשויות להיות יוזמות פרטיות שיפתרו את הבעיה?
  - כיצד ניתן לעודד יוזמות פרטיות לפתרון הבעיה?
  - מה צפוי לקרות ללא התערבות מצד הממשלה?
  - חסמים רגולטוריים?
  - חסמים לזרימת מידע?
  - האם נדרשת יצירת ביקושים ע"י הממשלה?
  - האם נדרשת הקצאת תמריצים לאקדמיה?
  - האם נדרשת הקצאת תמריצים ללימודי סטודנטים?

- **האם נדרשת התערבות ממשלתית על מנת ליצור סינרגיות?**
  - האם נדרשת התערבות ממשלתית על מנת ליצור קשרים / שיתופי פעולה בין מגזרים, שיניבו תועלות משמעותיות יותר מהתקדמות בתחום בצורה נפרדת? מהי?
  - האם היוזמות הכלולות בהקבץ תלויות בהקמת תשתית לאומית משותפת? מהי?

- **איך צריכה להיראות ההתערבות? כספית? רגולטיבית? הקמת גופים נוספים?**

3. הערכת היקף הפוטנציאל

- **מהו הפוטנציאל המשקי / תחרותי בכל אחד מהתחומים/הקבצים המזוהים?**
  - הכנסות ישירות (שוק מקומי, שוק בינ"ל)
  - ייצוא למדינות ידידותיות או לכלל המדינות?
  - הכנסות עקיפות (כולל הנפקות/מכירת חברות?)
  - תעסוקה (בהתפלגות לפי תחומי עיסוק)
    - האם צפויה השפעה על הפריפריה?
    - התפתחות של תחומים חדשים
    - אפקט המובילות והחדשנות
    - תרומה ל-GDP וליצוא (שיפור במאזן תשלומים)
    - טווח ההשפעה של היוזמה (כרונולוגית)
  - **מהו הפוטנציאל הבלתי מוחשי?**
    - שיתופי פעולה בין גורמים (ביטחון, אקדמיה, תעשייה, גורמים בינ"ל)
    - שיפור רמת האבטחה ותחושת ביטחון המידע בישראל / מניעת נזק פוטנציאלי
    - פטנטים / ידע

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4. הערכת עלויות נדרשות למימוש הפוטנציאל

- **מהו היקף ההשקעות הנדרש מהמדינה בתחומי הפעילות המזוהים?**
  - מהם המשאבים הדרושים?
  - מהן ההשקעות הדרושות?
- **מה מסתמן כמקור המימון האופטימלי (ממשלתי, פרטי, מדינה אחרת)?**
  - האם וכיצד ניתן ליצור שותפות עם גופים שונים למימון הקמת / תפעול היוזמה?
  - האם יש נכונות מצד החברות הצרכניות בתעשייה לשאת בעלויות? אם כן, כיצד?
- **מהם לוחות הזמנים העקרוניים להשקעות?**

3.4 מתודולוגיית בחינת התועלות הכלכליות – ברמה הכללית והפרטנית

1. יצירת הקבצים של יוזמות

אוסף היוזמות, הפרוייקטים והמהלכים, שוועדות העומק של המיזם הציעו, אוגדו להקבצים הומוגניים ככל הניתן, על מנת לנתח אותם באופן אחיד. ההקבצים הוגדרו על בסיס:

- זיהוי של קשרי גומלין בין יוזמות - תמה מאחדת בין היוזמות, מתן מענה משולב לבעיה, פנייה לתחום זהה / דומה
- הערכת השפעה סינרגתית - השפעה כוללת משמעותית יותר מביצוע היוזמות בצורה נפרדת, חסכון בעלויות המימוש כתוצאה משילוב היוזמות, "פריצת דרך" בתחום דומה, שיתופי פעולה בין גורמים

2. הערכת התרומה / הפוטנציאל הכלכלי של ההקבצים

בהתאם לרמת הקונקרטיזציה הנוכחית של היוזמות שהציעו ועדות העומק השונות, בוצעה הערכה יחסית של האטרקטיביות הכלכלית והתרומה הפוטנציאלית לפיתוח תעשיית הסייבר של כל הקבץ, על פי המרחבים הבאים:

- היקף הפוטנציאל / תרומה של ההקבצים - הערכת הפוטנציאל הכלכלי המשקי והבלתי מוחשי של ההקבץ, ו/או השפעה על פוטנציאל כלכלי.
- תרומה ליצירת יתרון תחרותי ברמת המדינה - זיהוי הנכסים התחרותיים שעליהם ניתן להתבסס בביצוע ההקבץ, ו/או השפעתו על בניית / חיזוק הנכסים לנוכח ניתוח מצב השוק העולמי הרלוונטי.
- השקעות למימוש הפוטנציאל - זיהוי והערכה ראשונית של ההוצאות העיקריות הנדרשות לביצוע ההקבץ, במונחים של השקעות הקמה והוצאות שוטפות לתפעול (5 שנתי).

תרשים 2 – הערכת אטרקטיביות כלכלית של פרויקטים: פרמטרים עיקריים

הערכת היקף הפוטנציאל

מהו הפוטנציאל המשקי בכל הקבץ?
- הכנסות ישירות (שוק מקומי, שוק בינ"ל) ועקיפות
- תעסוקה (בהתפלגות לפי תחומי עיסוק)
- התפתחות של תחומים חדשים

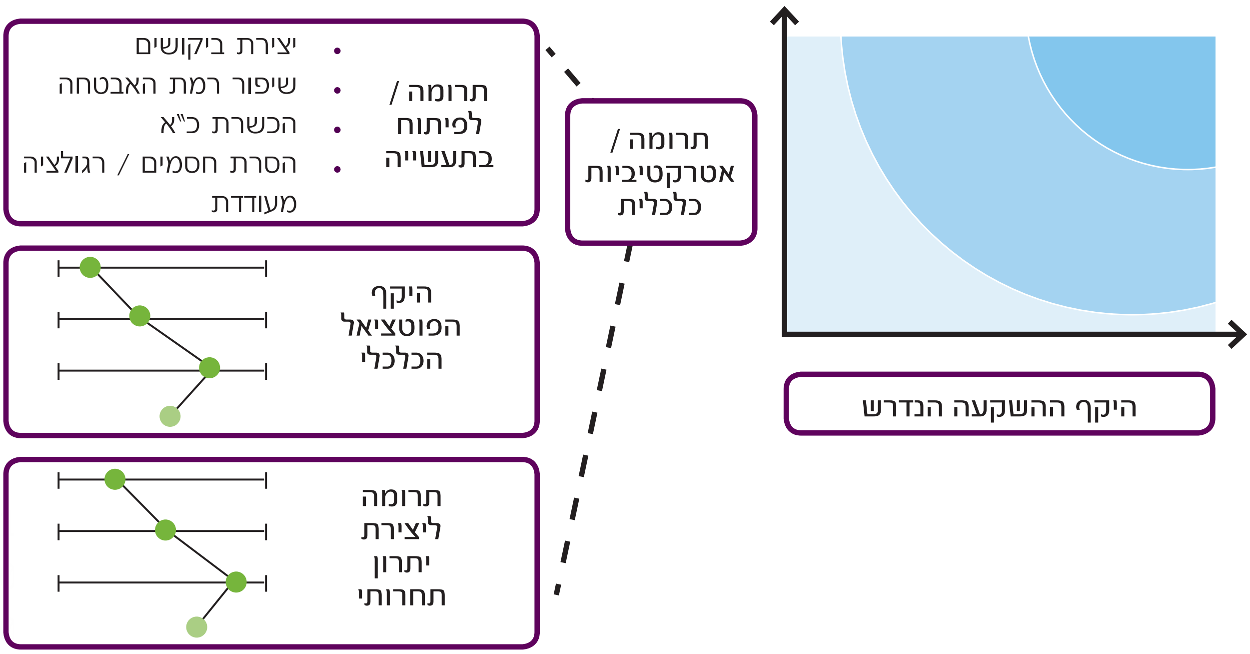
מהו הפוטנציאל הבלתי מוחשי?
- שיתופי פעולה נוצרים בין גורמים (בטחון, אקדמיה, תעשייה, גורמים בינ"ל)
- שיפור רמת האבטחה / מניעת נזק פוטנציאלי פטנטים / ידע

הערכת התרומה ליצירת יתרון תחרותי

מהם הנכסים התחרותיים של ישראל / תרומה צפויה לנכסים בתחום?
- יכולת מוכחת בתחום
- תדמית / "מותג" של מדינת ישראל
- חברות ישראליות מובילות בתחום
- פטנטים / ידע ייחודי שפותח בישראל
- ידע צבור בצה"ל / מע' הבטחון

מהו מצב השוק והתחרות בעולם?
- שוק בתולי או בשל
- חברות דומיננטיות או חלשות
- שוק ריכוזי או מבוזר

תרשים 3 – הערכת פוטנציאל כלכלי מתודולוגיה



לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4. הקבצי הפעילויות בתחום והערכת פוטנציאל כלכלי-תעשייתי

פרק זה מפרט את היוזמות שהציעו ועדות הליבה, לאחר שאוגדו לתשעה הקבצים אחידים. כל אחד מההקבצים מציג את הניתוחים, שביצעה חברת שלדור, לצורך הערכה ראשונית של העלות, וניתוח של התועלות הכלכליות העולות מהיוזמות, על פי הפרמטרים שהוועדה גיבשה, והמתודה שתוארה בפרק הקודם.

4.1 מעטפת הגנה למדינה במרחב הקיברנטי

1. יוזמות ההקבץ

- מערך זיהוי, דיווח ואיסוף אירועים חריגים.
- מערכת ניטור בכניסות למדינה ובנקודות מפתח בתוכה.
- מערכת שו"ב לאינטגרציית תקינות שירותים שונים.
- פטרול מדינתי סייברי בגבולות ובתוכם, תוך שמירה על זכויות הפרט.
- חדר מצב מדינתי, להצגת תמונת מצב עדכנית ותאום מערכי הפעולה.
- טכנולוגיות לאיסוף המידע תוך שמירת פרטיות האזרח / הגוף המסחרי.

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- חשיפה מופחתת לתקיפות ומניעת נזקים לממשלה, מערכת הביטחון, תשתיות קריטיות וגורמים נוספים ע"י ניטור ובקרה (intrusion detection & prevention).
- פרוייקט/ים גדול/ים ע"י חברות בתחום.
- פוטנציאל לפרוייקטים דומים בחו"ל בתחום גדול וצומח (בהנחת אישורי יצוא).
- בסיס לידע הניתן למימוש בתחומים נוספים.

3. הפוטנציאל הכלכלי של ההקבץ

הדרישה למעטפת הגנת סייבר למדינה, יוצרת ביקוש המאפשר את הפיתוח הבסיסי. כנגזרת מכך, נפתח שוק לחברות ישראליות ליצוא מוצריהן. שוק מערכות הגנת סייבר לאומיות מוערך במיליארדי דולרים, והנתח הרלוונטי עבור ישראל מתוכו מוערך במאות מיליוני דולרים. בניית המכ"מ תדרוש מחקר ופיתוח בתחום זיהוי אנומליות, שהינו בעל ערך (כנגזרת) גם בתחומים אחרים. ההכנסות הפוטנציאליות ממוצרים מבוססי טכנולוגיות הבסיס (למידה ממוחשבת, Data Analytics, כריית מידע) צפויות להיות משמעותיות ביותר.
מדובר בטכנולוגיות שזוהו כטכנולוגיות מפתח במציאות של שטף מידע גדל (לצורך ההמחשה, גודל שוק ה-Data Analytics בשנת 2007 הוערך ב- $5B, צפי גודל שוק לטכנולוגיות Data Analytics בשנת 2015, לתחום ה- Grid בלבד, מוערך ב- $4.2B, בעלות אפליקציות רבות ומגוונות, שפיתוחן צפוי להשפיע באופן משמעותי על השווקים הפוטנציאליים הנפתחים.
זאת ועוד, יישום ההקבץ ישפר את רמת הגנה וימנע נזק משמעותי פוטנציאלי לתשתיות הקריטיות של המדינה ולרשתות מחשוב של הממשלה, מערכת הביטחון וגופים אחרים.

4. תרומה ליצירת יתרון תחרותי של המשק

בשוק מעטפות הגנת הסייבר פועלות מעט חברות גדולות. המשך בפיתוח התחום יאפשר לגורמים ישראלים דריסת רגל בשוק כגורם משמעותי ומשפיע. חלק מטכנולוגיות הבסיס הכרוכות בפיתוח מעטפות הגנת סייבר נמצאות עדיין בחיתוליהן. פיתוחן עשוי להעניק יתרון תחרותי בעתיד מול חברות בינ"ל, שלא מפתחות את התחום. תרומה נגזרת נוספת של בניית המכ"מ, מתבטאת ביצירת מאגר אירועים ותעבורת מידע, שהוא בגדר נכס תחרותי לחברות אבטחת מידע, וצפוי להעצים פיתוח של מוצרים שכיום קשה לפתחם בשל מחסור במידע.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 400-500M₪, בהתבסס על ההנחות/הערכות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
פיתוח מכ"מ	125
הקמת מרכז פיזי	15
תחזוקה (שנתי)	35
משכורות (שנתי)	20

הנחת עבודה היא כי תחזוקת המערכת ותשלום משכורות מתבצע לאחר תחילת פעילות המערכת ולאחר סיום פיתוחה, פרק זמן שהוערך בצורה שמרנית בשלוש שנים.

4.2 תשתיות פיתוח לטכנולוגיות המרחב הקיברנטי

1. יוזמות ההקבץ

- הקמת סימולטור מבוזר לדימוי סביבות סייבר ואימון.
- הקמת מכון לבחינת קוד וחיסון מוצרי תוכנה ומעבדת הסמכה.
- יצירת מאגר אירועים ותעבורת מידע של ניסיונות תקיפה חיצוניים לשם מו"פ טכנולוגיות הגנה.
- יצירת שירות מוזל של תקיפות ארגוניות למטרות בחינת חוסן המערכות.

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- הקמת תשתית המאפשרת מחקר ופיתוח בתחום - יצירת IP, בסיס ליתרון תחרותי.
- שיפור רמת האבטחה של גורמים רבים ע"י בדיקות אמינות וחסינות.
- ביצוע פרוייקטים ע"י גורמים בתעשייה, כמו גם פוטנציאל לפרוייקטים דומים ונלווים בישראל ובחו"ל.
- הקמת תשתית של מחקר ופיתוח בתחום - יצירת IP, בסיס ליתרון תחרותי.
- שיפור רמת האבטחה של גורמים רבים באמצעות בדיקות אמינות וחסינות.

3. הפוטנציאל הכלכלי של ההקבץ

יישום הקבץ זה הוא בגדר תשתית מדינה, שכל חברה בפני עצמה אינה יכולה להצדיק את הקמתה. כתשתית, ערכה הכלכלי נובע גם מערכים כלכליים ישירים, אך בעיקר מערכים נגזרים, שהתשתית תאפשר להשיגם. בניית תשתית סימולציה, מכון לחיסון ובחינת מוצרי קוד ויצירת מאגר אירועים ותעבורת מידע, ישפרו את איכות המוצרים המפותחים בחברות השונות, ויאפשרו פיתוח של מוצרים שכיום קשה לפתחם, עקב מחסור בתשתיות/מידע. בנוסף, היוזמות בהקבץ זה יביאו להגברת חוסן המערכות המפותחות, ויפחיתו את הנזק הפוטנציאלי מתקיפת סייבר.

4. תרומה ליצירת יתרון תחרותי של המשק

כאמור, היוזמות בהקבץ זה עוסקות בהקמת תשתיות פיתוח סייבר ברמה לאומית. תשתית הפיתוח תאפשר לקיים מחקרים מתקדמים ולפתח מוצרים איכותיים ברמה עולמית, שיעניקו לחברות בתחום יכולות משמעותיות, שאותן (בסבירות גבוהה) לא היו מפתחות באופן עצמאי, ויקנו להן יתרון עולמי אל מול חברות בינ"ל אחרות. שוק הסייבר הינו שוק מגוון ודינמי, שקיימות ונוצרות בו נישות רבות המאפשרות צמיחה פוטנציאלית והתפתחות של חברות ישראליות. יוזמות ההקבץ בעלות פוטנציאל להשפיע רבות על יכולות בתחום הסייבר, אשר יאפשרו לחברות ישראליות להתבסס בנישות מגוונות קיימות / עתידיות בשוק.
מוצרים חדשניים, המפותחים על בסיס התשתית שתיבנה באמצעות יוזמות ההקבץ, יתרמו גם באופן משמעותי לשימור וחיזוק איכותו של המותג הישראלי כנותן פתרונות מצוינים ועדכניים בתחום.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות ל-5 שנים) - 150-200M₪, בהתבסס על ההערכות/הנחות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)	
סימולטור סייבר	עלות מוערכת להקמת סימולטור	70
	חידוש משק	15
	כ"א ומשכורות (לחמש שנים)	50
מעבדת הסמכה	עלות מוערכת להקמת מעבדת הסמכה	20
	כ"א ומשכורות (לחמש שנים)	10
	סבסוד תמיכה ב- Pen Test (שנתי)	5
	תחזוקת מאגר (שנתי)	2

הנחת עבודה היא כי תחזוקת המערכת ותשלום משכורות מתבצע לאחר תחילת פעילות המערכות ולאחר סיום פיתוחה, פרק זמן שהוערך בצורה שמרנית בשלוש שנים

4.3 עידוד מו"פ בתחומי המרחב הקיברנטי וחישוב–על

1. יוזמות ההקבץ

- הקמת מרכז מצוינות לתחומים של חישוב-על והמרחב הקיברנטי.
- עידוד ביצוע מחקרים בתחום במוסדות הקיימים באקדמיה ובתעשייה.

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- עידוד, יצירה וניוד של ידע מקצועי בין מערכת הביטחון לבין האקדמיה.
- הקמת ציוד ותשתית למו"פ בתחום ה-HPC והמרחב הקיברנטי.
- פריצה לתחומים בתוליים עם פוטנציאל צמיחה ומובילות עולמית (בעיקר בהקשר של Exascale).
- עידוד פיתוח נוסף של clusters חזקים קיימים.
- פיתוח כוח אדם איכותי; שימור/החזרת "מוחות".

3. הפוטנציאל הכלכלי של ההקבץ

שוק הסייבר העולמי עצום ומוערך בעשרות מיליארדי דולרים (לצורך ההשוואה, ה- U.S. Federal Cybersecurity marke לשנים 2010-2015 מוערך ב- $55B וצפוי לצמוח בממוצע של 6.2% במהלך שנים אלה).
מענקי עידוד וקידום מו"פ מאפשרים פיתוח של טכנולוגיות אשר יהוו בסיס למגוון מוצרים חדשניים בתחומים צומחים ומבטיחים בשוק, והקמה של חברות שיגדילו את מספר המועסקים במשק.
שוק מוצרי ה- HPC מוערך בכ- $9B, מתוכו נישות ממוקדות רלוונטיות התופסות אחוזים מסוימים מתוכו.

מרכז המצוינות יאפשר התפתחותם של תחומים חדשים הנגזרים ממחקר בסיסי הן בתחומי ה-HPC והן בתחומי הסייבר, מחקר אותו לא מקיימות חברות מסחריות באופן עצמאי. שיפור הידע והיכולות בתחום חישוב-העל והמרחב הקיברנטי צפוי להגדיל את הפוטנציאל הרלוונטי לחברות ישראליות בנישות בתחומים בהן הן פעילות כבר היום ואולי לפתוח נישות רלבנטיות נוספות. השפעה על הכנסות ב"נגזרת" לתעשייה צפויה גם כתוצאה ממענקי עידוד וקידום מו"פ המגדילים את כמות המוצרים החדשניים הנוצרים ע"י חברות.

בנוסף לידע המחקרי והמסחרי הנוצר באופן ישיר בתחומי ה- HPC והסייבר, הקבץ זה צפוי לסייע בחיזוק תחומים הנעזרים/נשענים על HPC וסייבר ככלים לצרכי מו"פ - כגון תעשיית הפיננסיים והאנימציה ב- HPC

ותעשיות הפיננסים והמסחר האלקטרוני במרחב הסייבר.
מרכז זה גם יעודד וירחיב שת"פ בין האקדמיה לתעשייה ולמערכת הביטחון והגדלת נצילותו לטובת צרכים והזדמנויות תעשייתיות כלכליות (כמו גם חיזוק היכולות במע' הביטחון).

4. תרומה ליצירת יתרון תחרותי של המשק

הפעלת מדיניות לעידוד מו"פ מתרגמת לחדשנות טכנולוגית אשר מובילה למוצרים איכותיים המגדילים את היכולות הקיימות כיום. בנוסף מאפשר הדבר יצירה של חברות חדשות מובילות בתחומן, קידום ודחיפה של חברות קיימות ויצירת פטנטים חדשים.

למדינת ישראל יש כיום מספר מרכזי עוצמה בתחום ה-HPC, כגון מובילת בתחום תקשורת מהירה ביותר (Interconnect), כגון חברת מלנוקס ומרכזי מו"פ של חברות בינ"ל. המשך השקעה בתחום תבסס חוזקות אלו, ותתרום לזיהוי מקורות ליצירת יתרונות נוספים.

מעבר לפעילות הישירה בהקשר למחשוב על, בישראל קיים הקבץ של חברות (רובן ממוקד בתחום עיבוד התמונה לסוגיו), אשר במוצריהם משולב כושר חישוב גדול (HPC-Embedded) - מחקר התומך בצורכיהן ישולב / יתרום למאמצים הרלוונטיים לתחום חישוב-העל הכללי. כלי ניהול משאבים בחישוב מקבילי / מבוזר ישרתו גם צביר עיבוד תמונה קיים, המפתח מוצרי HPC Embedded, אשר ישמש כ"קטר" לפיתוח טכנולוגיות -HPC Embedded הצפויות לצמוח עם התקדמות טכנולוגיות המזעור.

בתחום הסייבר, תרומת יוזמות הקבץ זה ליצירת יתרון תחרותי של המשק הינן הקניית היכולת לביצוע מחקרים מתקדמים המהווים תשתית מדעית לפיתוח מוצרים איכותיים בתחום המרחב הקיברנטי ברמה עולמית, בדומה להקבץ "תשתיות פיתוח לטכנולוגיות המרחב הקיברנטי".

כפי שצוין לעיל, שוק הסייבר המגוון והדינמי מכיל נישות רבות אשר צפויות לאפשר צמיחה פוטנציאלית והתפתחות של חברות ישראליות בהתבסס על יכולות מדעיות מתקדמות אשר תנבענה ממחקרים מתקדמים הנגזרים מהקבץ זה.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 350-450M₪, בהתבסס על ההערכות / הנחות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
הקמת מרכז ידע לאומי לחישוב-על - מרכז מצוינות (לחמש שנים, כולל שכר חוקרים חדשים, כולל מענקי מחקר)	95
עלות משוקללת תשתיות HPC (שנתי)	25
הגדלת תקציב המחקר הכללי של הקרן הלאומית למדע	1.75
קרן ייעודית בתקצוב מערכת הביטחון	4
עידוד פיתוח טכנולוגיות ופרוייקטים בנושאי הגנה בסייבר (בתעשייה)	[1]35
הקמת ועדת מעקב ובקרה במולמו"פ	0.2

4.4 פיתוח כלים לחירום במרחב הקיברנטי

1. יוזמות ההקבץ

- יצירת יתירות בתשתיות התקשורת הפנים-ארציות והבינ"ל.
- פיתוח כלי איתור מקור הנזק וזיהוי פלילי.
- פיתוח כלי "עזרה ראשונה" לתפעול ושיקום פגיעה.
- פיתוח יכולות התאוששות מהירה והשרדות במקרה חירום.
- התנעת מחשבה על מסגרת "מילואים" בסייבר.
- פיתוח מערכת Business Continuity Planning להבטחת רציפות תפקודית בחירום.

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- ביצוע פרוייקטים קטנים-בינוניים באמצעות גורמים בתעשייה.
- חשיפה מופחתת לתקיפות וצמצום נזקים ע"י תגובה מוכנה ומסונכרנת והתאוששות מהירה.
- פיתוח מוצרים בעלי פוטנציאל בשווקים בינ"ל.

3. הפוטנציאל הכלכלי של ההקבץ

עיקר הפוטנציאל של הקבץ זה הוא במניעת/צמצום נזק פוטנציאלי במקרה של מתקפת סייבר, ע"י קימום מהיר של המערכות והחזרתן לפעילות. מניעת אבדן מידע, ואפשור המשכיות פעולת המשק במקרה חירום הוא בעל ערך משמעותי למשק. השוק הגלובאלי המזוהה עם יוזמות הקבץ זה אמנם נמצא בשלב בתולי, אך צפוי לצמוח באופן משמעותי עם התעצמות האיומים, ועליית המודעות אליהם בקרב מקבלי ההחלטות בדרגים ובתחומים השונים. חלק מהפתרונות שיפותחו יהיו רלוונטיים ליישום גם בשווקים בינ"ל.

4. תרומה ליצירת יתרון תחרותי של המשק

חלקים בתחום מערכות ה-BCP הינם בתוליים יחסית, ללא מערכות שלמות המבוססות על תפיסות בשלות. גיבוש תפיסה לאומית ומערכת כלים לחירום, תשמש בסיס ליתרון תחרותי בשוק הנעדר מערכות אלה. תפיסת עמדות בשוק בתולי וצומח תשמש בסיס להתפתחות חברות דומיננטיות בתחומים אלה.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 100-150M ₪ (ללא יתירות קווי תקשורת[1]), בהתבסס על ההערכות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
יתירות בפריסת קווי התקשורת	TBD[2]
פיתוח מערכת BCP / DRP	100
כלי איתור מקור הנזק	10

1 מענק ממוצע לפיתוח 1.5 מש"ח, 40-50 פרוייקטים
2 טווח עלות יתירות פריסת קווי תקשורת: מאות עד מיליארדי ₪

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4.5 פיתוח פתרונות להגנה מקומית/מבוזרת

1. יוזמות ההקבץ

- עידוד פיתוח מערכות ניטור והתראה
- סנסורים תכנתיים המעבירים אינפורמצית ניטור על מצב הרשת
- מלכודות דבש לאיתור פוגענים ממוקדים
- הטמעת התקנת תוכנות הגנה אחרות

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- הפחתת חשיפה לתקיפות ומניעת נזקים בנקודות הקצה.
- ביצוע פרוייקטים קטנים-בינוניים באמצעות גורמים בתעשייה.
- פיתוח מוצרים בעלי פוטנציאל בשווקים בינ"ל.

3. הפוטנציאל הכלכלי של ההקבץ

הפוטנציאל הכלכלי של ההקבץ נובע בעיקר משיפור רמת האבטחה ומניעת נזק פוטנציאלי, כתוצאה מהטמעת מספר טכנולוגיות הגנה בצורה מבוזרת ומקומית. ביצוע פרוייקטים קטנים-בינוניים ע"י גורמים בתעשייה ישפיע בצורה בינונית על הכנסות ישירות בתחום, והיקף הפעילות הבינוני יחסית יגרור מספר נמוך יחסית של מועסקים.

4. תרומה ליצירת יתרון תחרותי

מספר נכסים תחרותיים רלוונטיים בהקבץ - הבולט מביניהם הוא ה'מותג' / תדמית של מדינת ישראל והחברות הישראליות הפועלות בתחום. בנוסף, קיימת סבירות גבוהה לתחרות משמעותית מצד חברות ומכוני מחקר בינ"ל.

5. הערכת עלות חמש – שנתית:

יוזמות הקבץ זה - כפי שהציגו ועדות העומק - הינם ברמת קונקרטיזציה חלקית מאד, ועל כן קשה להעריך את הפוטנציאל, ועל אחת כמה וכמה את ההשקעה הנדרשת. אינדיקציות נוכחיות מצביעות על טווח עלות של עשרות עד מאות מש"ח:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
עידוד פיתוח מערכות ניטור והתראה	175
סנסורים תוכנתיים המעבירים אינפורמציית ניטור על מצב הרשת	100
מלכודות דבש לאיתור פוגענים ממוקדים	10
תחזוקת מלכודות דבש (לשנה)	4
הטמעת התקנת תוכנות הגנה אחרות	TBD

נראה כי יוזמות הקבץ זה דורשות המשך בחינה במסגרת התקציבים הרלוונטיים במערכת הביטחון, ולא במסגרת המיזם הקיברנטי, בשל חשיבותן במרחב הביטחוני בלבד.

4.6 פיתוח טכנולוגיות/ פתרונות כחול–לבן

1. יוזמות ההקבץ

- הקמת עננים מסחריים ישראליים ובחינת שלוחות של עננים מחו"ל
- מערכות סינון תוכן והרשאות
- קומפיילר מאובטח

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

- אבני בניין לצופן
- חוסן לתשתיות קריטיות
- תוכנת אנטי וירוס ישראלית

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- מניעת חשיפה ל-backdoor ושיפור רמת הביטחון באמצעות אספקה בטוחה.
- ביצוע פרוייקטים קטנים-בינוניים ע"י גורמים בתעשייה.

3. הפוטנציאל הכלכלי של ההקבץ

הקבץ זה יגדיל את מספר המשרות במשק, עם התממשות היוזמות. עם זאת, לא צפוי שיהיה ניתן לייצא את המוצרים אשר יפותחו במסגרת ההקבץ, או אפילו למכור אותם במסגרת פנים ארצית. בנוסף, ההקבץ עוסק בתחומים קיימים (anti-X, קומפיילר, firewall, מערכת הפעלה) ולא בפיתוח תחומים חדשים. נראה כי התרומה הכלכלית המרכזית של ההקבץ תיגזר משיפור רמת אבטחת ומניעת נזק פוטנציאלי. יש להניח כי הנזק הפוטנציאלי הנמנע יהיה גדול, אם כי קשה להעריכו בשלב זה.

4. תרומה ליצירת יתרון תחרותי

הקבץ זה מתמקד בתחומים ומוצרים הקיימים בשווקים בשלים יחסית, עם שחקנים ותיקים ודומיננטים בעולם. לא נראה כי יש השפעה משמעותית על פיתוח יכולות בתחום, או יצירת ידע שמהווה יתרון תחרותי מהותי בראייה בינ"ל.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 550-750M₪ (ללא טכנולוגיות ענן[3]), בהתבסס על ההערכות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
פיתוח אנטי וירוס (שנתי)	42[4]
מערכות סינון תוכן והרשאות (שנתי)	35[3]
קומפיילר מאובטח (שנתי)	35[3]
אבני בניין לצופן	45[5]
חוסן לתשתיות קריטיות	29[4]

נראה כי יוזמות הקבץ זה דורשות המשך בחינה במסגרת התקציבים הרלוונטיים במערכת הביטחון, ולא במסגרת המיזם הקיברנטי, בשל חשיבותן במרחב הביטחוני בלבד.

4.7 מטה ורשות קיברנטיים לאומיים

1. יוזמות ההקבץ

- החלפת ועדת ההיגוי ב-84' במטה סייבר לאומי.
- הגדרת שר / יועץ בכיר לרה"מ המוביל ומסנכרן את הנושא באופן רוחבי.
- הקמת / הרחבת רשות סייבר לפיקוח על רמת האבטחה של מגזרים לא-ביטחוניים.
- הקמת "חדר מצב קיברנטי" להובלת מקרי חירום בתחום הקיברנטי.
- יצירת רגולציית אבטחת סייבר בחברות - חיוב דיווח תקופתי לדירקטוריון על רציפות תפעולית והגנת תשתיות בכל ארגון "משמעותי", יצירת מדד / דירוג "ביטחון סייבר".

[3] טכנולוגיות ענן לא נבחנו בשלב הנוכחי עקב כלליות היוזמה
[4] צוות של עשרות אנשים (לכל יוזמה) המפתח ומעדכן באופן שוטף
[5] הערכת ועדת צופן

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- יצירה ועדכון שוטף של מדיניות ותוכניות הקמת תשתיות.
- יצירת ביקושים בהתאם למדיניות.
- שיפור הסנכרון והעברת הידע בין הגורמים השונים.
- קידום הנושא בתודעת מקבלי החלטות בכירים.
- שיפור רמת האבטחה בקרב האוכלוסיה הכוללת.

3. מידת ההשפעה על הפוטנציאל הכלכלי של המשק

השילוב בין מטה סייבר, מועצה מתאמת, שר / יועץ בכיר ורשות לאבטחת מידע אזרחית מהווה מנגנון ארגוני, המוביל את נושא הסייבר בממשלה, מסנכרן בין הגורמים המעורבים בתחום, ומפעיל את המנופים הזמינים לממשלה לטובת ה-cluster (מדיניות רשויות, הקמת משאבים ותשתיות, יצירת ביקושים ופרוייקטים).

מנגנון זה מאפשר ראייה רוחבית ומקיפה של נושא הגנת הסייבר של המשק הלאומי כולו, ושל הצרכים הנגזרים ממנו (לרבות בתחום המו"פ התעשייתי), לאור האיומים המתפתחים. מנגנון זה, כתוצאה מרוחב הראייה שלו מחד, ונגישותו למקבלי ההחלטות מאידך, יצמצם חסמי מו"פ ובירוקרטיה המונעים / מעכבים פיתוח פתרונות בצורה יעילה וכלכלית, ישלב באופן טוב יותר בין תהליכי המו"פ והמוצרים הנובעים מהם לבין האיומים העדכניים, ויגביר את שיתוף הפעולה האקדמי / ביטחוני / כלכלי בין העוסקים בתחום הגנת הסייבר במדינה.

בנוסף, צפויה תרומה משמעותית להתפתחות של תחומים חדשים כתוצאה ממודעות, הכוונה ותמרוץ של הממשלה. הוספת מנגנון אכיפה למגזרים שאינם ביטחוניים וחיזוק האכיפה הרגולטיבית, יאפשר אכיפה על מגזרי המשק הרלוונטיים (הביטחוני ושאינו ביטחוני), ויש בו פוטנציאל ניכר להפחתת הנזק הלאומי (לרבות הכלכלי), אשר עלול להתממש בעקבות מתקפת סייבר רחבת היקף על המדינה.

4. תרומה ליצירת יתרון תחרותי של המשק

המנגנון שלעיל מהווה Enabler לתעשייה במאמצי מחקר ופיתוח ליצירת מוצרים בעלי רלוונטיות גבוהה בתחום הסייבר, ביחס לאיומים העכשוויים, ובעיקר לאיומים הצומחים שיהיו דומיננטיים בעתיד הקרוב / רחוק.

יצירה ועדכון שוטף של מדיניות ותוכניות להקמת תשתיות באמצעות המודל האופרטיבי, בונה סביבה פורייה המאפשרת לחברות בתחום למקסם את מאמציהן - וככל שהסביבה הרגולטורית תספק עידוד טוב יותר באופן יחסי למדינות אחרות, ישמשו מנופים אלה יתרון יחסי ברמת המדינה. יתרה מזו, שיפור הסנכרון והעברת הידע בין בעלי העניין כך שיזרום באופן חלק יותר ביחס למדינות אחרות, היא בגדר אבן יסוד משמעותית ביצירת יתרון תחרותי.

בנוסף, צפוי המנגנון לתרום לחיזוק הדימוי של ישראל כמדינה הנמצאת בחוד החנית ו"עם האצבע על הדופק" בכל הנוגע לאיומי סייבר.

5. **הערכת עלות חמש – שנתית:**
הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 50-100M₪, בהתבסס על ההערכות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
הגדרת יועץ בכיר ברה"מ להובלה וסנכרון של מאמצי סייבר לאומיים באופן רוחבי	1.5[6]
הקמת מטה סייבר לבחינה וקידום מדיניות ויוזמות בתחום	3[7]
הקמת רשות סייבר אזרחית לפיקוח רמת אבטחה על מגזרים לא-ביטחוניים	13[8]
הקמת "חדר מצב קיברנטי" להובלת מקרי חירום בתחום הקיברנטי	0.5
חיוב דיווח תקופתי לדירקטוריון על רציפות תפעולית והגנת תשתיות בכל ארגון "משמעותי"	1

נרה כי יוזמות הקבץ זה דורשות המשך בחינה מעמיק יותר של מבנה וסמכויות המנגנונים השונים, כמו גם תקצובם.

4.8 חינוך, השכלה גבוהה והעלאת המודעות למרחב הקיברנטי

1. **יוזמות ההקבץ**
- הגברת המודעות הציבורית לנושא הסייבר בכלל ולאיומים בפרט
- הטמעה של מידת הקריטיות של הנושא בקרב מקבלי ההחלטות בממשל ובתעשייה
- הגברת לימודי מדע, טכנולוגיה, הנדסה ומתמטיקה (STEM) בכלל, ובנושא הגנת הסייבר בפרט, במסגרות החינוך הקדם אקדמיות
- תוכניות לימודים אקדמיות בנושאי הגנת הסייבר
- מלגות ועידוד מחקרי הגנת הסייבר במסגרת תארים מתקדמים
- השתלמויות בתחום פיתוח מאובטח של קוד לחברות הזנק ולחברות מוצרי סייבר ישראליים
- הסמכת מומחים לתחומי הגנת הסייבר

2. **תרומת ההקבץ לפיתוח תעשיית סייבר**
- הפחתת חשיפה לתקיפות ומניעת נזקים.
- הרחבת מאגר כוח אדם רלוונטי בשלבי התפתחות מגוונים.
- הכשרת כוח אדם הנדרש לפיתוח תעשיית הסייבר.

3. **מידת ההשפעה על הפוטנציאל הכלכלי של המשק**
תוכנית מודעות לסייבר משפיעה על הפוטנציאל הכלכלי בשני היבטים - מפחיתה את הנזק שעלול להיגרם למשק במקרה של מתקפת סייבר בהיקף כזה או אחר, ובנוסף חושפת כח אדם פוטנציאלי לתחום הסייבר ולאפשרויות הגלומות בו. מדובר בהפחתת חסם מרכזי, שגורמים רבים בתעשייה זיהו: מחסור בכוח אדם איכותי המוכשר לעיסוק מתקדם בתחום. השלכות יישום תוכנית חינוך רחבת היקף על הפוטנציאל הכלכלי של המשק בתחומי הסייבר באות לידי ביטוי בשיפור איכות כח האדם העוסק בסייבר והגדלתו כתוצאה משיפור בכישורי העוסקים במלאכה, יתרחבו היקף ואיכות המו"פ בתחומי הסייבר - מוצרים רבים יותר ברמה גבוהה יותר (אשר יביאו גם לשיפור במצב ביטחון הסייבר הלאומי ברבדים השונים). כח אדם זמין, איכותי ורלבנטי יאפשר גם התפתחות של תחומי עיסוק נוספים המתמקדים או משיקים לתחום הסייבר.

6 עלות שכר בכיר במגזר הציבורי 80 אש"ח בחודש, לשכה 1.5 מש"ח.
7 3 תקנים ייעודיים, 80 אש"ח בחודש שכר בכיר, כל השאר נע"ת, משרד.
8 40 אנשים עלות שכר ממוצעת 300 אש"ח, 2 מש"ח תשתיות.

4. תרומה ליצירת יתרון תחרותי של המשק

אחד הנכסים התחרותיים המרכזיים של מדינת ישראל בתחום הסייבר הינו איכות כוח האדם בתחום. תוספת משמעותית של כוח אדם ברמה גבוהה מחזק ומעמיק את הנכס הזה. יתרה מזו, תוכנית חינוך רחבת היקף מעמיקה את הידע המדעי וההנדסי של הלומדים בה בתחומי הסייבר. תוכנית חינוך בעלת הכשרות מגוונות תאפשר זמינות כח אדם בטווח הקצר, כאשר עם חלוף הזמן הכמות והאיכות יגדלו. בנוסף, ידע הנדסי / מדעי מעמיק ויסודי בתחום הסייבר מהווה בסיס לפיתוח חברות חדשניות ופורצות דרך, המסתמכות על ידע ייחודי שנוצר באקדמיה, במערכת הביטחון או בחברות עצמן, וליצירה ופיתוח של פטנטים המהווים בסיס למוצרים חדשניים.

5. הערכת עלות 5 – שנתית:

עלות שנתית מוערכת למימוש מלא של הקבץ זה (כיסוי מלא של מערכת החינוך) עומדת על כ- 175 מש"ח. להערכתנו, במסגרת 5 השנים הקרובות נכון יהיה לבצע פיילוט של יוזמות אלה. היקף מימוש תוכנית הפיילוט מוערכת בכ-15% מעלות המימוש המלאה המופיעה לעיל (למעט תוספת מכסות הסטודנטים המתוקצבת במלואה לאורך כל טווח השנים). בהינתן זאת, העלות השנתית המוערכת למימוש תוכנית הפיילוט הינה כ-65 מש"ח לשנה (כ-325 מש"ח ל-5 שנים). אומדן הערכות עלות זה מבוסס על האומדן המופיע בטבלה זו:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
גדנ"עות סייבר	20[9]
מסלולי בגרות בסייבר	10[10]
מגמות (בתיכון) לטכנולוגיות סייבר	20[9]
מסלולי העשרה (תל"ן)	30[9]
שילוב נושאי הסייבר במסגרת הפנימיות הצבאיות	1
תנועות נוער (צופי סייבר)	5[11]
מסגרות חינוך כגון נוער שוחר מדע	1.5
שילוב במסלולי נוער מחונן	5
אולימפיאדה ותחרויות לאומיות לנוער (כגון Code Guru)	20
מחנות קיץ סייבר	13[12]
קמפיין הגברת מודעות	4[13]
השתלמויות פיתוח קוד מאובטח	4[14]
תוספת מכסות סטודנטים (מתוכנן ומתוקצב במסגרת תוכנית החומש של ות"ת)	40[15]
הגברת קמפיין מודעות	4

נראה כי חלק מיוזמות הקבץ זה דורשות המשך בחינה מקצועית מעמיקה יותר הן באשר לאופן הפעלתן במסגרת מערכת החינוך וההשכלה הגבוהה ובשילוב עם פעילויות קיימות במערכת החינוך וההשכלה הגבוהה, והן לבחינת גובה התקצוב הדרוש להן.

9 300 אש"ח למדריך לשנה, 1000 בתי ספר תיכוניים בארץ, תקן מדריך על כל 15 בתי ספר, 70 מדריכים
10 הכשרת 5,000 עובדים במקצועות נדרשים - 40 מש"ח.
11 תקציב צופים בקריית ביאליק 150 אש"ח.
12 משתתף תגלית ~ 5 אש"ח ל-10 ימים, 500 בני נוער, 3-4 שבועות
13 עלויות קמפיינים ממשלתיים ~ 2-5 מש"ח
14 הכשרה מקצועית ל-400 הנדסאים - 8 מש"ח
15 מבוסס על נתוני הוועדה האקדמית

4.9 מדיניות ורגולציה לעידוד תעשיית הסייבר

1. יוזמות ההקבץ

- התאמת החקיקה הנוגעת באישורי יבוא ויצוא מוצרי ושירותי סייבר (כולל מנגנונים תומכים כדוגמת pre-ruling, תקינה וכו').
- קידום רכש מוצרים כחול לבן במערכת הביטחון.
- שיפור ריכוז ושקיפות מידע על אפשרויות מו"פ סייבר בישראל.

2. תרומת ההקבץ לפיתוח תעשיית סייבר

- עידוד ניוד של ידע בין מערכת הביטחון לבין התעשייה.
- פתיחת אפשרות להכנסות גדולות יותר לחברות בתחום.
- הפחתת חוסר וודאות רגולטורית לחברות בתחום.
- עידוד והכוונת מחקר ופיתוח בתחום.

3. הפוטנציאל הכלכלי של ההקבץ

שוק מוצרי הפעולה הגלובאלי מוערך ב- $1B-1.5B. הסדרת רגולציית יצוא של מוצרי סייבר תקף על יצוא מוצרי פעולה, ותהפוך את השוק לרלוונטי עבור חברות הפעולה הישראליות בשיעור זה או אחר (תלוי רגולציה). שוק הפעולה הגלובאלי בשלבים "עובריים" - היקפיו הנוכחיים מצומצמים, אך הביקוש גובר והצמיחה מהירה. השוק נתפס כאטרקטיבי מאוד בעיני החברות הישראליות הפועלות בתחום ולאחרונה, גם חברות ביטחון אינטגרטוריות גדולות הכריזו על כוונתן להיכנס אליו.[16] קידום רכש כחול לבן במערכת הביטחון יגדיל את היקף הפעילות בתעשייה האזרחית בתחומי הסייבר בתוך ישראל, ויחד עם הסדרת רגולציית היצוא אף יגדיל את היקף הפעילות מחוצה לה. כמו כן, קידום הנושא יגביר את שיתוף הפעולה בין מגזרי הביטחון והתעשייה האזרחית בתחומי הסייבר.

4. תרומה ליצירת יתרון תחרותי של המשק

יצוא מוצרים איכותיים מחזק את תדמית מוצרי האיכות המיוצאים מישראל. צמצום חוסר הוודאות הקשור לאישורי היצוא יפחית מצבים שבהם נמנעות התעשיות ממאמצי פיתוח, וכן יעקוף חסמים באמצעות ביצוע הפיתוח מחוץ לגבולות המדינה. מדיניות ברורה וכלים שיספקו מענה מהיר יאפשרו המשך פיתוח יכולות תחרותיות משמעותיות במדינה בתחומים אלה.

5. הערכת עלות חמש – שנתית:

הערכה ראשונית של העלויות הצפויות בהקבץ זה (הערכת עלות לחמש שנים) - 200-250M₪, בהתבסס על ההערכות הבאות:

פירוט תכולה	הערכת עלות שנתית (מש"ח)
הסדרת רגולציה ליצוא מוצרי סייבר	5
קידום Outsourcing במערכת הביטחון	5

[16] על מנת להפחית חסמים למיצוי פוטנציאל בתחום הפעולה, ניתן להפוך את רגולציית הייצוא לסלקטיבית יותר: אפשור מכירת מוצרים שלא יגרמו נזק או יסכנו את מדינת ישראל, היתר למכירת מוצרים שלא נמצאים בחזית הטכנולוגיה ו/או בעלי תחליפים בשוק, הסרת הגבלה על התרחבות לפלטפורמות נוספות

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

5. אופי המימון של ההקבצים

מקורות מימון ליוזמות: התועלת הכלכלית של היוזמות השונות לתעשייה בעלת השלכות חשובות, בין היתר על עלות המימון הממשלתי בכל אחד מהפרוייקטים ומקורתיו:

- בחלק מהפרוייקטים, קיימת אפשרות לפיתוח ויישום הפרוייקט בשיתוף עם התעשייה ואף בהובלתה. זאת בתנאי שהיכולות והידע המפותחים יכולים לשמש בהמשך ליצוא מוצרים ושירותים - בין אם פותחו במסגרת הפרוייקט וניתנים ליצוא, ובין אם בשימוש בידע וביכולות לפיתוח מוצרים ושירותים אחרים (הניתנים ליצוא). במקרה של פרוייקטים בעלי תועלת ישירה גבוהה לתעשייה, חלק משמעותי במימון יכול לבוא מהשקעות פרטיות.
- במקרים שבהם ניתן לפתח את הפרוייקט בשיתוף חלקי או מלא של מדינה שלישית, עלות הפיתוח, המתחלקת על שתי מדינות, זולה בהרבה.
- במקרים שבהם התועלת לתעשייה עקיפה, כגון מרכזי מחקר אקדמיים, קשה יותר לשלב מקורות מימון בהיקף נרחב מהשוק הפרטי

הערכת עלות היוזמות ואופי מימונן:

הטבלה הבאה מרכזת את הערכת עלויות כלל היוזמות בכל אחד מההקבצים בחמש השנים הראשונות (עלות הקמה ועלות שוטפת בשנה החמישית), וכן את הערכת היקף המימון הפרטי הישיר ביוזמות הנ"ל (לא בעקבות היוזמה, אלא כחלק מפרוייקטי היוזמה). שני ההקבצים האחרונים הם בעלי השפעה נמוכה על פיתוח תעשיית סייבר ישראלית (זאת ללא התייחסות לחשיבותם במונחים של תועלות ביטחון לאומי או אקדמיה).

הערכת עלות הקבץ	הקמה (מיליוני ₪)	שנתית שוטפת (מיליוני ₪)	טווח מימון בחמש שנים (מיליוני ₪)	מימון ציבורי בחמש שנים (מיליוני ₪)	מימון פרטי בחמש שנים (מיליוני ₪)
מטה ורשות קיברנטיים לאומיים	שולית	20	50-100	90	
מעטפת הגנה למדינה במרחב הקיברנטי	140	55	200-300[17]	120	130
תשתיות פיתוח לטכנולוגיות במרחב הקיברנטי	90	22	150-200[18]	100	55
חינוך, השכלה גבוהה והעלאת המודעות למרחב הקיברנטי	שולית	65	300-350	325	
מדיניות ורגולציה לעידוד תעשיית הסייבר	שולית	10	50-100	50	
עידוד מו"פ בתחומי המרחב הקיברנטי וחישוב-על	משוקללות לתוך העלויות השנתיות	65	350-450	380	40
פיתוח כלים לחירום במרחב הקיברנטי	110	שולית	100-150	55	55
פיתוח פתרונות להגנה מקומית/מבוזרת *	280	5	275-325	200	100
פיתוח טכנולוגיות/ פתרונות כחול-לבן *	75	115	550-750	180	450

[17] הוצאות תחזוקה ותפעול מחושבות החל מהשנה הרביעית. נזק ל- או יסכנו את מדינת ישראל, היתר למכירת מוצרים שלא נמצאים בחזית הטכנולוגייה

[18] הוצאות תחזוקה ותפעול מחושבות החל מהשנה הרביעית.

* לא נראה כי לשני הקבצים אלו השפעה משמעותית על פיתוח יכולות או יצירת ידע המהווים יתרון תחרותי מהותי בראייה בין לאומית.

אופן מימון פרוייקטים: הוועדה סקרה מספר דרכים מרכזיות למימון פרוייקטים משותפים בין הממשלה והתעשייה, בהיבט של יצירת ביקוש לטכנולוגיה ושל היצע הטכנולוגיות, על ידי סבסוד פיתוחן:

- **הזמנה ממשלתית לרכש מוצר**, שירות או טכנולוגיה. מקל על החברה המפתחת לקבל מקורות מימון לפרוייקט, בפרט בשלבים המאוחרים של הפיתוח.
- **אכיפת רגולציה מחייבת בשימוש** בטכנולוגיה, תשמש כתמריץ לחברות טכנולוגיות לפתחה. עם זאת, חשוב להדגיש כי השוק הישראלי הוא קטן יחסית לשוק העולמי, ולכן יש ליצור רגולציה הממוקדת בטכנולוגיה מוגדרת.
- **שותפות ממשלתית בעלות הפיתוח** של מוצר, שירות או טכנולוגיה על ידי חברה. רלוונטי במיוחד לשלב פיתוח מוקדם, שהסיכון בו גבוה. במקרה כזה, הממשלה יכולה לדרוש אופציה לקנייה של המוצר במחיר עלות, בשל השתתפותה בפיתוח, ובמקביל למתן אפשרות מכירה וייצוא שתכסה את עלויות הפיתוח של החברה. מודל זה יכול לשמש בהתאמה גם עבור מימון פיתוח במשותף על ידי שתי מדינות או יותר.

כמובן, שניתן גם לפעול במספר כלים ולהשתמש **בחבילת מימון משולבת**, לדוגמא:

- הזמנה ממשלתית לרכש בעבור המערכות הממשלתיות, הביטחוניות והאזרחיות.
- שותפות חלקית במימון שלבי הפיתוח המוקדמים על ידי הממשלה, בתמורה להנחה במחיר הרכש.
- רגולציה מחייבת עבור חברות מפוקחות, שתיצור הזמנות עתידיות למוצר (עוצמת ההשפעה תלויה גם בקיומם של מוצרים אחרים המספקים את יכולת ההגנה).
- שותפות ממשלה זרה במימון שלבי הפיתוח המוקדמים, בתמורה להנחה במחיר הרכש, ולהעברת ידע ויכולות, ואף תוך ביצוע רגולציה מחייבת במקביל.
- השקעה פרטית להשלמת עלות הפיתוח.

6. המלצות הוועדה

6.1 המלצות לארגון התוכנית מול השוק הפרטי

1. הקמת מנהלת לפיתוח תעשיית הסייבר הישראלית, כחלק מבניית היכולות הלאומיות במרחב הקיברנטי.

- תעשיית הסייבר הישראלית הינה **רובד נוסף בבניית ההגנה הלאומית של מדינת ישראל** במרחב הקיברנטי, המאפשר מגוון רחב וגדול של יכולות מחקר ופיתוח טכנולוגיות בתחום. זאת מעבר לסל פעילויות ההגנה האזרחיות בתוכנית.
- קידום תעשיית הסייבר הישראלית צריך להיעשות על ידי **מנהלת ייעודית בעלת התמצאות ביטחונית–טכנולוגית רחבה**, בשל החשיבות הגבוהה לאינטגרציה בין מערכות ההגנה האזרחיות והמערכות הביטחוניות, וליצירת ממשקים חדשים מולן ומול התעשייה לאורך זמן. המנהלת צריכה להיות בעלת קשרים ענפים עם מערכות ההגנה האזרחית ומערכות הביטחון מחד, ובעלת הכרות מעמיקה עם פיתוח הטכנולוגיות הרלוונטיות והתפתחות האיומים מאידך. בעת בחינת הגוף המתאים ביותר להכפיף אליו את המנהלת, יש לוודא את קיומן של מספר יכולות:
  - הכרות מעמיקה עם טכנולוגיות הגנה ואבטחת מידע
  - יכולת ארגונית, שתאפשר הקמה מהירה ואפקטיבית של המנהלת
  - גישה למקבלי החלטות בדרג גבוה בזירה הפוליטית ובמערכת הביטחון
  - ממשק עבודה רציף והדוק מול מטה הסייבר של הצבא
  - יכולת עבודה בצמוד לרגולטורים הביטחוניים של מערכות המידע בגופים אזרחיים
  - יכולת לקיים קשרי עבודה שוטפים עם גופי מערכת הביטחון ועם גופים אזרחיים בעלי תשתיות מערכות מידע קריטיות, ועם חברות טכנולוגיות ישראליות

לא להפצה לשימוש רישמי בלבד - גירסה 02 להתיחסות

חשוב לציין, כי המלצה זו מדגישה את חשיבות הניהול והתיאום בתחום, אך לא בהכרח דורשת הפעלת כלים ממשלתיים חדשים או גורמים חדשים בזירת קידום המחקר והפיתוח התעשייתיים.

2. כינון מסגרת סייבר בין מגזרית ומינוי שר בכיר בראשותה, וגיבוש מדיניות לאומית במרחב הקיברנטי, הכוללת את קידום התעשייה הישראלית.

- כינון מסגרת לאומית (למשל מועצה או מטה) לתיאום הפעילויות במרחב הקיברנטי, וגיבוש מדיניות כוללת מטעם הדרגים הגבוהים ביותר היא בגדר **איתות חשוב וחזק לתעשייה הישראלית והבינלאומית** לגבי חשיבות התחום בישראל, ואינדיקאטור לגבי היכולות הטכנולוגיות שיפותחו בישראל.
- הרכב המטה צריך לכלול את כל הגורמים הרלוונטיים מהממשלה, כולל גופים האמונים על פיתוח תעשייה ומחקר.
- קיימת חשיבות לכך שעבודת המטה תרוכז בידי גוף מדיניות, ולא בידי אחד מגופי הביצוע. מטה הסייבר צריך להוציא מפת דרכים ברורה, עם מטרות, יעדים, כלי מדיניות ותוכנית של הרכב המטה. על מפת הדרכים של תוכנית המדיניות הממשלתית להיות שקופה וגלויה ככל האפשר, על מנת להעביר לתעשייה את המתווה האסטרטגי של פעילויות המדינה, ולייצר מדיניות ברורה ואחידה.
- גוף המדיניות המרכז את עבודת מטה הסייבר צריך לבצע **מעקב ובקרה** שוטפים אחר הפעולות שמבצעים משרדי הממשלה השונים בתחום, ולרכז את יצירת מדדי מעקב ויעדי הביצוע לתוכניות, ולוודא שהנתונים השונים יוצגו בפני מטה הסייבר.

6.2 המלצות כלליות לקידום תעשיית הסייבר בישראל

1. הגדלת היקפי המחקר והפיתוח הביטחוניים המבוצעים בתעשייה, תוך שיפור ההסדרה של יצוא טכנולוגיות

מהלך זה דומה למהלכים שבוצעו בעבר על ידי משרד הביטחון, כשהעביר את פיתוח וייצור אמצעי הלחימה אל מחוץ לצבא. המודל המוצע דומה לאופן פיתוח אמצעי הלחימה של חיל האוויר, שמבוצע על ידי מספר תעשיות ביטחוניות, תוך שותפות של הצבא בתהליך האפיון והפיתוח והתחייבות לרכש. במקרים רבים, המחיר שמשלם הצבא נמוך משמעותית מהמחיר שמשלמים צבאות זרים, שאינם שותפים לתהליכי הפיתוח והאפיון. מהלך זה ישנה משמעותית את יכולות ההצטיידות הצבאיים ואת היתרון היחסי של תעשיית הסייבר הישראלית:

- תתאפשר זליגה רבה יותר של יכולות פיתוח אל עבר מוצרים נוספים בתעשייה, בין היתר בשל המצאות הידע והיכולות בידי גורם שאיננו ביטחוני-צבאי, היכול למנף את הטכנולוגיות לפעילות עסקית נוספת.
- מיקומה של התעשייה הישראלית בחזית העולמית של התמודדות עם איומים במרחב הקיברנטי, תחזק את היתרון היחסי שלה במקומות אחרים בעולם.
- היכולת לנהל כוח אדם, תקציבים ופרוייקטים בחברות התעשייה גמישה יותר מאשר בשירות המדינה ובצבא. לכן, ניתן יהיה להרחיב צווארי בקבוק של פיתוח טכנולוגיות ויכולות במועדי זמן קצרים, ולהגדיל את יכולותיה וחוסנה של מערכת הביטחון הישראלית.
- תתאפשר הגדלה של היקפי היצוא של מוצרי סייבר, שתביא לעלייה משמעותית בהערכה למחקר ולפיתוח בישראל, זאת בכפוף להמלצה הבאה לגבי הסדרת יצוא הטכנולוגיות בתחום.
- תבוצע הסדרה של יצוא טכנולוגיות על מנת לאפשר לחברות להשקיע בפיתוח טכנולוגיות במרחב הקיברנטי, עבור ההגנה האזרחית, כמו גם עבור מערכת הביטחון, חייבת להתבצע הסדרה ברורה של היתרי יצוא הטכנולוגיה. ההסדרה צריכה לאפשר וודאות גבוהה ככל האפשר לחברות, עוד בטרם נכנסו לתהליך המחקר ופיתוח והנהלים צריכים להיות חדים וברורים ככל האפשר, גם עבור חברות שלא מכירות את נהלי היצוא הביטחוני בישראל. המלצה זו חופפת להמלצה מפורטת יותר של הוועדה למדיניות וחקיקה.

2. הגדלת השקיפות בתוכניות העבודה והפיתוח במערכת הביטחון ובמערכת ההגנה האזרחית, וחיזוק הממשקים בין הגופים הצבאיים לתעשייה ולאקדמיה

- למרות מגבלות סיווג, יש **להגדיל ככל הניתן את השקיפות במפת הדרכים** המכילה את תוכניות הפיתוח וההצטיידות של מערכת הביטחון - בין אם באמצעות הקמת מנגנוני סיווג לאנשי תעשייה אזרחית ולמשקיעים, ובין אם באמצעות פישוט התוכניות וביציאה לקולות קוראים לטכנולוגיות.
- יש לפעול **לחיזוק הממשקים בין הגופים הצבאיים לתעשייה ולאקדמיה**. ריבוי ממשקים למעבר אינפורמציה, קשרי עבודה והכרות הם רכיב מכריע בביסוס של יכולות התעשייה בתחום. יש להמשיך בפעילות הקיימת, אך להעצימה בכנסים, סדנאות עבודה ופעילויות נוספות.

3. יצירת רגולציה המעודדת שוק ראשוני להטמעת טכנולוגיות ומוצרים חדשים

הרגולציה על התשתיות הקריטיות, שמבצעת הרשות הממלכתית לאבטחת מידע (רא״מ), היא רכיב מרכזי בעיצוב ההגנה האזרחית בישראל והביקושים המקומיים. יש לנסות לבנות מסגרות המעודדות את החברות המפוקחות לבחון יישומים חדשים ו/או לשמש כאתרי בטא עבור חברות המפתחות טכנולוגיות חדשות. מסגרות אלה יאפשרו **הגדלה של השוק הראשוני המקומי** לטכנולוגיות ולמוצרים חדשים. בנוסף, ליווי של הניסוי/ ההטמעה על ידי מנהלת לפיתוח התעשייה בשיתוף רא״מ, יקטין את הסיכונים בניסוי/הטמעה מחד, וישפר את היכולות הטכנולוגיות של אנשי הרשות ושל הצוותים המקצועיים של החברות המפוקחות מאידך.

4. יצירת דירוג לרמת ההגנה עבור גופים וחברות, שישמש בסיס לבניית כלי מדיניות, ולניהול סיכונים פיננסיים וביטוחיים

מומלץ לקדם בניית מדדים לדירוג רמת המוכנות וההתגוננות של חברות פרטיות וגופים ציבוריים לאיומי סייבר. מדדים אלה יכולים לשמש בעתיד בסיס לבניית כלי ביטוח סייבר, ולהוות נדבך בדירוג סיכונים פיננסיים של לקוחות. חשוב להכריע אם קיים צורך עתידי ברגולציה בנושא, ולקבוע לוח זמנים להחלתה, ובכך לאפשר לגופים פרטיים לפעול לגיבוש מדדים (בדומה למדדי דירוג סיכוני אשראי או למדדי סיכונים סביבתיים). מעבר לכללי רגולציה, ניתן להעלות את רמת ההגנה המקומית גם באמצעות תמריצים, כגון הקלות מס להשקעה בציוד אבטחת מידע והגנה (למשל באמצעות פחת מואץ). הבעיה העיקרית היא, שלא ברור איזה ציוד יביא את התועלת הגדולה ביותר באופן גורף בכלל המשק, והאם הציוד לא היה נרכש בכל מקרה גם ללא הטבת המס. על מנת לתת תמריצים, יש לשפר באופן משמעותי את המידע הזמין לגופים ולחברות בנוגע לרמת ההגנה שלהם במרחב הקיברנטי, ובכך לאפשר למדינה לגבש מדיניות תמריצים מושכלת, ולגופים ולחברות לקבל החלטות מיטביות לגבי רכש מערכות הגנה.

6.3 המלצות לפעילויות מנהלת לפיתוח תעשיית הסייבר הישראלית

1. פעילויות ארגוניות של המנהלת

אסטרטגיית פעילות:

- ביסוס מוקד ידע במנהלת ולתוכנית, שיקיף את הצדדים המדעיים, הטכנולוגיים, הביטחוניים והעסקיים של התחום.
- יצירת מתודות עבודה למנהלת, מול הפעילויות המתנהלות במערכות הביטחוניות, האקדמיות והממשלתיות, ומול שותפים חיצוניים לתוכנית (כגון מדינות זרות)
- העלאת מודעות לתחום והתאמה של הכשרת כוח אדם לצרכים לאומיים.
- קידום רגולציה מעודדת חדשנות טכנולוגית בישראל, והשפעה על רגולציה ותקינה בעולם.

פעילויות:

- יצירת **מוקד ניהול** וידע על בסיס כוח אדם חדש וקיים, המגובה בתשתיות פנימיות של ציוד טכנולוגי ואופרציה ארגונית.
- **קידום תיאום ושיתופי פעולה בין גופים שונים העוסקים בתחום.** חשוב מאד ליצור ערוצים דינמיים, שיאפשרו את מעבר הידע בין מערכות הביטחון והאקדמיה לתעשייה, ליצור מסגרות של שיח משותף, וליבון של בעיות ופתרונות משותפים בין הגורמים הרלוונטיים וגופי הביצוע.

- ריכוז והפצת המידע על כלל הפעילויות המתקיימות בישראל בתחום, לרבות פעילויות בממשלה, במגזר העסקי ובאקדמיה, תוך פרסום התוכנית והצגתה בארץ ובעולם.
- הובלת הפעילות הבינלאומית מול גופים מקבילים בעולם.

2. שותפות המנהלת בהרחבת פעילויות למימון מחקר

אסטרטגיית פעילות:

- שותפות עם האקדמיה ומערכת הביטחון במימון מחקר בתחום, וביצירת קהילה אקדמית של חוקרים, תלמידי מחקר וסטודנטים; שיתוף פעולה עם חברות תעשייה מקומיות ובינלאומיות מובילות.

פעילויות:

- **שיתוף פעולה עם גופי ביטחון והמועצה להשכלה גבוהה בהקמת מרכז מחקר וידע בתחום**
- **שיתוף פעולה עם גופי ביטחון והמועצה להשכלה גבוהה במימון ובהזמנת מחקרים מהאקדמיה**
- **שיתוף פעולה אפשרי עם תוכניות רלוונטיות ומתאימות למחקר יישומי באקדמיה, המתנהלות באחריות לשכת המדען הראשי במשרד התמ"ת**

3. הרחבת פעילויות למימון יזמות ולקידום התעשייה על ידי המנהלת

אסטרטגיית פעילות:

- שותפות עם מערכת הביטחון והמדען הראשי בתמ"ת במימון מחקר ופיתוח תעשייתיים וחדשנות, ביצירת קהילת יזמים טכנולוגיים ועסקיים, ובקידום פעילות עסקית בתחום.
- קידום ניסויים ובדיקות של טכנולוגיות ישראליות במערכות ההגנה האזרחיות ובמערכת הביטחון.
- קידום פעילות מקומית של חברות רב לאומיות מובילות, ושל משקיעים, תוך מיצוב ישראל כיעד מועדף להשקעות פיננסיות בתחום הסייבר: במחקר ופיתוח, בחדשנות, בחברות תעשייה ישראליות ובתשתית המקומית.

פעילויות:

- **הקמת מוקד שירות לתעשייה וליווי מקצועי לחברות הזנק, שמטרותיו:**
  - יצירת מוקד מידע כללי לחברות תעשייה ישראליות ורב לאומיות.
  - בחינת טכנולוגיות ראשוניות וסיוע בהכוונת חברות לצרכי השוק.
  - קידום ניסויים (אתרי בטא) לטכנולוגיות, וליווי חברות הזנק במהלכם.
  - יצירת ממשקים אפקטיביים בין החברות ובין גורמים רלוונטיים במערכות הביטחוניות, משרדי הממשלה והאקדמיה.
- **קידום יזמות לפיתוח טכנולוגיות רלוונטיות, למשל במסגרת חממה טכנולוגית.**
  המטרה היא לקדם יזמים טכנולוגיים בשלבים מוקדמים של פיתוח טכנולוגיות בעלות חשיבות למעטפת הגנת הסייבר הלאומית, ולבחור ביניהם על פי שיקולים של תועלת להגנת הסייבר. מבנה הפעילות יכול להיות דומה לזה שבחממה הטכנולוגית בתוכנית החממות של המדען הראשי (פרטי-ציבורי), וניתן אף להפעילו במשותף עם תוכנית החממות של המדען הראשי במשרד התמ"ת. מומלץ לתת את הדעת לשיתופי פעולה מובנים עם גופי מערכת הביטחון במבנה החממה או פעילות קידום יזמות אחרת.
- **מימון יזמות לפיתוח טכנולוגיות בנושאי הגנת הסייבר במסגרת חברות הזנק**
  המטרה היא לקדם פיתוח של טכנולוגיות בעלות חשיבות למעטפת הגנת הסייבר הלאומית, במסגרת חברות הזנק. במסגרת דיוני הועדה עלתה הצעה למערכת הביטחון להקים מודל פעולה של קרן ההשקעות הממשלתית, בדומה לקרן In-Q-Tel האמריקאית.
  הקרן האמריקאית משקיעה משאבי ממשלה בחברות הזנק, ומאיצה פיתוח חדשנות בעלת פוטנציאל משמעותי לקהילת המודיעין האמריקאית. קיומה של קרן כזו בישראל עשוי להאיץ פיתוחים לתועלת מערכת הביטחון בחברות הזנק, ואף להאיץ את ההשקעות באותן חברות מצד קרנות וגופי השקעה פרטיים.

4. הרחבת פעילויות למימון פרוייקטים בתעשייה על ידי המנהלת

אסטרטגיית פעילות:

- מיקוד מאמצי מחקר ופיתוח בפרוייקטים גדולים ופורצי דרך במשותף עם התעשייה, על מנת להגדיל את רמת ההגנה במרחב הקיברנטי, תוך חיזוק משמעותי של היתרון היחסי של התעשייה המקומית.
- השקעה פרטית מקסימלית בעלות הפרוייקטים, תוך עידוד יצוא הטכנולוגיות, המוצרים והשירותים המפותחים בפרוייקט.
- שותפות עם מדינות זרות במימון פיתוח הפרוייקטים.

פעילויות:

- **הובלת פרוייקטים בתעשייה, תוך שיתוף פעולה עם גורמים אחרים.**
- **שותפות בפרוייקטים תעשייתיים גדולים או משמעותיים ובמימונם.**

6.4 בחירת פרויקטים בתעשייה

בחירת פרוייקטים בתעשייה על פי הצרכים הלאומיים להגנת המדינה במרחב הקיברנטי

אסטרטגית פעילות:

- יוזמת ומימון פרוייקטים בתעשייה צריך להתבצע מתוך צרכים לאומיים להגנת המדינה.
- בפרוייקטים גדולים ביוזמת או בשיתוף הממשלה, יש לתת דגש לביצועם בתעשייה ולמינוף היכולות והידע למען פעילות נוספת
של התעשייה הישראלית בשווקים העולמיים.

פעילויות:

- **תעדוף יוזמות על פי צורך לאומי להגנת המדינה ומגבלת משאבים**
תעדוף בין היוזמות וההקבצים צריך להיעשות לפי הצורך הלאומי ביוזמות להגנת המדינה, ועל פי מגבלת המשאבים העומדת בפני המיזם ושותפיו. התועלת הכלכלית היא רכיב נוסף בתהליך קבלת ההחלטות, ויש לה השלכות, בין היתר על עלות המימון הממשלתי בכל אחד מהפרוייקטים. את בחינת היוזמות שאינן בעלות השפעה משמעותית על פיתוח התעשייה או על המחקר האקדמי, צריכה רק מערכת הביטחון לערוך ולתקצב.
- **אפיון הפרוייקטים השונים בדרך שתקדם את התעשייה הישראלית**
יש לשתף גורמי ממשלה האמונים על קידום התעשייה הישראלית באפיון הפרוייקטים השונים, על מנת להגדיל ככל הניתן את היקף הפעילות בתעשייה, ולאפשר מינוף מרבי של הידע והיכולות שבידי התעשייה לפעילות עתידית נוספת בשווקים העולמיים.

דו"ח תת הוועדה לבחינת התועלות האקדמיות

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

1. תקציר מנהלים ועיקרי ההמלצות

עצמאות בעולם הסייבר תאפשר למדינת ישראל לשמר ולחזק בטווח הארוך את מקומה בתחום, ההולך וצובר תאוצה בעולם, ותשפיע על חיי התושבים, על ביטחון המדינה, על החברה, על עולם התקשורת וכן על נושאים נוספים שיתפתחו בעתיד. המשך הפעילות בתחום, וכניסה משמעותית יותר של המדינה אליו, תתרום לחיזוק האקדמיה הישראלית, לחוסנה של מערכת הביטחון ולקידום התעשייה הישראלית - שתוכל להמשיך להיות חלוצה ומובילה עולמית בתחום.

פיתוח וחיזוק של האקדמיה בתחומי הסייבר וחישוב-העל, בפן המחקרי וההוראתי, **הינם אבני היסוד של בניית ושימור יכולות לאומיות ברות קיימא במימד הקיברנטי.** אין ספק, כי האקדמיה היא המחוללת העיקרית של **ידע, חדשנות, וקניין רוחני**, כמו גם המקור **לכוח אדם מוכשר ומיומן** - ובכך מזינה לא רק את עצמה, אלא גם מגזרים אחרים, ובראשם התעשייה ומערכת הביטחון. בנוסף, ממלאת האקדמיה תפקיד של **צרכן**, בעיקר בכל הקשור למערכות חישוב מתקדמות ולתקשורת רחבת פס. לאקדמיה בישראל מספר **חוזקות בולטות בתחום,** בעיקר בכל הקשור לקריפטוגרפיה מתמטית ולאלגוריתמיקה, אשר עליהן נשענות גם במידה רבה התעשייה הישראלית ומערכת הביטחון. אולם זוהה **פער אקדמי, הנובע מחוסר במסה קריטית, במחקר** בתחומי הקריפטוגרפיה היישומית, הנדסת אבטחת מידע, שיטות פורמאליות במדעי המחשב וכן בתחום החומרה של חישוב מתקדם. כמו כן, זוהה פער **ביכולת התמיכה, ההכשרה והייעוץ** לאקדמיה, כמו גם לגופים נוספים, בכל הקשור לשימוש **ביכולות חישוב מתקדמות.** תת הוועדה לתועלות באקדמיה הוקמה כאחת משבע תתי ועדות של "המיזם הקיברנטי", ועליה הוטלה המשימה לבחון את הצרכים בתחום הסייבר, שהוגדר כתחום בעל משמעויות ביטחוניות, בהקשר האקדמי, להמליץ על תוכניות פעולה לקידום התחום ולנתח את העלויות והתועלות הלאומיות מתוכניות אלו בהיבט האקדמי[1].
העבודה נעשתה בשיתוף ובהתייעצות עם שש תת הוועדות האחרות של המיזם.
לאור האמור לעיל, ממליצה תת הוועדה על **חמש יוזמות עיקריות:**

1. הקמת **מרכז מצוינות מחקרי בתחום הסייבר,** במסגרת תוכנית ה-I-CORE
2. הקמת **מרכז ידע ומחקר בתחום ה– High Performance Computing (HPC)**
3. **תגבור מענקי מחקר אישיים** בתחום
4. **גידול במספר הסטודנטים** לתואר ראשון ושני בתחום
5. **שינוי מדיניות אמ"ן** לגבי פרסום עבודות אקדמיות[2]

בנוסף, תת הוועדה ממליצה לבחון בעתיד יצירת מסגרות מתאימות יותר למחקר בסיסי בתחומים רלוונטיים בתוך מערכת הביטחון.
כמו כן, בתחומים הרלוונטיים לעולם האקדמיה בלבד, ודורשים קביעה של סדרי עדיפויות פנימיים באקדמיה:

1. תת-הוועדה ממליצה על **שדרוג מיידי של רוחב הפס לתקשורת** בין המוסדות האקדמיים בארץ, ובינם לחו"ל. את המענה הפרטני ומימונו יקבעו בהיוועצות משותפת נשיאי האוניברסיטאות, פורום סגני נשיא למו"פ של האוניברסיטאות, מחב"א וות"ת.
2. תת הוועדה ממליצה לות"ת לדון האם וכיצד יש לפעול בנושא שדרוג **יכולות החישוב המקומיות** של האקדמיה. המענים שהוצעו נועדו ליצור מסה קריטית במחקר ובידע בתחומי הסייבר וה-HPC בארץ, ולפתח עבורם כוח אדם מוכשר, תוך הנעת תהליכים ארוכי טווח. **התועלות העיקריות** הצפויות מהמענים הן:

- פיתוח **ידע, חדשנות וקניין רוחני** בתחומים (אקדמי בסיסי; יישומי לתעשייה, למעהב"ט)
- פיתוח והרחבת **כוח אדם מחקרי** - סגל אקדמי בכיר ותלמידי מחקר (לאקדמיה, למעהב"ט, לתעשייה)
- פיתוח יכולות ייעוץ, תמיכה והכשרה **למשתמשי** HPC (באקדמיה, במעהב"ט ובתעשייה)
- הכשרת כוח אדם בתחום: הגדלת **מספר סטודנטים** (לאקדמיה, למעהב"ט, לתעשייה)
- הכשרת כוח אדם: פיתוח **קורסים** בתחומים רלוונטיים לתארים ראשון ושני (ע"י סגל מחקרי שיגיע לתחום)
- יצירת והרחבת **שיתופי פעולה** בין מוסדות אקדמיים שונים **בארץ** בתחום (דרך מרכז המצוינות)

[1] הרכב תת הוועדה ותהליך עבודתה מפורטים בסעיפים ב.2 ו-ג.2.
[2] מאחר שהנושא נתון להחלטות אמ"ן ומערכת הביטחון, תת הועדה ממליצה שאלו יבחנו את הסוגיה לעומק ויגבשו המלצות פרטניות בנושא.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

- יצירת והרחבת **שיתופי הפעולה** בתחום **אקדמיה – תעשייה, אקדמיה – מעהב"ט** (הזמנות מחקר, מחקרים משותפים, שירותי ייעוץ ותמיכה ועוד)
- העמקת **שיתופי הפעולה** המחקריים בתחום בין מוסדות אקדמיים **בארץ ובחו"ל** (דרך מרכז המצוינות)
- מרכז ידע בנושאי השלכות חברתיות וכלכליות של מדיניות סייבר - לטובת **מקבלי ההחלטות**
- שדרוג **יכולות חישוב–העל** של האקדמיה בארץ (דרך ציוד מחשוב ורוחב פס מתאימים) - בהתאם להחלטות שתתקבלנה
- **חילופי סטודנטים** בתחום עם מוסדות להשכלה גבוהה בחו"ל (בעקבות הרחבת שיתופי הפעולה עמם, "השבה" של חברי סגל ממוסדות שונים בעולם, וגידול מספר הסטודנטים בתחום)
- העלאת **המודעות** לתחום ולחשיבותו (השפעה על מערכת החינוך, תקינה ומדיניות ממשלתית, גמישות ופתיחות של אמ"ן ומעהב"ט בכלל, השקעות פרטיות בתחום ועוד)

סך כל התקציב הנדרש עבור היוזמות שלעיל (מרכז המצוינות בסייבר, מרכז ידע ומחקר ב-HPC, תגבור מענקי מחקר, גידול במספר הסטודנטים ושינוי במדיניות אמ"ן), מוערך בכ- 372 מיליון ₪ למשך חמש שנים (מעבר לתקציב הנוכחי המושקע בתחום), כלומר, בממוצע תוספת של כ- 74 מיליון ₪, כ-14%, לשנה (שתמומן בידי ות"ת, מערכת הביטחון, המוסדות השותפים וגורמים נוספים).[3] התקציב השנתי עבור התחום באקדמיה יסתכם בכ- 590 מיליון ₪ בשנה.

2. רקע

2.1 מטרת המסמך

מטרת מסמך זה היא לסכם את עבודת תת הוועדה לבחינת התועלות האקדמיות במסגרת "המיזם הקיברנטי". הוועדה קיבלה כמנדט לבחון את הפערים בין המצב הרצוי למצב המצוי בהקשר האקדמי, להמליץ על תכניות פעולה לקידום התחום, ולנתח את התועלות הלאומיות מתוכניות אלו בהיבט האקדמי. תת הוועדה החלה את עבודתה לקראת סוף דצמבר 2010, ובמהלך כארבעה חודשים בחנה את הסוגיות השונות וגיבשה את המלצותיה.

עיקרי הדברים מסוכמים במסמך זה.

המסמך סוקר בתחילה בקצרה את המצב הנוכחי בתחום הסייבר באקדמיה ובממשקיה עם התעשייה ומערכת הביטחון. לאחר מכן, ממופים עיקרי הצרכים בתחום (אלו של האקדמיה, ואלו הלאומיים המצריכים פעולה באקדמיה). לבסוף, מוצעים מענים אפשריים לצרכים, וניתנת הערכה ראשונית של עלותם והתועלת שבהם.

2.2 תת הוועדה לבחינת התועלות האקדמיות

תת הוועדה לבחינת התועלות האקדמיות הוקמה כאחת משבע תתי ועדות של "המיזם הקיברנטי", ועליה הוטלה המשימה לבחון את הצרכים בתחום הסייבר בהקשר האקדמי, להמליץ על תוכניות פעולה לקידום התחום ולנתח את העלויות והתועלות הלאומיות מתוכניות אלו בהיבט האקדמי.

לראשות הוועדה מונה פרופ' אהוד גזית, סגן הנשיא למו"פ באוניברסיטת תל אביב, המופקד על הקתדרה לננו-ביולוגיה ויו"ר הדירקטוריון של חברת "רמות" בע"מ. למזכירת הוועדה מונתה ד"ר ליאת מעוז, מנהלת פרוייקטים מיוחדים ומנהלת תוכנית מרכזי המצוינות במל"ג/ות"ת. הרכב הוועדה מגוון וכולל חוקרים באקדמיה, אנשי מערכת הביטחון העוסקים בתחומי הכשרת וגיוס כוח אדם ובתחומי חישוב-על, אנשי משרד התמ"ת העוסקים

[3] פירוט לגבי הערכת העלויות וגורמי המימון השונים, מופיע בהמשך העבודה.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

בתחומי המו"פ, נציג משרד האוצר, נציגי משרד ראש הממשלה ונציגי המל"ג/ות"ת.
רשימת חברי הוועדה מופיעה בתחילת המסמך.

חברי הוועדה התייעצו לצורך עבודתם עם הגורמים הבאים:
- חוקרים באקדמיה, מתחומים שונים הרלוונטיים לתחום הסייבר:
- צרכני חישוב מתקדם - חוקרים וסמנכ"לי אוניברסיטאות האמונים על תחום המחשוב
- מומחים בתחום החישוב המתקדם, ביניהם מומחים ממחב"א, והרצאת אורח של ד"ר דן צפריר מהפקולטה למדעי המחשב בטכניון
- גורמים הרלוונטיים ממערכת הביטחון - ביניהם אורי וינוקור מחיל המודיעין המנהל עבודת מטה ללימודים לקראת תואר ייעודי בסייבר, ואורי סתיו המנהל את גיוס כוח האדם בתחומים הרלוונטיים מחיל המודיעין
- מזכירי תת הוועדות השונות במיזם הקיברנטי

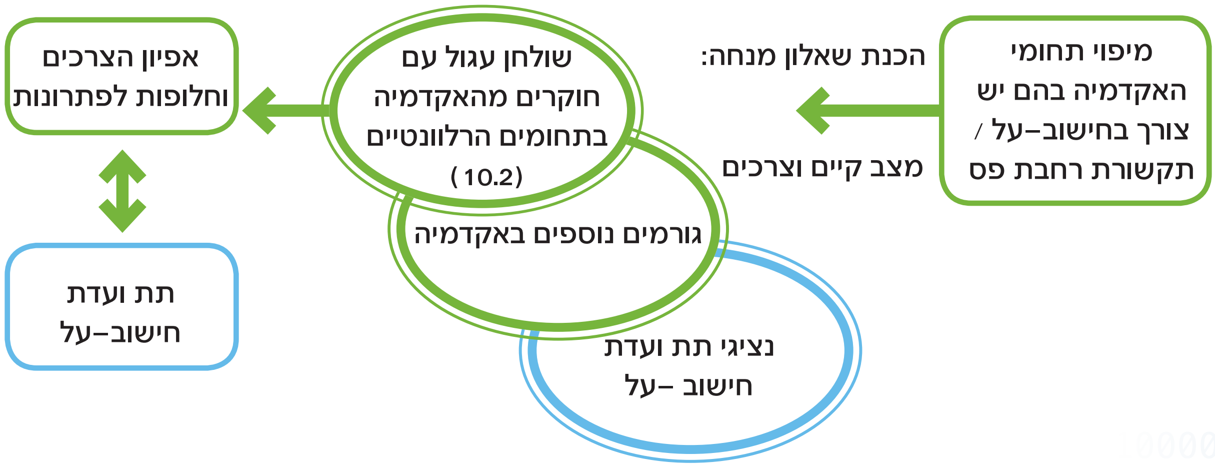
2.3 תהליך העבודה ומתודולוגיה

שלושה עקרונות מרכזיים הנחו את עבודת הוועדה:
- ריכוז כל ההיבטים הנוגעים לאקדמיה (כ"צרכנית" וכ"יצרנית" של כוח אדם, ידע, חדשנות וקניין רוחני)
- עבודה משותפת והדוקה עם תתי הוועדות השונות
- תהליך רחב המשתף חוקרים מתחומי האקדמיה הרלוונטיים, וכן גורמים רלוונטיים ממערכת הביטחון ומהתעשייה

עבודת תת הוועדה התמקדה באפיון התועלות האקדמיות מבניית יכולות בעולם הסייבר, בשני ממדים:
1. מענים של מהלכים אפשריים בעולם הסייבר על צרכי האקדמיה (בעיקר מהלכים בתחום מחשוב על ותקשורת)
2. מענים שהאקדמיה יכולה לספק לצורך בניית יכולות לאומיות בעולם הסייבר (בעיקר קידום מו"פ ויצירת הון אנושי)

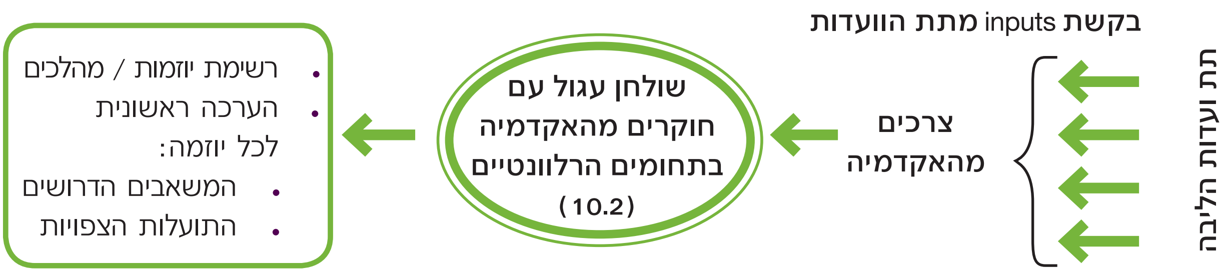
לפיכך, להלן תהליך העבודה שהוגדר:

1. מענים לצרכי האקדמיה:



לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

2. מענים באקדמיה לצרכים לאומיים:



תת הוועדה הגדירה את המשימות הפרטניות כדלהלן:

1. **אפיון צרכי האקדמיה, שיכולים לקבל מענה ממהלכים בעולם הסייבר**
   - מיפוי תחומי המחקר הרלוונטיים
   - אפיון איכותי של הצרכים בכל תחום מרכזי
   - מיפוי הפתרונות הנוכחיים והערכת החשיבות למצוא פתרונות מקומיים בעולם הסייבר
   - אפיון סוגי הפתרונות הדרושים (בתיאום עם תת הוועדה לחישוב-על ותשתיות תקשורת רחבות פס)
2. **אפיון מענים אפשריים של האקדמיה לצרכים הכוללים**
   - מיפוי וניתוח המצב הנוכחי
   - אפיון ועיצוב מענים ספציפיים לצרכים במסגרת מוגדרת
   - הערכה ראשונית של המשאבים הדרושים לכל מענה והתועלות הצפויות (לאקדמיה ו-spillover)
3. **גיבוש המלצות ותוכנית פעולה עקרונית**
   - תעדוף ואינטגרציה לכדי תוכנית קוהרנטית
   - הערכת המשאבים והגורמים השותפים הדרושים לתוכנית
   - הערכה ראשונית של המשאבים הדרושים והתועלות הצפויות לתוכנית כולה (לאקדמיה ו-spillover)

3. מיפוי המצב הנוכחי

3.1 יכולות ונכסים של האקדמיה הישראלית

3.1. מחקר:

באופן כללי, בתחום מדעי המחשב, ישראל חזקה מאוד מחקרית. התחום תופס נתח גבוה של העשייה המחקרית בכלל בישראל (גבוה משמעותית ממדינות אחרות: כ-4.5% מסך הפרסומים בישראל, בהשוואה לכ-3% מסך הפרסומים בעולם) וממוצע הציטוטים לפרסום בתחום - מדד לאיכות הפרסומים - הוא גבוה (כשני ציטוטים לפרסום ישראלי במדעי המחשב, לעומת ממוצע של 1.5 בעולם במדעי המחשב) בתת-התחום "מדעי המחשב - תיאוריה ושיטות" כמו גם בתת התחום "הנדסת תוכנה" נמצאת ישראל במקום השני בעולם בממוצע ציטוטים לפרסום. לעומת זאת בתת-התחום "מערכות מידע", היא נמצאת במקום שמיני, וב"חומרה וארכיטקטורה" במקום שביעי. תת הוועדה, בשיתוף עם תת הוועדות האחרות, זיהתה מספר תחומים עיקריים במחקר הסייבר. להלן מיפוי הנכסים, היכולות והחוסרים באותם תחומים, וכן מצב התחום בעולם:

	נכסים ויכולות	חוסרים	מצב התחום בעולם
הצפנה	הצפנה מתמטית: מובילות עולמית; כ-20 אנשי סגל עוסקים חלקית בקריפטולוגיה	קריפטואנליזה יישומית: רק 2-3 חברי סגל בכירים ועוד בודדים כסגל זוטר	תחום בשל ומפותח

הנדסת אבטחה	בהנדסה: עיסוק בתחום הרחב יותר של tamper detection	רק כ-10 חוקרים בנושא בארץ, מעטים עוסקים בו באופן מלא	תחום מפותח וצומח (מואץ מאז 11-9)
שיטות פורמאליות	מספר חוקרים בולטים בארץ; אפשרות למנף יכולות ולפתח מובילות עולמית	הגרעין בארץ לא מספיק גדול	תחום צומח. עדיין מעט עיסוק בעולם ב science of security
"הגנה"	מרכז אקדמי מפותח בתחומי הגנה באוניברסיטת באר שבע (בשיתוף דויטשה טלקום) ומרכז מתוכנן באוניברסיטת בר אילן	אין קבוצות מחקר בעלות שם עולמי	תחום מפותח וצומח
חישוב-על / חישוב מקבילי	מספר חוקרים בודדים מצוינים בתחום, בעיקר בצד התוכנה	מחסור במסה קריטית בארץ; חולשה בצד החומרה והארכיטקטורה	תחום מפותח מאוד (מוקדים בארה"ב, סין, ספרד)

קריפטואנליזה (מאת אורי סתיו, תת ועדת צופן):
כיום כ-20 אנשי סגל באקדמיה בארץ עוסקים כחלק מתחום עיסוקם בקריפטולוגיה. מתוכם רק 2 עוסקים בקריפטואנליזה - פרופ' אלי ביהם ופרופ' עדי שמיר. ניתן לכלול בנוסף אליהם גם את החוקרים ד"ר נתן קלר וד"ר אור דונקלמן, אף על פי שאינם חברי סגל, משום העיסוק הקבוע שלהם בנושא זה מספר שנים והפרסומים הרבים שלהם בתחום.

לשם השוואה:
באוניברסיטת לוקסמבורג, במעבדה לאלגוריתמים בקריפטולוגיה ובאבטחה חברים 7 אנשי סגל, ולצידם 16 עוזרי מחקר. ביניהם, ניתן למנות את ביריוקוב, קורון וחוברטוביץ' כחוקרים מובילים בתחום הקריפטואנליזה. יש 4 עוזרי מחקר נוספים שעוסקים בתחום הקריפטואנליזה. באוניברסיטת Shandong, במעבדה לטכנולוגיה קריפטוגרפית ואבטחת מידע חברים 7 אנשי סגל ו15 חוקרים נוספים. גם כאן רב העיסוק בתחום הקריפטואנליזה. בין החוקרים הבולטים בתחום - Xiaoyun Wang, Meiqin Wang, Hongbo Yu. כאן הספירה אינה כוללת את עוזרי המחקר והסטודנטים.

פעולה (מאת צחי שנרק, תת ועדת פעולה):
קיים מרכז אקדמי מפותח בתחומי הגנה באוניברסיטת באר שבע (במימון דויטשה טלקום) ומרכז מתוכנן באונ' בר אילן (במימון אירופי). מעורבות מעהב"ט מינימלית. פרט לכך קיימות קבוצות מחקר קטנות וחוקרים בודדים במרבית האוניברסיטאות.
קיימות פעילויות מעטות שמפא"ת מממנת בעיקר באוניברסיטת בן גוריון ובעבר גם באוניברסיטת תל אביב, בעיקר בתחומים הקשורים לניתוח התנהגויות של רשתות וזיהוי אנומליות.

ניתן לסכם ולומר, שבתחום הסייבר, יש באקדמיה הישראלית מספר תחומים שהמחקר הישראלי בהם מוביל עולמית, אולם ישנם כמה איים שבהם הפעילות המחקרית בארץ לא הגיעה למסה קריטית.

3.1.2 הוראה:

להלן הערכה של מספרי הסטודנטים בתחומים הרלוונטיים[4] במוסדות המתוקצבים להשכלה גבוהה תש"ע:

	אוניברסיטאות		מכללות מתוקצבות		סה"כ
	מדעי המחשב ומתמטיקה	הנדסת אלקטרוניקה ומחשבים	מדעי המחשב	הנדסת אלקטרוניקה ומחשבים	
תואר I	5,383	5,559	3,100	6,992	21,034
תואר II	651	824	160	226	1,861
דוקטורט	407	283	--	--	690
סה"כ	6,441	6,666	3,260	7,218	23,585

3.2 מיפוי שיתופי הפעולה בין האקדמיה לבין מערכת הביטחון והתעשייה

להלן מיפוי שיתופי הפעולה העיקריים בתחום הסייבר

- **שת"פ עם מערכת הביטחון:**
- מודלים של העסקת חוקרים מהאקדמיה (היקפן מוגבל, ככל הנראה בשל חוסר גמישות במדיניות פרסומים של מערכת הביטחון).
- הזמנות מחקר של מפא"ת מהאוניברסיטאות השונות - ברמת מת"ט (מחקר תשתיתי טכנולוגי) וברמת מו"פ.
- פעולה - מעורבות מינימלית של מעהב"ט; פעילויות מעטות שמפא"ת מממנת, בעיקר באוניברסיטת בן גוריון ובעבר גם באוניברסיטת תל אביב, בעיקר בתחומים הקשורים לניתוח התנהגויות של רשתות וזיהוי אנומליות.
- הגנה - שת"פ של רא"ם מול אוניברסיטאות בן גוריון, בר אילן ותל אביב (MBA).
- **שת"פ עם התעשייה:**
- מרכזי מחקר
- מרכז אקדמי מפותח לנושאי הגנה באוניברסיטת בן גוריון (במימון דויטשה טלקום)
- מוקד נקודתי באוניברסיטת תל אביב במימון צ'קפוינט
- במסגרת מגנ"ט מוקם בימים אלו "מאגד cyber - הגנת מערכות ממוחשבות מפני תקיפה דרך הרשת"[5]

3.3 מיפוי השקעות נוכחיות בתחום הסייבר באקדמיה הישראלית

ההשקעות בתחום באקדמיה נעשות בשני אפיקים מרכזיים - הוראה ומחקר.

הוראה:

תעריפי התקצוב של ות"ת לסטודנט (באלפים) הם:

	אוניברסיטאות		מכללות מתוקצבות	
	מדעי המחשב	הנדסת אלקטרוניקה ומחשבים	מדעי המחשב	הנדסת אלקטרוניקה ומחשבים
תואר I	32.6	37	26.2	31.3
תואר II	45.4	48	27	35.7

[4] מאחר שאין תחום לימודי סייבר, הנתונים כוללים את הסטודנטים לתארים במדעי המחשב ומתמטקה, וכן בהנדסת אלרטרוניקה ומחשבים

[5] תוכנית מגנ"ט (מו"פ גינרי טכנולוגי) פועלת במסגרת המדען הראשי, למען שיתוף פעולה אמיתי בין חברות תעשייתיות, ובינן לבין מוסדות מחקר, במו"פ של טכנולוגיות טרום-תחרותיות ובהטמעתן. שיתופי פעולה אלו מסייעים בקידום טכנולוגיות, פיתוח מרכיבי הידע של כל אחד מהשותפים, וכן ניצול הידע המצרפי לצורך פיתוחים עתידיים. ה"מאגד" הוא מסלול למו"פ של טכנולוגיות גנריות - התאגדות של תאגידים תעשייתיים ומוסדות מחקר, לביצוע פיתוח עצמי של טכנולוגיות גנריות. התאגידים ב"מאגד" מפנים את היכולות שנרכשו במגנ"ט לפיתוח מוצרים המבוססים על טכנולוגיות אלה. מגנ"ט הינה מנגנון אחד מני רבים שמפעיל המדען הראשי לעידוד שיתוף פעולה בין האקדמיה לתעשייה, ביניהם גם: מגנטון, נופר, קמין ומימד.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

במחקר, תקצוב ות״ת לאוניברסיטאות מתבטא ע״פ תפוקות מחקר[6], במענקי מחקר בתחומי הסייבר של הקרן הלאומית למדע (ה-ISF[7]) , במימון ות״ת, ותקציב ות״ת לפרוייקט ISRAGRID[8] במסגרת תל״ם[9].

על מנת להעריך פעילות בהוראה ובמחקר, שיכולה לתרום לתחום הסייבר במישרין או בעקיפין, נכללו התחומים מדעי המחשב[10], ו-40% מהפעילות בתחום הנדסת אלקטרוניקה ומחשבים.[11]

להלן הערכות לגבי סך כל הפעילויות באקדמיה בתחומים שלעיל, שהמדינה מתקצבת באמצעות ות״ת, כולל תקציבי הוראה ומחקר לאוניברסיטאות ולמכללות המתוקצבות, מענקים בתחומי הסייבר של הקרן הלאומית למדע (ה-ISF) ותקציב ות״ת לפרוייקט ISRAGRID במסגרת תל״ם:

(סכומים במלש״ח לשנה):	תקצוב אוניברסיטאות		תקצוב מכללות		הקרן הלאומית למדע (ISF)	תל״ם (ISRAGRID)	סה״כ
	מדעי המחשב	מתוך הנדסת אלק' ומחשבים	מדעי המחשב	מתוך הנדסת אלק' ומחשבים			
הוראה	103	98	86	91	0	0	378
מחקר	100	34	0	0	4	1	139
סה״כ	203	132	86	91	4	1	517

בסה״כ מדובר על **מעל חצי מיליארד** ₪ **בשנה** לשימושים שהוזכרו. מעבר לכך, ישנם תקציבי מחקר למוסדות מגורמים לא ממשלתיים (תרומות, קרנות מחקר חיצוניות וכו'), והכנסות למוסדות משכר הלימוד של הסטודנטים (במוסדות המתוקצבים, כמו גם במוסדות לא מתוקצבים).

לסיכום, בתחום מושקע תקציב גבוה, הן לפעילויות הוראה, והן לפעילויות מחקר, ובמובן זה אין כשל שוק באקדמיה.

6 תפוקות מחקר נמדדות על-ידי הות״ת בשלושה מדדים עיקריים: מספרי פרסומים משוקללים ב-impact factor, זכייה בקרנות מחקר תחרותיות ולא-תחרותיות ומספר תלמידי מחקר (דוקטורנטים וסטודנטים).

7 הקרן הלאומית למדע (Israel Science Foundation) היא הגוף המרכזי כיום התומך במחקר הבסיסי במדינת ישראל. מענקי המחקר של הקרן מחולקים על בסיס תחרותי, בהתאם למדדי מצוינות מדעית, על פי החלטה של מערך שיפוט והערכה בינלאומי הייחודי לקרן, וכולל יותר מ-10,000 מדענים מובילים בארץ ובעולם. פעילות הקרן מקיפה את כל התחומים: מדעים מדויקים וטכנולוגיה, מדעי החיים והרפואה ומדעי הרוח והחברה. מקבלי המענקים הם חוקרים באוניברסיטאות, במכוני המחקר, במוסדות להשכלה גבוהה אחרים ובבתי החולים

8 ISRAGRID הינו פרוייקט שמיועד, בראש ובראשונה, לקיים תשתית למחקר ופיתוח טכנולוגיית Grid ו-cloud בישראל. ISRAGRID נענית לצרכים של כלל גופי המו״פ, כולל גופי מו״פ ו-IT בארגונים בשלל תעשיות, בחברות היי-טק בשלות ובינלאומיות שהמו״פ הוא עיקר עיסוקן וכן בחברות הזנק בשלבים שונים, שנזקקות גם כן לסיוע טכנולוגי רב, ולהקטין את ההוצאות על ציוד וכוח אדם על מנת לשרוד. בכוונת ISRAGRID לספק תשתית Grid ו-cloud למו״פ עבור האקדמיה והתעשייה בישראל, וכן להגדיל את משאבי המחשוב ואת הניצול היעיל שלהם בידי ארגונים, חברות ומוסדות.

9 פורום תל״ם (תשתיות לאומיות למחקר ופיתוח) כולל את האקדמיה הלאומית למדעים , ות״ת, המדען הראשי במשרד התמ״ת, משרד המדע והטכנולוגיה, מפא״ת במשרד הביטחון ואגף התקציבים במשרד האוצר. פעילותו מתקיימת בסיוע משרד התמ״ת. מטרותיו המרכזיות הן:
תיאום בין גופי הפורום בנושאי מחקר ופיתוח
איגום משאבים מתקציבי הגופים שבפורום (וגופים נוספים על פי העניין).
קביעת אחריות ביצוע בדבר תשתיות מחקר ופיתוח לאומיות.
בימה לליבון בעיות משותפות ולעתים גם לקידום אסטרטגיה משותפת.

10 בניכוי הסטודנטים למתמטיקה באוניברסיטאות

11 הנושאים בלימודי תואר ראשון כלליים, ולא ניתן לשייך סטודנטים לתחום הסייבר. גם בתארים מתקדמים ובעבודות מחקר, קשה להפריד בין תוכן ישיר של תחום הסייבר, ובין תוכן שיש לו השלכות על התחום, או שיתרום בעתיד לפיתוחו. לפיכך, נקטנו בגישה של הערכת יתר, כמפורט, בלי להיכנס לתכני הלימוד או המחקר.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

4. אפיון צרכי האקדמיה

חוקרים בארץ משתמשים באופן גובר בחישוב-על (בתצורות שונות) בתחומים רבים: חקר המוח ורשתות נוירונים, ביו-אינפורמטיקה/ביולוגיה חישובית, כימיה חישובית, פיזיקה (אסטרופיזיקה, חלקיקים, קיפול חלבונים, פיזיקה קוונטית / מצב מוצק, מערכות מורכבות ועוד), מדעי כדור הארץ ומטאורולוגיה, הנדסה (אוירונאוטיקה, אקוסטיקה ועוד), מדעי המחשב, ועוד. מתוך דיון השולחן העגול שנערך עם חוקרים באקדמיה[12], ומתוך שיחות והתכתבויות עם סגני הנשיא למו"פ וחוקרים נוספים[13], עולה כי לרוב, צרכי החישוב אינם לחישוב מקבילי ממש, וכי פתרונות החישוב הם מקומיים. בחלק קטן מהמקרים, כאשר הפתרון המקומי אינו מספק, נעשה שימוש בשותפויות עם חוקרים בחו"ל או בשירותי מחשוב על מעל ענן. בדרך כלל, החוקרים הדגישו כי צווארי הבקבוק לפריצות דרך מחקריות אינן תלויות ביכולות חישוב-על מתקדמות בהרבה מאלה הקיימות. (עם זאת, ברור שצורת החשיבה וכיווני המחקר הנוכחיים מושפעים מיכולות החישוב הקיימות, וייתכן שקיום משאבי חישוב-על היה מביא לשינוי בנ"ל) התמונה הבאה עולה, לגבי צרכי החוקרים באקדמיה (על פי סדר חשיבות):

1. ידע ומיומנות:

צורך במרכז של ידע, ייעוץ והכשרה מקצועית ב-HPC: תחומי חומרה, ניהול המערכת, תכנות ואלגוריתמים, עם מחויבות למדענים ולהעברת הידע לסטודנטים. מרכז כזה יצטרך תשתית HPC cluster) קיים באקדמיה / יכולות HPC משלו) לשימוש עצמי מחקרי בלבד. הצורך נובע מכך, שעל מנת לנצל בצורה מיטבית את יכולות החישוב הקיימות, נדרש ידע מקצועי ומעמיק.

במקרים רבים נדרשים תלמידי מחקר להתמקצע בתחום ה-HPC. בכך יורד זמן מחקר יקר לטמיון, ובנוסף, הידע אובד כאשר תלמידי המחקר מסיימים את לימודיהם.

2. רוחב פס:

צורך אקוטי בשדרוג מיידי של רוחב הפס לאקדמיה, הן בתוך הארץ (בין מוסדות), והן בין הארץ לחו"ל, הנובע משימוש בכוח חישוב מרוחק, ומהצורך להעביר כמויות גדולות של מידע בקצבים גבוהים בין מוסדות שונים. חיבור האינטרנט של האקדמיה בישראל לחו"ל הוא באמצעות מחב"א[14], ברוחב פס של שני קווים של 2.5Gbps, שנשכרים ממד-נאוטילוס. רוחב הפס מגביל חוקרים שונים, בעיקר בתחומי הפיזיקה של אנרגיות גבוהות והביו-אינפורמטיקה. חיבור האקדמיה בתוך הארץ נעשה באמצעות מחב"א (כ-ISP), בקצב נמוך ביותר של Gbps1 מקווים שמחב"א שוכרת מפרטנר (וכן גיבוי של Mbps400 מבזק).

3. ציוד / יכולות חישוב HPC

- בחלק מהתחומים והמוסדות, יש צורך מהותי בשדרוג ה-clusters במוסדות (Interconnections ו- Cores), תוך יצירת תשתיות משותפות של מחשבים מרובי מעבדים.
- לא נמצא צורך ספציפי במחשב על או ביכולות HPC מרכזיות. חוקרים רבים אף מעדיפים יכולות חישוב מקומיות על פני מרכזיות.

[12] סיכום המפגש מופיע בנספחים.

[13] מכתבים שונים שהתקבלו מופיעים בנספחים.

[14] מחב"א - "מרכז החישובים הבין-אוניברסיטאי", הינו עמותה ללא מטרות רווח, שנוסדה על ידי שמונת האוניברסיטאות בישראל, ונתמכת על ידי הוועדה לתכנון ולתקצוב של המועצה להשכלה גבוהה. העמותה עוסקת בתשתיות תקשורת, שרותי מידע דיגיטאליים, טכנולוגיות למידה ובתשתיות גריד, ופועלת לטיפוח שיתוף הפעולה והסיוע בתחומים אלו בין המוסדות החברים בה, ובינם לבין מוסדות מחקר וארגונים בעלי עניין משותף, העוסקים בנושאי המחקר וההוראה האוניברסיטאית.

5. אפיון צרכים לאומיים שדורשים מענה במסגרת האקדמיה

להלן פירוט הצרכים שעלו בתת הוועדות הרלוונטיות[15]

הצרכים של האקדמיה (כפי שעלו בתת-ועדת אקדמיה ופורטו לעיל):

1. צורך במרכז של ידע ייעוץ והכשרה מקצועית ב-HPC
2. שדרוג רוחב הפס לאקדמיה, הן בתוך הארץ (בין מוסדות) , והן בין הארץ לחו"ל.
3. בחלק מהתחומים והמוסדות, צורך מהותי בשדרוג ה-clusters הקיימים במוסדות (Interconnections -ו Cores)

הצרכים בתחום חישוב-על (מאת אריאל פרנס, תת ועדת חישוב-על ותשתיות תקשורת רחבות פס):
מתוך עבודת הועדה עולה אם כן כי במדינת ישראל קיימים מספר "איים" של עיסוק בחישוב-על. איים אלה, הנמצאים במערכת הביטחון, האקדמיה ובתעשיות, עובדים ברוב המקרים באופן עצמאי, ועל כן לא נוצרת סינרגיה ביניהם. **העדר הסינרגיה** גורם לקושי ביכולת של כל אחד מהצרכנים להתמודד עם אתגרי חישוב על שלו. אולם מהמחקר עולה, כי לרוב הגופים הצרכנים אתגר משמעותי משותף והוא **פערי ידע** בתחומים המתקדמים של חישוב-על **וקושי באיתור הכשרה והעסקה** של אנשי מקצוע מובילים בתחום. עוד עולה בוועדה כי ציוד חישוב-על הוא בחלק מהמקרים פער, אך תמיד משני בחשיבותו ובקדימותו לפערי הידע והמומחיות. כאשר קיים צורך במחשבי על "סטנדרטים" - ניתן כיום לרכוש את הציוד הנדרש בעלויות סבירות ברוב המקרים, ואם קיים פער אזי מדובר בפער תקציבי (למשל בחלקים מהאקדמיה בישראל). כאשר קיים צורך בציוד לא סטנדרטי, הפער המרכזי הוא במחקר ופיתוח של ציוד כזה או ביכולת ובידע לנצל ציוד כזה בצורה אופטימאלית. האפשרות הנוספת בקשת האפשרויות היא המקרה שבו "לא קיים צורך" בחישוב-על. אפשרות זו יכולה אף היא להצביע, ולו בחלק מהמקרים, על פער ביכולת לזהות את הצורך - הנובע מפערי ידע בתחום.

על בסיס הלמידה והניתוח כפי שמסוכמים במסמך זה, חברי הוועדה מוצאים לנכון להמליץ על **הקמת "מרכז לאומי לחישוב-על"**, שייעודו יהיה הובלת מחקר ופיתוח בתחום חישוב-על וחישוב עתיר ביצועים.

הצרכים בתחום צופן וסימולציה (מאת אורי סתיו, תת ועדת צופן):

1. הגדלה משמעותית של כמות **כוח האדם החוקר** בתחומים האפליקטיביים.
2. **שינוי והגמשת המדיניות הביטחונית** על מנת לאפשר שיתוף פעולה עם חוקרים פעילים באקדמיה.

בתחומים העיקריים הבאים:

- **קריפטואנליזה יישומית:** מחקר יישומי לתכנון ותקיפה של אלגוריתמי הצפנה ומימושם במערכות תקשורת. המחקר מיועד למצוא שיטות תקיפה מתמטיות ואלגוריתמיות על מערכות ופרוטוקולי תקשורת מוצפנים. המחקר מכוון לתוצאות יישומיות אל מול מערכות ומימושים קיימים. פן נוסף של מחקר זה כולל את תחום התממת המידע (סטגנוגרפיה) - זיהוי שימוש בהתממות מידע ותכנון שיטות התממה.
- **הנדסת אבטחת מידע**: מחקר למציאת חולשות תכנון ומימוש של מערכות מחשוב על מנת לאפשר תקיפה שלהן. מחקרים מסוג זה יאפשרו חיסון של מערכות האבטחה וההצפנה הישראליות או מציאת ויצירת יכולות תקיפה בסייבר. המחקרים כוללים תכנון הגנות הן ברמת התוכנה והן ברמת החומרה וההגנות הפיזיות על מעבדים.
- **שיטות פורמאליות במדעי המחשב** (אימות, הוכחות קוד, איתור חולשות וכד'): מחקר המיועד לפתח שיטות ניתוח להוכחת חסינות של מערכות ושל קוד מפני פגיעות.

הצרכים בתחום פעולה (מאת צחי שנרק, תת ועדת פעולה): אין כיום **תוכניות לימוד מובנות** בתחום. אין קבוצות מחקר בעלות שם עולמי, **אין שת"פ** משמעותי עם תעשייה ישראלית או עם מעהב"ט. דוגמאות למשפחות תחומי מחקר אפשריים:

15 סיכום דיון "שולחן עגול" של תת-הוועדה האקדמית של המיזם הקיברנטי הלאומי עם נציגי תת-הוועדות השונות למיזם, מופיע בנספח.

1. חומרה (מיקרו אלקטרוניקה, רכיבים ומערכות)
2. הנדסת תוכנה
3. מתמטיקה ואלגוריתמיקה בפעילות שהתנענו מול אוניברסיטת בן גוריון הסקנו שהתואר הפשוט ביותר לפיתוח בתחום זה הוא תואר II היות ומדובר ביכולות מולטי דיספלינריות המחייבות ידע מוקדם במגוון תחומים. לא ברור מה הדרישות לתואר I בתחום.

נדרשים לפחות 10 מחקרים בשנה בתחומים שהוזכרו למעלה באקדמיה שיהיו מופנים למגזר הביטחוני (הערכה "מהבטן").

הצרכים בתחום מדיניות ורגולציה (לדברי יו"ר תת הוועדה): על מנת לגבש ולעדכן מדיניות לאומית בנושא הסייבר, ועל מנת שישראל תהיה חלק מתהליכים ומאמצים גלובליים בתחום, תת הוועדה רואה צורך בגיבוש מרכז ידע ומעקב בהקשר של תחום הסייבר בעולם (בתחומי מדיניות, משפטים, סוציולוגיה, מדעי ההתנהגות וכו'). לא ברור אם המרכז צריך להיות במסגרת אקדמית, או מדינית / ממשלתית.

עיקרי הצרכים – תמונה אינטגרטיבית

להלן עיקרי הצרכים שעלו מתת הוועדות השונות, באינטגרציה כוללת.לצורך העניין נגדיר את תחומי המחקר הרלוונטיים תחת המושג "סייבר":

- מדעים מדויקים: קריפטואנליזה יישומית, הנדסת אבטחת מידע, שיטות פורמאליות במדעי המחשב, למידה חישובית/ זיהוי אנומליות
- הקשרים של סייבר בתחומים הבאים: מדיניות ציבורית, משפטים, סוציולוגיה, חינוך, מדעי ההתנהגות, ניהול וכלכלה

הצרכים שעלו מתחלקים לשתי קטגוריות:

קטגוריה א': מחוץ לעולם האקדמיה – צרכים לאומיים לשם חיזוק תחום הסייבר וה-HPC (אקדמיה-תעשייה-מערכת הביטחון)

1. **חיזוק המחקר** המדעי בתחום ה"סייבר" בישראל וביסוס מעמדו כגורם מוביל בעולם:
   1. גידול **במספר חברי הסגל האקדמי** בתחומים הרלוונטיים -באמצעות "השבת מוחות" ועידוד מחקר של חוקרים ותיקים או חדשים בתחומים הרלוונטיים
   2. הגדלת **תקציבי המחקר** המופנים לתחומים הרלוונטיים
   3. שיפור ושדרוג התשתיות המחקריות הרלבנטיות באוניברסיטאות, ובכלל זאת - שדרוג רוחב הפס וה-clusters במוסדות הזקוקים לכך
   4. יצירת **מסה קריטית והעצמת היתרונות היחסיים** במחקר בתחום במוסדות האקדמיים השונים
2. הקמת **מרכז לאומי של ידע ומחקר, ייעוץ, והכשרה מקצועית בתחום חישוב-העל** (HPC)
3. עידוד שיתופי פעולה מחקריים בתחום הסייבר בין המוסדות להשכלה גבוהה, וביניהם לבין מערכת הביטחון והתעשייה.
4. חיזוק ההוראה בתחום, לשם הכשרת כוח אדם:
   1. קיום וקידום תוכניות הוראה והכשרה מתקדמות בתחום הסייבר - בארץ ובשת"פ עם חו"ל (International GraduatePrograms)
   2. גידול במספר הסטודנטים לתואר ראשון במדעי המחשב או הנדסת אלקטרוניקה ומחשבים
   3. גידול במספר הקורסים בתחומי הסייבר במסגרת תארים במדעי המחשב או הנדסת אלקטרוניקה ומחשבים
5. הגדלת שיתוף הפעולה בתחום בין האקדמיה לבין מקבלי ההחלטות וקובעי המדיניות

קטגוריה ב': בתוך עולם האקדמיה – צרכים של האקדמיה לשם חיזוק המחקר האקדמי בתחומים שונים

6. **שדרוג רוחב הפס** של האקדמיה, בתוך הארץ ומול חו"ל, כדי לאפשר יכולות חישוב-על מתקדמות.
7. **שדרוג יכולות החישוב המקומיות** של האקדמיה.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

6. אפיון מענים אפשריים של האקדמיה לצרכים שעלו

6.1 עקרונות לעיצוב המענים

1. יצירת מענים ברי קיימא, שיחזקו את התחום לטווח בינוני וארוך.
2. שימוש, ככל הניתן, במנגנונים ובכלים הקיימים באקדמיה.
3. עידוד וחיזוק המחקר וההוראה בתחומי הסייבר לא על חשבון איכות.
4. למרות שמדובר בתחום בעל חשיבות לאומית וצרכים שהם Top-Down, יש למצוא כלים המאפשרים לחוקרים באקדמיה, עד כמה שניתן, לבנות את המחקר וההוראה בתהליך Bottom-Up, במסלול התפתחות אורגנית.
5. ככל המדובר בצרכי האקדמיה בתחומי הסייבר וחישוב מתקדם - שקילתם אל מול צרכים נוספים של האקדמיה בתחומים אחרים.

6.2 מענים מוצעים

על פי העקרונות שפורטו לעיל, תת הוועדה לתועלות באקדמיה מציעה את המענים שלהלן, תוך אבחנה בין שני סוגי מענים - כאלה העונים באופן ספציפי לצרכים בקטגוריה א', וכאלה העונים לצרכים בקטגוריה ב', שבה בחירת המענים וסדרי העדיפויות מצויים תחת המנדט של ות"ת, ולפיכך נשתדל להימנע מהמלצות ספציפיות אלא נסמן כיוונים אפשריים.

1. מרכז מצוינות

תכנית מרכזי המצוינות[16] מספקת מענה הולם במיוחד לצרכים שתוארו לעיל בתחומי המחקר, הידע, הייעוץ המקצועי ותוכניות ההכשרה המתקדמות. לפיכך תת הוועדה רואה לנכון להמליץ לוועדת ההיגוי של תוכנית **מרכזי המצוינות על הקמת מרכז מצוינות מחקרי בתחומי סייבר ו–**High Performance Computing (HPC) (כשני מוקדים במרכז) שיכלול:

1. גיוס כ-15 חוקרים חדשים מחו"ל (שכר ותוספות מחקר, מענקי מחקר, מענקי ציוד)
2. שדרוג קלאסטר מחשוב קיים באחת האוניברסיטאות (היא "המוסד המתאם") לצרכי מחקר
3. מענקי מחקר לחוקרים קיימים שיהיו חברים במרכז, ולתלמידי מחקר
4. קיום סדנאות, כנסים ובתי ספר בינלאומיים, וכן תמיכה בחוקרים מבקרים ובביקורי גומלין
5. תוכניות של International Graduate Programs

[16] תכנית מרכזי המצוינות (I-CORE: Israeli Centers of Research Excellence) גובשה על ידי ות"ת כחלק מהתוכנית הרב-שנתית להשכלה הגבוהה, וממשלת ישראל אימצה אותה בהחלטה מ-14 במרץ 2010.
מדובר על תוכנית לאומית שמטרותיה העיקריות הן:
1. חיזוק המחקר המדעי בישראל וביסוס מעמדו כגורם מוביל בעולם;
2. "השבת מוחות": החזרת חוקרים מצטיינים לארץ ככלי מרכזי לחיזוק היכולות המחקריות והסגל האקדמי במוסדות להשכלה גבוהה;
3. יצירת מסה קריטית והעצמת היתרונות היחסיים בתחומי מחקר נבחרים במוסדות השונים;
4. שיפור ושדרוג התשתיות המחקריות באוניברסיטאות;
5. עידוד חדשנות אקדמית, לרבות שילובים בין מספר תחומי דעת רב-תחומיות
6. קיום וקידום תוכניות הוראה והכשרה מתקדמות בתחומים נבחרים;
7. עידוד שיתופי פעולה מחקריים בין המוסדות להשכלה גבוהה, אוניברסיטאות ומכללות כאחת.

הרעיון המרכזי הוא להקים כ- 20 עד 30 מרכזי מצויינות במהלך חמש השנים הקרובות, כל אחד בתחום מחקרי אחר, בתקציב ממוצע של 45 מלש"ח למרכז למשך חמש שנים, אשר שליש ממנו ימומן מהממשלה באמצעות ות"ת, שליש מהמוסדות השותפים ושליש משותפים אסטרטגיים. כל מרכז יאגד מסה קריטית של חוקרים מובילים בתחום - חברי סגל במוסדות השונים (אוניברסיטאות, מכללות, בתי חולים ומכוני מחקר), וכן חוקרים ישראלים בתחום שישובו מחו"ל ויצטרפו לאחד המוסדות ולמרכז מצוינות. המרכזים יציעו לכל חוקר חדש שיצטרף תנאים חסרי תקדים, הכוללים בין היתר מענק מחקר שנתי ומענק קליטה ראשוני גבוהים. כל מרכז מוקם בתהליך תחרותי שבמהלכו מתמודדות קבוצות שונות של חוקרים זו מול זו.

ארבעת המרכזים הראשונים שעתידים להתחיל לפעול במאי 2011 יעסקו בנושאים הבאים:
I. נושאים בחזית מדעי המחשב
II. גישות מערכתיות לחקר הבסיס המולקולארי למחלות בבני אדם: ממחקר גנומי לריפוי מותאם -אישי
III. מחקר מתקדם של תהליכים קוגניטיביים
IV. מקורות לאנרגיות מתחדשות, חילופיות ובנות קיימא

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

6. תקציב מחקר לפרוייקטים ניסיוניים (seed money) אחד מארבעת מרכזי המצוינות הראשונים, שעתידים להתחיל לפעול כבר במאי 2011, הוא במדעי המחשב. ועדת ההיגוי של התכנית שרויה בעיצומו של תהליך בחירת נושאים למרכזי המצוינות הבאים. לאור זאת, אנו רואים לנכון להמליץ לוועדת ההיגוי להקים מרכז המצוינות נוסף בתחומי הסייבר וה-HPC, בעיקר בשל הצורך הלאומי שעלה. המלצות תת הוועדה לגבי התאמות התוכנית לצרכים הלאומיים המיוחדים:

- חריגה מתקציב מרכז מצוינות רגיל (שהוא בממוצע 45 מלש"ח, ועד 70 מלש"ח לחמש שנים) והקמת מרכז גדול יותר עם שני מוקדים - בסייבר וב- HPC, בתקציב של כ-95 מלש"ח לחמש שנים - זאת בהנחה שמערכת הביטחון תהיה שותף אסטרטגי (הנושא בשליש מהעלות הכוללת) - פרטים בסעיף "הערכת העלות"
- שיתוף של חוקרים ותלמידי מחקר ממערכת הביטחון במרכז המצוינות -בחלקיות משרה (במקביל לעבודתם במערכת הביטחון), בחל"ת או לאחר שירותם במערכת הביטחון המוקד בנושאי הסייבר יעסוק בתחומים שבהם זוהו צרכים מיוחדים:
- מדעים מדויקים: קריפטואנליזה יישומית, הנדסת אבטחת מידע, שיטות פורמאליות במדעי המחשב, למידה חישובית / זיהוי אנומליות
- הקשרים של סייבר בתחומים הבאים: מדיניות ציבורית, משפטים, סוציולוגיה, חינוך, מדעי ההתנהגות, ניהול וכלכלה[17] המוקד ב-HPC יהווה מרכז לאומי של ידע ומחקר בתחום. מאחר שבאקדמיה אין כמעט צורך ביכולות חישוב מתקדמות מרכזיות לצרכי מחקר אקדמי, אלא במרכז ידע, שירות ותמיכה, תת הוועדה סבורה שבמסגרת מרכז המצוינות אפשר להקצות כ 5-10 מלש"ח על פני חמש השנים לשדרוג קלאסטר קיים באחת האוניברסיטאות החברות במרכז. כמובן, שאם יש גורם שלישי שמעוניין לתרום מחשב על / מערכת HPC (בעלות גבוהה של כ- 100 עד 150 מלש"ח לחמש שנים, כולל תחזוק ושדרוג), אין מניעה שיעשה זאת, אולם **זוהי אינה עדיפות של האקדמיה בישראל לעומת השקעה בתחומים אחרים.**

2. מענקי מחקר

תת הוועדה ממליצה, מעבר למענקים שיינתנו לחוקרים במרכזי המצוינות, גם על תגבור מענקי מחקר אישיים בתחום באמצעות הקרן הלאומית למדע. על מנת שלא לפגוע באיכות המחקר (המתבטאת בין היתר בשיעורי הזכייה במענקים), מוצע המנגנון הבא:
הגדלת תקציב המחקר הכללי של הקרן הלאומית למדע, ובנוסף לכך הקמת קרן ייעודית לתחום (בגודל של כ-4 מלש"ח לשנה במצב יציב - פירוט בסעיף "הערכת עלות"). הצהרה מראש שחוקרים אשר יגישו בקשות מחקר בתחומים רלוונטיים ויזכו, במסגרת הליך השיפוט התחרותי הרגיל של הקרן הלאומית למדע, יקבלו תוספת למענק מתוך הקרן הייעודית.
תת הוועדה גם ממליצה לשקול את מדיניות השימוש בתקציבי מחקר של ה-ISF לביקורי חוקרים או ביקורי גומלין. חוקר המבקר בארץ לתקופה משמעותית ומרצה בתחום מחקרו יכול לשמש כ"זרז" רב ערך, החושף תלמידים בפני תחום מחקר לא מוכר. הידע נטמע בקרב החוקרים המקומיים, וההזדמנויות לאינטראקציה וביקורי גומלין, הם בעלי ערך הרבה מעבר לתקופת הביקור.

3. גידול במספר הסטודנטים לתואר ראשון ושני

על מנת להגדיל את כמות כוח האדם הפוטנציאלי המתמחה בתחומי הסייבר, לצרכי האקדמיה, התעשייה ומערכת הביטחון, תת הוועדה ממליצה להגדיל את מספר הסטודנטים לתארים ראשון ושני במדעי המחשב ובהנדסת מחשבים ואלקטרוניקה. מאחר שתחום הסייבר ממוקד, ודורש ידע רחב במדעי המחשב ובהנדסה, תת הוועדה אינה ממליצה ליצור תואר ראשון בסייבר, אולם אין ספק שככל שיחול גידול במספר אנשי הסגל העוסקים בתחום, יתרבו גם הקורסים לתואר ראשון המספקים הכשרה רלוונטית בסייבר.

[17] הוצאות תחזוקה ותפעול מחושבות החל מהשנה הרביעית.
יש להדגיש כי מחקר בנושאים אלו יסייע לא רק למקבלי ההחלטות, אלא מדובר בכיווני מחקר חשובים ומבטיחים בפני עצמם. גם בעולם, מספר קבוצות אקדמיות מפתחות את הנושא לאחרונה באופן מרשים. לדוגמה, באוניברסיטת קמברידג' נחקרת הפסיכולוגיה של מנגנוני סיסמאות והרשאות; בהרווארד ובמיקרוסופט נחקרים היבטים כלכליים של תולעי רשת וספאם, וב-MIT נחקרים שילובים של מיקרו-כלכלה עם תורת ההצפנה. יתר על כן, מודעות לצרכי המדינה משפיעה גם על החוקרים בנושאים הטכניים; כך, לדוגמה, בעקבות הרצאות שניתנו ב-MIT אודות אסטרטגיית הסייבר של סין ובעיית החומרה הזדונית הנובעת מכך, עודדו את קבוצת הקריפטוגרפיה לפתח גישות פתרון טכניות.

יש לציין, כי תואר שני יכול להיות מחקרי ("עם תיזה"), או תואר ללא תיזה. מסלולי ההכשרה שאינם מחקריים תורמים ישירות להכשרת כוח אדם, במיוחד לתעשייה או למערכת הביטחון. בנוסף, הם תורמים מבחינה אקדמית, בהרחבת היצע הקורסים, וגיוס הסגל לטובת המערכת כולה. בחו"ל מספקות אוניברסיטאות רבות הכשרה מקצועית בתחום הסייבר ברמה גבוהה, במסלול תואר שני ללא תזה.

על פי התוכנית הרב-שנתית של ות"ת להשכלה הגבוהה, יתווספו בהדרגה מכסות של סטודנטים בתחומים הרלוונטיים במוסדות המתוקצבים בשנים הקרובות, שיסתכמו בעוד חמש שנים בכ-2,700 מכסות נוספות - גידול של כ-12% במספר הסטודנטים הנוכחי. במידה שהביקושים ללימודים בתחומים אלו יחרגו מעבר לכך, יוכלו המוסדות לשקול להסיט מכסות מתחומים אחרים. בנוסף, כמובן, מכללות שאינן מתוקצבות על ידי ות"ת חופשיות להגדיל גם את מספרי הסטודנטים שלהן בתחומים הרלוונטיים. תת הוועדה סוברת כי גידול זה יענה על הצרכים שהועלו. מעבר לכך, תת הוועדה ממליצה למערכת הביטחון לשקול חלוקת מלגות מחקר ייעודיות לעבודות דוקטורט בתחומים ספציפיים על פי הגדרתה.

4. שינוי מדיניות אמ"ן לגבי פרסום

אחד החסמים המרכזיים לשיתופי פעולה של האקדמיה ומערכת הביטחון, בעיקר בתחום הצופן, הוא איסור הפרסום הגורף של אמ"ן לעבודות אקדמיות בתחום הצופן. לפיכך, ובהתייעצות עם גורמים באמ"ן, ממליצה תת הוועדה על שינוי המדיניות והגמשתה. בנוסף, ממליצה תת הוועדה לפתח מודלים גמישים יותר להעסקת אקדמאים באמ"ן.

5. לבחינה עתידית: מחקר בסיסי בתוך מערכת הביטחון

רוב המחקר המתבצע היום במערכת הביטחון הוא יישומי, בעוד המחקר הבסיסי מתבצע באקדמיה, לעיתים בשיתוף עם מערכת הביטחון. נשאלת השאלה האם צריך ליצור מסגרות מתאימות יותר למחקר בסיסי בתחומים רלוונטיים בתוך מערכת הביטחון. תת הוועדה שמעה דעות לכאן ולכאן מגורמים במערכת הביטחון ומחוצה לה. כיוון שהנושא חשוב ודורש מידה רבה של התעמקות, תת הוועדה ממליצה לבחון אותו באופן נפרד ויסודי, בשיתוף גורמים המכירים את המנגנונים הקיימים על בוריים.

6. שדרוג רוחב הפס לאקדמיה

שדרוג רוחב הפס של האקדמיה, הן בתוך הארץ והן מול חו"ל, הינו מרכיב מכריע ביצירת מענה של יכולות חישוב מתקדמות לטובת האקדמיה, במיוחד מתוך התפיסה שיכולות החישוב צריכות להישאר מקומיות בעיקרן ולא ריכוזיות. מתוך שיחות עם נציגי מחב"א והאקדמיה, עולה כי לחוקרים באקדמיה יש צורך בשדרוג הקווים לכל הפחות ל-10Gbps, וכי יש ליצור סטנדרט מתעדכן לרוחב הפס. שדרוג רוחב הפס בחיבור לחו"ל אינו בעיה טכנית, אלא כספית - מחב"א תצטרך לרכוש את רוחב הפס הגדול יותר ממד נאוטילוס (כשהמדרגה הבאה אחרי רוחב הפס הנכחי היא 10Gbps) שדרוג החיבור בתוך הארץ ל-10 ג'יגה אפשרי גם כן מבחינה טכנית ע"י השכרת סיבים מגורמים שונים (כמו הוט, חברת החשמל, חברת הרכבת, פרטנר). אם חברת החשמל אכן תכנס לשוק כמפעיל נוסף, יתכן שהמחירים לשדרוג ירדו. תת הוועדה ממליצה לשדרג את רוחב הפס, ולקבוע את המענה הפרטני ואופן המימון בהתייעצות משותפת של נשיאי האוניברסיטאות, פורום סגני נשיא למו"פ של האוניברסיטאות, מחב"א וות"ת.

7. שדרוג יכולות החישוב המקומיות של האקדמיה

לאור השימוש ההולך וגדל של האקדמיה ביכולות חישוב מתקדמות, וקצב ההתיישנות של ציוד מחשוב על, נראה שבשנים הקרובות יהיה צורך בשדרוג תשתיות המחשוב באקדמיה (רכישה ורענון של ציוד). תת הוועדה ממליצה לות"ת לשקול האם וכיצד לפעול בנושא: האם למוסדות יש תקציב מספיק לשדרוג, או האם נדרש תקציב נוסף? האם יש לתמוך בשדרוג באמצעות החוקרים או המוסדות? האם יש להקים קרן ייעודית לנושא? האם יש להרחיב קרנות ציוד קיימות?

6.3 הערכת תועלות לאקדמיה, לתעשייה ולמערכת הביטחון

כלל המענים שהוצעו, נועדו ליצור מסה קריטית במחקר וידע בתחומי הסייבר וה-HPC בארץ, ולהכשיר עבורם כוח אדם, תוך
הנעת תהליכים ארוכי טווח. לתועלות הצפויות מהמענים שתת הוועדה המליצה עליהם יש מעגל השפעה ראשון ושני:

מעגל השפעה ראשון

- פיתוח ידע, **חדשנות וקניין רוחני** בתחומים (אקדמי בסיסי; יישומי לתעשייה, למעהב"ט)
- פיתוח והרחבת **כוח אדם מחקרי** - סגל אקדמי בכיר ותלמידי מחקר (לאקדמיה, למעהב"ט, לתעשייה)
- פיתוח יכולות ייעוץ, תמיכה והכשרה **למשתמשי** HPC (באקדמיה, במעהב"ט ובתעשייה)
- הכשרת כוח אדם בתחום: הגדלת **מספר הסטודנטים** (לאקדמיה, למעהב"ט, לתעשייה)
- יצירת והרחבת **שיתופי פעולה** בין מוסדות אקדמיים שונים **בארץ** בתחום (דרך מרכז המצוינות)
- יצירת והרחבה של **שיתופי הפעולה** בתחום בין **האקדמיה – תעשייה, אקדמיה – מעהב"ט** (הזמנות מחקר, מחקרים משותפים, שירותי ייעוץ ותמיכה)
- העמקת **שיתופי הפעולה** המחקריים בין מוסדות אקדמיים **בארץ ובחו"ל** (דרך מרכז המצוינות)
- מרכז ידע בנושאי השלכות חברתיות וכלכליות של מדיניות סייבר - לטובת **מקבלי החלטות**
- שדרוג **יכולות חישוב–העל** של האקדמיה בארץ (דרך ציוד מחשוב ורוחב פס מתאימים) מעגל השפעה שני:
- הכשרת כח אדם: פיתוח **קורסים** בתחומים רלבנטיים לתארים ראשון ושני.(ע"י סגל מחקרי שיגיע לתחום)
- חילופי סטודנטים בתחום עם מוסדות להשכלה גבוהה בחו"ל (בעקבות הרחבת שיתופי הפעולה עם מוסדות בעולם, "השבה" של חברי סגל ממוסדות שונים בעולם, וגידול מספר הסטודנטים בתחום)
- העלאת **המודעות** לתחום ולחשיבותו (השפעה על מערכת החינוך, תקינה ומדיניות ממשלתית, גמישות ופתיחות של אמ"ן ומעהב"ט בכלל, השקעות פרטיות בתחום

6.4. הערכת עלויות

1. מרכז מצוינות

להערכתנו, עלות המרכז מסתכמת ב–39 מלש"ח לחמש שנים על–פי הפירוט הבא[18]:

הערכת תקציב המרכז לחמש שנים	
קליטת חוקרים חדשים (שכר, תוספות מחקר, מענקי מחקר ומענקי הצטיידות)	24
כוח אדם מנהלי	2
פעילות מחקר	8
ציוד למרכז	2
תקורות	3
סה"כ	39

כמובן שהתקציב למרכז המצוינות יקבע בהליך הרגיל על-ידי ועדת ההיגוי לתכנית מרכזי המצוינות.

[18] כמובן תקציב המרכז, אם יוחלט להקימו, יקבע על-ידי ועדת ההיגוי של תכנית מרכזי המצויינות. להלן מופיעות הערכות שערכה תת-הוועדה, על מנת לקבל סדרי גודל.

יש להדגיש, כי הערכת התקציב לעיל מתבססת על ההנחה שמדובר במודל המימון הרגיל למרכזי מצויינות: שליש בתקצוב ות"ת, שליש בתקצוב המוסדות השותפים ושליש במימון שותף אסטרטגי וכי **מערכת הביטחון תפעל כשותף האסטרטגי**:

מימון העלות בין הגורמים השונים		
גורם	מימון לחמש שנים (מלש"ח)	%
המוסדות השותפים	13	33%
ות"ת	13	33%
מערכת הביטחון (שותף אסטרטגי)	13	33%
סה"כ	39	100%

2. מרכז ידע ומחקר בתחום ה-High Performance Computing (HPC)

להלן הערכת תקציב המרכז לחמש שנים:

1. **ציוד ומבנה תשתיתי ל**–HPC, כולל הקמה, תחזוקה ותקורות - 75 מלש"ח
2. **קליטת חוקרים חדשים**
   - שכר ותוספות מחקר - 1.25 מלש"ח לקליטה של כל חוקר
   - מענקי מחקר בסכום כולל של 10 מלש"ח
   - מענקי הצטיידות חד פעמיים בסכום כולל של 2 מלש"ח
3. **כוח–אדם מנהלי –** 2 מלש"ח
4. **פעילות מחקר לחוקרים הותיקים**
   - תלמידי מחקר ופוסט דוקטורנטים: 4.5 מלש"ח
   - פעילות בינלאומית ופרוייקטים ניסיוניים - 3.5 מלש"ח

סך תקציב המרכז לחמש שנים מלש"ח	
שכר - אקדמי ומנהלי (לפי 6 חוקרים נקלטים)	10
פעילות מחקר	20
ציוד תשתיתי, הפעלתו ותחזוקו	75
סה"כ	105

חלוקת תקציב המחקר בין הגורמים השונים

א'. המוסדות: שכר לסגל האקדמי ולסגל המנהלי: כ- 10 מלש"ח לחמש שנים

ב'. בהתאם למנגנון שיבחר, ישאו הגורמים האחרים (חברי פורום תל"ם במנגנון הראשון או מפא"ת וות"ת במנגנון השני) בעלויות של כ-95 מלש"ח לחמש שנים. בכל מקרה רוב המימון לרכיב זה יגיע ממפא"ת ומתקציב תוספתי במסגרת המיזם הקיברנטי.

2. מענקי מחקר

- מענקי מחקר אישיים - סה"כ תוספת של כ- **5.5 – 6.0 מלש"ח בשנה** (תוספת של 138% - 150% בתקציב)
- הגדלת תקציב המחקר הכללי של הקרן הלאומית למדע: בתוך התוכנית הרב שנתית - גידול ממוצע של כ- **1.5–2 מלש"ח** לשנה למענקים בתחום הסייבר / HPC במהלך חמש השנים הבאות (סה"כ 7.5-10 מלש"ח) - תקצוב ות"ת (גידול מעבר לכ-4 מלש"ח בשנה היום לתחום)
- הקמת קרן ייעודית לתחום: תגבור של כ-**4 מלש"ח בשנה** למענקים בתחומים הרלוונטיים (קרן ייעודית

בתקצוב מערכת הביטחון). מדובר בתגבור של כ- 20 מענקים חדשים בשנה, כל אחד בכ-25% (תוספת של כ-50 אלש"ח לשנה למשך 4 שנים).

3. גידול במספר הסטודנטים לתואר ראשון ושני

העלות של גידול מדורג במספר הסטודנטים, שיגיע לכ- 2,700 סטודנטים נוספים בעוד חמש שנים, היא **בממוצע 40 מלש"ח לשנה לחמש השנים הקרובות** (כלומר, בשנה החמישית מדובר על תקצוב של 80 מלש"ח מעבר לתקצוב הנוכחי, ובסה"כ בכ- 200 מלש"ח נוספים על-פני חמש השנים הקרובות). בעלות זו תישא ות"ת כחלק מהתוכנית הרב-שנתית להשכלה הגבוהה.

4. שינוי מדיניות אמ"ן לגבי פרסום

ללא עלות נוספת

5. לבחינה עתידית: מחקר בסיסי בתוך מערכת הביטחון

לבחינה עתידית

6. שדרוג רוחב הפס לאקדמיה

הרחבת החיבור לחו"ל לשני קוים של 10Gbps אינה בעיה טכנית, אלא כספית בלבד : מחב"א משלמת היום 580 אלף יורו לשנה עבור תקשורת בינ"ל. על פי ההערכה, ביוני 2012 יעמוד המחיר לפעמיים 10 ג'יגה על כ- 3 מיליון יורו עבור דנטה (פי שלוש מהיום). סביר להניח שמחב"א ישלמו גם כן פי שלוש מהיום, כלומר כ- 1.6 מיליון יורו לשנה (תוספת של מילון יורו לשנה - כ- 5 מיליון ₪ לשנה).

שדרוג החיבור בתוך הארץ ל- 10 ג'יגה אפשרי באמצעות שכירת סיבים מגורמים שונים (כמו הוט, חברת החשמל שאולי תיכנס כמפעיל נוסף, רכבת ישראל, פרטנר). הערכת העלות במשך שש השנים הקרובות במצטבר נעה בין 7 ל- 25 מלש"ח (תלוי בגורם המשכיר). לשם השוואה, הערכת העלות של הרשת הקיימת באותה תקופה היא 7.9 מלש"ח.

עלות ציוד הקצה לשדרוג רוחב הפס אינה משמעותית (תשלום חד פעמי של כחצי מלש"ח) לסיכום, שדרוג רוחב הפס של האקדמיה בתוך הארץ ומחוצה לה אפשרי מבחינה טכנית בטווח המיידי, וידרוש בסה"כ תוספת של כ- 6-7 מלש"ח בשנה (ייתכן שבקרוב המחירים ירדו, עקב כניסה אפשרית של חברת החשמל בארץ ושל בזק בינ"ל והוט לחו"ל). כיום מחב"א ממומנת על ידי המוסדות הנהנים משירותיה בלבד. כאמור, המענה הפרטני ואופן מימונו יקבעו בהתייעצות משותפת של נשיאי האוניברסיטאות, פורום סגני נשיא למו"פ של האוניברסיטאות, מחב"א וות"ת.

7. שדרוג יכולות החישוב המקומיות של האקדמיה

לשם הערכת העלות דרושה עבודה פרטנית מול כל אחד מהמוסדות האקדמיים הרלוונטיים. כאמור, תת הוועדה ממליצה לות"ת לשקול האם וכיצד לפעול בנושא.

סיכום

סך כל התקציב הדרוש עבור היוזמות שיש להן חשיבות לאומית - יוזמות 1 - 4 (מרכז מצוינות, תגבור מענקי מחקר, גידול במספר הסטודנטים ושינוי במדיניות אמ"ן), הוא: סך הכל לחמש שנים: 292 מיליון ₪ נוספים (מעבר לתקציב הנוכחי בתחום), כלומר, תוספת ממוצעת של 58.4 מיליון₪ לשנה.

מתוכם: כ-240 מיליון ₪ מות"ת (200 לתוספת מכסות סטודנטים, 32 למרכז מצוינות, ו-8 למענקי מחקר נוספים) כ-52 מיליון ₪ ממערכת הביטחון (32 למרכז מצויינות ו-20 למענקי מחקר נוספים) מדובר על תוספת של כ-11% לשנה, מעבר ל-517 מיליון ₪ לשנה שות"ת משקיעים כבר היום באקדמיה, כך שהתקציב השנתי עבור התחום באקדמיה יגיע לכ- 575 מיליון ₪ בשנה.

7. נספחים

נספח א– סיכום דיון "שולחן עגול" של תת הוועדה לבחינת התועלות האקדמיות

סיכום של דיון "שולחן עגול" של תת הוועדה לבחינת התועלות האקדמיות של המיזם הקיברנטי הלאומי עם חוקרים שונים מהאקדמיה שהתקיים בתל–אביב ביום ו' באדר א' תשע"א, 10.2.2011

נכחו:

שלומי דולב, מדעי המחשב, אונ' בן-גוריון; יו"ר מחב"א	רודד שרן, ביואינפורמטיקה, המחלקה למדעי המחשב, אונ' ת"א
אן וייל זרחיה, מדעי המחשב, הטכניון	הנדסת אלקטרוניקה ומחשבים
אלון קורנגרין, מדעי החיים, בר אילן	סול עפרוני, ביולוגיה חישובית, הפקולטה למדעי החיים, בר אילן
פנחס אלפרט, מדעי כדור הארץ ומדעים פלנטריים, אונ' ת"א	עודד הוד, כימיה חישובית, המחלקה לכימיה, אונ' ת"א
יעל שומר, מדעי המדינה, אונ' ת"א	ליאור קרוניק, חומרים ופני שטח, המחלקה לכימיה, מכון וייצמן
שלום אברבנאל, מתמטיקה שימושית, אונ' ת"א	טל אלכסנדר, אסטרופיזיקה, המחלקה לפיזיקה, מכון וייצמן; אחראי מחשוב על בועדת המחשוב של מכון וייצמן.
חברי ועדות המיזם הקיברנטי הלאומי	לורן לוינסון, פיזיקה של חלקיקים ניסיוני, המחלקה לפיזיקה, מכון וייצמן
מאיר נצר, יו"ר תלם	אהוד דוכובני, פיזיקה של חלקיקים ניסיוני, המחלקה לפיזיקה, מכון וייצמן
רם לוי, מולמו"פ	מיכה ברקוז, פיזיקה של חלקיקים, המחלקה לפיזיקה, מכון וייצמן ; יועץ בכיר לנשיא המכון לנושא טכנולוגיות מידע
ליאת מעוז, ותת	ריצ'רד ברקוביץ', המחלקה לפיזיקה, בר אילן
נדב לירון, המחלקה למתמטיקה, הטכניון	גיא תל-צור, מדעי המחשב, אונ' בן-גוריון
שירה נבון, ותת	טל הסנר, מדעי המחשב, האונ' הפתוחה
דני גלושנקוב, אגף תקציבים, מש' האוצר	
אבי שביט, לשכת המדען הראשי, מש' התמ"ת	
גיל ארז, לשכת המדען הראשי, מש' התמ"ת	
יוסי אבראבנאל, חמ"ן, צה"ל	
דורון חבצלת, מפא"ת	
יעל עטיה, ותת	

רם לוי, מזכיר הוועדה למיזם הקיברנטי הלאומי, פתח את המפגש בסקירה של המיזם עם מצגת:
- חזון ומטרת המיזם
- ניתוח המטריציוני - מו"פ המתבצע ואינו מתבצע

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

בדיקת היכולות השונות בידי ארבע ועדות, וכן שלוש ועדות רוחב - לתועלת כלכלית, תועלת אקדמית ומדיניות וחקיקה
- כתבי מינוי לוועדות
- התוכנית הסופית
- תהליך הבחינה

ד"ר מעוז הציגה את עצמה וציינה כי תחום העבודה של תתהוועדה יהיה מעבר לאופק האקדמיה. מטרת תת הוועדה היא לבחון את צרכי החוקרים שעוסקים בעולם החישוב, האינטרנט וכו': כוח חישוב ותשתיות תקשורת. בחלק השני של עבודתה תיבחן תת הוועדה איך האקדמיה יכולה לתרום לתחום ולפתח את הידע בו. הדיון הנוכחי מיועד להפגיש בין חוקרים מתחומים שונים, על מנת לברר את הצרכים בתקשורת רחבת פס, סימולטור קיברנטי וכוח חישוב, וכן נושאים נוספים שיציעו הנוכחים.
שלוש שאלות מרכזיות:
מה הצרכים היום בתחומים השונים?
מה הפתרונות שבשימוש היום? והאם הם מספקים?
אם היה כוח חישוב גדול מאד, מה היו עושים איתו?

הערות:

- מר גלושנקוב (מאגף התקציבים במשרד האוצר) הזכיר כי שאלת הצרכים צריכה להיות מלווה בשאלה - האם יש מוכנות להשתתף במימון?
- הודגשה חשיבות מיפוי הצרכים, ומה יכולה להיות התועלת, בעוד שאלת הכדאיות (הכספית) תדון מאוחר יותר.
- כמו כן, יש לחשוב על השאלה - מה יקרה אם לא יהיה כושר חישוב-על?
- צוין כי לדעת הדובר, כל השאלות מובילות להקמת מתקן (facility) מרכזי. הוא ציין, שבמכון וייצמן מנוהל ה-HPC בצורה שונה ורוצים לחזק את היכולות של החוקרים במכון.

הנוכחים הציגו את עצמם כולל תחום העיסוק המדעי שלהם והשימוש בחישוב-על.

הערות של משתתפים שונים:

- תהיה נטייה לטובת המשתמשים הכבדים, אך יש חוקרים שאינם משתמשים ב-HPC.
- משתתף ציין שכאשר לא היתה לו יכולות ולא ידע להשתמש בציוד, הוא למד.
- אנשים רבים לא רוצים לשנות את הקו המקצועי שלהם ולהפוך לאנשי מחשבים. הם רוצים לקבל פתרונות מדף, בידיעה שבכך יצטרכו, אולי, להתפשר קצת. תשובות כמו "אם אתה צריך, תתאמץ" - אינן מתאימות.
- ד"ר מעוז הבהירה שכרגע יש למפות את הצרכים, וביקשה מהמשתתפים להציג את התחומים שלהם.
- יש לחשוב בשתי רמות: ברמה הלאומית וברמה המוסדית. עכשיו, יש לחשוב ברמה הלאומית.
- הפתרון של רכישת עוד מחשב אינו מצדיק את עצמו: בעוד ארבע שנים, הכל יהיה מיושן.
- ד"ר מעוז ביקשה להתמקד בצרכים לפי תחומים.
- צריך להקים קבוצה אשר תחקור HPC.
- הבעיה העיקרית היא רוחב הפס (דובר מתחום פיזיקה של אנרגיות גבוהות).

מדעי החיים:

- יש קלאסטר (cluster) עם 160 תחנות, אשר משרת את המרכז (במדעי המוח). חשוב שתהיה תוכנית אינטראקטיבית, ודרוש חישוב parallel. הרשת (grid) האירופית אינה די אינטראקטיבית. אינו משתמש ב-Isragrid. משתמשים בכרטיסים גרפיים, שהם טובים. קשה לנבא את הצרכים בעתיד. כל הפתרונות נקודתיים. הצרכים תלויים בתקשורת: אין תקשורת מהירה שהיא CPU-intensive.

ביואינפורמטיקה:

- יש קלאסטר ייעודי עם 8 קורים, וזה מספיק. כנראה שלא עושים חישובים מסובכים מדי. תוכנות ל-integer programming תופסת את רוב השימוש. המשתמשים יכולים, בתיאוריה, לפתור דברים, וגילו שעדיף לעסוק במחקר מאשר בדברים אחרים (חישובים).

Isragrid

- נשאלה שאלה - האם הנוכחים שמעו על Isragrid? הרוב השיבו שלא שמעו. משתתף הסביר לאחרים מהו Isragrid.
- מטרת ה-Isragrid היא לקשר בין מרכזי חישוב במוסדות שונים, על מנת לשפר מהירות ורוחב פס.
- הודגש הצורך להפיץ את המידע על Isragrid ודומיו, כדי שהחוקרים יוכלו להשתמש בהם.

חזרה לביואינפורמטיקה:

- חוקר ציין כי פותרים בעיות בעזרת Amazon elastic compute clouds. קיימת בעיה של רוחב פס ונפח תקשורת בין ארה"ב וישראל. החוקר ציין, כי בעבר נסגרה הגישה שלו לתקשורת באינטרנט בגלל שימוש יתר. משתמשים בחישוב בשיטת embarrassingly parallel.
- במדעי החיים פותרים - פחות או יותר - את הבעיות, והבעיה העיקרית היא תקשורת.
- אין מחשב שמנוצל עד הסוף. מחקרים מותאמים לפי היכולות.

כימיה:

בתחום **חיזוי תכונות של חומרים** נדרשים חישובים כבדים מאד. במחלקה לכימיה (מכון וייצמן) יש קלאסטר גדול (1000 קורים). חלק מהעבודה מתבצעת באמצעים שהחוקר מגייס בארה"ב. כוח חישוב גדול יותר יכול לאפשר מחקר של מערכות מורכבות יותר. העמיתים בחו"ל, שעוסקים באותו תחום, יושבים במרכזי מחשבי העל בארה"ב. אפשר לקבל שעות חישוב בדרכים שונות. השיטה: HPC ו-parallel אמיתי. חלק מהחוקרים מפתחים תוכנות scaling. תוספת כוח חישוב מאפשרת מחקר במערכות ביולוגיות, בין היתר.

- יש דברים שלא ניתן לעשות בגלל כוח החישוב. דרושה תקורה אדירה להשקעה בעבודה ב- GPU. [דובר נוסף הסכים להערה זו.]
- ה-GPU מהווה צוואר בקבוק. דרוש GPU נפרד לכל סוג של אפליקציה, ואיש מקצוע שמתמחה בנושא.
- האם משלמים על שיתוף הפעולה בחו"ל של חוקרים ישראלים?
- דובר ענה: לא תמיד, לפעמים בשל בעיות של רישוי (licensing) אשר מחייב אותנו לעשות את כל העבודה בתוך המוסד, ולא בשיתוף פעולה בחו"ל.
- אין לזרים גישה למעבדות הלאומיות הגדולות בארה"ב (במיוחד אלה שקשורות במשרד הביטחון האמריקאי). הגישה אליהן מוגבלת.
- האם החוקרים בארץ יכולים להשתמש בכוח החישוב של הצבא? [משתתפים ענו: חלקית]
- האם אותה מערכת יכולה לשמש צבא וחוקרים כאחד?
- בעיות גדולות של export license מגבילות את האפשרויות.
- בתחום הכימיה, מחצית מהחוקרים הם משתמשים בסיסיים ומחצית נמצאים בתת יכולות, בשל חוסר אמצעים. החוקר מסר, שיש דברים שיש ברשותו יכולת וידע לעשות אך אינו עושה, כי אין לו את כוח החישוב הדרוש.
- עושים מה שאפשר לעשות ביכולות הקיימות.
- בתחום הכימיה התיאורטית, יש קלאסטר של 300 קורים, אשר נמצא ב-50% capacity. כוח חישוב גדול יותר, בסדר גודל של פי עשר, היה מאפשר לעסוק בבעיות מורכבות יותר, ופותח המון אפשרויות.

פיזיקה:

- חוקר בתחום האסטרופיזיקה: כוח החישוב - יש קלאסטר בשיטת embarrassingly parallel ומשתמשים בכל הספקטרום של החישובים. חזית המחקר אינה מוגבלת על ידי יכולות ה- HPC, אלא על ידי היכולות להבין את הפיזיקה (לא יודעים מה להכניס לסימולציה). תהליך ההיפותזה והאישור יהיה מהיר יותר עם כוח חישוב אחר. בתחום ההידרודינמיקה יש חשיבות לחישובים וסימולציות. השאל היא כמה ניתן לעשות

בעזרת פתרונות מדף? אם עובדים ב-HPC, דרוש אדם מיוחד לטפל במחשוב. לכן, רצוי לעבוד עם פתרונות מדף, ורצוי מרכז השתלמויות ארצי על מנת להדריך סטודנטים להשתמש בחישוב. יש מגוון שימושים, ולכל אחד ה-scaling שלו. החסם אינו טיב המחשב, אלא לדעת איך לנצל יותר טוב את המחשב שיש.

- קבוצה של 20 אנשי HPC שיכולים לעזור ולייעץ לחוקרים, תתרום יותר מאשר ציוד חזק יותר.
- חוקר בתחום **הפיזיקה של מצב מוצק**: התוכניות שמשתמשים בהן היום מפותחות in-house. חוקרים שרוצים לפתח תחום, חייבים לפתוח קלאסטר. אין נוהל מסודר לבקש מימון לדברים כאלה. הוא משתמש בקלאסטר של 160 קור - לא סימולציות - embarrassingly parallel, על מנת לכסות משטח גדול של פרמטרים. צוואר הבקבוק הוא זמן מחשוב. בחו"ל, יש פי עשר יכולות חישוב. יכולות כאלה היו מאפשרות לכל הסטודנטים שלו לעבוד. בפי מאה יכולות היו יכולים להיערך מחקרים שונים, לגבי סוג חדש של בעיות (למשל, לחקור quantum devices) בצורה דו-מימדית ולא רק בצורה חד-מימדית. לגבי כוח חישוב בחו"ל - הוא משתף פעולה, אך זה מחייב לפתוח את המחקר לאנשים בחו"ל (ולא תמיד רוצים לשתף אנשים בחו"ל).
- חוקר טען, שלאף אחד אין צורך ב- dedicated high performance computer. לדבריו, הוא ניסה להשתמש ב-GPU, ללא הצלחה.
- פרופ' שלום אבראבנאל ביקש להתייחס לרמה הלאומית. כאשר מדברים על grand challenges לא אומרים שצריך פי עשר יכולות או כדומה. אם רוצים שישראל תהיה בין חמש המדינות המובילות מבחינה מדעית, יש לשאוף לכך שנוכל להקיף בעיות שהן בגדר grand challenges, אך בינתיים מסתפקים במה שיש. לדעתו, השיקול צריך להיות: האם יש חוקרים שהיו יכולים לטפל בבעיות מסובכות יותר אילו היה להם כוח חישוב - חישוב-על - מתאים. לפעמים, כאשר מקבלים כוח חישוב גדול, לא יודעים להשתמש בו. מחשב עם כמה אלפי קורים היה עוזר, כי היום יש פחות מ-500 קורים. חוקרים ישראלים בחו"ל עובדים על 10,000 קורים, ולא יכולים לחזור לארץ כי אין בה כוח חישוב כזה. נחוץ מחשב על כדי להשתתף בנסיונות עולמיים לפתור grand challenges, ולהיות "חברי המועדון המדעי העולמי", אשר מוכיחים שאפשר לעשות דברים שאחרים רק חולמים עליהם. חישוב-על חיוני לשם כך.
- חוקר בתחום **המטאורולוגיה** ציין, שבקפריסין בונים מרכז HPC גדול, ובישראל עשו פרוייקט HPC עם link scheme כדי לראות מה המצב לפני שהקפריסאים יבנו את המרכז. ליפנים יש מחשבים אשר מאפשרים ריצת earth simulation. לפעמים, בשל המגבלות עוסקים בתחומים שלא היו רוצים לעסוק בהם (כמו חיזוי אנרגיות רוח). אי אפשר לחקור דברים בקנה מידה של מטר, אלא רק קילומטר, ואי אפשר להריץ מאה שנות נתונים הנחוצים כדי לעסוק בחיזוי אקלים. לשם כך חייבים חישוב-על.
- **פיזיקה חלקיקים** - עובדים במאיץ הגדול ב-CERN. יש קלאסטר עם 1000 קורים בשלושה אתרים, המנוהל כמו אחד. הצורך גדל בכל שנה. חייבים לתמוך במשתמשים הפיזיקאים בארץ, וצריכים לאחסן קבצים עבור כל המשתמשים בעולם, כי חוקרים צריכים לשאוב נתונים מכל העולם. ישנן בעיות טכניות ברשת זו. התדר בחו"ל כה גדול שדברים הולכים לאיבוד כי בארץ איטיים מדי, רוחב הפס קטן מזה אשר באירופה.

דיון כללי:

- חוקר ציין, שהסטנדרט הבינלאומי גבוה הרבה יותר מהישראלי: רוחב פס בארץ קטן מהמקובל בעולם.
- חוקר הדגיש את הצורך לרכוש רוחב פס נוסף: אולי אחד לצרכי ביטחון ואחד לצרכי האקדמיה.
- חוקר ציין, כי בחו"ל משתמשים בפס ברוחב פי עשר מבישראל, שבה גם יש פי-ארבע משתמשים מעל המותר ברוחב הנוכחי.
- חוקר ציין כי בנוסף לציוד, צריך להכשיר אנשים. הציוד הדרוש יאפשר להכשיר כוח אדם לפיתוח.
- משתתף הביע חשש מהמלצות שלא ניתן לממשן. לגבי רוחב הפס, הוא ציין שקל להגדיר benchmark ועל סמך זה לראות מה המצב. יש להיצמד ל-benchmark.
- צוין כי כל המדינות באירופה עובדות ברוחב פס פי עשר, לפחות, מאשר בישראל. מה שיש בארץ אינו מספיק.
- חוקר ציין, כי קשה לגייס כסף למחשוב ולציוד (מקרנות מחקר): הקמת קלאסטרים של מחשבים.
- המשתתפים הדגישו, כי חייבים להעסיק מומחה למחשבים כדי להפעיל את המערכות, וזוהי הוצאה יקרה

מאד שאינה ממומנת ע״י קרנות המחקר.

- חוקר טען, שאין זה משנה איזה סוג של פתרון בוחרים: השקעה חד פעמית לא תצליח.

ד״ר מעוז שאלה אם יש חוקרים שמשתמשים בסימולטור קיברנטי ואם יש בכך צורך.

המשך דיון:

- משתתף ציין, שבתחום **מדעי המחשב**, אין סימולציות קיברנטיות. רוצים דברים שאפשר לעשות בטלפון. לדעתו, אין קורלציה בין כוח החישוב לבין פריצות דרך, אך יש קורלציה בין כוח החישוב לבין מספר הסטודנטים שניתן להדריך. דרושים דברים שאפשר לעשות במהירות, כי יש לחץ גדול על מוסדות הלימוד והמחקר, והסטודנטים לא יכולים לעבוד כי אין תשתיות, כגון חיבורים של רוחב פס וכדומה. הנפח חשוב יותר מהאיכותיות. התשתיות חשובות מאד, יותר מהאיכות.
- **תחום מדעי המחשב** בארץ נמצא בין 10 המקומות המובילים, בעיקר בתיאוריה, ופחות במעשי. צריך להכשיר תלמידים שיודעים לעשות high performance computing. ותלמידים אלה דרושים לצבא ולתעשייה. הציוד מכתיב את אופי המחקר שנעשה עכשיו. ישראלים בחו״ל יודעים לעשות דברים שלא ניתן לעשות בארץ, בגלל כוח החישוב. מרכז מחשוב גדול לא רק יתן שירות, אלא גם יפתור בעיות מחקריות. הגישה למחשבים בארה״ב מוגבלת, ויש חשש שתהיה גישה רק למחשבים מיושנים.
- ה-NSF מקים מרכזים לאומיים, ולאחרונה גם Institute of Computation and Experimental Mathematics. זו תשובה לשאלות של הנוכחים על מומחיות בחישובים.
- האם רצוי להקים מרכז לאומי כזה?
- חוקר ציין, שהוא מלמד חישוב מקביל ומכשיר בכל שנה כ-120 אנשים, על בסיס מחשוב עלוב.

מדעי החברה:

נחוץ יותר נפח מ-high performance כדי להתחרות עם עמיתים בארה״ב.

ד״ר מעוז ציינה כי העבודה בנושא תימשך. היא ביקשה מהנוכחים לשלוח חומר/הערות וכיו״צ במייל.

המפגש הסתיים.
רשמה: יעל עטיה

נספח ב- מייל של אשר רוטקופ, אוניברסיטת תל-אביב, 17.2.11

-----Original Message-----
From: Asher Rotkop [mailto:AsherR@tauex.tau.ac.il
Sent: 09:07 2011 ה 17 פברואר
To: VPR - Vice President For Research & Development - Ehud Gazit; Chana Sofer (post)
Cc: Liat Maoz; 'itzikbenisrael@gmail.com'
Subject: RE: RE: סקר צרכים - מחשוב-על

שלום רב

לאחר סיום קבלת התשובות של החוקרים בנושא מחשוב על אני מצרף את התשובה שנשלחה למחב״א :

שלום לכולם

בהמשך לפנייתו של פרופ שלומי דולב בנושא מחשבי על, ביצענו סבב מקיף בין מרבית קבוצות המחקר הרלוונטיות באוניברסיטת תל אביב כדי לקבל את הצרכים שלהם בנושא.
הסיכום של התגובות הוא חד משמעי :

המכנה המשותף הרחב של כל הקבוצות למעט קבוצה אחת הוא בקשה לשימוש בקלסתרים עתירי מיחשוב (HPC) עם כמויות גדולות ככל שניתן של מעבדים, אשר מאפשרים הרצות כבדות של מערכות מקביליות.

רק קבוצה אחת נדרשת ליכולות ספציפיות של מחשבי על (דהיינו שימוש רחב ב SHARED MEMORY + ווקטוריזציה של העבודות) לכן לדעתי במידה והתמונה גם בשאר המוסדות דומה (ראה תגובתו של פרופ דני דולב מירושלים בנושא) - הכיוון שיכול לשרת את מרבית הצרכים של מרבית החוקרים - אינו בכיוון של מחשבי על אלא בכיוון של יצירת תשתיות משותפות של מחשבים מרובי מעבדים שבהחלט יש מקום לחשוב על תשתית משותפת כזו אם כתשתית מחבאית ואם כתשתית ענן בניהול מחבא״י.

כמובן שנושא זה מותנה בקיום תקציבים יעודיים, ובבחינה של נושאים טכנולוגיים נוספית - כגון יכולת גישה למסדי נתונים מדעיים לפי צרכי הקבוצות ועוד.

אשר רוטקופ

נספח ג– מכתבם של נציגי מכון וייצמן 17.2.11

במכון וייצמן תוכנית מיחשוב-על (HPC) עשירה בכל פקולטאות המכון. למעשה, בימים אלה אנו בתחילתה של יצירת תוכנית אב למיחשוב על במכון למספר השנים הקרובות. מטרת מסמך זה להציג את ניסיון חלק מקבוצות המחקר ואת עקרונות הפעולה שהוכיחו את עצמם עד כה, כמו גם לציין במה נוכל להיעזר ביוזמה הלאומית בנושא תשתיות טכנולוגית מידע. ביחס לשאר האקדמיה אנו יכולים רק להעריך את הצרכים ואופני הפעולה הרצויים. לגבי שותפים אחרים כגון תעשייה ובטחון איננו יכולים או מנסים לספק תובנות.

א. סיכום של ניסיוננו במיחשוב על:

1. יש לחשוב על מיחשוב על באקדמיה כציוד מדעי לכל דבר. לפיכך כל התהליך החל מאפיון הצורך, דרך אפיון טכנולוגיה, דרך יישום ועד האפליקציה המדעית באחריותו של המדען/ית. המדען הוא בעל המוטיבציה המרכזית והאחריות לעשיית המדע הטוב ביותר עם הציוד שברשותו, ולכן הוא גם בעל הסמכות בתהליך כולו.

2. במכון מגוון רב של מערכות מיחשוב על. האפשרות למגוון הכרחית בשל תחומי המחקר המגוונים במכון, ובשל רמת התחרותיות באספקט זה השונה מתחום לתחום, וכפועל יוצא מהשאיפה לניצול מירבי בהתאם לצרכי כל קבוצה. המגוון הוא הן ברמה הטכנולוגית של בחירת ארכיטקטורה ופלטפורמות והן ברמה הארגונית. מדען יכול להקים מערכת מיחשוב על בעצמו, או להתאגד עם מספר מדענים לרכוש ולנהל במשותף מערכת מיחשוב על, או להשתמש במערכת המכונית המנוהלת ע״י אגף מערכות מידע (אך היא מצומצמת בגודלה). היתרונות והחסרונות של האפשרויות השונות הן:

הערות	חסרונות	יתרונות	מודל
ואריאנט על מודל זה היא חווה שמדען רוכש, אבל היא נמצאת פיזית באגף מרכזי שמספק תשתית קרור, חשמל וכו וגם מסייע בנושאי מערכת ההפעלה.	1. מחייב בניית מיומנות במיחשוב-על בתוך הקבוצה, לא רק בנושאי אפליקציות אלא בכל נושאי החומרה ומערכת ההפעלה. הדבר כרוך בהשקעה מתמדת רבה. 2. פחות יעיל לקבוצות שאינן משתמשות במיחשוב-על אינטנסיבי.	1. אפשרות להתאמת החומרה לצרכים המדעיים. 2. יעילות מירבית בקבוצות שבהם: א) המדע נדרש בצורה אינטנסיבית למיחשוב על, ב) מוכנות להשקיע בפיתוח ושמירת מיומנויות מיחשוב על בקבוצה. 3. זמני תגובה קצרים ותחרותיות מירבית. 3. יעילות בהכשרת סטודנטים בתפר שבין מיחשוב על ומדע. 4. קטליזטור למדענים נוספים בסביבה להשתמש במיחשוב על.	המדען הוא הבעלים של חוות מעבדים ומתחזק אותה. המדען הוא בעל מוטיבציה מיידית ושליטה בהצלחת התהליך.
ספירת כמות הליבות של מחשב מרכזי והשוואתו למספר הליבות של חווה פרטית הוא כמובן פיקטיבית לגמרי. מחשב על גדול פי מאה המשרת מאה מדענים יכול להיות יעיל יותר או יעיל פחות ממאה מערכות קטנות יותר. הדבר תלוי בפרטי המדע, בפרופיל המשתמש, בפרופיל נותן השרות, ובנהלי העבודה.	1. לכאורה המדען אחראי רק לאפליקציות המדעיות. למעשה עדיין נדרש ידע אודות ה"קרביים של המכונה" ואנרגיה רבה כדי להשתמש בתבונה במשאב. התקשורת בין המדענים ובין הצוות המרכזי מהווה צוואר בקבוק משמעותי, המצריך התייחסות מתמדת. 2. מתאים רק לפרופיל משתמשים מאוד מסוים - ראה יתרונות.	1. היתרון הגדול ביותר הוא למדענים א. שאינם רוצים להשתמש במשאבי מיחשוב על בצורה כבדה במחקריהם אלא באחוז לא מאוד גבוה של אלו, ב. מעוניינים להתמקד רק במספר אפליקציות מדעיות בעיקר במתודולוגיה קיימת, ג. אינם מעוניינים להשקיע במיחשוב-על בצורה כבדה ממשאביהם, ד. גמישים בכמות ובתזמון זמן מיחשוב העל שהם דורשים. 2. ניהול החומרה ומערכת ההפעלה ע"י צוות קבוע פחות או יותר, עם פוטנציאל לפיתוח מיומנות גבוהה. 3. מחויבות מוסדית לרכישת ורענון הציוד 4. שימוש יעיל יותר בניצול מחשב העל במידה ומשתמשים שונים צריכים את משאבי המחשב בזמנים שונים. 5. הוזלת עלויות רכישה ותחזוקה.	
		מודל זה מסוגל לשלב את היתרונות של המודלים הקודמים אם קבוצת מדענים מסוגלת לזהות זהות באינטרסים שלהם - למשל אילוצי חומרה דומים, מדע דומה, התאמה בדרישות זמן המיחשוב ונוהלי העבודה, סמיכות פיזית המאפשרת העברת מידע חלקה וכו.	מודל ביניים - חווה בבעלות ובניהול קבוצה של מדענים המתארגנים עצמאית

3. ככלל אנו סבורים שריכוז כמויות מיחשוב גדולות במערכת מרכזית אחת, יחסית אחידה המבוססת על פשרה בין דרישות צרכנים שונים, מתאימה רק לתחומים בהם השאלות המדעיות השימוש במיחשוב על הם ותיקים.בתחומים פורצים, צעירים ודינמיים יותר - שהם מנועי הצמיחה של האקדמיה - דרישות החוקרים השונים ממיחשוב על מאוד שונות, וכל חוקר רשאי (ואף נדרש) לשנות את אופני העבודה שלו בהתאם לשינויים בתחום. בתחומים אלה צוואר הבקבוק המדעי - ברוב המכריע של המקרים - אינו כוח חישוב נטו אלא שילוב של עבודה חכמה עם משאבים הולמים.

4. שיתופי פעולה בינלאומיים הם הכרחיים בתחומי המדע, ומהווים חלק חשוב במעמדו הבינלאומי של המדען. הדבר נכון גם למדענים המשתמשים במיחשוב על. למעשה ייתכן ונדרש לשנות חלק ממדיניות אבטחת המידע של מכון וייצמן על מנת לאפשר למדענים מחו"ל לגשת לחוות מיחשוב העל במסגרת שת"פ. שימוש משותף במיחשוב על עדיין לא יצר כשלעצמו, נכון לעכשיו, בעיות חדשות בתחום הקניין הרוחני.

5. תמיכת המכון בחוות פרטיות או של התאגדות מדענים ניתנת בכפוף לבחינה של איכות המדע המוצע, כל מקרה לגופו.

ב. חסמים, והעזרה הנדרשת להתמודדות איתם (בסדר עדיפות יורד):

1. עזרה בבניית ושמירת מיומנות במכון ובקבוצות המחקר:

אנו מתקשים לגייס ולשמור על אנשי מיחשוב על מצטיינים אל מול תחרות בתעשייה, בשל פער המשכורות. בשנים הקרובות מכון וייצמן יידרש לכ-3 אנשי מיחשוב על באגף מערכות מידע (כיום יש אחד), ולכ-1-2 אנשים בכל פקולטה, סה"כ כ-8-10 בפקולטות, בעלי ידע גם בטכנולוגיה של מיחשוב על וגם ביישומים המדעיים או ידע נלווה של ניתוח מידע, כריית מידע, סטטיסטיקה ונומריקה, ויזואליזציה וכו (כיום אין אף אחד בפרפיל זה ממש. יש כ-2-3 מומחי מיחשוב על מהצד הטכנולוגי בפקולטות, ומדענים ממלאים את החסר באופן חלקי מהצד המדעי). ברמה ארצית, על פני 7 אוניברסיטאות מדובר ב 70-90 איש.

אנו רואים כאפשרות משמעותית - וכתרומתנו למלחמה בבריחת המוחות - את היכולת להביא אנשי מיחשוב על מחו"ל לישראל לתפקידים אלה, אולם נצטרך סיוע בפתרון בעיית התחרות מול התעשייה ומול המשכורות בחו"ל.

2. מקור תקצוב לאומי קבוע לרכישה ורענון ציוד מיחשוב על:

בהיקף הנוכחי מכון וייצמן צריך כ-800 אלף דולר בשנה לרכישה ורענון ציוד מיחשוב על (מתוכם $150k לאטלס, $300-400k לחווה המשותפת של מדעני כימיה, והיתר לשאר המערכות במכון). בתור כלל אצבע אנו מעריכים שציוד בן 3-4 שנים הוא מיושן ומצריך החלפה. במקביל, קשה מאוד להשיג כסף למחשבים בקרנות הרגילות. כל גידול בפעילות יגדיל מספרים אלה.

אנו מבקשים קרן ייעודית, או הרחבת קרנות הציוד, על בסיס תחרותי בין המדענים לנושא זה, כמו גם קרן מוסדית נלווית לנושא. בחישוב של 7 אוניברסיטאות מדובר בהשקעה של 5-6 מיליון דולר בשנה.

3. סיוע בהכשרת סטודנטים ופוסט-דוקים:

בשל הבעיה בסעיף 1, כיום רוב הקבוצות מטפלות בצרכי מיחשוב העל שלהם בעזרת סטודנטים או עמיתים בתר-דוקטוריאליים. מצד אחד הדבר מהווה ברכה - זו הדרך היעילה ביותר להכשיר אנשים שיצאו לתעשייה בתחומי מיחשוב על שהם גם בחזית הטכנולוגיה מחד ועם הפנים לתפוקות מאידך. מאידך, סטודנטים אלה נדרשים להכשרה ייחודית בטכנולוגיה שמשתנה כל הזמן. אנו זקוקים למערך של הכשרה ברמה הלאומית ותמיכה במערך

ההכשרה המקומי לאנשים אלה, ולמלגות לתמיכה בהם בשל זמן הלימוד וההכשרה הממושך יותר.

4. רכישה מרוכזת של תוכנות וחומרות סטנדרטיות דרך מחב"א או גוף דומה.

5. קרן לאומית לפיתוח טכנולוגיות חדשות. מכון וייצמן משקיע כמאה אלף דולר בשנה בטכנולוגיות חדשות, כאשר על הפרק כעת שימוש ב- GPU.

6. רכישה מרוכזת של זמן מיחשוב על בענן ומכירתו באופן מסובסד מקבוצות חוקרים.

ג. כמה הערות על יוזמה הלאומית מרכזית:

אנו סבורים שהמשוכה הגבוהה ביותר שעומדת בפני יכולות מיחשוב העל של האקדמיה בישראל אינה בעיית חומרה אלא בעיית ידע ומיומנות. הדרך החשובה והיעילה ביותר שבה יוזמת מיחשוב-על לאומית תהיה מכפיל כוח מיידי היא אם היא תתמוך בפתרון בעיה זו במוסדות, ובעצמה תייצר מרכז של ידע ושל הכשרה מקצועית בתחומי חומרה, ניהול המערכת, תכנות ואלגוריתמים עם מחויבות למדענים ומחויבות להעברת הידע לסטודנטים. ראוי לציין גם שסף הכניסה הכספי למיחשוב-על איננו גבוה לכאורה (העלויות האמיתיות בזמן, כ"א וכסף לחידוש ציוד מתבררות רק אחרי זמן מה). הדבר אומר שמדען שירגיש מתוסכל מאספקט כלשהוא של היוזמה הארצית - בין אם זמן מיחשוב, או עזרה מקצועית או זמן תגובה כללי - יוכל בקלות עדיין לרכוש חווה משלו. קרי, קיים מכניזם לסחף מתמיד משימוש במשאבי היוזמה המרכזית לטובת מתקנים עצמאיים כך ש 1) צרכי מיחשוב העל בקבוצות או במוסדות לאו דוקא ירד בצורה משמעותית, 2) מרכז מיחשוב העל יכול בקלות להפוך לפיל לבן המתיישר לפי מספר צרכנים קטן בעלי דרישות מצומצמות ורגועות יותר.

יוזמה לאומית יכולה לעבוד במספר רבדים או מודלים, שלכל אחד רמת סיכון ורמת פוטנציאל שונים.

א. רובד הכרחי של תמיכה בקבוצות ובמוסדות: ברובד זה מספקים תמיכה כספית וכ"א למוסדות, בדומה למודל המענקים הקיים היום. רובד זה הכרחי ויעיל מהסיבות הבאות:
   1. מהווה מכפיל כוח מיידי מחד וגמיש מאידך,
   2. יתן מענה לקבוצות בעלות צרכים מיוחדים ורעיונות שונים הדוחפות את המעטפת של השימוש המיחשוב על,
   3. מהווה בסיס ל-diversity במערכת שהיא הבסיס לצמיחה ארוכת טווח,
   4. מהווה גורם תחרות מתמיד,
   5. מהווה מודל נכון להכשרת מספר רב של סטודנטים,
   6. ממילא יהיה מספר רב של קבוצות שישתמשו במשאבי מיחשוב על עצמאי למדע ראוי.

ב. רובד של שת"פ בין המוסדות וגורמים נוספים בהכשרת כוח האדם המקומי, שלאחריה מסגרת להחלפת ידע מתמדת בין מומחים בגורמים השונים, ולפרויקטי פיתוח טכנולוגיות חדשות משותפים. היתרון המרכזי הוא שכל מומחה מקומי קשוב אחראי כלפי הפרויקט המדעי ומפתח מיומנויות בשטח מחד, אך מקבל ותורם ממאגר ידע גדול כלל ארצי (זהו המודל שבכוונתנו ליישם במסגרת מכון וייצמן).

ג. מודל אחר הוא של פרויקט מבוזר לפיו משאבים, מערכות, מומחים וזמן מיחשוב מפוזרים במוסדות אבל כפרויקט משותף ותחת אלמנטים של הנהלה משותפת. מודל כזה דומה לב' אבל מדגיש את הקשר בין המוסדות ובקהילת מיחשוב העל. מודל זה הוא בעל פוטנציאל רב אך הוא מורכב, וניסיון העבר בהסדרים דומים הראה שהוא עובד רק אם לגורמים השונים יש זהות אינטרסים מספקת ומרכיב מרכזי בהצלחה הוא על בסיס קבוצתי. ברור שהדבר יתאים רק לחלק הקבוצות המדעיות או המוסדות. מאידך, ניתן לעבור באופן יחסית חלק בין מודל זה והמודל בסעיף הקודם.

בכל מקרה מודל זה ככל הנראה אינו ישים כרגע בשל מגבלות רוחב פס בין המוסדות.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

ד. מודל של מרכז מיחשוב-על מונוליטי יחיד שמכיל גם את החומרה וגם את המומחיות ומציע את שירותיו למדענים.

מודל זה עובד היטב במספר מקומות בחו"ל - לא במקום אלא במקביל להשקעה משמעותית במוסדות השונים. מאידך הניסיון מראה שבתנאים הישראליים מודל זה עתיר סיכון בכל אספקט. מרכז בזה יכול להתקיים רק אם יתקיימו התנאים הבאים:

- תרבות ארגונית: המרכז יהיה מחויב להצלחת הפרויקטים של לקוחותיו במאה אחוז, ויעבוד בנהלי עבודה ברורים ושקופים (כאן כמובן קיימת מכשלה מרכזית - ללא בקרה רבתי, מרכז עצמאי עלול לעבוד בנקל למען מטרות שהוא יגדיר לעצמו, למרות שהוא לא "בשטח", ולא עבור הפרויקטים של הלקוחות).
- טכנולוגיה: המרכז יכיל מספר מחשבי על בתצורות שונות שיענו לצרכים השונים. כאמור למעלה מדובר על כ 5 מיליון דולר בשנה למיחשוב לאקדמיה רק לרענון חומרה (וזאת רק כדי לשמור על נפח יכולת החישוב הקיימת, ללא גידול דרמטי).
- מומחיות: הוא יכיל מספר גדול מספיק של מומחים שיענו לכל הצרכים. כהערכה ניתן לקחת את המספר של 70-90 מומחים שמופיע למעלה (המבוסס על צרכי מכון וייצמן * 7), על מנת שיהיה יעיל, המומחיות צריכה להיות לא רק בנושאי מיחשוב על אלא גם בנושאי data analysis, data mining, numerical and statistical analysis, visualization וכו.
- מחויבות רבת שנים: התיקצוב שלו יהיה רב שנתי ויכיל מראש גם את עלויות רענון הציוד כל 3-4 שנים ועלויות כ"א. גישה זו משתקפת במרכזי מיחשוב אחרים שאנו מכירים ובפרט ב-TACC שהוא מכון לאומי ליד אוניברסיטת טקסס באוסטין בו אחד מאיתנו עבד, שהמספרים בו דומים www.tacc.utexas.edu בארץ, לעומת זאת, ניסיון העבר בארגון מעין זה שלילי (ובאופן סדרתי למדי). בכל מקרה מודל זה ככל הנראה אינו ישים כרגע בשל מגבלות רוחב פס בין המוסדות.

ד. רוחב פס לאקדמיה רוחב הפס לאקדמיה – הן מחו"ל לארץ והן בתוך הארץ – הינו ירוד ביותר בהשוואה למדינות מפותחות אחרות. נדרשת יוזמה לאומית מיידית לפתרון בעיה זו.

החיבור של האקדמיה בישראל לחו"ל הוא תת-סטנדרטי עם קוים של1.5*2 Gbps (הקוים מאפשרים 3*2 Gbps אבל לא כל הקיבולת נרכשה. 1 Gbps מתוקצב ל-2011 אבל עדיין לא נרכש). יחסית לאירופה רוחב הפס שלנו יותר גבוה רק משל קפריסין, מקדוניה, מלטה ומונטנגרו.

רוחב הפס בארץ לא ניתן לתיאור אלא כאומלל ב- 1 Gbps נומינלי.

הדבר כבר גורם לבעיות בשת"פ עם CERN. בעיה יותר חמורה מצפה לנו בשנים הקרובות כאשר כל כמויות המידע האדירות שמיוצרות ב- bioimaging ותחומי ביולוגיה וכימיה אחרים יידרשו משאבי רשת משמעותיים בעקבות מסגרות שת"פ בינלאומיות או בשת"פ בתוך הארץ.

יש צורך בטיפול מיידי בנושא זה. אנו מציעים שבמקום לבחון את הנושא אחת לכמה זמן במסגרת יוזמות מיוחדות נאמץ סטנדרט קבוע שאליו נצמד נאמר ב-20 או 50 השנה הקרובות. כסטנדרט מינימלי-ריאלי אנו מציעים את רוחב הפס של מדינות מזרח אירופה, שכבר כעת פתח פער גדול ביחס אלינו (כיום ב - 2*10 Gbps). ניתן למצוא benchmark דומה לרוחב פס בתוך ישראל.

בתודה,
פרופ' טל אלכסנדר, אסטרופיזיקה, הפקולטה לפיזיקה, מכון וייצמן; אחראי מיחשוב-על בועדת המיחשוב של מכון וייצמן.
עופר ארונסון, ראש תחום תשתיות, האגף למערכות מידע, מכון וייצמן

פרופ' מיכה ברכוז, פיזיקה של חלקיקים,הפקולטה לפיזיקה, מכון וייצמן ; יועץ בכיר לנשיא המכון לנושא טכנולוגיות מידע,

פרופ' אהוד דוכובני, פיזיקה של חלקיקים ניסיוני, הפקולטה לפיזיקה, מכון וייצמן,

ד"ר לורן לוינסון, פיזיקה של חלקיקים ניסיוני, הפקולטה לפיזיקה, מכון וייצמן,

פרופ' ליאור קרוניק, חומרים ופני שטח, הפקולטה לכימיה, מכון וייצמן.

נספח ד – מתוך מכתבו של פרופ' בר יוסף מהטכניון, 10.2.11

From: Zvi Pinhas Bar-Yoseph [mailto:medean@tx.technion.ac.il]
Sent: Thursday, February 10, 2011 9:26 AM
To: 'Hagit Sabo'
Cc: 'Irit Gertzwolf'
Subject: RE: שולחן עגול בתחום בנושא יכולות מיחשוב מתקדמות ותקשורת נתונים מהירה באקדמיה בישראל

שלום רב,

לצערי, עקב ההתראה הקצרה, ובשל מחויבויות קודמות, לא אוכל להשתתף בישיבה זו. להלן ההתייחסות של דוקטורנט שלי, לב פודשיבלוב, לשאלות מטה:

מס' ליבות: במקרה של המחקר שלנו אם הייתה גישה למחשב עם כ - 500 ליבות אפשר היה לפתור את כל המודל של העצם. אנחנו היינו מוגבלים למספר הליבות הקיימות על 64 - NANCO.

גודל זיכרון: להערכתי כ - 4 גיגה לליבה.

תקשורת פנימית: כמה שיותר מהירה. במקרה של 64 ליבות כ - 8 אחוז מהזמן הלך על תקשורת (בקוד שלי). אם מגדילים את מספר תת-תחומים, הזמן הזה נהיה משמעותי. לא יודע לתת ערך מספרי.

במקרה שלנו מדובר על חישוב מקבילי אמיתי, כי יש תקשורת והעברת נתונים בין תתי-תחומים.

אם היינו מקבלים כוח חישוב יותר גדול ניתן היה לפתור מודלים מלאים ולא רק חלקים מהם. לא חושב שבמקרה שלנו זה היה מוביל לפריצת דרך. בסה"כ הוכחנו ייתכנות השיטה תוך שימוש בכוח חישוב קיים.

מידע נוסף:
היום מדובר על MULTI SCALE ANALYSIS. כלומר, מדובר על מידול בו זמני של כמה סקלות [מרמת המקרו ועד לרמה האטומיסיטית], ולכן ברור שככל שנקבל יותר משאבים ה"תיאבון יגדל" ונוכל לחקור בעיות יותר מורכבות ויותר קרובות למה שנדרש. במקרה של לב פודשיבלוב, מדובר במידול של עצמות. כיום הוא יכול לעבוד רק על ביופסיה של עצם וברמות ממקרו ועד מיקרו. בכדי לרדת לרמת התאים בעצמות מרמת השלד, צריך יכולות חישוב בסדרי גודל יותר גדולים ממה שיש לנו היום.
דוגמא שנייה: מערכת כלי הדם בגוף- אנליזה כוללת של זרימת הדם במערכת כלי הדם, תוך ירידה לרמה של תאי דם [למשל מידול תופעות קרישת דם, ופקקת בכלי דם- יש לי דוקטורנט בנושא זה] תדרוש משאבים שכיום אין לנו גישה אליהם, ולכן אנו מסתפקים במידול מקומי של תהליך קרישת הדם בעורק חסום. שימוש ב Isragrid? - טוב אולי לחברי ממדעי המחשב , לא יעזור לנו לפתרון בעיות מהסוג שהוזכר לעיל.

לגבי שאלתכם:

- מהם הפתרונות שאתם מוצאים היום? (שימוש ב Isragrid? שימוש בכוח חישוב בחו"ל?) האם הפתרונות מספקים?

בעבר הייתי משתמש במחשבי העל של JULICH [הודות לשיתופי פעולה עם חוקר מהאוניברסיטה הטכנית של דרמשטדט]. אם מדובר על פתרון לחוקר פרטני אזי זה אולי יכול להיות פתרון מספק. אם מדברים על חינוך משתלמים וקבוצות מחקר, אזי אני מסופק אם פתרון זה נכון. יש משמעות לכך שישראל תהא על מפת המיחשוב העולמי ולא תהא סמוכה על שולחן של קפריסין [פתטי!]. אודה לכם אם תיידעו את המוזמנים לישיבה על מכתבי זה, תשמרו אותי בתמונה, ותשלחו לי את הפרוטוקול של הישיבה.

בתודה,

Pinhas Z. Bar-Yoseph
Professor and Dean
Samuel & Anne Tolkovsky Chair
Faculty of Mechanical Engineering
Technion City - Haifa 32000, Israel
Tel: 972-4-8292084, 8292079, Fax: 972-4-8295710
E-Mail: medean@technion.ac.il
http://meeng.technion.ac.il

נספח ה – מכתבו של פרופ' גיא תל צור, אונ' בן–גוריון מה–22.10.10

22/10/2010

שלום רב,

ברצוני למסור את תגובתי למכתבו של יוני פרח מהמחלקה להנדסת מכונות בנוגע לצורך בחישוב מבוזר באב"ג.

אני מברך על כל יוזמה בכיוונים אלה ומסכים כי תשתית חישובית מסוג זה, בפרט נוכח היותה קלה יחסית ליישום וזולה, היא דבר ראוי שיתקיים בכל מוסד להשכלה גבוהה המכבד את עצמו ומקיים פעילות מחקרית

בשנת 2004 עם שובי משבתון מהאונ' של ויסקונסין במדיסון שם עסקתי בחקר ה Condor [1] שהינה מכלי התוכנה המשובחים ביותר לחישוב מבוזר , התחלתי ביוזמה להקמת תשתית חישובית מבוזרת, מבוססת קונדור, בקמפוס, על בסיס משאבי מחשב מזדמנים.

במסגרת המאמצים לעשות נפשות לנושא אירחתי באב"ג את פרופ' מירון לבני - ראש פרויקט הקונדור. פרופ' לבני שהינו חוקר בעל שם עולמי, הרצה במחלקה למדעי-המחשב ובמחלקה להנדסת תעשייה וניהול. כמו כן, נערכו פגישות שלו עם מנהל אגף המחשוב ומערכות המידע, סגן הנשיא ודיקן למו"פ וחוקרים נוספים. מאז התחלתי בפריסה של מערך קונדור באב"ג. הפריסה בוצעה באופן מדורג בכיתות מחשב ציבוריות. המערך המבוזר פעיל עד לעצם היום הזה ומשמש אותי להוראה בקורס "מבוא לעיבוד מקבילי", שניתן על ידי זו השנה השישית, במחלקה להנדסת חשמל ומחשבים. איור מספר 1 מראה מוניטור של תוכנת קונדור באב"ג [2] . באיור ניתן לראות כי כיום קיימים באופן זמין בסביבות 150 מעבדים בתשתית המבוזרת.

בשיאו מערך הקונדור באב"ג הגיע לכדי יותר מ 200 מעבדים בכיתות ומעבדות במחלקות להנדסת חשמל ומחשבים, תעשייה וניהול, הנדסה גרעינית, מחשבים מסויימים במחלקה לפיסיקה וכיתת מחשבים נוספת בבית הסטודנט. המערך מכיל מערכות לינוקס וחלונות.

פעלתי רבות לאתר חוקרים אשר היו עשויים לנצל את התשתית המבוזרת, לצערי בהצלחה מועטה. סימוכין מספר [3] מפנה לדף הבית שהקמתי לעניין קונדור באב"ג כבר לפני שנים רבות וניתן להגיע אליו מתוך אתר הבית של אגף מיחשוב ומערכות מידע.
בנוסף לכך קיים באב"ג קלאסטר ששייך למספר חוקרים בו מותקנת התוכנה SGE (Sun Grid Engine) אשר דומה במהותה לקונדור.
פרויקטים נוספים אשר הייתי מעורב בהם בתחום החישוב המבוזר באב"ג היו חיבור אב"ג עם רשת הגריד האירופאית EGEE, בתמיכת ה- Israel Academic Grid [4], בשיתוף עם פרופ' שלומי דולב מהמחלקה למדעי המחשב ויוזמה, יחד עם דר' עופר לוי מהמחלקה תעשיה וניהול, להקמת מערך קונדור בבי"ח סורוקה.

לעניין הצעתו של יוני פרח ליישם באב"ג את תוכנת BOINC . לדעתי תוכנה זו נחותה לאין שיעור מכלי כגון Condor ואינה מתאימה לצרכי המחקר באב"ג.

לסיכום:

א. יישום תשתית של חישוב מבוזר אינו נושא חדש באב"ג.
ב. קיימת תשתית מבוזרת כל הזמן והיא מחכה לחוקרים שיענו לאתגר לנצלה.
ג. גיוס לתשתיות המבוזרות יתרונות בשימושה ויקשה לכך מאוד החוקרים
ד. יש להעלות את הנושא לתודעת החוקרים העוסקים במחקר עתיר משאבי מחשב.
ה. אשמח להמשיך ולהיות מעורב ואף להוביל את קידום הנושא באב"ג.

בהוקרה,

ד"ר גיא תל-צור

חוקר, קמ"ג
מרצה מן החוץ, אב"ג
יו"ר האיגוד הישראלי לטכנולוגיות גריד (IGT)
gtelzur@bgu.ac.il
054-4443477

References

[1] Condor home page: http://www.cs.wisc.edu/condor

[2] BGU Condor real time monitor: http://matserv.ee.bgu.ac.il/condor/

[3] BGU Condor home page: http://www.ee.bgu.ac.il/~tel-zur/condor/

[4] Israel Academic Grid home page: http://iag.iucc.ac.il/

נספח ו – מתוך מכתבו של פרופ׳ דרור פייטלסון, 1 בפברואר 2011

From: dror.feitelson@gmail.com [mailto:dror.feitelson@gmail.com] On Behalf Of Dror Feitelson
Sent: ג 01 פברואר 2011 14:37
To: Liat Maoz
Subject: Re: FW: התייעצות - שמות חוקרים לשולחן עגול בתחום יכולות מיחשוב ותקשורת נתונים

the big question is whether it is more efficient to have local facilities, or to use remote facilities via the internet. in general the current trend seems to be towards using remote facilities (i.e. clouds). this saves infrastructure and maintenance costs and can be very effective. however, there are two main reasons why local facilities may still be preferable:
1) when processing massive data, getting the data to the remote site may be the biggest problem. with a local site you have the data at hand. even with a national site you can drive over with a box full of terabyte disks.
2) centralized sites tend to be volatile, in the sense that data and software are continuously updated. as a research project may take months, such volatility may make it hard to obtain consistent results. with a local facility you can freeze it for the duration of the project.

that being said, in the past I think the machba supercomputers and internet2 connections were underutilized, and having them was actually like massive subsidies for a very small number of projects. I tend to think that the danger of this is reduced now, because there are many more computer and data intensive projects, e.g. in bioinformatics. but still, the real needs should be checked carefully. there are many ways to support academic research in Israel, and it is not obvious that this is the most important one.

all the best,
-- dror

נספח ז – מכתבו של פרופ' עודד הוד, אוניברסיטת תל-אביב, 8 במרץ 2011

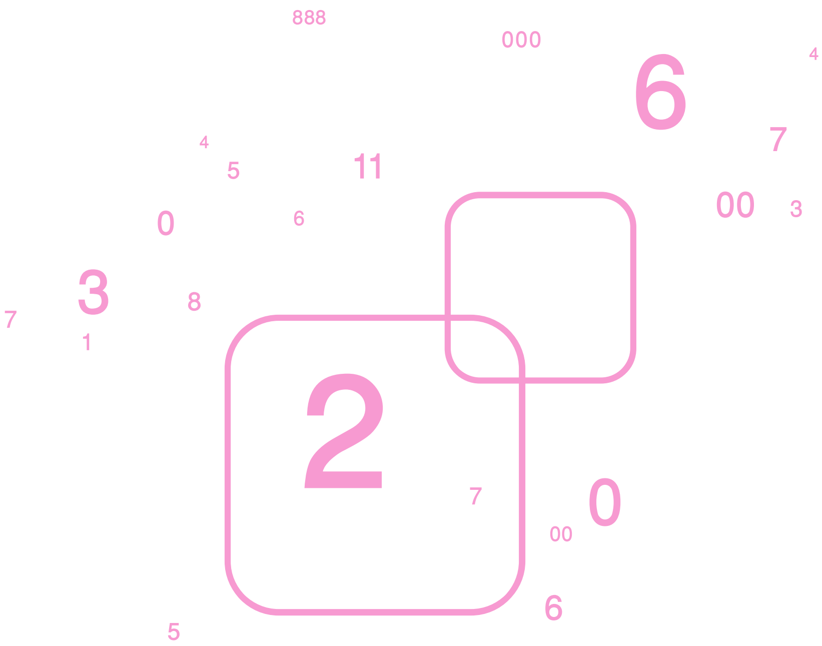
From: Oded Hod [mailto:odedhod@post.tau.ac.il]
Sent: ג 08 מרץ 2011 09:16
To: Liat Maoz
Subject: Re: הזמנה לשולחן עגול בנושא יכולות מחשוב מתקדמות

Hi Liat,

Our cluster at TAU is at 200% capacity (and growing) not 50% capacity as you wrote. This means that at any point in time the number of Qed jobs is at least equal to the number of running jobs.

Thanks,

Oded



תת ועדת מדיניות וחקיקה

1. תמצית מנהלים

המשימה שעמדה בפני צוות תת ועדת מדיניות וחקיקה היתה משולשת: (1) **למפות את המצב הנוכחי במדינות העולם ובארגונים בינלאומיים רלוונטיים** בנוגע למדיניות המו"פ בתחום הקיברנטי; (2) **לברר ולמפות את המצב הנוכחי במדינת ישראל** בארבע זירות בתחום זה (מדיניות מו"פ, שיתופי פעולה בפועל, חקיקה ותקינה); ו-(3) **לעמוד על הפערים** בין שני הסעיפים. כמו כן, הצביע הצוות על **מספר מודלים לחיקוי** (best practices) מתוך הפעילות של מדינות וארגונים בינלאומיים בתחום המו"פ הקיברנטי, שעשויים לקדם את מטרות המיזם בישראל. התוצר הסופי של עבודת תת הוועדה הינו **המלצות לדרכי פעולה ספיציפיים בתחומי מדיניות מו"פ, שיתופי פעולה, חקיקה ותקינה,** שלדעתנו יקדמו את יעדי המיזם.

יצויין, כי בשלב מוקדם של עבודת תת הוועדה הסתבר כי מרבית המדינות שנחקרו השיקו תוכנית מו"פ קיברנטי שנגזרת מהמדיניות הלאומית הכללית של ביטחון קיברנטי (cybersecurity). על סמך זאת, הוקמה תת ועדה נוספת במסגרת המיזם, שתכליתה לגבש מסמך מדיניות כוללת להגנה קיברנטית. אם כן, חומר מחקרי על אודות מדיניות כללית ולא רק מו"פית נכלל בפרק זה, ומשתקף בממצאיו ובהמלצות.

על סמך הממצאים העיקריים שמפורטים להלן, צוות תת הוועדה ממליץ על **שני צירי פעילות בשלב הבא של המיזם, האחד במישור הבינלאומי והשני בתוך המדינה. בראש וראשונה, חיוני שישראל תצטרף בצורה פרו-אקטיבית, מושכלת ושיטתית לתהליכים הבינ"ל המוצאים** בתחום המו"פ הקיברנטי בפרט, ובתחום גיבוש מדיניות הביטחון הקיברנטי בכלל. דוגמאות בולטות לפעילות מסוג זה, שישראל אינה די מעורבת בה כעת, הן **יוזמות בנאט"ו, ב-OECD, ב-ITU, ובקהילה האירופית**[1]**; האמנה נגד פשע קיברנטי של מועצת אירופה משנת 2001;** פעילות רגולטורית ויוזמות תקינה במסגרת ה-ITU; **ותהליכי התקינה** בוועדות המקצועיות הכפופות ל-JTC1 של ISO ו- IEC.

ברמה המדינתית, הוועדה ממליצה על ארבעה מסלולי פעילות. ראשית, כיוון שהמידע הרגולטורי והעסקי לגבי אפשרויות המו"פ הקיברנטי בישראל מפוזר על פני מספר מוקדים (המדען הראשי, מפא"ת, תעשייה, מוסדות ההשכלה הגבוהה וגורמים נוספים), **חיוני לרכז את המידע** במקום אחד (מסמכי מדיניות ממלכתיים, חקיקה, "הסברה עסקית", נתונים כלכליים ועוד), **זמין לציבור ואינטראקטיבי באופן נוח ויעיל** עם המערכת הרגולטורית, כגון אתר אינטרנט מיוחד לנושא. שנית, יש לקבל **החלטה בטווח הקצר כדי לשפר את רמת השקיפות בתהליכי הייצוא והייבוא הרלוונטיים למו"פ** קיברנטי, ולאפשר תהליך של **חוות דעת מוקדמת** (pre-ruling), במיוחד במסגרת חוק הפיקוח על ייצוא ביטחוני, התשס"ז - 2007 ותהליכי הרישוי במסגרת חקיקת הצופן. בנוסף, מעבר לתחום המו"פ, **חשוב לערוך בדיקה מערכתית של חקיקה ישראלית נוספת** הרלוונטית לתחום הקיברנטי, כגון חוק התקשורת, חוק העונשין, חקיקה שנוגעת לזכויות יסוד של הפרט (הגנת הפרטיות, חופש הביטוי), חקיקת החירום של ישראל ועוד. לבסוף, יש להגביר את המעורבות של **גורמי תקינה,** כמו מכון התקנים הישראלי, במעקב אחר תהליכי התקינה בתחום המו"פ הקיברנטי בעולם, ובפיתוח תקינה מקומית ככלי רגולטורי לפיתוח המו"פ הקיברנטי הישראלי.

[1] בנאט"ו ובקהילה האירופית, קיימות מסגרות פעולה הפתוחות גם למדינות שאינן חברות בארגונים אלה .

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

2. ממצאים וניתוח צרכים ופערים

תת הוועדה זיהתה מספר מגמות ופערים רלוונטיים לקידום המיזם הקיברנטי בהמשך:

1. מדינות וארגונים גוזרים את מדינות המו"פ ממדינות כללית של ביטחון קיברנטי. ברוב המקרים, מדינות מקימות גורם שמרכז את הטיפול הממלכתי במדיניות הקיברנטית, לרבות המו"פ הקיברנטי, ברמה הלאומית. לכל גורם יש מודל שונה של פעילות, כגון ריכוז סמכויות מדיניות וביצוע ברשות קיברנטית חדשה (צרפת), ארגון מטרייה של גופים ממלכתיים קיימים (סינגפור), ומודל מעורב (ארה"ב).
2. מספר מדינות (ארה"ב, אוסטרליה) מגדירות תחומי מחקר חיוניים לפיתוח יכולות ליבה בתחום הקיברנטי ומעניקות תעדוף להשקעת משאבים לאומיים בתחום. הדוגמה הבולטת היא "מפת הדרכים למו"פ בתחום הביטחון הקיברנטי" שפירסם ה-Department for Homeland Security בנובמבר 2009. גם ה-OECD ונאט"ו קבעו תחומים ספיציפיים לקידום המו"פ ע"י מדינות חברות.[2]
3. לעיתים קרובות, ראש המדינה עצמו הוביל את תהליך גיבוש המדיניות, ואף חתם על התוכנית הלאומית (צרפת, רוסיה, ארה"ב).
4. שיתוף פעולה בינלאומי הוא מרכיב מכריע במדיניות הקיברנטית כללית ובתחום המו"פ. החשיבות של השתתפות במהלכים הבינלאומיים המתפתחים בקצב מואץ מתבטא במספר מישורים:
   1. אחידות במושגים ובהגדרות במדיניות הקיברניטית מאפשרת למדינות ולארגונים שיח רגולטורי יעיל. בתחום המו"פ, אחידות המושגים מאפשרת פיתוח של תוכניות והשוואת תוצאות באופן שקוף יותר.
   2. תהליכי תקינה בינלאומיים בתחום הקיברנטי, כגון Joint Technical Committee 1 של ISO ו-IEC, מהווים זירה שבה נבחנים כיווני פיתוח והשקעה של מדינות מובילות: ישראל אינה משתתפת בפורומים האלה באופן שיטתי.
   3. האמנה בנושא הפשע הקיברנטי של מועצת אירופה משנת 2001 (כעת בתהליך של עדכון במסגרת הקהילה האירופית)[3] מעניקה בסיס רחב לשיתוף פעולה בין 30 המדינות החתומות, ומספקת כלי אכיפה נגד פשע קיברנטי, היבט אחד של ביטחון קיברנטי.
4. מפגשי מומחים רבים בתחום הקיברנטי נערכים בקרב ארגונים בינלאומיים בשנים האחרונות. לישראל אין נציגות קבועה בכנסים אלה.
5. הזדמנויות לשיתוף פעולה רב-צדדי בתחום המו"פ הקיברנטי קיימות במספר ארגונים מובילים, וישראל טרם ניצלה אותם באופן מלא. לדוגמה, ה- NATO Research and Technology Organisation; ה- International Multilateral Partnership Against (Cyber Threats (IMPACT של איגוד הבזק הבינלאומי (ה- ITU).
6. חלק מהמדינות שנבחנו עורכות כעת תהליך של עדכון חקיקה קיימת, כדי לטפל כראוי בפעילות החדשה במתחם הקיברנטי. בכמה מקרים, יש התייחסות ואף אימוץ של מושגים והגדרות שמקורם באמנה האירופית נגד פשע קיברנטי ובמודל החקיקה הלאומית שמקדם ארגון ה-ITU. קיימות שתי גישות רגולטוריות אפשריות בנוגע לחקיקה שמתייחסת להיבטי התחום הקיברנטי בתוך מדינה. הראשונה דוגלת בריכוז כל החקיקה הרלוונטית - חקיקת המו"פ ומרבית החקיקה הכללית שנוגעת לפעילות קיברנטית - בדבר חקיקה אחד. השנייה תומכת בהשארת החקיקה הרלוונטית, שכבר קיימת בצורה מבוזרת, המשקפת את תהליכי ההתפתחות ההיסטוריים שלה. הוראות הדין שרלוונטיות לתחום המו"פ, הינם, בעיקר, דיני היצוא והיבוא, דיני הצופן ודיני שמירת זכויות יוצרים. במישור הכללי, דברי חקיקה שעשויים להיות רלוונטיים להגברת הביטחון הקיברנטי של ישראל כוללים את הדין החל על תשתיות קריטיות, דיני העונשין, דיני נזיקין, דיני הגבלים עסקיים, דיני הגנת הפרטיות, דיני שעת חירום ועוד.

[2] ב-7 בפברואר 2011, נפגשו נציגים ממדינות נאט"ו השונות כדי לדון בקידום שיתוף הפעולה הבינלאומי בתחום הגנת הסייבר, ולשרטט פרוייקטים בינלאומיים משותפים שיאפשרו לחברות נאט"ו לשפר את יכולות ההגנה שלהן, באופן משותף ויעיל. הנושאים שנדונו כללו חילופי מידע לגבי איומים, טכנולוגיות ויכולות חדשות ורכישה משותפת של יכולות תגובה לתקריות מחשוב. בזירת ה- OECD, הצביע המסמך שסיכם את מדיניות וסדרי העדיפויות בתחום ה-ICT בקרב החברות בשנת 2010, על קידום מחקר ופיתוח של מערכות הגנה על מערכות ורשתות כאחד התחומים המרכזיים ביותר לחדשנות.

[3] הצעת הדירקטיבה 14436/10 מיום 30.9.2010.

7. בנוגע לצורך בשקיפות רבה יותר בתהליכים הרגולטוריים הקשורים ליצוא טכנולוגי: משרד הביטחון קובע קריטריונים ליצוא מוצרים ושירותים בתחום המו"פ הקיברנטי. המדיניות השתנתה בתחילת 2011, ונקבעה חלוקה לתחומים שהיתרי היצוא יינתנו בהם ביתר קלות (בעיקר בתחום ההגנה), והמדינה תקפיד בהם יותר על יצוא. בהקשר הזה, אין בינתיים פתרון משביע רצון לסוגיה של יצוא שאינו מפוקח על ידי המשרד, ויש להסתפק באכיפת הכללים הקיימים, שאף לגביהם, חשוב להדגיש, יש צורך בשקיפות רבה יותר. פרק זה מפרט גם דברי חקיקה רלוונטיים.
8. יש חשיבות רבה לחינוך הציבור הכללי בתחום הביטחון הקיברנטי, ולציבור המשקיעים בתחום המו"פ הקיברנטי. אחת הדרכים המקובלות היא פיתוח אתר אינטרנט עבור הציבור הכללי, ואתר נוסף עבור ציבור המשקיעים במו"פ קיברנטי. דוגמה בולטת היא קבוצת אתרי האינטרנט של ה- IDA של סינגפור.

3. המלצות מפורטות של תת ועדת הסדרה וחקיקה

חמש ההמלצות שלהלן עוסקות בטיפול בפערים שזוהו במצב הנוכחי בין ישראל לבין מדינות אחרות, ובפעילות הפנים-ישראלית העכשווית:

3.1. המלצות ספיציפיות בתחום מדיניות וחקיקה

1. יש לגבש הגדרות עבודה ומושגים אחידים, בשפה העברית, לפעילות בתחום הקיברנטי בכלל; ובתחום המו"פ בפרט. מושגים והגדרות אלה צריכים לעלות בקנה אחד עם המינוח הבינלאומי. נספח ב' כולל מספר דוגמאות, כגון "ביטחון קיברנטי" ו"מו"פ קיברנטי".
2. מדינת ישראל, כמו מדינות אחרות, צריכה לגבש מסמך מדיניות קיברנטית, לרבות תוכנית ביצוע הכוללת תוכנית מו"פ קיברנטי אסטרטגי, המצביעה על יכולות ליבה שהמדינה מעונינת לפתח ואת סדרי העדיפות ביניהם.
3. בהמשך ל-(2), חשוב לרכז את המידע בנוגע להתפתחויות במדיניות הלאומית, הכללית ומו"פ, כולל יוזמות עסקיות בתמיכת המדינה, מקורות מימון והתפתחויות בינלאומיות באתר אינטרנט ממוקד. השקיפות והזמינות של המידע והתהליכים הרגולטוריים הכרוכים בהשקעה ופיתוח במו"פ, הן קריטיות ל"הסברה העסקית" שעשויה לקדם את המו"פ הקיברנטי. המודל הסינגפורי, שכולל גם מידע למשקיעי חוץ, רלוונטי לישראל.
4. יש להצטרף לתהליכים הבינ"ל בצורה פרו-אקטיבית, מושכלת ושיטתית. כאמור, קיימים תהליכים במישור הכללי של גיבוש מדיניות גלובאלית בתחום הביטחון הקיברנטי, ותהליכים שלובים ועצמאים בתחום המו"פ הקיברנטי. ביתר פירוט:
    1. יש לקדם את הצטרפות ישראל לאמנה נגד הפשע הקיברנטי של מועצת אירופה משנת 2001; ולבחון מקרוב את הנסיון הנוכחי של הקהילה האירופית לשדרג את האמנה. על פניו, אין קושי מהותי בכך.
    2. על ישראל לבחון הצטרפות ו/או העמקת מעורבות במנגנונים הפועלים למען שיתוף פעולה רב-צדדי בתחום המו"פ הקיברנטי. על פי ממצאי המחקר, עד כה ישראל לא גילתה מעורבות משמעותית, למשל, ב- NATO Research and Technology Organisation - אף לא ברמה של מעקב אחר הנעשה; וגם לא בתוכנית IMPACT של ה- ITU, למרות שישראל הצטרפה ליוזמה זאת.
    3. מומלץ לשדרג את המעורבות הישראלית, הממלכתית והמסחרית, בארגוני התקינה המובילים בתחום הקיברנטי: ISO, IEC, ITU, IEEE, ANSI ועוד. תיפקוד מוגבר של מכון התקנים עשוי לסייע ליישם המלצה זאת.
4. נוכחות ישראלית בפגישות מומחים בתחום הקיברנטי חייבת לקבל תשומת לב משודרגת ותקצוב מהגורמים הרלוונטיים: משרד ראש הממשלה, משרד החוץ, משרד התמ"ת וגורמי ביטחון. כיום ישראל אינה משתתפת בשיח הבינלאומי, המקצועי והדיפלומטי בתחום.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

2. חשוב לערוך עיון מחדש, מסוג clean slate, בחקיקה בתחום המו"פ הקיברנטי. חוק המו"פ הישראלי, לכשעצמו, מתאים למשימת המיזם; אך זוהו שתי קבוצות של דינים בישראל שטעונות בחינה לעומק ושיפור, כלהלן:
   1. חקיקה שנוגעת לאישורי יבוא ויצוא של מוצרים ושירותים (חוק הפיקוח על יצוא ביטחוני, התשס"ז - 2007 ; פקודת היבוא והיצוא (נ"ח), תשל"ט- 1979 ; ודברי החקיקה במסגרת צו הצופן). סוגיות עיקריות באשכול זה כוללות אכיפה יעילה של יבוא ויצוא מוצרי מו"פ בעולם מקוון; התאמת הגדרות במסגרת צו הצופן וההדרת הליך הרישוי, לרבות החובות שחלות על מבקש הרישיון בשלב המו"ם המסחרי; והבטחת קווי ייצור של מוצרי מו"פ, בישראל ובחו"ל.
   2. חקיקה שנוגעת לשמירה על זכויות קניין במוצרי מו"פ (חוק זכות יוצרים, התשס"ח - 2007; חוק הפטנטים, תשכ"ז-1967).

במישור הכללי, מעבר לחקיקה הנוגעת ישירות למו"פ קיברנטי, חשוב לבחון אשכולות נוספים של חקיקה, לאור הפעילות המוגברת במתחם הקיברנטי, הכוללים דיני עונשין, הגנות על זכויות יסוד כמו חופש הביטוי והעיסוק ושמירה על זכויות הפרט, וחקיקת החירום של ישראל.

לבסוף, יש לבחון את הגישות השונות למדיניות הרצויה, לפיהן ניתן לאחד הוראות חקיקה שרלוונטיות למתחם הקיברנטי בדבר חקיקה אחד, או לחילופין להשאיר הוראות רלוונטיות במיקומן "ההיסטורי", או לשלב בין הגישות.

3. בענין תהליכי היצוא הביטחוני הקיימים עפ"י החקיקה הנ"ל, יש להכין מנגנון של pre-ruling או חוות דעת מקדמית ליוזמי פרוייקטי מו"פ; ולהביא לידיעת הציבור מידע על האפשרות של pre-ruling כמרכיב של ההסברה העסקית של מדינת ישראל בתחום המו"פ הקיברנטי.

4. מבוא

תת ועדת מדיניות וחקיקה במיזם הקיברנטי הגדירה שתי מטרות מרכזיות לפעילותה:

- גיבוש הצעות למדיניות בתחום המו"פ הקיברנטי;
- גיבוש הצעה לתוכנית תמיכה בעבודת המטה של תתי הוועדות האחרות בהיבטי מדיניות וחקיקה, מבנים ארגוניים, שת"פ בינ"ל ותקינה

בהתאם למטרות אלו, נקבעו המשימות הבאות:

- **מיפוי המצב הנוכחי** ותובנות על בסיס ניסיון **בחו"ל** בהיבטי אסטרטגיות של הסדרת נושא המו"פ הקיברנטי, תכניות מו"פ לאומיות ובינלאומיות, תקינה וארגוני תקינה, מדיניות וחקיקה;
- **מיפוי המצב הנוכחי בישראל**, לרבות שיתופי פעולה בתחום, יתרונות ומגבלות במדיניות וחקיקה ובחינת התקינה הקיברנטית;
- **ניתוח הצרכים וזיהוי הפערים** בהיבטים אלה;
- **הגדרות ומושגים** משותפים למיזם;
- **המלצות למדיניות וסדרי עדיפויות** לפעילות במו"פ הקיברנטי בישראל.

מסמך זה מיועד לרכז את הידע הקיים בנוגע לכל אחת ממשימות הצוות, מצד אחד; ומצד שני לאבחן את הפערים הקיימים בישראל בטיפול במו"פ בתחום הקיברנטי, מתוך כוונה לשפר, לייעל ולמצות את התחום בצורה האופטימלית ובהתאם למטרות המיזם. בנוסף, המסמך ממפה את תהליכי ההתפתחות והמגמות העתידיות בתחום מו"פ קיברנטי. מטרות אלה משקפות את היעדים שנקבעו בכתב המינוי של ועדת המיזם.[4]

[4] כתב המינוי לוועדה בנושא המיזם הקיברנטי, 26.12.2010.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

יצויין כי בשלב מוקדם של עבודת תת הוועדה, זיהה הצוות מגמה ברורה במדינות ובארגונים שנבחנו, לפיה מדיניות המו"פ נגזרת ממדיניות קיברנטית כללית יותר. לאור זאת, משימת ההסדרה הכללית הועברה לצוות נוסף[5], אך חלק מעבודת המיפוי והפקת הלקחים מהנעשה בקרב מדינות אחרות וארגונים בינלאומיים בתחום המדיניות הכללית נכלל גם בפרק זה.

5. מיפוי של תהליכי גיבוש מדיניות וחקיקה בתחום הקיברנטי בקרב מדינות וארגונים נבחרים

5.1 כללי

פרק זה מיועד לרכז את הידע והנסיון של מדינות אחרות וארגונים בינלאומיים רלוונטיים, בהתמודדותם עם האתגר החדש והמורכב של מדיניות מו"פ בתחום הקיברנטי. לצורך כך, נבחנו תוכניות למדיניות במתחם הקיברנטי בכלל, ומדיניות מו"פ לאומיות ספציפיות בתשע מדינות; תוכניות מו"פ רב צדדיות; ותקינה בינלאומית רלוונטית. בנוסף, נותחו היוזמות של מספר ארגונים בינלאומיים מובילים בתחום הסדרת הסייבר, כגון, ה-OECD, הקהילה האירופית, נאט"ו ואיגוד הבזק הבינלאומי (ה- ITU). ראוי לציין, שתחום זה של מדיניות המו"פ הקיברנטי חדש, חדיש, ו"חם", ומתפתח בקצב מהיר בכל המדינות שפעילות במתחם הקיברנטי. מדינות רבות התחילו לתת עליו את הדעת ולגבש מדיניות לאומית כללית ומדיניות מו"פ פרטנית, בעיקר בחמש השנים האחרונות. לאור זאת, המדינות שנבחנו נמצאות בשלבים שונים, אך התחלתיים במרבית המקרים, בתהליך של גיבוש אסטרטגיה של ביטחון קיברנטי, מיפוי צרכים ויכולות קיברנטיות ברמה הלאומית, והקצאת משאבים. המדינות המובילות בתחום, כצפוי, בעלות אינטרס אסטרטגי מובהק במתחם הקיברנטי, בין אם הוא כלכלי, ביטחוני, חברתי או שילוב של כל אלה. בארה"ב, בסינגפור ובקהילה האירופית מתבצעת עבודת מטה מצוינת בתחומים אלה.

הצורך לטפל במשימות אלה נולד בעקבות המתקפות על אתרי האינטרנט של ממשלת אסטוניה - ושל גורמים אזרחיים נוספים - במאי ויוני 2007. כתוצאה מחוסר האונים של המערכת הבינלאומית לנוכח המתקפה על אסטוניה (ושל ארגון נאט"ו במיוחד, שפתח מרכז מצוינות להגנה קיברנטית באסטוניה בשנת 2006)[6], התחילו מדינות להבין את הצורך המיידי בהסדרת הפעילות במתחם הקיברנטי, על מנת למנוע מצבים דומים בעתיד, או לכל הפחות להקטין את הנזק הפוטנציאלי במצבים אלה[7]. אסטוניה, אם כן, היא המדינה הראשונה, מבחינה כרונולוגית, שפרק זה מציג את המדיניות הקיברנטית שלה.[8]

מהו מו"פ קיברנטי?

חוק המו"פ מגדיר מחקר ופיתוח כ"חקירה מתוכננת במטרה לגלות ידע חדש מתוך צפייה שידע זה יהא מועיל בפיתוח מוצר חדש או תהליך חדש או לשיפור מהותי במוצר או בתהליך קיימים"; ויישום הממצאים של המחקר והידע האמורים.

"המתחם הקיברנטי" הינו המתחם הפיזי והמקוון ("המתחם החמישי") שמורכב מהגורמים הבאים ומכל מצבור שלהם: מחשבים, מערכות ממוכנות ורשתות; תוכנות, מידע ממוחשב; התוכן של אלה האחרונים; נתוני תעבורה ובקרה שלהם; ומשתמשי כל אלה.

[5] ר' סיכום דיון התנעה לצוות ההסדרה מיום 21.3.2011.
[6] ר' את האתר של מרכז המצוינות בטאלין, http://www.ccdcoe.org/11.html.
[7] אמנם גורמים צבאיים בקרב מדינות העולם וארגונים בינלאומיים מסויימים הקדישו מאמצים לגבש דוקטרינות צבאיות ומדיניות גלובאלית (בהתאמה) בנוגע לפעילות במתחם לפני אירועי אסטוניה, אך ההתפתחויות המשמעותיות במישור הבין-ממשלתי והבינלאומי התרחשו רק לאחר מכן.
[8] ר' M. Lander and J. Markoff, Digital Fears Emerge After Data Siege in Estonia , New York Times, May 24, 2007 (http://www.nytimes.com/2007/05/29/technology/29estonia.html)

כמבוא לניתוח להלן, ראוי להתייחס לאמירה של ה-OECD בנוגע לחשיבות של מו"פ ממוקד בהפחתת איומים קיברנטיים ועמידה באתגרים של הבטחת הביטחון הקיברנטי. בדו"ח שפורסם בינואר 2011 בשם Reducing Systemic Cybersecurity Risk, נאמר:

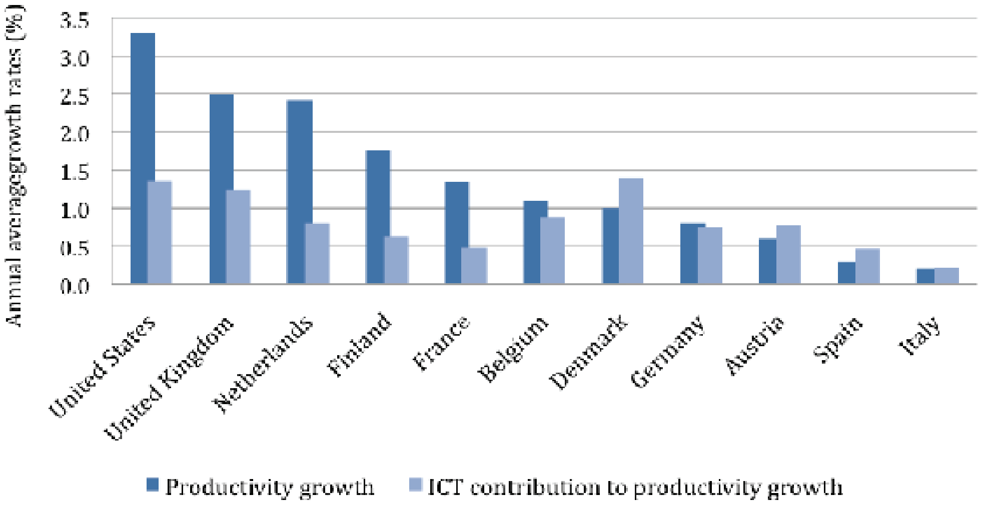
Traditional computer security research has operated on the technological problem/ technological solution model and there is still an ongoing requirement for innovation in such areas as access control services, malware and intrusion detection systems, secure database design and cryptography. Much work is also needed in developing forensic and tracing tools and techniques. A further area is within intrusion and fraud detection [....] The growing enthusiasm for cloud computing has brought further challenges.[9]

הדו"ח ממשיך לתאר את האתגר המחקרי במתחם הקיברנטי, ומדגיש את הצורך בגישה רב-תחומית, לא רק באופן תיאורטי: כל מדינה שנערכת להתמודד ברמה גבוהה מול אתגר מסוג חדש, כגון הסדרת המתחם הקיברנטי, מדגיש ה-OECD, צריכה להיות ערה לכך שיש עקומת למידה שמסתמכת על תחומי מומחיות רבים. במספר יוזמות, כמו אלו של ארה"ב, בריטניה, והקהילה האירופית, גישה זאת כבר מיושמת.[10] לסיכום נקודה זאת מחברי הדו"ח כותבים:

An important feature of all of these [cyber research] initiatives has been to compel researchers from very different backgrounds to appreciate each other s work and in particular to understand their respective use of terminology.[11]

בהמשך לתובנה זאת, ובנסיון ליצור מונחים בשפה העברית שיתמכו בעבודת תתי הוועדות במיזם, מצורפת בנספח ב' רשימה של מושגים, המוצעים לשימוש משותף במיזם.

בנוסף להגברת היכולות הלאומיות להתמודד עם אתגר הביטחון הקיברנטי באופן רב-תחומי, מזהה ה-OECD קורלציה בין ההשקעה במו"פ בתחום התקשוב[12] לבין גידול בפריון כוח העבודה, כדלהלן[13]:



9 OECD, Reducing Systemic Cybersecurity Risk, 14th January 2011, p. 69.
10 ר' עמ' 70 וההפניות ליוזמות של תוכניות המסגרת (Framework Programme) מספרי 6 ו-7 של של הקהילה האירופית.
11 שם.
12 "תקשוב", או Information and Communication Technolgies הוא מונח שמאפשר מדידת "השקעות בתחום הקיברנטי" כעת, עד שייערכו ניתוחים מדוייקים יותר באמצעות מינוח חדש שמתאים למתחם הקיברנטי.
13 הערה 5 לעיל, עמ' 54.

Contribution of ICT capital growth to labour productivity growth in market services (1995-2004) Source: OECD (2008a: 27)

באופן כללי, מדינות הפעילות במתחם הקיברנטי החלו לגבש מדיניות מו"פ ממוקדת להאצת המעורבות של משאבים לאומיים בתחום, החל מסוף שנות ה-90. נראה כי הדחף העיקרי לפריסת תוכניות המו"פ נבע מתפיסה חדשה של האיומים האסטרטגיים שעלולים לצמוח מההתפתחויות במתחם הקיברנטי, שחורגים מן האפשרויות החיוביות שצפונות במתחם החמישי החדש.[14]

ההתמודדות הבינלאומית הממוקדת הראשונה היתה מול האיום של פשע קיברנטי, שהביאה לחתימת הסכם בינלאומי ראשוני ויחידי בתחום הקיברנטי בשנת [15]2001. כיום, 30 מדינות חתומות על ההסכם: ישראל אינה אחת מהן.

יצוין כי ישראל משתתפת בשנים האחרונות בתהליך רב-צדדי בחסות מזכ"ל האו"ם, שמטרתו לגבש כללי התנהגות במישור הבינלאומי עבור מדינות במתחם הקיברנטי[16]; אך השפעת תהליך זה על המו"פ הקיברנטי אינה משמעותית.

רק בשנת 2008 הוגדר המכלול של האתגרים והאיומים הקיברנטיים - ולא רק אלה בתחום הפשע הקיברנטי - באופן אחיד ברמה הבינלאומית, על ידי אחד מהארגונים הבינלאומיים המובלים בפעילות קיברנטית: איגוד הבזק הבינלאומי (ה- ITU). המושגcybersecurity, או ביטחון קיברנטי, פותח ברמה הרב צדדית במסגרת תהליכי העבודה של ה- ITU5 ומאז מהווה מושג יסוד של האו"ם, ה- OECD, הקהילה האירופית, והמדינות החברות בארגונים אלה, בגיבוש מדיניות קיברנטית בכלל, ומו"פ קיברנטי בפרט.

מהו ביטחון קיברנטי?

המכלול של כלים, מדיניות, תפיסות ביטחון, מגנוני אבטחה, הנחיות, דרכי פעולה מומלצים (best practices), פעולות, ניהול סיכונים וכלים טכנולוגיים שנועדו לארגן את הסביבה הקיברנטית ולהגן עליה ועל נכסי המשתמשים.

מטרות הביטחון הקיברנטי הינן זמינות המערכות הקיברנטיות (availability), שלמותן (integrity), ושמירה על נתונים חסויים (confidentiality).

בהקשר הישראלי, מוצע להוסיף להגדרת ה- ITU:

החיוניות של הסדרה מתואמת של ניצול המתחם הקיברנטי במישור הלאומי: החשיבות בפיתוח מתמיד של אמצעי הגנה פעילים במתחם, מפני ניצולו לרעה במתכוון או שלא במתכוון; מרכזיות המו"פ המתמשך כחלק בלתי נפרד של ביטחון קיברנטי.

להלן סקירה של תכניות המו"פ של תשע מדינות פעילות במתחם הקיברנטי.

[14] ר' את הנתונים שמרכז ה-OECD בהקשר זה. יצוין כי המושג "מו"פ קיברניטי" אינו מושג מוכר באיסוף נתונים כלכליים ברמה העולמית כיום. המושג הסטטיסטי הקרוב ביותר הינו "תקשוב", או ICT; ו-Information Technology (IT). ר' את הדו"ח האחרון של ה-Information Technology Outlook 2010 ,OECD ב- http://www.oecd.org/document/23/0,3746,en_2649_34449_33987543_1_1_1_1,00.html.

[15] ההסכם שנחתם בשנת 2001 בחסות מועצת אירופה מופיע כאן: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

[16] ר' A/65/201, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July, 2010. ישראל השתתפה בקבוצה של 15 מדינות שגיבשו את הדו"ח. ר' ניתוח של הדו"ח בD. Housen-Couriel, Not Just a Virtual Threat , HaAretz, 13 August 2010.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

5.2 תוכניות מו"פ לאומיות של מדינות נבחרות

5.2.1 אוסטרליה

במסגרת המדיניות הכללית לביטחון קיברנטי, קובעת הממשלה אסטרטגיה לאומית לביטחון וחידושים מדעיים (National Security Science and Innovation Strategy)[17] ניסוח המטרות מלמד על התמקדות כפולה, מחד בצרכים מיידיים ומאידך באתגרים עתידיים:

The National Security Science and Innovation Strategy (NSSIS) aims to advance the application of science and innovation to national security. The NSSIS encourages better targeted resource allocation through clearly defined national security objectives and priorities for science and innovation. The NSSIS policy framework aligns the national security and science and innovation policy environments by providing a balanced approach to delivering national science and innovation outcomes that meet immediate requirements while building the capacity to meet longer term challenges.[18]

במסגרת המדיניות הכללית לביטחון ומו"פ לאומי (National Security Science and Innovation Strategy), קובעת ממשלת אוסטרליה אסטרטגיה לאומית לביטחון קיברנטי וחידושים מדעיים[6] ביטחון קיברנטי הינו אחד מתריסר התחומים של סדר עדיפות לאומית במו"פ;[7] וניסוח שש המטרות המוצהרות מלמד על התמקדות כפולה, מחד בצרכים מיידיים, ומאידך באתגרים עתידיים: מנהיגות בתחום הקיברנטי ברמה הלאומית, חלוקת אחריות לבטיחות המתחם בין כל משתמשיו, שותפות בין-מגזרית, מעורבות של אוסטרליה בתהליכים גלובאליים, הערכת סיכונים, והגנה על ערכי המדינה[8]. מו"פ קיברנטי מחייב מאמץ אנושי וכלכלי:

A technically skilled workforce, supported by cutting edge research and development, is fundamental to Australia s ability to develop innovative solutions to emerging cyber security challenges. This priority covers initiatives to build and retain this expertise within government and to harness the resources of Australia s .research community in support of the Australian Government s cyber security efforts

המאמץ יורכב מתקציב מיועד וקביעת סדרי עדיפות לאומיים, כלהלן:

- providing targeted funding and support for cyber security research and development activities [ ][.t] his includes not only technological areas such as quantum cryptography, but may also include research into areas of behavioural change, policy and market-based incentive mechanisms to address systemic cyber security issues, and
- developing an annual set of research and development priorities to inform the broader science and innovation community of the priority work required to achieve the Australian Government s cyber security policy[9].

הגורם הממשלתי המוביל את המדיניות הקיברנטית האוסטרלית הוא היועץ המשפטי לממשלה, המכהן כיו"ר הוועדה הממשלתית הממונה, ה- Cyber Security Policy and Coordination (CSPC) Committee[10], ואגף במשרדו מרכז את עבודת המטה[11].

בעקבות פרסום מסמך המדיניות בשנת 2009, מינתה הממשלה בספטמבר 2010 מרכז לאומי למדיניות קיברנטית לטיפול בכל ההיבטים של ביטחון קיברנטי, הכפוף ישירות לראש הממשלה, ומנהל את תוכנית המו"פ הלאומית. תיאום הסמכויות בין המרכז לבין משרד היועץ המשפטי טרם הובהר. בתחילת 2011 התפרסם מסמך אסטרטגי נוסף, בשיתוף פעולה בין היועץ המשפטי לממשלת אוסטרליה לבין מכון מחקר פרטי[12].

17 Australian Government, Cyber Security Strategy, 2009; Research support for National Security Program, p. 25.
18 שם, עמ' 25.

תובנות מרכזיות מאוסטרליה:

- המדיניות האוסטרלית אמנם דוגלת בפיתוח תוכנית מו"פ, אבל נראה כי סדרי העדיפות הלאומיים מתמקדים באבטחת הבטיחות של שימוש המתחם על ידי אזרחי המדינה.
- הסמכויות בתחום הקיברנטי, לרבות תחום המו"פ, מתחלקות בין משרד ראש הממשלה והיועץ המשפטי למשרד ראש הממשלה.
- מו"פ אינו מוגדר בצורה מפורשת כמנוף להובלה אוסטרלית במתחם הקיברנטי.

5.2.2 אסטוניה

בעקבות המתקפות, בשנת 2007, על אתרי האינטרנט של ממשלת אסטוניה ועל מספר גדול של גורמים אזרחיים, וחוסר היכולת של המדינה ובנות בריתה להגיב באופן יעיל למתקפות אלה[13], קידמה אסטוניה תהליך מזורז של גיבוש מדיניות קיברנטית לאומית. מסמך המדיניות אומץ ע"י הממשלה שנה לאחר האירועים, במאי 2008[14]. משרד הביטחון של אסטוניה הוביל את תהליך הגיבוש של המדיניות הקיברנטית, אך משרדים נוספים היו מעורבים, ומסמך המדיניות כיוון לתוכנית ביצוע של המדיניות הכללית[15]. המו"פ הקיברנטי נקבע כיעד לאומי במישור של אימון כוח אדם מתאים והיערכות לאומית כללית (ר' להלן), ובנוסף, מסמך המדיניות בפירוש מצביע על החשיבות של מו"פ בתחום הביטחון הקיברנטי בכדי להבטיח את ביטחון המדינה[16]. זאת ועוד, משרד החינוך והמחקר של אסטוניה קבע תוכנית מחקר המעניקה סדר עדיפות ליכולות הקיברנטיות שלה[17]. המדיניות הלאומית שפורסמה בשנת 2008 קובעת באופן ספציפי את יעדי המו"פ, כלהלן[19]:

2. Increasing competence in cyber security In order to achieve the necessary competence in the field of cyber security, the following objectives have been established for training and research:

- to provide high quality and accessible information security-related training in order to achieve competence in both the public and private sectors; to this end, to establish common requirements for IT staff competence in
- information security and to set up a system for in-service training and evaluation;
- to intensify research and development in cyber security so as to ensure national defence in that field; to enhance international research co-operation; and to ensure competence in providing high-level training;
- to ensure readiness in managing cyber security crises in both the public and private sectors;
- to develop expertise in cyber security based on innovative research and development.

המוקד הוא דווקא על שיתוף פעולה בינלאומי בתחום המו"פ, הן במסגרת מרכז המצוינות של נאט"ו שהוקם בטלין באוגוסט 2008, Cooperative Cyber Defense Center for Excellence[18], והן במסגרת התוכניות הכלל אירופיות. גישה זו הינה חלק מוצהר מן המדיניות הקיברנטית:

It is also necessary to encourage Estonia s participation in international research and development networks, to focus attention on enhancing the IT and information security competence of Estonian universities and to enhance co-operation with internationally-recognised research centres and development institutes [19]

[19] ר' פרק הסיכום של Estonian Cyber Security Strategy, Cyber Security Strategy Committee, Ministry of Defence, ESTONIA, Tallinn 2008. ר' את האתר של משרד הכלכלה והתקשורת של אסטוניה: http://www.riso.ee/en

מדובר בגישה שדוגלת בשיתוף פעולה בינלאומי בתחום המו"פ הקיברנטי. אסטוניה נהנית, בהקשר זה, משיתוף פעולה עם נאט"ו, המחוייב בפניה לפיתוח יכולות בתחום הביטחון הקיברנטי20 . התפתחויות במדיניות המו"פ של אסטוניה מאז 2007 נכללות במסגרת התוכנית של מגזר התקשוב משנת 2006, The Estonian Information Society Strategy, שעודכן בשנת 2010[20].

תובנות מרכזיות מאסטוניה:

- אסטוניה, המדינה הראשונה שעברה מתקפה קיברנטית כוללת במשך זמן ממושך, הזדרזה לקבוע מדיניות קיברנטית לאומית בעקבות האירועים.
- היא דוגלת בגישה של מו"פ באמצעות שיתוף פעולה בינלאומי, במסגרת כלל אירופית ובמסגרת הפעילות של נאט"ו.
- אסטוניה מעורבת בהתפתחויות שונות במתחם הקיברנטי באמצעות החיבור לנאט"ו ומרכז המצוינות הקיברנטית בטאלין.

5.2.3 ארצות הברית

המאפיין העיקרי של הסדרת נושא הביטחון הקיברנטי בכלל, ומו"פ בתחום בפרט, הינו ריבוי מערכות במישור הפדראלי בארה"ב. כ-70 סוכנויות שונות מטפלות בהיבטים שונים של הביטחון הקיברנטי ברמה הפדראלית, ובנוסף להם פועלים גורמי הסדרה אחרים בתוך כל מדינה.[21] בדו"ח של שירות המחקר של הקונגרס מינואר 2010, נאמר:

There is no single congressional committee or executive agency with primary responsibility over all aspects of cybersecurity; each entity involved pursues cybersecurity from a limited vantage point limited by committee jurisdiction. Many different initiatives exist, but **because of fragmentation of missions and responsibilities, "stove-piping," and a lack of mutual awareness between stakeholders, it is difficult to ascertain where there may be programmatic overlap or gaps** in cybersecurity policy[21].

בדו"ח של הנשיא אובמה מחודש מאי 2009, הפורס את מדיניות ארה"ב במתחם הקיברנטי באופן כללי[22], יש לסוגיית המו"פ מקום מרכזי בהתמודדות עם האתגרים החדשים במתחם. הבית הלבן מצביע על פערים בין הצורך בהבטחת ביטחון ואמידות בתשתיות קיברנטיות, לבין ההשקעות בפועל:

Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help addresscybersecurity vulnerabilities while also meeting our economic needs and national security requirements.[23]

[20] The Estonian Information Society Strategy 2013 is a sectoral development plan, setting out the general framework, objectives and respective action fields for the broad employment of ICT in the development of knowledge-based economy and society in Estonia in 2007-2013. Several internationa and EU-level policy documents, notably the EU i2010 and eGovernment action plans, were taken into account[.] In 2010, the Implementation Plan for 2010-2011 of the Estonian Information Society Strategy 2007-2013 followed. The document sets out six priority areas: increasing the knowledge, skills and participation of individuals; development of Estonia s next generation broadband network; development of electronic business environment; development of public services; large-scale uptake of e-ID; increasing the interoperability of state information systems. Implementation plan for the years for 2011 2013 is currently under development. (שם)

[21] ר' מצגת שמנתחת את מצב הסדרה הקיים בארה"ב: M. Hathaway, Cyber Policy: A National Imperative , Belfer Center of the Harvard Kennedy School, March 1, 2011.

[22] ר' האתר המצויין של ה- NITRD: http://www.nitrd.gov/About/about_nco.aspx .

מעניין לציין, כי מטרת ההשקעה במו"פ, על פי תפיסת נשיאות ארה"ב, היא כפולה: ביטחונית וכלכלית. פרק 5 של הדו"ח (Encouraging Innovation) מפרט את גישת הממשל למו"פ:

The Federal government should greatly expand coordination of these strategies with industry and academic research efforts to avoid duplication, leverage and synchronize complementary capabilities and agendas, and ensure that technology transitions and enters into the marketplace[24].

לבסוף, אחד היעדים שנכללו ברשימה של הנשיא, קבע כי יש להקים מסגרת לאסטרטגיות מו"פ קיברנטי, הכוללת את הנדבכים הבאים:

- פיתוח טכנולוגיות המשנות את כללי המשחק (game-changing)
- גישה למאגר נתונים רחב (event data) לקהילת המחקר
- ניתוח סיכונים אסטרטגיים, כדי לקבוע סדרי עדיפויות במו"פ
- עידוד שיתוף הפעולה בין מעבדות אקדמיות ותעשייתיות, כדי לזרז יישומים של מו"פ
- לאור סדרי עדיפויות במו"פ, לקדם יוזמות בארגוני התקינה הלאומיים והבינלאומיים
- חידוד האסטרטגיה של רכישות ממשלתיות ושיפור תמריצי שוק, על מנת לעודד מו"פ למוצרים עמידים (resilient) ולשירותים בטוחים יותר[25]

יעדים אלה מפורטים בתכנית מו"פ שפרסם בנובמבר 2009 מרכז המו"פ המיועד של המחלקה לביטחון פנים, A Roadmap for Cybersecurity Research [26]. הפעילות בתחום המו"פ מרוכזת ברמה הלאומית ב-National Coordination Office for Networking and Information Technology Research and Development [22], וב- Cyber Security Research and Development Center.

מעבר להסדרת נושא המו"פ ברמה הלאומית, גורמים אזרחיים ואקדמיים מקדמים תהליכי חשיבה מחוץ לכתלי הממשל[27]. ברמה התקציבית, המחלקה לביטחון פנים הודיעה בסוף חודש ינואר 2011 על הקצעת תקציב של 40$ מיליון למו"פ בתחום הקיברנטי[28].

תובנות מרכזיות מארה"ב:

- מסמך שמתפרסם ברמת הנשיא, הפורס מדיניות קיברנטית לאומית, ומדגיש את החיוניות של שיתוף פעולה בין מגזרי מסוג חדש.
- הקמה של מרכז המיועד למו"פ בתחום הביטחון הקיברנטי, עם ממשק אינטרנטי לציבור. (אתר ה- NITRD וה-Cyber Security Research and Development Center).
- עידוד דיון ציבורי בנושאים המשיקים למו"פ במכוני מחקר.
- משאבים פדרליים משמעותיים מוקדשים למו"פ הקיברנטי: הקצעת תקציב בסך $40 מיליון לשנת 2011.

5.2.4 בריטניה

ביוני 2009 פרסמה ממשלת בריטניה נייר מדיניות בתחום הביטחון הקיברנטי, שפרס את סדרי העדיפויות האסטרטגיים של המדינה בתחום. נושא המו"פ מפורט תחת הכותרת " Workstream 5, Technical Capabilities and Research and Development"[23]. באותו הפרק, הממשלה מפרטת את מחויבותה לפיתוח פתרונות טכנולוגיים ומדעיים לאתגרי המתחם הקיברנטי, בתיאום עם גורמים מהאקדמיה ומהמגזר העסקי, וכן שותפים בינלאומיים. המחויבות לתקצוב מאמץ המו"פ הלאומי מתווסף לסדר העדיפות המוצהר במישור של סחר בינלאומי "to provide opportunities for the UK's world class high tech companies"[24].

23 United Kingdom Cabinet Office, Cyber Security Strategy of the United Kingdom, June 2009 Workstream 5, p.
24 שם.
25 שם, עמ' 9.
27 ר' Government ICT Strategy, UK Cabinet Office, March 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-government-government-ict-strategy_0.pdf
28 Federal Republic of Germany, National Plan for Information Infrastructure Protection, 2005.בפתח מסמך המדיניות,

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

הממשלה מציבה את ההשקעה במו"פ בראש סדרי העדיפויות הלאומיים, ומציינת דווקא את החשיבות של פיתוח לשימוש מקומי (domestic), לצורך ההגנה על מערכות לאומיות.[25] המדיניות הבריטית עברה תהליך של ביקורת עצמית ועדכון, ובחודש מרץ 2011 התפרסם ה- Government ICT Strategy, שמציג גישה קפדנית ומדוייקת יותר מבעבר בכל הנוגע להתמודדות עם אתגרי הביטחון הקיברנטי, לרבות בתחום המו"פ[26]. את המדיניות מיישמת בפועל רשות, הפועלת בשיתוף פעולה עם משרד ההגנה הבריטית, ה-Office of Cyber Security and Information Assurance[27].

תובנות מרכזיות מבריטניה:

- לעקוב אחרי היעילות של תוכנית המו"פ הלאומית, למדוד את תוצאותיה באופן קפדני ולבחון מחדש את מטרותיה;
- בחברה דמוקרטית ופתוחה, ערך השקיפות מחייב פרסום ציבורי של אופן ביצוע מדיניות מו"פ ומדיניות כללית, לרבות אלו שאינם מיושמים באופן אופטימלי.

5.2.5 גרמניה

המדיניות של מו"פ קיברנטי בגרמניה נקבע כעקרון השמיני בנייר המדיניות הכללי[28], שעודכן בפברואר 2011[29]. הדגש הוא על פיתוח יכולות ליבה אסטרטגיות, רב-גוניות במו"פ ועמידה בתקינה בינלאומית.

8. Use of reliable and trustworthy information technology

The availability of reliable IT systems and components must be ensured on a permanent basis. The development of innovative protection plans for improved security which take into account social and economic aspects is strongly supported. To this end, we will continue and intensify research on IT security and on critical infrastructure protection. Furthermore we will strengthen Germany s technological sovereignty and economic capacity in the entire range of core strategic IT competences, include them in our political strategies and develop them further. Wherever it makes sense, we will pool our resources with those of our partners and allies, particularly in Europe. We are in favour of diversity in technology. Our aim is to use components in critical security areas which are certified against an international recognized certification standard.

תובנות מרכזיות מגרמניה:

- יש להתמקד בפיתוח יכולות ליבה אסטרטגיות.
- הגישה למו"פ הלאומי היא רב-גונית (diversity in technology).
- העמידה בתקינה בינלאומית היא יעד מוגדר.
- המושג "ריבונות טכנולוגית" במדיניות הגרמנית הוא ייחודי.

5.2.6 סינגפור

לסינגפור מדיניות קיברנטית מתקדמת וייחודית[30], הממוקדת במטרה הכפולה של הפיכתה ל"מדינה חכמה" (Intelligent Nation) עד שנת 2015, ומינוף היכולות הכלכליות של מגזר המו"פ כדי להיטיב עם הכלכלה המקומית. תוכנית החומש הנוכחית, Intelligent Nation 2015, מתוארת להלן:

IDA launched its infocomm masterplan, Intelligent Nation 2015 (iN2015), in June 2006, which aims to innovatively harness infocomm technologies to enhance our national competitiveness. It aims to transform Singapore into an intelligent nation, powered by infocomm. By 2015, an ultra high-speed, pervasive, intelligent and trusted infocomm infrastructure will be established and the Government, key economic sectors and society will be transformed through more sophisticated and innovative use of infocomm.

29 Federal Ministry of the Interior, Cybersecurity Strategy for Germany, February 2010.
30 ר http://www.ida.gov.sg/Programmes/20060925100740.aspx?getPagetype=36; http://www.ida.gov.sg/News%20and%20 Events/20080417090044.aspx?getPagetype=20 Singapore s Strategy in Securing Cyberspace, 2005 and Singapore s Infocomm Security Master Plan 2, 2008.

Singapore s success in this area will be determined by its ability to provide a secure and trusted infocomm environment. To continue our infocomm security efforts, Singapore launched its first three-year Infocomm Security Masterplan in 2005. Against the backdrop of pervasive use of infocomm technology by the Singapore Government, businesses and society, the first Masterplan focused on further developing Singapore's infocomm security capabilities and improving existing efforts to detect and prepare for cyber threats.[31]

בנוסף להתמקדות בפיתוח התעשייה הקיברנטית המקומית, סינגפור פונה לגורמי חוץ - מדינות וחברות - כדי למשוך משקיעים למגזר. כך, למשל, אתר האינטרנט של Infocomm מהווה מודל חיובי לחשיפת מידע רגולטורי, פיננסי וחינוכי לציבור הכללי ולציבור המשקיעים[32].

תובנות מרכזיות מסינגפור:

- תוכנית החומש של סינגפור למינוף המדינה כולה כגורם מוביל בהקשר הקיברנטי ייחודית, הן מבחינת הרתימה של כלל האוכלוסיה, והן מבחינת הראייה של ההטבות הכלכליות הפוטנציאליות למדינה.
- חשיפת מידע מגוון לכלל הציבור באופן מרוכז, דרך אתר Infocomm, מאפשר נגישות מקומית ובינלאומית למידע רב ורלוונטי למעוניינים להשתתף במו״פ קיבירנטי בסינגפור.

5.2.7 צרפת

בשנת 2008 הוקמה ANSSI, הרשות הצרפתית לביטחון רשתות מידע[33], כתוצאה מגיבוש תוכנית הביטחון הלאומי, שהתפרסמה באותה שנה בחתימת ראש הממשלה סרקוזי[34], וזיהתה איומים לאומיים בתחום הקיברנטי הראויים לטיפול ממוקד. על פי התוכנית, האיום הקיברנטי הוא אסטרטגי במישור הלאומי כמו גם במישור הכלל אירופי. היא ממליצה על הקמת רשות חדשה לביטחון מערכות תקשוב, לימים ANSSI, ועל פתיחת אתר אינטרנט ממוקד לצרכי קהילת המחקר בנושא.[35] אחד מיעדי הליבה של ANSSI, הינו למנוע איומים קיברנטים על ידי פיתוח מוצרים ושירותים אמינים עבור גורמים ממשלתיים וכלכליים[36].

באופן יוצא דופן, הציבור היה שותף להכנת המדיניות הצרפתית. כשתהליך הגיבוש של התכנית החל בקיץ 2007, פתחה הוועדה בסדרה של מפגשים פתוחים עם הציבור ששודרו בטלוויזיה, והשיקה אתר אינטרנט שהסביר את המשימה, והזמין את הציבור להעיר ולהגיב. האתר זכה ליותר מ-250,000 ביקורים[37]. זהו מודל חדיש וייחודי של שיתוף ושקיפות.

31 Infocomm Development Authority, Fact Sheet: Infocomm Security Masterplan 2, http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf

32 ר http://www.ida.gov.sg/home/index.aspx.

33 ר' את תיאור ההקמה, בתרגום לאנגלית: The French White Paper on Defence and National Security, published on June 17th, 2008, has identified cyber attacks as one of the main threats to the national territory. Indeed, society's growing dependence on information and communication technologies has made prevention and reaction to cyber attacks a major priority in the organisation of national security. In order to strengthen France s capabilities to face the challenges posed by information system security, the White Paper on Defence and National Security has planned the creation of a French Network and Information Security Agency (FNISA or ANSSI in French, standing for Agence Nationale de la S curit des Syst mes d Information), in a similar way to France s main partner nations. This new agency is placed under the authority of the Prime Minister and is attached to the Secretary General for National Defence. http://www.ssi.gouv.fr/site_rubrique88.html

34 שם.

35 שם, עמ 12-13. ר גם ANSSI , Network Resilience within the French NIS Strategy , Leroy, S.

36 To prevent threats by supporting the development of trusted products and services for governmental entities and economic actors;

37 שם, עמ' 3. ר' את אתר הדו"ח, שמתאר את תהליך ההתיעצות הציבורית: http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html

בפועל, לצרפת יש מספר יוזמות בתחום המו"פ הקיברנטי, חלקם בשיתוף הקהילה האירופית[38]. בשנת 2003 שדרגה צרפת את רשת המחקר שמחברת את האוניברסיטאות במדינה ברוחב פס 2.5 GB, Renater-3. הרשת הצרפתית מתחברת לרשת המחקר הכלל אירופית בשם Giant[39]. נכון ל-2010, צרפת משקיעה 2.08% מה-GDP במו"פ, 10% מכך בתחום טכנולוגיות התקשוב (ICT) [40].

תובנות מרכזיות מצרפת:

- ראייה אסטרטגית של התפקיד המוביל של צרפת בביטחון הקיברנטי.
- השתלבות בתוכניות המחקר של ה- EU.
- מסע הסברה מואץ בתוך צרפת, לרבות שיתוף אזרחים ומגזר פרטי בגיבוש המדיניות הקיברנטית הלאומית.

5.2.8 רוסיה

לרוסיה יש דוקטרינה של "ביטחון מידע" - מושג שקדם למושג הביטחון הקיברנטי - שפורסם בחודש ספטמבר 2000 בחתימת הנשיא פוטין[41]. התפיסה של ביטחון מידע אינה כוללת בצורה מפורשת התייחסות לאיומים ולאתגרים הקיברנטיים של זמננו, אך מעניין לציין, שרוסיה הבינה בשלב מוקדם יחסית את החשיבות של גיבוש מדיניות בנוגע למתחם החמישי.

יצויין כי רוסיה היתה, ככל הנראה, אחת המדינות הראשונות שנצלה את המתחם הקיברנטי ככלי לפעולה פוליטית, אם לא צבאית, נגד מדינות אחרות. ההתקפות הדיגיטליות נגד אסטוניה באביב 2007 ונגד ג'ורג'יה בשנת 2008 מיוחסות בספרות ובמדיה לרוסיה, למרות שהרוסים לא הודו בכך, ולא הוכח קשר רשמי של מוסדות המדינה לאירועים[42].

המרכיב השלישי של הדוקטרינה מפרט בצורה מפורשת את הצורך במו"פ בתחום התקשוב, כלהלן:

The third component of the national interests of the Russian Federation in the information sphere includes the development of modern information technologies, a domestic information industry, including an industry of informatization and telecommunications means, providing for the needs of the internal market with its products and putting these products in the world market as well as ensuring the accumulation, storage and effective use of national information resources. Under present-day conditions it is only on this basis that the problem of creating science-intensive technologies, technical modernization of industry and multiplying the achievements of the domestic science and technology can be solved. Russia must occupy a worthy place among world leaders in the microelectronics and computer industry. To achieve this it is required:to develop and improve the infrastructure of the single information space of the Russian Federation; to develop the national industry of information services and use the state information resources more effectively; to develop the production in the Russian Federation of competitive means and systems of informatization and telecommunications, to broaden the participation of Russia in international cooperation of the producers of such means and systems; to ensure state support of national fundamental and applied research and development in the sphere of informatization and telecommunications.[43]

38 משרד ההוראה הגבוהה והמחקר,

39 ר' ftp://trf.education.gouv.fr/pub/rechtec/brochure/rdtfen.pdf

40 משרד ההוראה הגבוהה והמחקר, La recherch et l innovation en France en 2010, http://www.enseignementsup-recherche.gouv.fr/cid50819/la-recherche-innovation-france-2010.html . ר' גם את הדו"ח השנתי של המשרד שפורסם בספטמבר 2010, Recherche et developpement, innovations et partenariats 2009.

41 Russian Federation, Information Security Doctrine of the Russian Federation, September 2000, p. 3.

The Economist, Marching Off to Cyberwar , Dec. 4, 2008, http://www.economist.com/node/12673385?story_id=12673385

42. the economist, marching off to cyberwar, dec. 4,2008, http://www.economist.com/12673385?story_id=12673385

43 שם, עמ' 3.

For its part, Russia has for more than a decade led an effort in the framework of the United Nations to establish some rules of

סדר העדיפות האחרון מדגיש דווקא את תמיכת המדינה במו"פ קיברנטי, ומשתלב עם סדר העדיפויות שנקבע לפיתוח תעשיות הטכנולוגיה ושיתוף פעולה בינלאומי בתחום.

בנוסף להצהרת המדיניות המוקדמת שלה, רוסיה קידמה יוזמות שונות במהלך העשור האחרון כדי לגבש אמנה בינלאומית בתחום הקיברנטי, ללא הצלחה[44]. לאחרונה, מגמה זאת מתחזקת, עם נכונותה של ארה"ב להירתם לנושא[45].

במגזר המו"פ הרוסי - למרות שלא נמצאה תכנית לאומית ממוקדת בנושא - יש לציין את הרמה הגבוהה של החינוך הטכנולוגי במדינה[46], יתרון המנוצל ע"י חברות זרות, שבוחרות למקם תעשיית מו"פ קיברנטי ברוסיה, כגון IBM, Cisco, ו-Google, למשל. בשנת 2007, הממשלה הקימה קרן השקעות כדי למנף את מגזר התקשוב במדינה, והשקיעה, לפי ההערכות, 54 מיליון דולר[47].

תובנות מרכזיות מרוסיה:

- ראייה של ביטחון קיברנטי בפרספקטיבה של מדיניות מידע
- התמקדות ביכולות פנימיות של מו"פ קיברנטי רוסי
- קידום תוצרים מקומיים

5.2.9 טבלה מסכמת לגבי מדיניות קיברנטית של מדינות נבחרות

מדינה	שנת גיבוש מדיניות קיברניטית כללית / מו"פ	גורם לאומי המרכז טיפול	הערות
אוסטרליה	2009	Cyber Security Policy and Coordination Committee	קביעת סדרי עדיפויות בתחום המו"פ; דגש על פיתוח כוח אדם
אסטוניה	מאי 2008 / 2010 (עדכון)	Estonian Informatics Center (incl. Dep t for Critical Information Information (Infrastructure Protection, CERT	דגש על שיתוף פעולה בינלאומי; הקמת מרכז מצוינות של נאט"ו, Cooperative Cyber Defense Center for Excellence
ארה"ב	2009 / 2010	Office of Homeland Security; White House Cybersecurity Coordinator	סדרי עדיפויות של מו"פ; שיתוף פעולה בין-ארגוני ברמה הלאומית, למרות ריבוי הגורמים
בריטניה	2009 / מרץ 2011	Office of Cyber Security and Information Assurance	פיתוח מגזר בתוך בריטניה; צורך בשיתוף פעולה בינ"ל; החשיבות של הבחינה מחדש של תוכן המדיניות וביצועה
גרמניה	2005	National Cyber Security Council	פיתוח יכולות ליבה אסטרטגיות; רב-גוניות במו"פ; עמידה בתקינה בינלאומית; "ריבונות טכנולוגית"

44. the game
45. (F-S. Gady and G. Austin, Russia, the United States and Cyber-Diplomacy, EastWest Institute, 2010, p. 3
שם, עמ' 4; והדו"ח הרב-צדדי שהוגש למזכ"ל האו"ם ביולי 2010.
46, IDefense , Global Threat Research Report: Russia, 2007, p.13
47 ר' שם, עמ' 18: This year, The Ministry of Information Technologies and Communications [ ] has initiated: the process of forming a joint stock company, the Russian Investment Fund for Information and Communication technologies. Several different ministries and other independent government agencies will also participate in the establishment of this fund. The startup costs, $54 million, will be totally provided by the Russian Investment Fund. [The Ministry] will be a .shareholder on behalf of the Russian Federation

ניו זילנד	2008	Cyber Security Section, Ministry of Economic Development	סדר עדיפויות לפיתוח כוח אדם מקומי ויצירת מקומות תעסוקה בתחום מו"פ הקיברנטי
סינגפור	2008 / 2005	Infocomm Development Authority	תוכנית חומש להפוך ל"חברה חכמה"; מינוף מגזר התקשוב לטובת הכלכלה המקומית; פנייה להשקעות מבחוץ
צרפת	2010 / 2008	National Network and Information Security Agency	ראיית המדינה כבעלת תפקיד אסטרטגי מוביל בתחום הקיברנטי; מו"פ במסגרת האירופית; אפשרות לאזרחים ומגזר פרטי להשתתף בגיבוש המדיניות הקיברנטית הלאומית
רוסיה	2007 / 2000	לא ידוע	חשיבות "מדיניות המידע" (שונה מביטחון קיברנטי); התמקדות בשוק המקומי בפיתוח מו"פ, שירותים ומוצרים קיברנטיים; התמקדות בשת"פ בינלאומי לגיבוש כללים קיברנטיים משותפים

5.3 מדיניות ותוכניות מו"פ בארגונים בינלאומיים נבחרים

מעבר לתהליכי הסדרת המו"פ הקיברנטי, המתרחשים בקרב מדינות מאז סוף שנות ה-90, גם במסגרת של ארגוני מדינות וארגונים מגזריים, החלו להתייחס בשנים האחרונות להתמודדות הרגולטורית עם פעילות במתחם הקיברנטי, לרבות בתחום המו"פ. בחרנו לבחון את המרכזיים שבהם: האיחוד האירופי, ה- OECD, ארגון הבזק הבינלאומי (ITU) ונאט"ו.

5.3.1 האיחוד האירופי

כניסתה לתוקף של אמנת ליסבון בדצמבר 2009, הביאה לשינוי של מרכיבים מסוימים במסגרת האבטחה והביטחון האירופית. במרץ 2010 החליט הפרלמנט האירופי ליישם אסטרטגיית אבטחה אירופית, שכוללת מפת דרכים לפיתוח נוסף של מדיניות ההגנה המשותפת למוסדות האירופים. למרות חילוקי דעות בתחומים מסוימים, קיים קונצנזוס רחב לגבי הצורך בפעילות רבה יותר בתחומים כגון הביטחון הקיברנטי. נושא נוסף שנתון לדיון באופן קבוע בקרב קובעי המדיניות הבכירים באיחוד האירופי, הוא האפשרות לגשר בין יכולות אזרחיות וצבאיות. בסוף שנת 2010, גובשה הצעת דירקטיבה שמשקפת גישות חדשות אלה, Proposal for a Directive on Attacks against Information Systems[48], שלא מזכירה במפורש את סוגיית המו"פ - היא מתמקדת בהגברת האכיפה של מערכת הדין האירופית במתחם הקיברנטי, ובפיתוח נוסף של האמנה נגד פשע קיברנטי - אך מיעדיה עולה בברור הצורך במו"פ של אמצעי אכיפה ברמה טכנולוגית מתוחכמת יותר, והדבר אף מצוין בדברי ההסבר.[49]

מדינות האיחוד מכירות בעובדה, שהממד הבינלאומי של מדיניות ההגנה והאבטחה מצריך פתרונות גלובאליים ושיתוף פעולה בין המדינות ובין מסגרות רב צדדיות נוספות. אלו מציבים הזדמנויות טובות לניתוח צרכים ולמחקר ופיתוח.[50]

48 ר' 14436/10, European Council, Brussels, 4 October 2010.
49 שם, עמ' 5.
50 ISC Intelligence in Science, 2011

הטיפול בנושא הקיברנטי זוכה להתייחסות במישור הביטחוני, כמו גם במסגרת סדר היום לאירופה דיגיטאלית משנת 2010 (A Digital Agenda for Europe)[51] המהווה את אחד מהיסודות המרכזיים לחזון של אירופה מתקדמת, מאוחדת ובעלת טכנולוגיה מתקדמת וסביבה עסקית מפותחת; ומצד שני, יש מודעות לאתגרים, שנוגעים בין היתר גם לסוגיות של פרטיות ואבטחה, ולמחקר ופיתוח לא מספק בתחום.

בנוסף, יש מודעות לכך שמדינות הקהילה לא יקדמו טכנולוגיות שמאפשרות רמה גבוהה יותר של בטיחות ברשת עבור משתמשים פרטיים. בהתאם לכך, על פי הנציבות, אחת המטרות המרכזיות של אירופה היא להביא לכך שמערכות המידע והרשתות באיזור יהיו חסינות ובטוחות בפני כל סוגי האיומים הקיברנטיים, ובמיוחד ברמת התשתיות הקריטיות[52]. הטיפול באתגרים הוא בגדר אחריות משותפת של האזרחים והגופים הציבוריים.

במסגרת היישום של עקרונות אלו, והמאבק של מדינות הקהילה כנגד פשעים קיברנטיים, נוצרה באירופה, כמו באיזורים אחרים, רשת של קבוצות תגובה לאירועי רשת -Computer Emergency Response Team , או CERT [53]. בנוסף, הנציבות הציבה שורה של צעדים בתחום ההגנה של רשתות מעבר ל-CERT, וזאת במקביל לתקצוב של מו"פ בתחום הקיברנטי.[54] הסוכנות האירופית לאבטחת מידע ורשתות, ה- European Network and Information Security Agency (ENISA), קוראת לשיתוף פעולה בינלאומי בפעילות נגד פשעי מחשב.

5.3.2 ENISA

הסוכנות האירופית לאבטחת רשתות ומידע[55], ENISA, הוקמה ב- 2004, והחלה לפעול בספטמבר 2005. זוהי הסוכנות המרכזית של האיחוד האירופי לנושאי אבטחה וביטחון במתחם הקיברנטי, הפועלת למען מוסדות האיחוד האירופי והמדינות החברות.

תפקיד הסוכנות הוא להשיג רמה גבוהה ויעילה של ביטחון רשתות ומידע בתוך האיחוד האירופי. ביחד עם מוסדות האיחוד והמדינות החברות, ENISA שואפת לפתח תרבות של אבטחת מידע ורשתות לטובת אזרחים, צרכנים וארגוני הסקטור הציבורי ברחבי האיחוד האירופי, ולהפוך את אתר האינטרנט שלה למרכז אירופי של החלפת מידע וניסיון בתחום אבטחת המידע[56]. בפועל, ENISA תומכת בעבודת הנציבות האירופית, המדינות החברות והקהילה העסקית, הכוללת טיפול, תגובה ובעיקר מניעה של בעיות אבטחת רשתות ומידע. הסוכנות גם עוזרת לנציבות האירופית בהכנה הטכנית של חקיקה בתחום אבטחת מידע ורשתות.

הסוכנות פועלת בחמשת התחומים הבאים: העלאת מודעות ציבורית; זהות, פרטיות ואימון; עמידות של שירותי רשתות תקשורת ציבוריות; ניהול סיכונים; ובניית יחסים עם בעלי עניין.

העלאת מודעות ציבורית – מתוך ההכרה שהמימד האנושי הוא החוליה החלשה בכל מסגרת אבטחת מידע, צריך לשנות באופן משמעותי את תפיסת המשתמש, או התרבות הארגונית, כדי להפחית את מספר פריצות האבטחה. לכן, מודעות אישית גבוהה לסכנות, כמו גם לצעדי המנע, היא הקו הראשון של ההגנה בתחום. בעלי עניין, משתמשי קצה ואנשים פרטיים או מהתעשייה צריכים לקחת אחריות בנושא. לאור זאת, הארגון פיתח מודלים של העלאת מודעות ופלטפורמות של שיתופי פעולה.

51 European Commission A Digital Agenda for Europe, 2010,
52 ר', למשל את הדירקטיבה בנושא ההגנה על תשתיות קריטיות של המדינות החברות משנת 2008, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345 of 23.12.2008.
53 http://www.cert.org/archive/pdf/10tr045.pdf
54 European Commission, Digital Agenda for Europe 2010 2020, Action 28
55 European Network and Information Security Agency (http://www.enisa.europa.eu)

צוותי CERT הם הכלי המרכזי להגנת תשתית מידע חיונית. לכל מדינה יש מחויבות ויכולות להגיב ביעילות למקרי אבטחת מידע, אבל הצוותים הללו משמשים כמקור לשירות האבטחה הראשי לממשלות ואזרחים, ובו זמנית גם כמעוררי מודעות ומחנכים. ENISA מיועדת למפות את היכולות של צוותי התגובה הלאומיים בעולם, ולצמצם את הפערים על ידי הקמה, אימון ותרגול של מרכזי התגובה.

זהות, פרטיות ואמון – ההצהרה של [57] Future Internet Assembly (FIA) לגבי הגישה האירופית לאינטרנט העתידי, חוזה את הפיתוח וההצבה של טכנולוגיות המבטיחות את החסינות והביטחון של הרשתות, ניהול זהויות, אבטחת פרטיות ויצירת אמון בעולם המקוון. בהקשר זה, ENISA נוקטת באסטרטגיה הבאה:

- סיוע בהצבה מהירה של תוצאות מחקר, בהתמקדות במודלים חילופיים של אמון, כגון מוניטין ורשתות אמון, כמו גם צרוף שיטות אימות.
- קידום גישה כלל אירופית לפרטיות: התמקדות בזכויות ומחויבויות של משתמשים, כמו גם של נותני שירות. אספקת קווים מנחים לשימוש בטכנולוגיות מקדמות פרטיות קיימות, והמשמעות שלהן לאנונימיות.
- פיתוח קווים מנחים לבחינה רגולטורית ופירושה, תוך התמקדות בזיהוי ואימות בתרחישים חדשים (כגון מיחשוב ענן RFID).
- להימנע מדרישות לא מציאותיות מגופים עסקיים ופגיעה בחירויות הפרט.

הארגון מעריך, כי יש תוצאות משמעותיות ל"טכנולוגיות שמקדמות את העמידות של הרשתות והאמון בתשתית", ולנושאי ביטחון שרלוונטיים לאפליקציות זיהוי אישיות[58].

עמידות של שירותי רשתות תקשורת ציבוריות – רשתות ושירותי תקשורת אמינים הם קריטיים לרווחת הציבור וליציבות הכלכלית. הנציבות מדגישה את החשיבות של אבטחת מידע ורשתות, ושל השותפות בין כל בעלי העניין בהגנה בפני האיומים, ובמיוחד הביטחון העצמי של האזרחים בתשתיות[59]. כדי להשיג מטרות אלה, ENISA פועלת בשלושה תחומים שונים אך משלימים:

- המדיניות והאסטרטגיה: המדיניות הלאומית והסביבה הרגולטרית במדינות האיחוד.
- הספקים: פרוצדורות, נורמות וטכניקות שמאומצות על ידי הספקים כדי לחזק את העמידות של הרשתות שלהם.
- הטכנולוגיה: מנתחת את הטכנולוגיות הרלוונטיות ומדגישה את האלמנטים הקשורים לביטחון ועמידות.

ניהול סיכונים – בעיקר ניהול המידע לניהול והערכת סיכונים, כמו גם פעולות ואירועים בתחום.

בניית יחסים עם בעלי עניין– היחסים עם בעלי העניין השונים והמגוונים הם גורם מפתח בהצלחה של המשימה הכללית. הקשרים הרשמיים והלא רשמיים מביאים לתובנות שאין כמותם, ומספקים גישה למומחים בתחום. כל זה מאפשר לזהות סיכונים, ולהכין את המדינות והארגונים הציבוריים והפרטיים טוב יותר, ולשפר את השותפות בתחום בין הסקטור הציבורי והפרטי. בין הפעילויות:

- **ניהול רשתות של בעלי עניין מקרב האיחוד האירופי, גורמים מגזריים, לאומים ובינלאומיים**
- **דו"חות לפי נושאים**
- **תיווך של מידע על ניסיון מצטבר**
- **דיווח לפי מדינות**
- **דו"ח רבעוני של ENISA**

הדו"חות הנ"ל הם מקור מצוין לעקוב אחר ההתפתחויות בארגון אירופי מרכזי זה.

56 שם.
57 http://www.future-internet.eu
58 תשתית אמינה מאופיינת במידה גבוהה של עמידות בפני אתגרים, ENISA פועלת בתחום מאז 2008.
59 ועדת ה-EU בנושא תשתיות קריטיות מכירה בתפקיד המוביל של ENISA בהקשר זה .

5.3.3 תוכנית המסגרת השביעית למחקר ופיתוח

תוכנית המסגרת השביעית למחקר ופיתוח טכנולוגי הינה הכלי המרכזי של האיחוד האירופי לתמיכה במימון מחקר ופיתוח באירופה בשנים 2007-2013[60]. התוכנית מיועדת גם ליצור צרכי תעסוקה, תחרותיות בעולם הגלובאלי ואיכות חיים. העיקרון המנחה בה הוא יצירת שיתופי פעולה, בדרך כלל בצורה של קונסורציום, לפרוייקטי מחקר ופיתוח של משתתפים מארצות שונות. סך כל התקציב של התוכנית כ- 51 מיליארד יורו, מתוכם כ- 32.4 מיליארד בתחום שיתופי הפעולה.[61]. הנושא הקיברנטי נכלל בשני תחומים מקצועיים: ICT (תקשוב) ו-security (ביטחון).

ICT

תחום ה- ICT מיועד לשפר את התחרותיות של התעשייה האירופית, ולאפשר לאירופה לעצב את ההתפתחויות בתחום בהתאם לדרישות החברה והכלכלה. התקציב הכולל של תכנית ה-ICT הוא 9.5 ביליון יורו. תוכנית הפעולה לשנים הקרובות קובעת את סדרי העדיפויות במסגרת המדיניות הכללית וסדר היום בתחום הדיגיטאלי. מסמך המדיניות בנושא ה-ICT מתאר את המטרות השונות בפרוייקטים[62].

באופן ספציפי, תוכנית הפעולה מזהה שמונה אתגרים אסטרטגים מרכזיים. הראשון והרלוונטי ביותר, Pervasive and Trusted Network and Service Infrastructures, שתקציבו כולל 625 מיליון יורו. עוסק ברשתות אמינות ותשתיות שירות, כולל תשתיות רשתות עתידיות (תשתיות פיזיות), מיחשוב ענן, ניהול וגישה לאינטרנט, אבטחת מידע באינטרנט, פרוטוקולים למחקר באינטרנט ועוד. מטרה 1.4 Trustworthy ICT (תקציב - 80 מיליון יורו), הרלוונטית ביותר, מגדירה את המעבר לעולם פתוח ומחובר מצד אחד, אבל מצד שני, מצריך אמון ואחריות, שיתוף פעולה ומידע, ורגולציה בשימוש במידע. פרוייקטים בתחום כוללים: ניהול זהויות, פרטיות, מדיניות אמון, אבטחת תשתית רשתות, שירותי תשתית, הגנה על תשתיות קריטיות וכו'.

ביטחון קיברנטי

הביטחון הוא התחום השני שכולל את נושא הסייבר, ותקציבו מסתכם ב- 1.4 מיליארד יורו. המחקר בו מיועד לפתח טכנולוגיות וידע לבניית יכולות הנחוצות לצורך אבטחת אזרחים מפני איומים כגון טרור, פשע, אסונות טבעיים ותאונות תעשייתיות[63]. כל זאת תוך שמירה על זכויות אדם ודיני הגנה על צנעת הפרט במדינות אירופה.

בימים אלה נערכים דיונים ראשונים לגבי התוכנית השמינית, ונושא הסייבר צפוי לקבל משקל מרכזי. עדיין לא ברורה מידת שיתוף הפעולה שהמדינות יהיו מוכנות לקיים.

5.3.4 EUREKA

יוריקה היא מסגרת מחקר נוספת בחסות הקהילה האירופית, המהווה פלטפורמה למחקר ופיתוח על ידי התעשייה בתחום היישומי, הקרוב יותר לצרכי השוק הנוכחי (לעומת תוכניות המסגרת, למשל)[64]. בארגון חברות כעת 39 מדינות, ביניהן ישראל, שאף משמשת כיו"ר במהלך 2010-2011[65]. הארגון מקדם שיתוף פעולה בינלאומי וחדשנות, ותומך בעיקר בפרוייקטים של מוצרים חדשים, תהליכים ושירותים לשוק. בשלב זה, שני פרוייקטים פועלים בתחום המו"פ הקיברנטי.

60 European Commission 7th Framework Programme
61 מתוך מצגת של ISERD, הגוף הישראלי שמטפל בתוכנית המסגרת של תכנית שיתוף הפעולה. שמטרתה להביא יחדיו את מיטב הכישרונות מרחבי אירופה (חוקרים, תעשייה וחברות קטנות ובינוניות)
62 ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/ict/c-wp-201101_en.pdf
63 כך, לדוגמא, תחום 10.2.5 עוסק בפשעי סייבר.
64 ר' את האתר כאן: http://www.eurekanetwork.org
65 מתוך האתר של יוריקה: In 2010-2011, Israel assumes the Chairmanship of EUREKA. Israel's appointment reflects the significant contribution of Israeli academia and industry to innovation, and the robust participation and leadership of Israeli companies in EUREKA projects.

5.3.5 OECD

ה-OECD עוסק למעלה מעשור בפעילות במתחם הקיברנטי של המדינות החברות בו[66]. הארגון משמש כצומת מידע ומרכז נתונים על המדיניות הקיברנטית, לרבות המו"פית, של המדינות החברות, ובזאת חשיבותו. כך, לדוגמא, מחקר של הארגון מ- 2007[67] בדק את המדיניות של אוסטרליה, קנדה, קוריאה, יפאן, הולנד, בריטניה וארה"ב בנוגע להגנה על תשתיות קריטיות מבחינת המתחם הקיברנטי, ואשתקד נבחנו אסטרטגיות וכלי מדיניות לניהול זהויות דיגיטאליות[68], היבט חשוב של המאבק נגד פשע קיברנטי.

מסמך שסיכם את המדיניות וסדרי העדיפויות בתחום ה- ICT בקרב החברות בשנת 2010[69], הצביע על קידום מחקר ופיתוח של מערכות הגנה על מערכות ורשתות כאחד התחומים המרכזיים ביותר לחדשנות. מספר התפתחויות מרתקות נוספות מעידות על העניין שמגלות בתחום מדינות השונות, כלהלן:

במסגרת פרויקט שמיועד לבדוק זעזועים גלובאליים עתידיים ("Future Global Shocks"), פורסם במחצית ינואר 2011 מחקר של שני חוקרים בריטיים, במסגרת ה- OECD [70]. החוקרים מציינים את הצורך של ממשלות להיערך בצורה מפורטת לעמידה או התמודדות בפני מגוון רחב של אירועי סייבר בלתי רצויים, ומזהים מספר פעולות שממשלות חייבות לבצע בתחום. בין העיקריות שבהן:

- המדיניות הלאומית של הגנת הסייבר צריכה לכלול את הצרכים של כל האזרחים, ולא רק של מתקנים ממשלתיים מרכזיים
- עידוד שימוש רחב היקף באמנות בינלאומיות בתחום
- תמיכה בחינוך של המשתמש הסופי
- שימוש בכוח רכישה, תקינה ורישיונות כדי להשפיע על ספקי תעשיית המחשבים על מנת שיספקו חומרה ותוכנה שנבדקו כיאות
- פיתוח משאבי מחשוב של משטרה מיוחדת בתחום
- תמיכה בכוח תגובה מיוחד כמו CERT
- תמיכה במחקר לתחומים כגון חיזוק פרוטוקולי אינטרנט, חקר סיכונים, תכנון השרדות

קבוצת עבודה בתחום ההגנה על מידע ופרטיות, שפועלת במסגרת ה-OECD, החלה בשנתיים האחרונות לדון בשיתוף פעולה במידע לגבי תוכניות של אבטחת מידע, כתוצאה מעמדות שהציגו מדינות שונות בנוגע לגישתן לנושא ותוכניותיהן לעתיד. הדיונים בפורום של ה- OECD סייעו לזהות מגמה של גישות של "אסטרטגיה של ביטחון קיברנטי": כאשר מצרפים את עמדות המדינות החברות בארגון ביחד, הן מצביעות על התפתחות בהיקף ובגישה, לעומת המדיניות והעמדות שהוצגו בשנות ה-90[71]. כתוצאה מכך, הוחלט לבצע ניתוח השוואתי של אסטרטגיות קיברנטיות אלו, כחלק מתכנית העבודה של קבוצת העבודה ב- 2011 ו- 2012. בין המדינות המשתתפות: אוסטרליה, ברזיל, צרפת, יפאן, בריטניה וארה"ב.

תוכנית העבודה בפרוייקט, שהופצה בתחילת פברואר 2011, מציפה מאפיינים משותפים לתוכניות האסטרטגיות של המדינות השונות, כולל הבנת האיומים המשתנים, עדיפות של הגנת סייבר בתוך הממשלה, הרחבת קווי המדיניות להגנת מידע ורשתות ועידוד תרבות של הגנה. יותר מאי פעם, הקשר בין הגנת רשתות מידע קריטיות, נכסים ומערכות הם חלק מתוכנית ההגנה הלאומית. במקביל, האסטרטגיות מורחבות מעבר להגנת מערכות מידע, וכוללות גם את הגנת הכלכלה והחברה[72]

66 OECD, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, 2005.

67 http://www.oecd.org/dataoecd/25/10/40761118.pdf

68 Draft Report on National Strategies and Policies for Digital Identity Management in OECD countries, OECD, 3 December, 2010

69 OECD Information Technology Outlook 2010, page 239.

70 http://www.oecd.org/dataoecd/57/44/46889922.pdf

71 אבחנה שנעשתה על בסיס הדיווחים הראשוניים של הצוותים השונים.

72 OECD, Work plan for a comparative analysis of National Cyber Security strategies, 8.12.2010.

יצוין, כי האסטרטגיות גם עונות על הצורך והרצון של המדינות החברות ב-OECD למקסם את ההטבות של הביטחון הקיברנטי במונחים של פעילות חברתית וכלכלית, חדשנות, חברה מבוססת ידע ומימדים אחרים, לרבות הגנה על צנעת הפרט. השילוב של שני המימדים, זה של ההגנה על המדינה במתחם הקיברנטי וזה של קידומה הכלכלי והחברתי בו, הולך וגדל. בנוסף, הגישה הנוכחית מדגישה מרכיב מרכזי של בינלאומיות, במטרה ברורה לעודד שיתוף פעולה חיובי בין מדינות במו"פ, ולמנוע התנהגות שתחליש את היתרונות של טכנולוגיות חדשות. בעבר, נהגו האסטרטגיות קודם כל לאמץ מדיניות לאומית ורק אח"כ לחפש שיתופי פעולה בינלאומיים. כיום, האסטרטגיות מדברות על שיתוף פעולה בינלאומי כבר בשלב הראשון של הפעילות. מימד בולט נוסף באסטרטגיות של מדינות בארגון, הינו תיאום פעילות בין מגוון רחב של גורמים בסקטור הממשלתי ובין גורמים בסקטור הפרטי, בשל הצורך למצוא צורות חדשות של שיתוף פעולה בין גופים ציבוריים ופרטיים, או להדקן.

העבודה בשנת 2011 תעסוק באסטרטגיות קיברנטיות של מדינות חברות, הן להגנת הכלכלה והחברה והן לטיפוח התפתחות כלכלית, חדשנות, מחקר ופיתוח, צמיחה ויעדים כלכלים וחברתיים אחרים. הן יכללו רעיונות לאמצעים, מנועים ותמריצים ליצירת תנאים למשיכת השקעות בתקשוב (IT - המושג הקרוב ביותר בשפת ה- OECD למו"פ קיברנטי)[73] ובתחומים אחרים, לקידום תחרותיות בסקטור ה- IT, לאימוץ מודלים חדשים וצומחים של טכנולוגיית מידע וטכנולוגיות שיאפשרו פעליוות כלכליות חדשות ויתרונות בפריון, כמו גם רווחה חברתית (לדוגמא: מחשוב ענן, ניהול זהויות, רשתות חברתיות).
תובנות מרכזיות מהפעילות של ארגון ה-OECD עולות בקנה אחד עם התובנות שעליהן הצביעה סקירת הפעילות הפרטנית של מדינות בתחום: (1) מדינות רבות התחילו להאיץ תהליך אסטרטגי של קביעת מדיניות; (2) לצד המניע ההגנתי, יש הכרה שצריך לנצל את התחום להתפתחות כלכלית, כולל קידום מחקר ופיתוח; (3) דגש בולט על שיתוף פעולה בינלאומי בקידום המו"פ הקיברנטי.

5.3.6 NATO

ארגון נאט"ו החל ב- 2008 להכיר בעובדה שהאינטרנט הופך לשדה קרב חדש, ודרושה עבורו אסטרטגיה חדשה להתמודדות. ההכרה חלחלה שהסייבר הוא מימד חדש של מלחמה. כדי להתמודד עם האיומים, קבוצה של חברות בנאט"ו, כולל ארה"ב וגרמניה, ייסדו תחילה קבוצת חשיבה פנימית שהתמקמה בטאלין שבאסטוניה.
כאמור לעיל, התקפת הסייבר על אסטוניה ב-2007 חשפה את הפגיעות של מדינות נאט"ו ללחצים חיצוניים. ב- 17 במאי 2010, נאט"ו פרסמה ניתוח והמלצות של קבוצת מומחים לאסטרטגית הגנה חדשה לנאט"ו לקראת 2020.[74] המומחים ציינו, שהאיומים הכי צפויים לבעלות הברית בעשור הקרוב הם הבלתי קונבנציונאליים: התקפה על ידי טילים בליסטים, פעילות של קבוצות טרור והתקפות סייבר ברמות שונות של חומרה.[75] כמו כן, הם פירטו מקרים שבהם התקפה על מערכות השליטה והבקרה של נאט"ו או רשתות האנרגיה, תביא להפעלת האמנה.[76]
בעקבות זאת, החל ארגון נאט"ו לנקוט בצעדים לפתח את היכולות באמצעות רשות לניהול ביטחון קיברנטי, ע"י הקמת מרכז מצוינות באסטוניה.

למרות יוזמות הארגון לטפל באיומים קיברנטיים, עדיין קיימים פערים ביכולות ההגנה של נאט"ו במתחם החמישי. התפיסה האסטרטגית החדשה קובעת שנאט"ו צריך להדגיש במיוחד את הטיפול בפגיעות הנוכחית של מדינות חברות. על כן, בשנתיים האחרונות, הייתה האצה בפגישות בנושא במסגרת נאט"ו. באוגוסט 2010 נוצרה יחידה חדשה במטה הארגון, שמיועדת, בין היתר, לעסוק באיומים הקיברנטיים, שהוגדרו בפסגת נאט"ו, שהתקיימה בנובמבר 2010 בליסבון, כאיומים אסטרטגיים משותפים,[77] במטרה לפרסם ביוני 2011 מדיניות חדשה ומעודכנת, הכוללת תוכנית פעולה שתעסוק בשתי שאלות עיקריות: על מה רוצה הארגון להגן בעתיד וכיצד הוא יפתח את היכולות המתאימות לכך.

73 ר' הערה 8 לעיל.
74 http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf
75 שם, עמוד 17.
76 שם, עמ' 45.
77 http://www.nato.int/cps/en/SID-4D826BDB-E940B960/natolive/news_70049.htm

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

ההיבט של מחקר ופיתוח

במקביל לגיבוש המדיניות בנאט"ו, נערכות פגישות תכופות בין מומחים מהמדינות החברות, כדי לדון בפרוייקטי מחקר ופיתוח ובמטרות המחקר והפיתוח העתידיות[78]. למשל, ב-7 בפברואר 2011, נפגשו נציגים כדי לדון בהאצת שיתוף הפעולה הבינלאומי בתחום[79]. המטרה הספציפית הייתה לשרטט פרוייקטים בינלאומיים משותפים, שיאפשרו לחברות נאט"ו לקדם את יכולות ההגנה שלהן בשיתוף ובאופן יעיל. הנושאים שנדונו כללו חילופי מידע לגבי איומים, טכנולוגיות ויכולות חדשות, ורכישה משותפת של יכולות תגובה לתקריות מחשוב. הגוף שאחראי על מו"פ בתוך נאט"ו הינו ארגון המחקר והטכנולוגיה (NATO Research and Technology Organisation[80]), הכולל כ- 3,000 מדענים במגוון טכנולוגיות, לרבות טכנולוגיות שתומכות בסימולציות שהארגון עורך. מועצה של המדינות החברות של נאט"ו, ה-Research and Technology Board, מנחה את הארגון וקובעת את סדר היום המחקרי שלו[81].

להלן תובנות מרכזיות מהפעילות בנאט"ו: (א) החשיבות של קבלת החלטה אסטרטגית ברמה הגבוהה ביותר, על מנת להדגיש את נושא הביטחון הקיברנטי באופן מיוחד במסגרת הפעילות הכללית של הארגון; (ב) ההבנה כי חייבת להיות גם תוכנית פעולה לביצוע ההחלטה; (ג) החשיבות של יצירת מתכונת קבועה למפגשי מומחים, כדי לדון בשאלות שנוגעות להגנה קיברנטית ולתחומי המחקר הנחוצים; (ד) הכרה כי אחד הקשיים הגדולים טמון בכך שההתקדמות הטכנולוגית היא בידיים של הסקטור הפרטי, ויש צורך להתאים את המסגרות הקובעות את המדיניות והמסגרת החוקית.

5.3.7 ITU

ה-ITU הינו הסוכנות המיוחדת של האו"ם (specialized agency) לנושאי מידע וטכנולוגיות תקשורת, ונקודת המוקד לממשלות ולסקטור הפרטי בפיתוח רשתות ושירותים. ב- 2009 פורסם מסמך מדיניות של ה- ITU בנושא הביטחון הקיברנטי[82], המקדיש חלק נכבד לתיאור ההיבטים הטכניים של האיומים השונים והתקנים הקיימים של בטיחות ברשת, ומונה גם שורה של צעדים לבניית יכולות, במישור הלאומי כמו גם במישור הרב צדדי, תוך הדגשה על כך שאחד הנושאים שצריך לפתח הוא מחקר ופיתוח בתחום.[83]

בוועידה העולמית של ה-World Summit on the Information Society , שפועל בחסות ה- ITU, שהתקיימה בשנת 2010, התגבשה יוזמה של הובלת התיאום הבינלאומי[84], בעקבותיה החליט מזכיר הארגון להשיק סדר יום גלובאלי להגנת סייבר (Global Cybersecurity Agenda), שהינו המסגרת לשיתוף פעולה גלובאלי שמטרתו להגדיל את הביטחון והאבטחה[85]. יוזמה נוספת של הארגון, משותפת לסקטור הפרטי והציבורי, הינו IMPACT (International Multilateral Partnership against Cyber Threats)[86]: ישראל שותפה ליוזמה.

ההיבט של מחקר ופיתוח

ה- ITU הוא מקור מצויין למעקב אחר תהליכים והנחיות, כולל בהיבט הטכני. מעורבותו הישירה בשת"פ מוגבלת, אך תחום ההשקעה בתשתיות התקשורת של מדינות מתפתחות יוצא דופן מבחינה זו. הגוף ITU-D אחראי לתיאום ומעקב בנושא זה, הכולל הנחיית רשויות ממשלה, פיתוח כוח אדם, אסטרטגיות מימון, פיתוח אזורי ואף תיאום השקעות במדינות[87] .

78 http://www.nato.int/cps/en/SID-EDF70412-83E36FCF/natolive/news_66528.htm ו-http:// RTO (http://www.rta.nato.int). www.nato.int/cps/en/SID-275E8A6D-9E396F11/natolive/news_65981.htm
79 http://www.nato.int/cps/en/SID-B35C2FE3-D558E4A9/natolive/news_70519.htm
80 http://www.rta.nato.int
81 הסבר מלא של מנגנון המו"פ של נאט"ו, לרבות פרוייקטים ספציפיים, נמצא באתר ה-RTO
82 http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html
83 שם.
84 http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf. 192 מדינות חברות בארגון, הקובע את עיקר התיאומים בהיבט הטכנולוגי של התקשוב הגלובאלי.
85 http://www.itu.int/cybersecurity/
85 http://www.itu.int/osg/csd/cybersecurity/gca/impact_index.html
87 ר' על פרוייקטים של ה- ITU-D ב: http://www.itu.int/ITU-D/projects/index.html

5.4 תקינה בינלאומית

בחלק זה נדון בביטחון קיברנטי כפי שהוא נתפס על ידי קובעי מדיניות ואנשי תוכן בתחום התקינה. בדומה לעולם הפטנטים, עולם התקינה מגדיר תחום התענינות במישור של קניין רוחני (intellectual property), ובוחן את האינטרסים של גופים מסחריים ולאומיים ליצור הנחיות או קודים בתחום. מטרות התקינה, כפי שהן מתבטאות באחד התקנים המובילים, הינן שלוש:

[…] the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required).[88]

בנייר עבודה של הבית הלבן שפורסם 60 יום לאחר כניסתו של הנשיא ברק אובמה לתפקיד, נסקרה המדיניות הקיברנטית של ארה"ב, והוגדרה באופן הבא[89]:

The global challenge of securing cyberspace requires an increased effort in multilateral forums. This effort should seek in continued collaboration with the private sector to improve the security of interoperable networks **through the development of global standards**, expand the legal system s capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective Internet governance.

על פי הבית הלבן, המאמץ לאבטח את המרחב הקיברנטי הגלובאלי במישור התקינה צריך להתמקד בפורומים בינלאומיים, תוך שילוב של הסקטור העסקי ופיתוח תקנים מתאימים כבסיס לפעילות אכיפה גלובאלית יעילה.

מהו תקן?
תקן מוגדר כמסמך המפרט את הדרישות החלות על מוצר או שירות כדי שיתאים לייעודו. התקן דן בתכונות שונות של מוצר כגון חומרים, מבנה, מידות, תפעול, סימון ואריזה. קיימים גם תקנים המגדירים שיטות בדיקה, מונחים ותוכן. בהקשר של ביטחון קיברנטי ומו"פ קיברנטי, עוסקים התקנים במיוחד בהנחיות לבדיקת מוכנות של ארגון, או בדרך הטיפול במרכיבים הקשורים למימד הקיברנטי (הגדרות , כתיבת קוד, ובדיקת והגדרת חומרה).

תקנים משמשים ככלי עזר חיוני לשמירה על איכות המוצר ולשמירה על אחידות במידות, במשקלות, בסמלים, במונחים ועוד. התקנים חשובים ביותר לבטיחות הציבור ולבריאותו, וכוללים הנחיות לביצוע מלאכות שונות. כל הגורמים הפועלים בשוק נעזרים בהם, לרבות המגזר התעשייתי, ציבור הצרכנים, משרדי הממשלה וארגוני מסחר שונים. כאמור, בתחום הקיברנטי נבחנת המשמעות במספר מישורים: הגדרת המתחם הקיברנטי, תכולת התקנים והאינטרסים לתקנֵנם.

5.4.1 תהליך התקינה בארגונים בינלאומיים

תהליך התקינה בעל אופי התנדבותי, לעומת אופי מחייב, עבור המדינות, הארגונים והגורמים המסחריים המשתתפים בו[90]. כמו כן, היישום של התקנים ככלל הינו על פי רצון המדינות. תהליך התקינה הוא יוזמה של המדינות החברות בארגון שבו מתבצעת התקינה[91].

88 תקן ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security management
89 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
90 בפרק זה נעשה מאמץ לשלב מונחים בעברית. המונח "התנדבותי" בפסקאות הבאות יתאר פעילות voluntary; כלומר, שאין בה חובה בינלאומית מטעם האו"ם או ארגון בינלאומי אחר.
91 ארגונים בינלאומיים מנסחים תקנים באמצעות תהליכים מובנים. ישנם סיווגים שונים לתקנים ולכן ניתן לפגוש כותרות שונות למסמכים שעברו תהליך תקינה סדור אך נוגעים בתחומים עיסוק שונים. כאשר התקן הוא לשיטת תקשורת הוא עשוי להיקרא פרוטוקול. קיימים ארגונים המכנים את התקנים אותם הם מפרסמים המלצות. במידה ובתחום עניין של ארגון התקינה נאסף מידע טכני רב שאינו מתכנס לכדי תקן מלא יפרסם הארגון נייר טכני בנושא שישמש את החברים עד לגיבוש תחום הפעולה או תקן מלא.

בדרך כלל, חברה או גורם אחר המציע פיתוח תקן נדרשת לגייס תמיכה בקרב בעלי עניין נוספים. בשלב הראשון מתכנסות ועדות מומחים ומציעות טיוטה לתקן, לאחר אישורה, נשלחת הטיוטה לסבב ביקורת חיצונית, ולאחר התייחסות להערות נסגר התקן ומפורסם. השימוש בתקן אינו נכפה על אף שותפה. התקן משמש כשפה משותפת, על הגדרותיה, למפתחים ומתכננים ממדינות שונות. לעתים, הוא הופך להיות מחסום או מגן מפני שירותים וסחורות המופצים על ידי מדינות שאינן עושות שימוש בתקן, ומכאן חשיבותו המסחרית, וההסבר למיקומם של ארגוני התקינה במשרדים למסחר ותעשייה.. ניווט נכון של תקנים ושימוש יעיל ומהיר בהם יכול להוות יתרון מסחרי למדינות החברות בארגוני סחר בינלאומיים, והמספקות מוצרים "איכותיים" בשווקים הבינלאומיים[92].

הארגונים הבינלאומיים המובילים בתחום התקינה הרלוונטית למו"פ הקיברנטי הינם: ISO, ITU ו- W3C. נסקור בקצרה את פעילותם באופן כללי, כאשר מובן כי התהליכים הכלליים חלים גם על פיתוח תקנים בתחום הביטחון הקיברנטי, ועשויים להוביל תהליכי מו"פ ולהשפיע עליהם בקרב הגורמים שמאמצים את התקינה הרלוונטית.

5.4.2 International Standards Organization - ISO

ISO נוסד בשנת 1947, כגוף בינלאומי המאחד ארגוני תקינה לאומיים, כמו מכון התקנים הישראלי. ISO מפרסם תקנים מסחריים ותעשייתיים, ההופכים לחוק או לתקן מחייב במרבית המדינות החברות בו, כולל ישראל, על אף שהארגון אינו ממשלתי. הארגון מקיים קשר הדוק ומושפע רבות מעמדות המדינות החברות והגורמים המסחריים בתוכן.

הליך התקינה ב- ISO מורכב משלושה שלבים בסיסיים[93]:

- העלאת הצורך בתקינה על ידי סקטור תעשייתי, באמצעות נציג של מדינה החברה בוועדה, במכתב מפורט. לוועדה הראשית.
- לאחר שהצורך הוכר, מוגדרת תכולת התקן בקבוצות עבודה טכניות (WG) המורכבות מנציגי המדינות המעוניינות בתקן.
- לאחר שחברי הקבוצה תחמו את ההצעה, התקן עובר לשלב השני, הנקרא שלב בניית הקונצנזוס, במהלכו דנים נציגי המדינות בתכולה הטכנית של התקן .
- השלב האחרון כולל את ההצבעה ואישור התקן, שמחייב תמיכה של 75% מהמשתתפות בתוצר הסופי. אם מתקבל אישור, התקן מתפרסם.
- תקני ISO עוברים הערכה ועדכון לפחות כל חמש שנים. התוצרים שהארגון מנפיק בהקשר הביטחון הקיברנטי הם תוצאה של עבודה משותפת של ISO וארגון IEC (International Electrotechnical Commission), במסגרת ועדה בשם JTC1[94]. דוגמה מתחום אבטחת המידע היא ה-ISO/IEC Code of Practice for Information Security Management [95].

5.4.3 ITU – International Telecommunications Union

כאמור לעיל, ה- ITU הוא סוכנות או"ם המתמחה בתחום הבזק והמידע[96]. מגזר ה- ITU-T מתמחה בתקינה בתחום התקשורת, לרבות פרוטוקולים לקישור אינטרנטי ואבטחת רשתות תקשוב, ואחראי גם על לימוד טכני של סוגיות תפעוליות ותמחיריות, ופרסום המלצות בראי התקינה העולמית בתחום. תחת ה- ITU-T פועלות מספר "קבוצות לימוד", ביניהם Study Group 17 , האחראית על הביטחון[97,98].

92 ראיון שבוצע עם מומחי תוכן במכון התקנים.
93 http://www.iso.org/iso/standards_development/processes_and_procedures/how_are_standards_developed.htm
94 ר' תחומי הפעילות של JTC1 כאן: http://www.iec.ch/dyn/www/f?p=103:6:0.
95 http://www.iso.org/iso/catalogue_detail?csnumber=33441 .
96 Part 1: ICT Standards Development Organizations and Their Work. (2008). Retrieved January 8, 2011, from International Telecommunication Union: http://www.itu.int/ITU-T/studygroups/com17/ict/part01.html
97 שם.
98 סקר שנתי שהוטל על הארגון ע"י הכינוס הבינלאומי להתפתחות World Telecommunication Development Conference (Doha,2006.

הקבוצה מורכבת משלוש קבוצות עבודה (Working Parties): WP1-Network and information security; WP2-Application security; ו- WP3- Identity management and languages. דוגמאות של תקינת ה-ITU-T בתחום הביטחון הקיברנטי כוללות התפתחויות במסגרת[99] Question 22/1, והמלצותיו 805 ו-1205 מסדרת X[100].

5.4.4 WWW Consortium – W3C

קבוצה בינלאומית שאינה ממשלתית, המפתחת את תקני הרשת (www), שהוקמה ב-1994 כארגון המאגד חברות מהתעשייה ומוקדש ליצירת קונצנזוס סביב טכנולוגיות הרשת. משימתו היא להוביל את הרשת למיצוי הפוטנציאל, על ידי פיתוח פרוטוקולים וקווים מנחים, שיאפשרו גידול בהיקפי השימוש בה לטווח ארוך. מאז 1994, פיתח ה-W3C יותר מ-110 תקנים, המכונים "המלצות", וכוללים תקנים ומסמכי הנחייה ידועים נוספים, כגון W3C[102]. HTML[101], PNG, RDF, XML, CSS מגדיר את יעד תקינה שלו כמאפשר תקשורת מותאמת ברשת ויכולת פעולה הדדית (webinteroperability). על ידי פרסום תקנים חופשיים (ללא בעלים ולשימוש פתוח), מבקש W3C למנוע פיצול של השוק, העלול להיגרם אם גופים בעלי עניין יפתחו תקנים שהם proprietary, כפי שעשוי היה להתרחש בעולם ה- DVD וה- BLUERAY, כשהתחרות בין התקנים פיצלה את העולם החזותי הדיגיטלי. דוגמה של תקן בשלבי גיבוש W3C בתחום הביטחון הקיברנטי הוא Web Security Context: User Interface Guidelines [103], אשר פורסם כטיוטה ב- 9 במרץ 2010.

5.4.5 תקינה וביטחון קיברנטי

גוף התקינה המשותף לאיגוד התקינה הבינלאומי ולוועדה הבינלאומית לאלקטרוניקה (להלן [104]ISO/IEC) מגדיר במבואת הטיוטה לתקן מס' 27032 (להלן "התקן") את הביטחון הקיברנטי באופן הבא:

This complex environment is build [sic] on interconnecting networks and systems, as well as any ICT devices, belonging to different organizations and service providers that allow for the flow of information. However, there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices because of gaps between these domains. Cyberspace security, or Cybersecurity, is about the security of the Cyberspace. It provides guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment. At the same time, Cybersecurity provides an infrastructure for collaboration between security stakeholders in the Cyberspace[105].

התייחסות נוספת לתקן למרחב הקיברנטי, בדגש על הקשיים בתהליכי התקינה בתחום:

Cyberspace is evidently a complex, highly variable environment, and hence information security risks in cyberspace are tough to pin-down. Furthermore, constant innovation makes it especially tough to set international standards in this area.

אם כן, גופים ממשלתיים מסוימים מתייחסים להצעה לתקן למרחב הקיברנטי כלא בשלה, עקב בעיות מבניות ופערים. כמה מדינות מטילות ספק בצורך בתקן בתחום שהוא במהותו לא מוגדר, בעוד שאחרות ממהרות לאשרו. בשלב זה עצם ההגדרה של הביטחון הקיברנטי, העומדת בלב התקן, נבחנת ומאותגרת על ידי השותפים[106].

99 Question 22-1. (2006). Retrieved January 8, 2011, from International Telecommunication Union: http://www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/Questions/Q22-1.pdf

100 סדרת התקינה מסוג X מתייחסת ל- Data networks, open system communications and security ב-ITU-T.

101 לא לכולם יש תוקף של תקן מלא, לדוגמה: HTML היא שפת markup שעומדת בתקן ISO8879 (http://www.w3.org/TR/1999/REC-html401-19991224/); ו-PNG הינו פורמט של תמונה, כמו JPEG.

102 W3C עוסק גם בהשכלה, בסיוע, ופיתוח תוכנה, ומשמש כפורום פתוח לדיון בנושא הרשת.

103 http://www.w3.org/TR/2010/WD-wsc-ui-20100309

104 פירוט על פעילות ארגון התקינה הבינלאומי. ראו להלן על ארגוני התקינה.

105 בהמשך מפרט התקן מה אינו נכלל במושג "ביטחון קיברנטי":
Cybersecurity is, however, not synonymous with Internet security, network security, information security, or critical information infrastructure protection (CIIP).

106 http://www.iso27001security.com/html/27032.html

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

Some national bodies evidently consider the CD immature with various structural problems and gaps, as well as the usual typos etc., and a few are still questioning the need for a standard in such an ill-defined area, while yet others approve. Even the definition of 'cybersecurity' (which is of course central to the entire standard) is still being challenged.

ארגון התקינה הבינלאומי החל בתהליך התקינה של ISO/IEC 27032. התקן יסקור את האתגרים הביטחוניים במרחב הקיברנטי במלואם. בטיוטת התקן מוגדרת המורכבות של המרחב הקיברנטי באופן הבא:

The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

התקן נמצא כרגע בשלבי טיוטה[107].
על אף שתהליכי תקינה בהקשר של ביטחון קיברנטי מתקדמים ברמה הבינלאומית, מספר רב של נושאים עדיין ממתינים לטיפול, כגון:

- יישומי רשת דור שני (Web 2.0), לרבות "software as a service"
- בלוגים, לרבות אלה שכוללים מידע שמע וחזותי
- רישות הדדי (peer-to-peer)
- הודעות מסוג instant messaging
- סביבות וירטואליות כגון Second Life
- משחקי מחשב מתקדמים

דוגמאות נבחרות של של תקינה עתידית של ISO/IEC, הנמצאת כרגע בפיתוח, הינן:

ISO/IEC 27007 Guidelines for information security management systems auditing (focused on the management system)
ISO/IEC 27014 Information security governance framework
ISO/IEC 27015 — Information security management guidelines for the finance and insurance sectors
ISO/IEC 27032 Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
ISO/IEC 27035 Security incident management
ISO/IEC 27036 Guidelines for security of outsourcing
ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence

התקינה בעולם הביטחון הקיברנטי נמצאת כרגע בשלב מכריע. למול מדינות, חברות וארגונים שאינם מעוניינים בתקינה מחייבת, משיקולים שונים, ניצבות מדינות המעוניינות בשיתוף פעולה ובהגדרות שיתופיות, שיאפשרו להפוך את המתחם החמישי החדש לבטוח, מוגן וודאי יותר.

5.5 מיפוי המצב הנוכחי בארץ בנוגע למו"פ בתחום הקיברנטי והסדרתו

חלק זה מיועד למפות את המצב הנוכחי בארץ בכל הנוגע למו"פ הקיברנטי בשלושה היבטים: המנגנונים ושיתופי הפעולה ברבדים השונים; המערכת הרגולטורית, לרבות דברי חקיקה; והתקינה הקיימת. לצורך כך הסתמכה תת הוועדה על הידע הקיים של חברי הצוות ועל ראיונות משלימים עם אנשי מקצוע בתחומים השונים.

[107] לא תהיה התייחסות למשתמשים יחידים במסגרת התקן. אף על פי כן, ה- CD הראשון כולל התייחסות רחבה ל-end users ו consumers במסגרת הארגונים.

5.5.1 גופים ושיתופי פעולה קיימים

את שיתופי הפעולה הקיימים בישראל ניתן לבדוק מכמה זוויות: סוגי השחקנים המשתתפים במו"פ (ביטחוני, אזרחי, אקדמיה) והצרכים (ביטחוני או אזרחי), כמו גם התשתיות הקשורות בתמיכה במו"פ. בחלק זה, נבחן מספר דוגמאות מזוויות ראייה שונות.

I. מיפוי גופים מעורבים בתחום המו"פ בישראל ניתן לזהות מספר גופים מרכזיים שפועלים בתחום המו"פ הקיברנטי: השב"כ, צה"ל (מפא"ת וגורמים אחרים), מטה לוט"ר, המדען הראשי במשרד התמ"ת, תהיל"ה, חברות בתעשייה, לרבות חברות זרות פועלות בישראל, וגורמים באקדמיה.

להלן פירוט של פעולותם של שניים מהגורמים הנ"ל: לשכת המדען הראשי במשרד התמ"ת ומפא"ת[108].

5.5.2 פעילות לשכת המדען הראשי במשרד התמ"ת

לשכת המדען הראשי במשרד התעשייה, המסחר והתעסוקה (המינהל למחקר ופיתוח תעשייתי) פועלת מתוקף החוק לעידוד מחקר ופיתוח בתעשייה, התשמ"ד - 1984. הלשכה מופקדת על פיתוח התעשייה הישראלית על כל ענפיה, באמצעות עידוד החדשנות הטכנולוגית והתעשייתית, במטרה לקדם את היצוא, ליצור מקומות עבודה ולשפר את מאזן התשלומים של המדינה. כמו כן, מופקדת לשכת המדען על כריתת הסכמים בינ"ל, דו צדדיים ורב צדדיים, לקידום מטרות החוק.

הלשכה תומכת במו"פ התעשייתי על ידי סיוע כספי ישיר בהתאם לחוק המו"פ. היא מובילה פיתוח של מודלים ארוכי טווח ומודלים בתגובה לצורכי השוק הישראלי, שמזוהים על ידה, תוך ראייה ארוכת טווח. פיתוח תשתיות הידע, הטמעת החדשנות והמו"פ במספר סקטורים ייחודיים, מתרחש במספר מסלולים, כפי שיפורט בהמשך[109]. במקביל לפעילות זו, מופעלות תוכניות תמיכה הכפופות לחוק המו"פ על פי הוראות מנכ"ל, כמו: פיתוח והרחבה של תשתית טכנולוגית לתעשייה באמצעות סיוע למו"פ גנרי במסגרת תוכניות "מגנ"ט", טיפוח שיתופי פעולה בינלאומיים בתחום המו"פ התעשייתי, תמיכה ביזמים באמצעות חממות טכנולוגיות למימוש רעיונות טכנולוגיים חדשניים, עידוד יזמים בתחילת דרכם במסגרת תוכנית "תנופה" ועוד[110].

מסגרות התמיכה של לשכת המדען הראשי תומכות מדי שנה במאות תוכניות מו"פ בכל שלבי הפיתוח. המכנה המשותף לכל החברות המשקיעות במו"פ חדשני הינו הסיכון הרב שהן לוקחות על עצמן. בשונה מתמיכה ממשלתית במדינות אחרות בעולם, חברות שמצליחות במכירת מוצרי מו"פ שנתמכו ע"י לשכת המדען הראשי, משלמות תמלוגים אשר משמשים כמענקים לחברות אחרות. בעשרת השנים האחרונות תמך המדען הראשי במאות פרוייקטי מחקר ופיתוח הקשורים במתחם הקיברנטי. להלן פירוט של חלק ממסלולי המו"פ שהמדען הראשי תומך בהם בתוך ישראל.

108 הפעילות של מרבית הגורמים הנוספים נכללת בעבודת המטה של תתי-ועדה אחרות במיזם.
109 למשל, בתחומי המו"פ בתעשייה מסורתית, ננו-טכנולוגיה, ביו-טכנולוגיה, מים ואנרגיה.
110 ר' אתר המדען הראשי, http://www.tamas.gov.il/NR/exeres/3C96E1CF-EDFA-4F16-BACE-216773805124.htm

תוכנית מגנ"ט (התכנית לקידום מו"פ גנרי–טכנולוגי)
מטרת תכניות מגנ"ט היא לחזק ולהרחיב את התשתית הטכנולוגית של התעשייה בישראל, באמצעות פיתוח מקומי של טכנולוגיות גנריות טרום תחרותיות, הפצה והטמעה של טכנולוגיות גנריות הנחוצות למגוון רחב של תאגידים, קידום העברת טכנולוגיה מהאקדמיה לתעשייה וגישור בין המחקר הבסיסי למחקר היישומי בתחומים מוגדרים. התוכנית מופעלת בחמישה מסלולים: "מאגדים", "איגודי משתמשים", "מגנטון" "נופר" ו"קטמון". ועדה ציבורית מאשרת את התוכניות. לשכת המדען הראשי מיישמת את ההחלטות, ומבצעת מעקב ובקרה.

מאגד – מסלול למו"פ של טכנולוגיות גנריות
התאגדות של תאגידים תעשייתיים ומוסדות מחקר, לביצוע פיתוח עצמי של טכנולוגיות גנריות באמצעות היכולות שנרכשו במגנ"ט. בשנת 2009 פעלו במסגרת מגנ"ט: 17 מאגדים, ביניהם שלושה חדשים בתחומי רשתות וידאו עתידיות, אנרגיה סולארית וננו-צינוריות; 14 ותיקים במגוון תחומים כגון: מים, תקשורת אלחוטית מתקדמת, בקרה מבוססת דימות, ביוטכנולוגיה; וקבוצת חברות המקדמות טכנולוגיות עיבוד למתכות קלות בתחום התעשייה המסורתית. לאחרונה יצא קול קורא להקמת מאגד בתחום הסייבר לשיתוף פעולה בביצוע מו"פ גנרי בתחום (ר' **נספח ג'**).

איגוד משתמשים – מסלול הפצה והטמעה של טכנולוגיות
פעילות משותפת של תאגידים תעשייתיים המשתמשים בטכנולוגיות מתקדמות להפצה, הטמעה והדגמה של טכנולוגיות גנריות מתקדמות בתחומי עיסוק (לומדים יחד מניסיונם של אחרים). בשנת 2009 פעלו שלושה איגודי משתמשים בטכנולוגיות מתקדמות: איגוד אילט"ם, איגוד משתמשים לתחום התקשורת הניידת ואיגוד למשתמשי טכנולוגיית ה-GRID . האיגודים מקיפים כ- 200 חברות, הפועלות להפצה והטמעה של טכנולוגיות בתחומי המערכות המשולבות, תקשורת סלולארית ורשתות מחשבים מתקדמות. כל האיגודים הרחיבו את מעגל המשתתפים ב-10% ויותר.

מגנטון – העברת טכנולוגיות מהאקדמיה לתעשייה
מסלול לשיתוף פעולה בין קבוצת מחקר מהאקדמיה לבין חברה תעשייתית, במטרה לצמצם את אי הוודאות של הפוטנציאל השיווקי של טכנולוגיות הנמצאות בפיתוח באקדמיה, לפני להעברת הטכנולוגיה מהאקדמיה לתעשייה להמשך פיתוח מוצר בעל פוטנציאל כלכלי.

לסיכום, היתרונות של תכניות המדען הראשי טמונים בפתיחות שבתהליך הבקשה לתמיכה. התכניות פתוחות לכל חברה ישראלית, ועיקרן עידוד חדשנות וחלוקה בסיכון של הפיתוח בין החברה והמדינה, בכפוף לכך שהפרויקט מוכר כחדשני. כפי שראינו, יש מספר מסלולים הקשורים לשלב שהחברה נמצאת בו, כולל מימון בצורה פרטנית, הצטרפות לתכנית של מאגדים כדוגמת מגנט לפיתוח טכנולוגיה יותר גנרית, או תכניות שת"פ בינלאומי. בפועל, מספר גדול של חברות ישראליות שפעילות בתחום הקיברנטי נהנות ממסלולי תמיכה של המדען.

בצד המגבלות והחסמים לשיתופי פעולה, יש לציין כי תקציב המדען הראשי מוגבל בהיקפו, אך התקצוב בפועל לפרוייקטים בתחום הסייבר גבוה. בנוסף, למרות הניסיון המצטבר, קיים עדיין חשש של חברות בעבודה משותפת לפיתוח טכנולוגיות גנריות.

5.5.3 מפא"ת – המינהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית
מפא"ת הוא גוף מטה משותף למשרד הביטחון ולצה"ל, שאחראי להתוות את מדיניות המחקר והפיתוח במערכת הביטחון. מערך המחקר והפיתוח הביטחוני בארץ מבוסס על שיתוף פעולה בין ארבעה נדבכים: חילות וזרועות צה"ל המגדירים את צרכיהם; גופי תכנון וניהול מו"פ במשרד הביטחון וצה"ל; התעשיות הביטחוניות (רפא"ל, תע"א, תע"ש ועוד); ומוסדות מחקר שעבודות המחקר והפיתוח מתבצעת בהם.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

מתוקף אחריותו, מבצע מפא"ת את הפעילויות העיקריות הבאות:

בניית וקידום התשתית המדעית והטכנולוגית – באחריות מפא"ת לבנות ולקדם את התשתית המדעית והטכנולוגית הנחוצה להבטחת כושר פיתוח מערכות אמל"ח עתידי מתקדם לצורכי צה"ל. בניית התשתית מתבצעת באמצעות קניית יכולת שליטה בספקטרום רחב של טכנולוגיות, טיפוח כוח אדם ומוקדי ידע מדעיים וטכנולוגיים, וכן הבטחת קיומם התקין והיעיל של מתקני התשתית הדרושים לפיתוח אמל"ח מתקדם.

הכוונת פוטנציאל המו"פ – ייזום ובחינה של יוזמות חדשות לאמל"ח עתידי בעל יתרון יחסי, המתבססות על ניצול הזדמנויות טכנולוגיות. הפעילות מחייבת שליטה ברמה המתקדמת ביותר בעולם (state of the art) בתחומים טכנולוגיים כמו: אווירונאוטיקה, אופטרוניקה, אלקטרוניקה, מיקרואלקטרוניקה, מדעי המחשב, מכ"מ, תקשורת, חמרים, תהליכים ומבנים, סימולטורים ואמצעי ניסוי, רפואה צבאית ועוד. **רכש וניהול פרוייקטי פיתוח עבור זרועות וחילות צה"ל** – מפא"ת הוא הגוף האחראי לרכישת פרוייקטי פיתוח העונים לדרישות זרועות צה"ל. פרוייקטים מרכזיים בעלי היקף תקציבי גבוה מתנהלים על ידי מינהלות פרוייקטים.

ניתוח ותיאום העבודה של כלל צה"ל בנושאי מו"פ, לרבות המו"פ הקיברנטי – כגוף מטה המשותף למשרד הביטחון ולצה"ל, מפא"ת מנתח ומתאם את פעילות המו"פ הביטחוני בצה"ל ובמערכת הביטחון. מעבר לפעילות בישראל, הוא גם מקיים קשרים עם גורמים בחו"ל בנושאי התשתית והמו"פ הביטחוני.

לתת הוועדה לא היה מידע מפורט על אודות פרוייקטים ספיציפיים של מפא"ת: בשלב הבא של המיזם, יהיה צורך לקבל את המידע ולנתחו, על מנת לזהות פערים נוספים בפעילות המו"פית הקיברנטית בישראל.

5.5.4 פרוייקטים מעורבים: מערכת הביטחון והמגזר הפרטי בישראל

דוגמה לשיתוף פעולה בין מערכת הביטחון לבין המגזר האזרחי בישראל היא תוכנית ממ"ד, מסלול מתוכנן לתמיכה במחקר דואלי (dual use) בעל יישומים צבאיים ואזרחיים. משרדי התמ"ת והביטחון, בתיאום עם משרד האוצר, החליטו לפעול במשותף לקידום המו"פ של טכנולוגיות דואליות העשויות לתרום לביטחון המדינה, מצד אחד; וכן להיות בסיס לפוטנציאל כלכלי בשוק המסחרי הבינלאומי, האזרחי והצבאי, מצד שני.

המטרה היא להקים תוכנית שתנוהל במשרד התמ"ת, על ידי ועדת היגוי בראשות משותפת של ראש מפא"ת והמדען הראשי בתמ"ת, המיועדת לעודד חברות קטנות עד בינוניות לקדם רעיונות יצירתיים וחדשניים, העשויים לסייע לצה"ל להתמודד עם אתגריו המבצעיים, ובמקביל לפתח מוצר מסחרי בר תחרות בחו"ל. התכנית תטפל בכל רובדי המו"פ, החל ממחקרים ראשוניים, דרך שת"פ בין האקדמיה לתעשייה, ועד מדגימים למוצרי העתיד. תנאי המימון יהיה כמקובל במסלולי הסיוע של המדען הראשי, בהתאם לאופי הפרוייקט והתאמתו. התקציב המתוכנן של התכנית הוא כ-60 מיליון ₪ לשנה, החל משנת 2013.

5.5.5 שיתופי פעולה של גורמים ישראליים עם גורמים בחו"ל

שיתופי פעולה טכנולוגיים עם גופים בחו"ל מאפשרים, מצד אחד, להשתתף בידע ובמשאבים נוספים, ומספקים גישה לשווקים ולמקבלי החלטות במדינות שונות. מצד שני, פרוייקטים משותפים עם גורמים מחו"ל עלולים להביא לזליגה לא רצויה של ידע וטכנולוגיות ישראליות לגופים זרים. סוגיה זאת מטופלת, באופן חלקי, במסגרת חוק הפיקוח על יצוא ביטחוני, התשס"ז - 2007, שאליו נתייחס להלן.

בשלב הראשון, מטרתנו לזהות את המכניזם הנוכחי על מנת להעריך טוב יותר את הפוטנציאל וההזדמנויות הלא מנוצלים. הפרק שלעיל עוסק בנקודה זו בהקשר של תחום המו"פ הקיברנטי בארגונים בינלאומיים.

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

שת"פ עם גופים אזרחיים בחו"ל
חברות ישראליות מבצעות פרוייקטים רבים בחו"ל, שכוללים, בין היתר, שיתוף פעולה במו"פ. מספר חברות ישראליות בתחום התקשוב (שחופף לתחום הקיברנטי[111]), נרכשו על ידי חברות זרות, שעדיין מפעילות מרכזי מחקר בארץ. חלק ניכר משיתוף הפעולה בתחום האזרחי מתבצע באמצעות הכלים והמנגנון שמפעילה לשכת המדען הראשי במשרד התמ"ת.

הפעילות הבינלאומית של לשכת המדען הראשי בתמ"ת
המדינה מקדמת שיתוף פעולה בינלאומי במו"פ בין חברות תעשייה ישראליות לזרות, כדי לסייע לחברות הישראליות לייצר שיתופי פעולה אסטרטגיים עם חברות מתאימות בחו"ל, וכך לשפר את כושר התחרות של החברות הישראליות וחדירתן לשווקים הבינלאומיים. לשכת המדען הראשי יוזמת מסגרות והסכמים לשיתופי פעולה בינלאומיים, ומשתתפת במימון תוכניות המו"פ המאושרות של החברות הישראליות. ועדת המחקר מאשרת את תוכניות המו"פ, ולשכת המדען הראשי מיישמת את ההחלטות ומבצעת מעקב ובקרה אחר עמידה בתנאים ואבני דרך. לשם כך נוצרו מספר מודלים של שת"פ בינלאומי:

- קרנות דו-לאומיות
- הסכמים דו-לאומיים לתמיכה מקבילה
- הסכמים רב-לאומיים באירופה לשת"פ טכנולוגי תעשייתי
- הסכמי שת"פ עם תאגידים רב-לאומיים
- תוכנית המסגרת למו"פ של האיחוד האירופי ISERD
- נציבות המדע והטכנולוגיה ישראל-ארה"ב.

להלן שתי דוגמאות של שת"פ מו"פ בינלאומי שמתרחש בישראל, תוכניות ISERD ותוכנית יורקה.

ISERD – תוכנית המסגרת למו"פ של האיחוד האירופי
תוכנית המסגרת למו"פ של האיחוד האירופי היא הגדולה ביותר בעולם לשיתוף פעולה מדעי ותעשייתי, ומהווה את המרכיב הפיננסי המרכזי של המרחב האירופי למחקר, - European Research Area ERA. התוכנית מתחדשת מדי כמה שנים, ומתכונתה הנוכחית היא תוכנית המסגרת השביעית, שתיארך שבע שנים, בין 2007-2013, ותקציבה הכולל הוא כ- 50 מיליארד יורו. ישראל היא המדינה היחידה מחוץ לאירופה המשתתפת בתוכניות המסגרת למו"פ של האיחוד האירופי כמדינה נלווית מאז 1996. להשתתפות בתוכנית יש ערך מוסף משמעותי עבור התעשייה הישראלית, המתבטא בהשתלבות במו"פ ובעולם העסקים האירופי, יצירת קשרים אסטרטגיים עם חברות אירופיות מובילות, חשיפת התעשייה הישראלית ויכולותיה לתעשייה האירופית, והיא מעניקה קרש קפיצה להחדרת טכנולוגיות ישראליות לשוק האירופי, הזדמנות לזיהוי מגמות שוק, מודיעין עסקי, חשיפה לטכנולוגיה באירופה והידוק הקשר בין התעשייה והאקדמיה הישראליות. בנוסף, ההשתתפות בתוכנית מאפשרת לחברות ישראליות להיות עם "יד על הדופק" במהלך פיתוח סטנדרטים והליכי תקינה טכנולוגיים באירופה, והיא חשובה ביותר עבור חדירה עתידית של טכנולוגיות המפותחות בישראל לשוק האירופי והגלובאלי. לשכת המדען הראשי רואה חשיבות רבה במעורבות התעשייה הישראלית בתוכנית המסגרת, וחברות ישראליות רבות בתחום הסייבר משתתפות בדיונים והתייעצויות הנוגעות לפעילות קיברנטית.

תכנית יוריקה Eureka
יוריקה היא מסגרת כלל עולמית גדולה לשת"פ במו"פ תעשייתי, שנדונה לעיל בהרחבה. מדובר בתוכנית כלל אירופית, בהשתתפות 40 מדינות[112]. ישראל הינה החברה הלא אירופית היחידה במעמד של חברה מלאה (והיו"ר בשנות 2010-11). המדען הראשי חתם בשם המדינה על הסכם עם יוריקה, ולשכתו פועלת להרחבה והעמקה של ההשתתפות הישראלית במסגרות השונות של התוכנית.

111 ר' הערה 8 לעיל.
112 ר' האתר של יורקה, http://www.eurekanetwork.org

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

שת"פ עם גורמים ביטחוניים בחו"ל
תת הוועדה לא הצליחה לקבל תמונה, אפילו ראשונית, של מגוון שיתופי הפעולה הביטחוניים של ישראל עם גורמים בחו"ל. בעבודה המשותפת של ישראל וארה"ב במסגרת ה- Technical Support Working Group הפדראלי[113], לדוגמה, לא נמצאו נתונים פומביים על העיסוק בתחום הקיברנטי.

יש לציין, כי העדר שיתוף הפעולה של ישראל, לכאורה, עם ארגון נאט"ו הינו פער שלדעתנו יש לצמצמו ולהגביר את המאמצים להשתתף בפעילות המו"פ של נאט"ו בתחום הקיברנטי בהקדם.

6. הסדרה, חקיקה ותקינה בישראל

6.1 חקיקה ישראלית רלוונטית למו"פ בתחום הקיברנטי

6.1.1 מבוא
השימוש המוגבר ברשת האינטרנט בעשור האחרון, והצורך הנגזר מכך בביטחון הקיברנטי, מציב אתגרים חדשים למערכות משפטיות במישור המדינתי והבינלאומי. האופי הגלובאלי של האתגרים מחייב חשיבה אסטרטגית בשני המישורים, ולא רק בהקשר של הוראות דין מהותיות: ללא חשיבה רב צדדית על אכיפה משותפת של הוראות הנוגעות לביטחון קיברנטי מעבר לגבולות המדינה, קשה יהיה להגיע בטווח הארוך לרמת אכיפה אפקטיבית גם בתוך הגבולות[114]. מספר ארגונים בינלאומיים, שחלקם נסקרו לעיל, עוסקים כעת בהתאמת נורמות והליכים. אחד מהם, ה-OECD, מצביע על תהליכי התיאום הבינלאומיים שהחלו:

Given the rapid diffusion of the Internet since the late 1990s, states have taken a more coordinated approach to developing national and international legal responses to these problems. The Council of Europe, in cooperation with a number of non-European countries, developed an influential convention on cybercrime that came into force in 2004   the Budapest Convention, The United Nations has developed model laws and provided other technical assistance to its members on reducing cybercrime and attacks on information systems. Regional organisations such as the Organisation of American States and APEC have coordinated their members legal and regulatory responses. The European Union has gone furthest in developing binding laws on network and information security.[115]

יודגש כי ישראל אינה משתתפת כעת בתהליכים הגלובאליים האמורים בצורה מתוכננת ושיטתית[116].

היקף הניתוח הנוכחי אינו מאפשר בחינה מעמיקה של מערכת המשפט הישראלית בנוגע לאתגרי הביטחון הקיברנטי, אך יש לשקול בחיוב בחינה כזאת בשלב הבא של המיזם[117]. כעת נסקור בקצרה את התהליך הרצוי בכל הנוגע לבחינה העתידית, ונתמקד בשינויים הרגולטוריים אשר יש לשקול בטווח הקרוב בתחום המו"פ הקיברנטי בישראל בלבד.

113 ר' /http://www.tswg.gov
114 גבולות פיזיים של שטח המדינה מקבלים משמעות חדשה, ועדיין לא ברורה, בנוגע לפעילות במתחם הקיברנטי.
115 הערה 5 לעיל, עמ' 71.
116 למיטב הבנת המחברים, יוזמה ישראל השתתפות רק בתהליך אחד עד כה, במסגרת ה- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary General, A/65/201, 30 July 2010.
117 במספר יוזמות ברמה הרב צדדית ניתן ללמוד על כיווני פעולה אפשריים. ר' שם, עמ' 71-76; ו- ITU Toolkit for Cybercrime Legislation, February 2010, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

6.1.2 סקירה עתידית של מערכת הדין הישראלית שעוסקת בפעילות במתחם הקיברנטי

שתי גישות רווחות לגבי החקיקה שעוסקת בתחום הקיברנטי[118]. הראשונה דוגלת בריכוז כל הוראות החקיקה הרלוונטיות בדבר חקיקה אחד. הגישה השנייה קוראת להשאיר את החקיקה הרלוונטית שכבר קיימת בצורה מבוזרת במקומה "ההיסטורי", המשקף את תהליכי ההתפתחות של הדין. לפי גישה זאת, שינויים ועדכונים נחוצים ישולבו במידת האפשר בחקיקה הנוכחית הנוגעת לפעילות קיברנטית[119].

יתכן שבמבט ראשון, נראה קל יותר ליצור "חוק סייבר" אשר ירכז את כל ההיבטים של פעילות אזרחי המדינה במתחם ויסדיר אותם באופן מרוכז[120]. אך למעשה, המלאכה אינה דבר של מה בכך[121]: היא מורכבת מאוד, וספק אם היא רצויה בשלב הראשון. זאת כיוון שהוראות הדין שמטפלות בתחום הקיברנטי, לרבות תחום המו"פ, מגוונים בטיבם - כפי שפעילות אנושית במתחם הקיברנטי מגוונת - ועשויים להימצא בדיני העונשין, דיני הצפנה, דיני שמירת זכויות יוצרים, דיני הייצוא והייבוא, דיני שעת חירום, הדין החל על תשתיות קריטיות, דיני הגבלים עסקיים, דיני הגנת הפרטיות, הדינים שחלים על חופש הביטוי ועוד.

בעצם, לפי גישה זו, השימוש במתחם הקיברנטי עשוי להיות אמצעי של הפעולה או המעשה, ולא תכונה מהותית, שמשנה בהכרח את מהות הפעולה או המעשה רק כיוון שהתבצע ברשת. כך, למשל, פרסום ברשת של מידע כוזב שגורם לפחד ובהלה בציבור (מידע כוזב על פלישת צבא זר לשטח המדינה או על מתקפת טילים באיזור מסוים), אינו מחייב יצירת נורמה משפטית חדשה. אמצעי הפרסום ואולי קצב התפשטות המידע הם חדשים, אך מהות העבירה עצמה אינה חדשה[122].

מאידך, פריצה למאגר מידע מקוון של קופת חולים, המכיל מידע רפואי פרטני לגבי מצב בריאותם של רבבות חברי הקופה, ומחיקה או שינוי של המידע, הינה מעשה בעל מהות חדשה. פעולה זו, כאמור, מוגדרת כעבירה בסעיף 4 לאמנה נגד פשע קיברנטי של מועצת אירופה משנת 2001, כלהלן:

Section 1- Substantive Criminal Law Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems [.] Article 4 Data Interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm[123].

118 ר' הניתוח של שתי הגישות ב- K. Kaska, A-M. Taliharm, E. Tikk, Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007 in International Cyber Security Legal and Policy Proceedings, NATO CCDOE, Talinn, 2010, pp. 43-44 and 48-57.

119 ככל הנראה, הגישה השנייה היא זאת שישראל פועלת על פיה כעת. לא נודע לתת-הוועדה על יוזמה חקיקתית ברוח הגישה הראשונה.

120 ר' ITU Toolkit, טבלה השוואתית של "חקיקת הסייבר" של שמונה מדינות, מועצת אירופה (אמנת בודפשט) והקהילה האירופית: ארה"ב, בריטניה, אוסרליה, קנדה, גרמניה, יפן, מקסיקו, סינגפור, הודו וסין.

121 למשל, מדובר בתהליך מורכב של "הזזת" חקיקת משנה ומסמכים נוספים בעלי תוקף סטטוטורי.

122 ר' סעיף 159 לחוק העונשין, התשל"ז-1977: " המפרסם או משעתק אמרה, שמועה או ידיעה העלולות לעורר פחד ובהלה בציבור או להפריע את שלומו, והוא יודע, או יש לו יסוד להניח, שהן כוזבות, דינו - מאסר שלוש שנים." כשאר פרסום מוגדר בסעיף 34כד כ-"[...] כתב, דבר דפוס, חומר מחשב, או כל מוצג חזותי אחר וכן כל אמצעי שמיעתי העשויים להעלות מלים או רעיונות, בין לבדם ובין בעזרת אמצעי כלשהו."

123 Council of Europe, Convention on Cybercrime, Budapest, 2001 (http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm).
ר' גם את סעיף 2 לחוק המחשבים (שם), הקובע את האיסור בדין הישראלי על "שיבוש או הפרעה למחשב או לחומר מחשב".

חלק מהמדינות שנבחנו עורכות תהליך מקיף של עדכון חקיקה קיימת כדי לטפל כראוי בפעילות החדשה במתחם הקיברנטי. בכמה מקרים, יש התייחסות ואף אימוץ של מושגים והגדרות מן האמנה האירופית נגד פשע קיברנטי וממודל החקיקה הלאומית של ה- ITU[124]. בולטת במיוחד פעילות הקהילה האירופית בתחום, שמקדמת מסגרת רחבה ואחידה בתחום הביטחון הקיברנטי בשנים האחרונות[125].

למיטב הבנתנו, טרם נערכה סקירה מקיפה של דברי חקיקה ישראליים כדי לבחון את צרכי ההתאמה למתחם הקיברנטי. קיימות יוזמות ממוקדות לביצוע ההתאמה, כגון חקיקת חוק המחשבים, התשנ"ה-1995[126] ותיקון מס' 40 לחוק התקשורת (בזק ושידורים), התשמ"ב-1982 בעניין דואר זבל[127]. בנוסף, בנוגע להגנה על מידע אישי במתחם הקיברנטי, יש לציין את העבודה השוטפת עם ה-OECD והקהילה האירופית של הרשות למשפט, טכנולוגיה ומידע של משרד המשפטים בתחום[128]. יחד עם זאת, נחוץ מבט כללי על דברי חקיקה רלוונטיים, לרבות אלה שעודכנו בשנים האחרונות, כדי למנוע מצבים של העדר אחידות בהגדרות. לדוגמה, המושג "פרסום", במובן של הפצת מידע במתחם הקיברנטי, מופיע בלפחות שלושה דברי חקיקה: חוק העונשין[129], חוק התקשורת (לענין פרסום מסחרי)[130], וחוק איסור לשון הרע[131]. כמו כן, מספר דברי חקיקה מגדירים באופן שונה את המונח "מידע"[132]. מעבר להתאמת הגדרות, יש כמובן צורך לבחון התאמת נורמות מהותיות.

נעסוק כעת בסוגיית ההסדרים בנוגע למו"פ בישראל, ובאופן ספיציפי דברי החקיקה העיקריים שזוהו.

6.1.3 שיפורים רגולטוריים לטווח הקרוב

דברי החקיקה בטבלה שלהלן נותחו, במסגרת עבודת תת הוועדה, לפי שלושת המדדים הבאים: מהות דבר החקיקה; הרלוונטיות להסדרת המתחם הקיברנטי בישראל בכלל; והרלוונטיות והמשמעויות למו"פ. אלה האחרונים **מסומנים בכוכבית ובהדגשה**, וינותחו בהמשך מבחינת התאמתם הנוכחית למו"פ הקיברנטי.

דברי חקיקה שאינם מסומנים באדום נבחנו במסגרת המדיניות הקיברנטית הכללית של ישראל, כדי לוודא שהם עונים על הצרכים של החברה הישראלית, לאור האתגרים של הפעילות במתחם הקיברנטי ואיומיו. אין ספק, כי דברי חקיקה נוספים, כגון חוק העונשין ופקודת הנזיקין, רלבנטיים גם הם לבדיקה. מבין המדינות שערכו את התהליך האמור, נוקטה ארה"ב, למשל, בגישה של clean slate, כלומר בחינת ההוראות הקיימות מיסודן.

124 שם.

125 ר' מקורות בביבליוגרפיה וגם Council of Europe (2008), Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, Council of Europe, Strasbourg.
Council of the European Union (2005), Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69, 16.3.2005, p. 67.
Council of the European Union (2008), Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75.

126 ספר החוקים תשנ"ה, 366.

127 התקבל בכנסת ביום כ"ב באייר התשס"ח (27 במאי 2008); הצעת החוק ודברי הסבר פורסמו בהצעות חוק הממשלה - 182, מיום י"ג בסיון התשס"ה (20 ביוני 2005), עמ' 886.

128 ר' במיוחד Commission Decision of 31 January 2011 on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (2011/61/EU, Official Journal L/27/39).

129 סעיף 34כד לחוק העונשין: פרסום כולל הפצת פריט מידע "... לציבור באמצעות מחשב בדרך הזמינה לציבור, או להציעו לציבור באמצעות מחשב."

130 סעיף 30א' לחוק התקשורת (בזק ושידורים): "דבר פרסומת - מסר המופץ באופן מסחרי, שמטרתו לעודד רכישת מוצר או שירות או לעודד הוצאת כספים בדרך אחרת"

131 סעיף 2 לחוק איסור לשון הרע: "פרסום, לענין לשון הרע - בין בעל פה ובין בכתב או בדפוס, לרבות ציור, דמות, תנועה, צליל וכל אמצעי אחר".

132 ר', למשל, את ההבדל במושג בין החלטת ממשלה 84ב', אזכרת הפיקוח של צו הצופן , חוק הפיקוח על מצרכים ושירותים וחוק הגנת הפרטיות.

דבר החקיקה וסעיפים רלוונטיים	מהות	משרד מבצע	הנגיעה למו"פ קיברנטי והערות נוספות
**חוק לעידוד מחקר ופיתוח בתעשייה, התשמ"ד 1984- סעיפים: 1,2,3,4	מטרת המו"פ; הגדרות מחקר ופיתוח שבסמכות המדען הראשי	משרד התמ"ת	החוק העיקרי שנוגע להסדרת המו"פ האזרחי בישראל. לא נראה שיש צורך לשנות את החוק או להשפיע על תהליכים שנובעים ממנו.
**פקודת הייבוא והייצוא (נוסח חדש) תשל"ט-1979	הסדרי ייבוא וייצוא כלליים כללים	משרד התמ"ת	הוראות פרשנות כללית לגבי ייצוא וייבוא; הגדרת "ידע", "טובין" ו"שירותים". ר' גם בצו יבוא חופשי, התשס"ז-2006, הגדרת "טכנולוגיות ופיתוח"
**חוק הפיקוח על ייצוא ביטחוני, התשס"ז - 2007	כל החוק רלוונטי	משרד הביטחון	סוגיות הליבה של דבר החקיקה הינן הגדרת ידע ביטחוני; ייצוא ידע, שירותים וציוד; תהליך הייצור המקומי של אלה; פיקוח על ציוד דו-שימושי; ומערכת הרישוי של הייצוא הביטחוני, לרבות תפקידי הרשות המוסמכת והוועדה המייעצת. פרק ד' עוסק בתהליך הבקשה לקבלת רישיון ייצוא: לגביו נדרשת יותר שקיפות והסברה מסחרית במסגרת מיזם המו"פ.
**חוק הפיקוח על מצרכים ושירותים, תשי"ח - 1957 ; צו בדבר הסדר העיסוק באמצעי הצפנה - 1974; אכרזת הפיקוח על מצרכים ושירותים, התשנ"ח - 1998133 סעיפים: 1,2,3,4,5,6,8,9,10	הגדרות, סמכויות, שמירת סודיות אמצעי הצפנה והפיקוח על ייצואם,, הגדרת "מידע" לעומת חוק הגנת הפרטיות	שר הביטחון	אזכרת הפיקוח כוללת הגדרות של אמצעי וכלי הצפנה, "הצפנה", "מידע", "ייצוא ידע" ועוד. תהליך הרישוי מחייב רישיון עיסוק בהצפנה (כללי, מוגבל, או מיוחד), כאשר תוקף שני הראשונים הוא לשנה . יש חובת דיווח על לקוחות. ועדה מייעצת מסייעת למנכ"ל משרד הביטחון בהליך קביעת מדיניות הרישוי.
**אכרזת הפיקוח על מצרכים ושירותים (ציוד לחימה וידע ביטחוני) התשמ"ז - 1987	כל האכרזה רלוונטית	שר הביטחון	--

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

**חוק הסדרת הביטחון בגופים ציבוריים, התשנ"ח - 1998 סעיפים: 1,2,10,12, 15, 20 והתוספות	כל החוק רלוונטי לעניין ההגדרות של "מערכות ממוחשבות חיוניות", "פעולות אבטחה פיזית", "פעולות לאבטחת מערכות ממוחשבות חיוניות" וכדומה	השר לביטחון פנים	החוק רלוונטי להבנת התחומים שבהם מו"פ קיברנטי מקדם סדרי עדיפויות הקשורים ליעדי החוק; השפעה על צרכי השוק הפנים ישראליים
**החלטת הממשלה 84 /ב (2002)	כל ההחלטה רלוונטית	משרד ראש הממשלה	קביעת האחריות להגנה על מערכות ממוחשבות בישראל; הגדרות של "מידע", "מערכת ממוחשבת חיונית" ועוד; הסדרת ההגנה של גופים מונחים, כולל ע"י ועדת ההיגוי העליונה; וקביעת גופים אלה בנספחים
חוק התקשורת (בזק ושידורים), התשמ"ב - 1982 סעיפים: 1,2,13א', 30א', 53א'	הגדרת בזק, חובת הרישוי, דואר זבל, פיקוח על ציוד קצה, משבר תקשורת ומצבי חירום נוספים	משרד התקשורת	החוק מעניק לשר התקשורת סמכויות רבות על בעלי רשיון ISP, טלפוניה פנים-ארצית ובינלאומית, לרבות בעלי רישיון להפעלת כל תשתיות התקשורת בישראל. בעלי רישיון אלה מנתבים את מרבית הפעילות הישראלית במתחם הקיברנטי. נחוצה חשיבה נוספת בנוגע למינוף הסמכויות במישור הביטחון הקיברנטי.
פק' הטלגרף האלחוטי [נ"ח], התשל"ב - 1972 סעיפים: 1,2,3,4,5	הגדרות, חובת הרישוי, סמכות החילוט של ציוד קצה, ניצול משאב הספקטרום האלקטרומגנטי	משרד התקשורת	--
חוק העונשין, התש"נ - 1977 סעיפים: 34כד	הגדרת "פרסום" ו"פרסם"; הפנייה לחוק המחשבים	שר המשפטים	--
חוק המחשבים, תשנ"ה - 1995	הגדרת "מחשב", "חומר מחשב"; כל החוק רלוונטי	שר המשפטים	החוק מאפשר אכיפה של מספר דברי חקיקה אחרים מהמתחם הקיברנטי, וקובע עבירות שספיציפיות למתחם.

חוק ההגבלים העסקיים, תשמ"ח - 1988 סעיפים: 1,2,3,7	הגדרת הגבל עסקי, הסדר כובל מהו ומה לא נמצא בגדרו, רישוש הסדר כובל ואישורו	משרד התמ"ת	יש לבחון את האפשרות לקבוע הסדר כובל בין גורמים מסחריים, ששותפים בלעדיים למערכת ניטור והתרעה קיברנטית או למידע בנוגע לאיום.
חוק הגנת הפרטיות, התשמ"א - 1981 סעיפים: 1,2,3,7,8,13,17 ב,23	איסור על הפגיעה בפרטיות, הגדרת הפגיעה; העונש על פגיעה; הגדרת "מחזיק" לעניין מאגר מידע ו-"מידע"; ניהול מאגרי מידע; זכות העיון במידע; אחריות לאבטחת מידע; איסור על מסירת מידע מטעם גוף ציבורי	שר המשפטים	--
חוק איסור לשון הרע, התשכ"א - 1965 סעיפים: 2, 3, 6, 7, 23	הגדרת "לשון הרע" ו-"פרסום"; דרכי הבעת לשון הרע; עבירה ועוולה אזרחית; הוכחת פרסום ברבים	משרד המשפטים	--
חוק האזנת סתר, תשל"ט - 1979 סעיפים: 1,2	הגדרת "האזנה", "האזנת סתר", "שיחה"; איסור האזנת סתר	משרד ראש הממשלה ומשרד המשפטים	--
חוק למניעת הטרדה מינית, התשנ"ח - 1998	טיפול בהטרדה מינית באמצעות האינטרנט	שר המשפטים	--
חקיקת חירום (פקודת המשטרה [נ"ח], התשל"א-1971, חוק ההתגוננות האזרחית, התשי"א - 1951, והצעת חוק לתקן חוק זה (תיקון מס' 15)	הגדרת מצבי חירום מסוגים שונים וסמכויות ממשל במצבים אלה	משרדים שונים, לרבות משרד הביטחון, המשטרה, משרד התקשורת	קיים מגוון מצבי חירום בישראל, ולא ברור כיצד החקיקה תחול, אם בכלל, על מצבי חירום מהסוג החדש במתחם הקיברנטי. ביניהם: אירוע אסון המוני לפי ס' 90א' של פק' המשטרה; מצב מיוחד בעורף לפי ס' 9ג' לחוק ההתגוננות האזרחית; שעת התקפה לפי חוק זה; הפעלת מערך מל"ח; ומשבר תקשורת.

להלן מספר הערות נוספות.
חוק המו"פ הישראלי, אחד מדברי החקיקה המרכזיים שחלים על המיזם, נראה מתאים למשימה ללא שינוי או עדכון. לעומת זאת, זוהו שני אשכולות של דינים שטעונים בחינה לעומק ושיפור בתהליכי היישום והאכיפה.

6.1.4 ייצוא וייבוא תוצרים ושירותים שהם תוצר תהליך של מחקר ופיתוח

ראשית, מדובר בחקיקה שנוגעת לאישורי ייבוא וייצוא של מוצרים ושירותים (חוק הפיקוח על ייצוא ביטחוני, התשס"ז - 2007; פקודת הייבוא והייצוא (נ"ח), תשל"ט- 1979; והחקיקה שנוגעת לצופן (ר' לעיל). הסוגיות העיקריות באשכול כוללות אכיפה יעילה יותר של ייבוא וייצוא מוצרי מו"פ בעולם מקוון, שבו "ייצוא" של מוצר מתרחש בלחיצת כפתור; הצורך בריענון הגדרות בצו הצופן, ובבחינת היקף התחולה על השלבים המוקדמים של מו"פ, לרבות שלבי מו"מ מוקדמים כהגדרתם בחקיקת הצופן; ובהקשר של ייבוא מוצרים ושירותים - הבטחת קווי ייצור של מוצרי מו"פ המיובאים מחו"ל (provenance).

בעניין תהליכי הייצוא הביטחוני הקיימים על פי החקיקה הנ"ל, יש לערוך מראש מנגנון של pre-ruling או חוות דעת מקדמית עבור יוזמי פרוייקטי מו"פ. כך ניתן יהיה להגביר את רמת השקיפות לגבי תהליכי האישור לייצוא מו"פ, ולהביא לידיעת הציבור את האפשרות של pre-ruling כמרכיב של ה"הסברה העסקית" בתחום המו"פ הקיברנטי. כך, למשל, יהיו הקריטריונים שמיישם משרד הביטחון בהתאם לחוק הפיקוח על ייצוא ביטחוני, התשס"ז - 2007, לייצוא מוצרים ושירותים בתחום המו"פ הקיברנטי הביטחוני, נגישים לציבור רחב יותר.

בהקשר הזה, אין בינתיים פתרון משביע רצון לסוגיה של ייצוא שאינו מפוקח על ידי המשרד (למשל, ייצוא תוכנות על ידי אנשים פרטיים שעובדים באופן עצמאי), ויש להתמקד בחשיבה נוספת על אכיפת הכללים הקיימים.

6.1.5 שמירת זכויות יוצרים

שנית, יש לבחון את הדין החל על שמירה על זכויות קניין במוצרי מו"פ (חוק זכות יוצרים, התשס"ח - 2007; וחוק הפטנטים, תשכ"ז-1967). במיוחד חשוב לבחון את המדיניות הנוכחית בצה"ל, לפיה אין להסדיר את נושא זכויות היוצרים של מוצרים ושירותים המפותחים בחסותו, עד לשלב ההשקה של תהליך המו"פ[134].

בשלב הבא של המיזם, חשוב לבחון את המדיניות הרצויה מבחינת האסטרטגיה של תחולת הוראות הדין הרלוונטיות על פעילות במתחם הקיברנטי: בין אם לאחד הוראות חקיקה רלוונטיות בדבר חקיקה אחת, או לחילופין להשאיר הוראות רלוונטיות במיקומן "ההיסטורי", או לשלב בין שתי הגישות.

6.2 תקינה ישראלית ומו"פ קיברנטי

6.2.1 תהליך התקינה הישראלית

התקינה הישראלית הופקדה במלואה בידי שר התמ"ת, פעילותו עוגנה בחוק התקנים, התשי"ג - 1953[135] על תיקוניו (תיקונים: תשי"ח, תשל"א, תשנ"ח). בחקיקת המשנה כללי התקנים (עיבוד תקנים ישראליים), התשנ"א - 1991[136], סעיף 21 תת- סעיף א' קובע כי יוזמת התקינה היא בידי הציבור, כלומר: "(א) כל אדם רשאי להציע למכון נושא לעיבוד תקן". יחד עם זאת, הסמכות הבלעדית לקביעת תקן במדינת ישראל שייכת למכון התקנים, כאמור בסעיף 6 לחוק האמור:

המכון, והוא בלבד, רשאי לקבוע מיפרט, או כללים טכניים של תהליך עבודה, לרבות הגדרות טכניות, כתקן ישראלי (להלן -תקן); המכון יפרסם כל תקן בדרך הנראית לו.

134 עפ"י דיווחים של נציגי צה"ל במסגרת המיזם.
135 http://www.israel-industry-trade.gov.il/NR/exeres/D603917E-B905-4854-BE5F-8BA2A02A4F77.htm
136 http://www.israel-industry-trade.gov.il/NR/exeres/7B386A4C-6ECB-4328-A086-D5A959794EB8.htm

הכללים לעיבוד תקנים בישראל מפורטים בסעיף 7 לחוק.

התקינה הישראלית מורכבת מתקן ישראלי (ת"י) ותקן רשמי (ת"ר). תקן ישראלי על עדכוניו נכנס לתוקף החל ממועד פרסומו ברשומות[137]. "תקן רשמי" הינו תקן שנקבע ככזה ע"י משרד התמ"ת עקב היותו חיוני לבטיחות, בריאות הציבור, הגנה על איכות הסביבה או מניעת נזק למשתמש. כאשר מדובר ב"תקן רשמי", אסור להשתמש במוצר שאינו עונה לדרישות התקן. נוסף על הכרזת "תקן רשמי", יכול השר לפרסם צו לייצור מוצרים שחל עליהם "תו תקן חובה"[138]. עיון באתר הרשמי של מכון התקנים הישראלי[139] מעלה כי הסיבות להפיכת תקן לתקן רשמי הינן:

- שמירה על בריאות הציבור
- שמירה על בטיחות הציבור
- הגנה על איכות הסביבה
- אספקת מידע, כאשר לא קיים מידע או מנגנון חילופי העשוי להקנות הגנה לצרכן
- הבטחת תאימות או חליפיות של מוצרים
- מניעת נזק כלכלי משמעותי העלול להיגרם לצרכן כתוצאה משימוש במערכות, בחומרים או במוצרים המשמשים לבנייה, הגלויים לעין.

6.1.3 אימוץ תקינה בינלאומית בישראל

תיקון בחוק התקנים שאושר בכנסת בסוף שנת 1999 לפיו, בקביעת התקן, יאמץ מכון התקנים, ככלל, תקינה בינלאומית אשר נהוגה בקרב המדינות המפותחות[140]. בקביעת תקן כאמור, יובא בחשבון אופי הסחר בין ישראל למדינות העולם. כאשר קיימים תקנים שונים במדינות המפותחות, רשאי המכון לקבוע תקנים חילופיים, ובלבד שכל תקן שייקבע יתבסס במלואו על תקן קיים.

בנסיבות מיוחדות, כאשר יש הכרח לעשות כן, בשל קיומם של תנאים ייחודיים למדינת ישראל, רשאי המכון לשנות תנאים מסוימים הקבועים בתקינה הבינלאומית, תוך פירוט הנימוקים לכך בדברי הסבר אשר יצורפו לתקן.

137 יש לבדוק אם התקן רשמי, או אם חלקים ממנו רשמיים. תקן רשמי או גיליון תיקון רשמי (במלואם או בחלקם) נכנסים לתוקף 60 יום מפרסום ההודעה ברשומות, אלא אם בהודעה נקבע מועד מאוחר יותר לכניסה לתוקף."תקן" הוא מסמך חשוב, אך נחשב בגדר המלצה כל עוד לא הפך ל"תקן מחייב". אפשר להפוך תקן למחייב ע"י אזכור שלו בתקנה, או ע"י הגדרתו כ"תקן רשמי".
138 http://www.cleo.co.il
139 http://www.sii.org.il/71-he/SII.aspx
140 http://www.tamas.gov.il/NR/exeres/C8F4E2AD-0ABE-4BD3-9660-ECFF9E012D09.htm

7. סיכום

תת ועדת מדיניות וחקיקה סקרה התפתחויות בעולם בנוגע למדיניות המו"פ הקיברנטי; וערכה השוואה בין המצב הנוכחי בישראל לבין המצב הגלובאלי. ההתמקדות בארבעה תחומים - מדיניות מו"פ, שיתופי פעולה בפועל, תקינה וחקיקה - איפשרה התמקדות במספר כיוונים ומגמות בתחום, שלדעתנו חשוב לקדמם בקצב מואץ בהמשך המיזם.

8. ביבליוגרפיה נבחרת

Council of Europe, Convention on Cybercrime, Budapest, 2001.
Department of Homeland Security, A Roadmap for Cybersecurity Research, 2010.

Department of Homeland Security, Enabling Distributed Security in Cyberspace, March 23, 2011.
ENISA, Quarterly Review, December 2010.

EU Council, Proposal for a Directive on Attacks against Information Systems, European Council, Brussels, 4 October 2010 (EC/14436/10).

EU Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 8 December 2008, Official Journal L345/75, 23.12.2008.

EU Commission Decision of 31 January 2011 on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, (2011/61/EU, Official Journal L/27/39).

European Council, Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69, 16.3.2005, p. 67. M. Hathaway, "Cyber Policy: A National Imperative", Belfer Center of the Harvard Kennedy School, March 1, 2011. ITU, Part 1: ICT Standards Development Organizations and Their Work, 2008. Retrieved January 8, 2011, from International Telecommunication Union: http://www.itu.int/ITU-T/studygroups/com17/ict/part01.html

NATO, NATO 2020: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17 May 2010.

NATO, Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008 (Cyber Defence Management Authority established as outcome of #47)

National Academy of Sciences, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy, 2010.

OECD, Reducing Systemic Cybersecurity Risk, January 14, 2011.

UN Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July 2010, A/65/201.

The White House, Cyberspace Policy Review, 2009.
*****

9. נספחים

נספח א – הגדרות ומושגים במיזם הקיברנטי

להלן הצעות להגדרות לשימוש בעבודת תת-הוועדות. המסמך מיועד להביא בפני הצוותים את ההגדרות המובילות בתחום במישור הבינלאומי והישראלי, ולאפשר את התאמתם לעבודת הצוותים. יודגש כי רק במספר מצומצם של מקרים קיימות הגדרות מוסכמות, וחלק מעבודת המיזם כרוכה בגיבוש שפה משותפת בעברית למושגי הליבה שלו.

מחקר ופיתוח קיברנטי CYBER R&D מקורות: 1.חוק לעידוד מחקר ופיתוח בתעשייה, התשמ"ד -1984 ס"ח תשמ"ד, 100. 2. הגדרת המתחם הקיברנטי - להלן.	חוק המו"פ מגדיר מחקר ופיתוח כ- "חקירה מתוכננת במטרה לגלות ידע חדש מתוך ציפיה שידע זה יהא מועיל בפיתוח מוצר חדש או תהליך חדש או לשיפור מהותי במוצר או בתהליך קיימים"; יישום הממצאים של המחקר והידע.עשוי לכלול גיבוש של קווי תוכנית או בדיקתם, הכנת תוכנית ומדגמים, בניית אב-טיפוס, הפעלת דגם ניסוי או מתקן חצי-חרושתי.המתחם הקיברנטי הינו המתחם הפיזי והמקוון ("המתחם החמישי") שמורכב מהגורמים הבאים וכל מצבור שלהם: מחשבים, מערכות ממוכנות ורשתות; תוכנות, מידע ממוחשב; התוכן של אלה האחרונים; נתוני תעבורה ובקרה שלהם; ומשתמשי כל אלה.
המתחם הקיברנטי, CYBERSPACE. מקורות: 1. ITU Toolkit on Cybercrime Legislation 2. White House Cyber Policy Review, 2009 + National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) 3. 1. R. Clarke, Cyber War (2010) 4. The Economist, 2010 5. US Deputy Sec y of Defense W. Lynn, Foreign Affairs, 2010	המתחם הקיברנטי הינו המתחם הפיזי והמקוון ("המתחם החמישי") שמורכב מהגורמים הבאים וכל מצבור שלהם: מחשבים, מערכות ממוכנות ורשתות; תוכנות, מידע ממוחשב; התוכן של אלה האחרונים; נתוני תעבורה ובקרה שלהם; ומשתמשי כל אלה.

הסדרת המו"פ הקיברנטי REGULATION OF CYBER R&D מקור: לוי וכו', המיזם הקיברנטי הלאומי, 2009.	המושג "הסדרה" של תחום פעילות כלשהו מתייחס למכלול התפיסות, החוקים, המדיניות (לטווח קצר, בינוני וארוך), ניירות העמדה והגישות הלא רשמיות של הטיפול הממלכתי בתחום הפעילות המדובר (במקרה זה, "מו"פ קיברנטי"). כמו כן, הסדרה כוללת את היישום בפועל של המכלול, לרבות באמצעות חקיקת משנה, תכניות יישום, פסיקה והנחיות ממלכתיות. היא כוללת, בנוסף, שיתופי פעולה של המדינה במישור הבינלאומי לקדם את הטיפול בתחום, לרבות אמנות ויוזמות משותפות. בתחום המו"פ הקיברנטי מדובר בהסדרה שנוגעת לייצור מוצרים ותהליכים שמקדמים את הביטחון הקיברנטי בישראל, באופן ש: משמר את מעמדה של ישראל בעולם כמרכז לפיתוח טכנולוגיות מידע מקנה לה יכולות מעצמתיות במתחם הקיברנטי בכדי להבטיח את חוסנה הכלכלי והלאומי של ישראל כחברה פתוחה, דמוקרטית ומבוססת ידע המטרה של הסדרת המו"פ הקיברנטי הישראלי הינה להציב את ישראל בחמישייה המובילה של מדינות העולם במתחם הקיברנטי עד 2015.
ביטחון קיברנטי CYBERSECURITY מקור: ITU-T Resolution X.1205, 2008	ביטחון קיברנטי מוגדר כמכלול של כלים, מדיניות, תפיסות ביטחון, מגנוני אבטחה, הנחיות, דרכי פעולה מומלצות (best practices), פעולות, ניהול סיכונים, וכלים טכנולוגיים שנועדו להגן על הסביבה הקיברנטית וארגונה, ועל נכסי המשתמשים. מטרות הביטחון הקיברנטי הינן זמינות המערכות הקיברנטיות (availability), שלמותן (integrity) , ושמירה על נתונים חסויים (confidentiality) . בהקשר הישראלי, מוצע להוסיף להגדרת ה- ITU: החיוניות של הסדרה מתואמת של ניצול המתחם הקיברנטי במישור הלאומי מרכזיות המו"פ המתמשך כחלק אינטגרלי של ביטחון קיברנטי החשיבות בפיתוח מתמיד של אמצעי הגנה פעילים (active defense) במתחם, מפני ניצולו לרעה במתכוון או שלא במתכוון.

תשתית קריטית CRITICAL INFRASTRUCTURES מקורות: 1.סעיף 2(a) ל-דירקטיבה של הקהילה האירופית 114 משנת 2008 2.החלטת נשיא ארה"ב בענין Homeland Security No. 7, 2009 + Critical Infrastructures Protection Act of 2001(section 1016(e) of the USA PATRIOT Act of 2001) 3. ITU Toolkit on Cybercrime Legislation	תשתית קריטית הינה נכס או מערכת, פיזית או מקוונת, מלאה או חלקית, ההכרחית לשמירה על פעולות חברתיות חיוניות, בריאות, בטיחות, ביטחון, ושלומם הכלכלי או החברתי של אנשים; כאשר כל פגיעה או ביטול של אלה תפגע באופן משמעותי במדינה.
מערכות ממוחשבות חיוניות CRITICAL COMPUTERIZED SYSTEMS מקור: חוק הסדרת הביטחון בגופים ציבוריים, תשנ"ח- 1998	"מערכות ממוחשבות שנקבעו כחיוניות על ידי הגוף שהסמיכה לכך הממשלה" והנספח לחוק שממנה את רשימת התשתיות שמתעדכנת מפעם לפעם."
בזק ורשת בזק ציבורית TELECOMMUNICATIONS AND PUBLIC ICT NETWORK / ELECTRONIC COMMUNICATIONS NETWORK מקורות: 1. סעיף 1 לחוק התקשורת (בזק ושידורים), התשמ"ב - 1982 2. חוקת ה- ITU, נספח ההגדרות דירקטיבה של הקהילה האירופית 21 משנת 2002	בזק הינו המונח העברי ל"telecommunications", ומוגדר (בהעתקה של ההגדרה ב-ITU) כ- "שידור, העברה או קליטה של סימנים, אותות, כתב, צורות חזותיות, קולות או מידע, באמצעות תיל, אלחוט, מערכת אופטית או מערכות אלקטרומגנטיות אחרות רשת בזק ציבורית הינה מערכת של מתקני בזק, המשמשת או המיועדת לשמש לאספקת שירותי בזק לכלל הציבור בכל הארץ או לפחות באזור שירות, הכוללת ציוד מיתוג וניתוב, ציוד תמסורת ורשת גישה, לרבות מערכת רדיו, טלפון נייד ומערכת בזק בינלאומית, ולמעט ציוד קצה"
משבר תקשורת מקור: סעיף 13א' לחוק התקשורת (בזק ושידורים), התשמ"ב- 1982	לפי חוק התקשורת, משבר תקשורת הינו "העדר יכולת להפעיל באופן תקין מערכת בזק או חשש ממשי להעדר יכולת כאמור, בנסיבות של אסון טבע, פעולת איבה או בשל פגיעה משמעותית בשלום הציבור או חלק מסוים ממנו, והכל למעט בנסיבות שבהן ניתנו הכרזה, אישור או החלטה כאמור בפסקאות (1) עד (3) להגדרה החלטה על שעת חירום"
פשע קיברנטי CYBERCRIME מקור: 1. סעיפים 2,3,4,5,6 ל- Council of Europe Convention on Cybercrime, 2001	פשע קיברנטי מוגדר באמנה האירופית משנת 2001 כאחת משש פעולות במתחם הקיברנטי שאינן מוגדרות בחקיקת המדינה כמותרות: (1) גישה למערכות ממוחשבות; (2) יירוט (interception) של מידע פרטי; (3) שינוי או מחיקה של נתונים במערכות ממוחשבות; (4) שינוי או הפרעה למערכת ממוחשבת באמצעות נתונים (data) ; ניצול לרעה של ציוד קצה, סיסמאות ואמצעי גישה אחרים.

ציוד קצה ואישור סוג
TERMINAL EQUIPMENT AND TYPE APPROVAL
מקור:
סעיף 1 לחוק התקשורת (בזק ושידורים), התשמ"ב - 1982

ציוד קצה הינו כל ציוד תקשורת שמופעל על ידי משתמש הקצה: טלפון נייד או נייח, טלוויזיה, פקס, מסוף מחשב וכו'.
לפי חוק התקשורת (בזק ושידורים), ציוד זה מוגדר כך:

"ציוד בזק, לשימושו של מנוי, המתחבר או המיועד להתחבר מחצריו של המנוי או מכל מקום אחר לרשת בזק ציבורית באמצעות המישק המיועד לכך לרבות ציוד רדיו טלפון נייד, מפענח או ממיר אפיקים ולרבות כל התקן אחר המותקן בחצרי המנוי והמיועד לשמש לקליטת שידורים בחצריו וכן ציוד קצה לוויני כהגדרתו בסעיף 6מג [לחוק התקשורת (בזק ושידורים)]".

אישור סוג הינו אישור שניתן על ידי כל מדינה לסוגים של ציוד קצה שמותר להשתמש בהם באותה המדינה. קנה המידה לקבלת אישור סוג מתבסס על מידת ההתאמה של הציוד לרשת הבזק שאליה הוא אמור להתחבר.

לפי חוק התקשורת (בזק ושידורים), ציוד זה מוגדר כך:

"אישור שניתן לפי] חוק התקשורת (בזק ושידורים)] לדגם של ציוד קצה לשם חיבורו לרשת הבזק של בעל רישיון כללי, לרבות אישור כאמור המעיד על כך שציוד הקצה שלגביו ניתן האישור תואם במאפייניו העיקריים דגם של ציוד קצה שלגביו ניתן אישור סוג קודם"

נספח ב – ניתוח דברי חקיקה ישראליים רלוונטים

דבר חקיקה וסעיפים רלבנטיים	מהות
חוק לעידוד מחקר ופיתוח בתעשייה, התשמ"ד - 1984 1, 2, 3, 4	מטרת המו"פ; הגדרות מחקר ופיתוח שהם בסמכות המדען הראשי
פקודת היבוא והיצוא (נוסח חדש) תשל"ט - 1979	--
חוק הפיקוח על מצרכים שירותים, תשי"ח - 1957 וצו בדבר הסדר העיסוק באמצעי הצפנה 1,2,3,4,5,6,8,9,10(1974)	הגדרות, סמכויות, שמירת סודיות
חוק העונשין, תשל"ז-1977	
חוק הסדרת הביטחון בגופים ציבוריים, התשנ"ח - 1998 1,2,10,12, 15, 20 + תוספות	קביעת גופים מונחים ומסגרת הסמכויות עליהם
החלטת הממשלה 84 / ב (2002)	כל נוסח ההחלטה
חוק התקשורת (בזק ושידורים), התשמ"ב - 1982 1, 2, 13א'	הגדרת בזק, חובת הרישוי, משבר תקשורת ומצבי חירום נוספים
פק' הטלגרף האלחוטי [נ"ח], התשל"ב - 1972 1,2,3,4,5	הסדרת השימוש בספקטרום האלקטרומגנטי; חובת הרישוי
חוק ההגבלים העסקיים, תשמ"ח 1988- 1,2,3,7	הגדרת הגבל עסקי, הסדר כובל מהו ומה לא נמצא בגדרו, רישום הסדר כובל ואישורו
חוק הגנת הפרטיות, התשמ"א, 1981 ב', 2,3,7,8,13,17,23	איסור הפגיעה בפרטיות, הגדרת הפגיעה; העונש על פגיעה; הגדרת "מידע"; ניהול מאגרי מידע; זכות העיון במידע; אחריות לאבטחת מידע; איסור על מסירת מידע מאת גוף ציבורי
חוק איסור לשון הרע, התשכ"א - 1965 2	הגדרת "פרסום"
חוק האזנת סתר, תשל"ט - 1979 1,2	הגדרת "האזנה", "האזנת סתר", "שיחה"; איסור האזנת סתר
הצעת חוק פיקוד העורף	תחולה על מצבי חירום קיברנטי

נספח ג – מאגד סייבר של המדען הראשי

משרד התעשייה המסחר והתעסוקה
לשכת המדען הראשי
מנהלת תכנית מגנ"ט

מאגד CYBER

הגנת מערכות מחשב בפני תקיפה דרך הרשת

1. הקמת המאגד - רקע

בעידן הנוכחי, התקפות מערכי מחשב דרך רשתות התקשורת מהוות איום הולך וגובר העלול לפגוע במערכות הכלכלה ומרקם החיים התקינים. תקיפות שכאלו מאיימות לפגוע בפרטיות (חיסיון) המידע, זמינותו ושלמותו. השימוש הנרחב באינטרנט, חוסר המגע עם הנתקף, חוסר הצורך בלקיחת האחריות על ההתקפה לצד הסוואת התקיפה ויכולת שמירה על אנונימיות התוקף, חוברים ליצירת אתגר קשה מאד להגנה על תשתיות חיוניות ברמת הארגון ו/או ברמת המדינה.

2. חזון המאגד

חזון המאגד הינו פיתוח טכנולוגיות בגישה Multi Tiered לשיערוך, איתור, ניתוח והבנה של התקפות על מערכי מחשב המבוצעות דרך רשת התקשורת בסביבות מחשוב דינמיות (בפרט: ענן המחשוב וטלפונים חכמים) בזמן רלוונטי ולחיזוי ארוך טווח, על מנת לאפשר פיתוח מנגנוני הגנה, מעבר להגנה על מחשב בודד.

3. מסגרת הפעילות

המאגד יתמקד בפיתוח אבני הבניין הבאות על בסיס ניתוח מידע תקשורתי ממקורות רבים ושונים ברשתות מחשוב מבוזרות:

- אלגוריתמים לניתוח דפוסי התקפה ואנומליות בזרימת המידע;
- אלגוריתמים לזיהוי התקפה ואנומליות בזרימת המידע החל משלב ההכנות דרך נסיונות ועד למימוש ההתקפה, כולל שיערוך מקור האיומים וכוונות התקיפה;
- אלגוריתמים חכמים לאיתור APT (Advanced Persistent Threats);
- אלגוריתמים לניתוח ההתקפות ומציאת קורלציה בין איומים;
- אלגוריתמים יעודיים לניתוח, הבנה וסיווג התקפות (פרטיות ,שלמות וזמינות המידע).

4. תוכנית מגנ"ט

תוכנית מגנ"ט, היא מסלול סיוע של המדען הראשי במשרד התעשייה המסחר והתעסוקה. מטרת התוכנית לעודד מחקר ופיתוח של טכנולוגיות חדשניות בחזית הידע הטכנולוגי על מנת להקנות יתרון יחסי לתעשייה הישראלית בשווקים הבינלאומיים. מאגד בתוכנית מגנ"ט הוא התאגדות של תאגידים תעשייתיים ומוסדות מחקר אקדמיים לביצוע מו"פ של טכנולוגיות גנריות טרום תחרותיות על בסיס שיתופי פעולה מהותיים בין חבריו, מתוך מגמה להשיג ביחד הרבה יותר מהיכולת של כל אחד בנפרד.

5. מפגש התנעה

ביום 12 לאפריל 2011 יתקיים מפגש של נציגי חברות תעשייתיות, מוסדות אקדמיים ומוסדות מחקר שיש להם עניין להצטרף למאגד. המעוניינים מתבקשים לפנות בכתב/דואר אלקטרוני למנהלת מגנ"ט, תוך ציון תחום עיסוק רלוונטי ונתונים כלליים של החברה. הזמנות למפגש ההתנעה ישלחו לגופים הרלוונטיים בלבד, סמוך למועד המפגש.

6. מידע

מידע על מאגד CYBER ניתן לקבל אצל קרן אלעזרי, Verint Systems, 09-962-4658. Keren.elazari@verint.com, או אצל זיו איכילוב מחברת "רדוור", 03-7689650, zivi@radware.com, או אצל ד"ר אלון קאופמן, 09-9728602, alon.kaufman@rsa.com.

לפמ

מנהלת מגנ"ט : טל': 03-5118110, פקס: 03-5100622
דוא"ל: info@magnet.org.il ובאתר מגנ"ט: www.magnet.org.il

דו"ח תת ועדת ההסדרה על מערכות ממוחשבות חיוניות במדינת ישראל

נספח א - רשימת חברי הוועדות

חברי הועדה העליונה למדע וטכנולוגיה (הועמ"ט)

	שם	תפקיד
יו"ר הוועדה	פרופ' אלוף (מיל.) יצחק בן ישראל	יו"ר המועצה הלאומית למחקר ופיתוח (המולמו"פ)
חברים בוועדה	פרופ' מנואל טרכטנברג	יו"ר הוועדה לתכנון ולתקצוב שליד המועצה להשכלה גבוהה (ות"ת)
	אופיר שהם	ראש המינהל למחקר, פיתוח אמצעי לחימה ותשתית טכנולוגית במשרד הביטחון (מפא"ת)
	ד"ר אבי חסון	המדען הראשי, משרד התעשייה, המסחר והתעסוקה (התמ"ת)
	ד"ר אודי ניסן	ראש אגף התקציבים, משרד האוצר
	פרופ' יעקב זיו	ראש הפורום לתשתיות לאומיות למחקר ולפיתוח (תל"ם)
	פרופ' רות ארנון	יו"ר האקדמיה הלאומית הישראלית למדעים
	פרופ' יוג'ין קנדל	ראש המועצה הלאומית לכלכלה במשרד ראש הממשלה
	פרופ' דני וייס	המדען הראשי, משרד המדע והטכנולוגיה
חברים נוספים	מנחם גרינבלום	מנכ"ל משרד המדע והטכנולוגיה
	תא"ל נדב צפריר	מפקד 8200
	תא"ל איליה חכים	מפקדת היחידה לתקשוב ולטכנולוגיות המידע, צה"ל
	ארז קריינר	ראש הרשות הממלכתית לאבטחת מידע
	פרופ' דובי שוורץ	המדען הראשי, הוועדה לאנרגיה אטומית
	ערן פולק	סגן ראש אגף התקציבים, משרד האוצר
	רם לוי	עמית מחקר, סדנת יובל נאמן למדע טכנולוגיה וביטחון אוניברסיטת תל אביב מזכיר המיזם הקיברנטי

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי תת ועדת הגנה, ניטור ובקרה

	שם	תפקיד
יו"ר הוועדה	פרופ' דני דולב	האוניברסיטה העברית
מזכיר הוועדה	אופיר חסון	הרשות הממלכתית לאבטחת מידע
חברים בוועדה	פרופ' אלי ביהם	דקאן הפקולטה למדעי המחשב, הטכניון
	ד"ר דורית דור	סמנכ"לית מחקר ופיתוח, צ'קפוינט
	יניב הראל	מפא"ת, משרד הביטחון ומטה הסייבר, צה"ל
	בוקי כרמלי	משרד הביטחון
	רם לוי	עמית מחקר, סדנת יובל נאמן למדע טכנולוגיה וביטחון אוניברסיטת תל אביב מזכיר המיזם הקיברנטי
	ד"ר עודד מרגלית	יועץ
	שירית פלמון	רמ"ח טכנולוגיות, המטה ללוחמה בטרור, המטה לביטחון לאומי
	פרופ' בני פנקס	אוניברסיטת בר אילן
	ליאור פרנקל	מנכ"ל ווטרפול
	אבי שביט	יועץ ביטחון המולדת, לשכת המדען הראשי, משרד התמ"ת
	סא"ל עדי שגיא	רע"ן אבטחת מידע, צה"ל
	סרן עומר שניידר	רמ"ד אבטחת מידע, צה"ל
	ערן גרוסברד	יועץ, הרשות הממלכתית לאבטחת מידע

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי תת ועדת חישוב-על ותשתיות תקשורת רחבות פס

	שם	תפקיד
יו"ר הוועדה	תא"ל (מיל.) יעקב נגל	סגן מדעי לראש מפא"ת
מזכיר הוועדה	סא"ל אריאל פרנס	רע"ן טכנולוגי, צה"ל
	פרופ' יהושע יורטנר	האקדמיה הלאומית הישראלית למדעים
	פרופ' דורון חבצלת	רמ"ח מיגון ומחשוב, מפא"ת
	ד"ר גיא תל-צור	יו"ר ארגון הגריד הישראלי וחוקר HPC באוניברסיטת בן גוריון
	ד"ר מארק זילברשטיין	חוקר HPC, הטכניון
	ד"ר מרים ברקת	חברת המועצה הלאומית למחקר ופיתוח
חברים בוועדה	סא"ל (ד"ר) יוסי אברבנאל	מומחה אלגוריתמיקה, צה"ל
	יוני אלבז	חוקר, וועדה לאנרגיה אטומית
	אבי שביט	יועץ ביטחון המולדת, לשכת המדען הראשי, משרד התמ"ת
	דניאלה פרתם	רפרנטית ביטחון, אגף התקציבים, משרד האוצר
	ראובן לוי	סגן ראש ההמטה לביטחון לאומי לפיתוח אסטרטגי
	סרן ערן אסף	אגף התקשוב, צה"ל

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי תת ועדת צופן וסימולציה

	שם	תפקיד
יו"ר הוועדה	פרופ' מינה טייכר	אוניברסיטת בר אילן וחברת המועצה הלאומית למחקר ופיתוח
מזכירת הוועדה	סא"ל דניאל נבנצאל	רע"ן מחקר, אגף התקשוב, צה"ל
חברים בוועדה	פרופ' עדי שמיר	מכון וייצמן למדע
	ד"ר נדב כהן	רע"ן תשתית מדעית, מפא"ת
	פרופ' אלי פורת	אוניברסיטת בר אילן
	סרן אורי סתיו	צה"ל
	ניר חנגל	חוקר אבטחת מידע, הרשות הלאומית לאבטחת מידע

חברי תת הוועדה לבחינת התועלות

	שם	תפקיד
יו״ר הוועדה	פרופ׳ אהוד גזית	סגן נשיא למו״פ, אוניברסיטת תל אביב ויו״ר הדירקטוריון, חברת ״רמות״ בע״מ
מזכירת הוועדה	ד״ר ליאת מעוז	מנהלת פרוייקטים מיוחדים ומנהלת תוכנית מרכזי המצוינות, המועצה להשכלה גבוהה / הוועדה לתכנון ולתקצוב
חברים בוועדה	פרופ׳ רון שמיר	פרופ׳ למדעי המחשב, אוניברסיטת תל אביב
	פרופ׳ נדב לירון	חבר המועצה הלאומית למחקר ופיתוח ופרופ׳ למתמטיקה בטכניון
	שירה נבון	ממונה תחום מתודולוגיה ומאקרו, אגף תקצוב, המועצה להשכלה גבוהה / הוועדה לתכנון ולתקצוב
	דני גלושנקוב	רפרנט השכלה גבוהה ומדע, אגף תקציבים, משרד האוצר
	שגיא דגן	כלכלן בכיר, המועצה הלאומית לכלכלה, משרד ראש הממשלה
	אבי שביט	יועץ ביטחון המולדת, לשכת המדען הראשי, משרד התמ״ת
	תא״ל (מיל.) עוזי עילם	חבר המועצה הלאומית למחקר ופיתוח וראש מפא״ת לשעבר
	ד״ר אביתר מתניה	אחראי תחום תלפיות, מפא״ת
	סא״ל (ד״ר) יוסי אברבנאל	מומחה אלגוריתמיקה, צה״ל
	סא״ל אריאל פרנס	רע״ן טכנולוגי, צה״ל
	ד״ר ערן טרומר	ביה״ס למדעי המחשב, אוניברסיטת תל אביב

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי תת הוועדה למדיניות וחקיקה

	שם	תפקיד
יו"ר משותף	עו"ד דבורה האוסן-כוריאל	עמיתת מחקר, סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב
	תא"ל (מיל.) ניצן נוריאל	ראש המטה ללוחמה בטרור במטה לביטחון לאומי
מזכיר הוועדה	גיל ארז	לשכת המדען הראשי, משרד התמ"ת
חברים בוועדה	שירית פלמון	רמ"ח טכנולוגיות, המטה ללוחמה בטרור, המטה לביטחון לאומי
	אל"מ (מיל) יובל שרשבסקי	יועץ, לשעבר רמ"ח איסוף, צה"ל
	דני גלושנקוב	רפרנט השכלה גבוהה, אגף התקציבים, משרד האוצר
	טל דקל	עמית מחקר, סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי תת הוועדה לבחינת התועלות הכלכליות

	שם	תפקיד
יו"ר הוועדה	פרופ' יוג'ין קנדל	ראש המועצה הלאומית לכלכלה, משרד ראש הממשלה
מזכירת הוועדה	שירה ברלינר	כלכלנית, המועצה הלאומית לכלכלה, משרד ראש הממשלה
חברים בוועדה	שגיא דגן	כלכלן בכיר, המועצה הלאומית לכלכלה, משרד ראש הממשלה
	אבי שביט	יועץ ביטחון המולדת, לשכת המדען הראשי, משרד התמ"ת
	דני גלושנקוב	רפרנט השכלה גבוהה ומדע, אגף התקציבים, משרד האוצר
	רם לוי	עמית מחקר, סדנת יובל נאמן למדע טכנולוגיה וביטחון, אוניברסיטת תל אביב מזכיר המיזם הקיברנטי
	דן מרום	בית הספר למנהל עסקים, האוניברסיטה העברית בירושלים
	צביקה בנדט	סמנכ"ל שלדור

סיוע בעבודת המטה ובבניית דו"ח הוועדה:

לאוניד בקמן, המכון הישראלי למדיניות מדע טכנולוגיה וחדשנות

ג'ון דייויס, יועץ בכיר, שלדור

נועם מני, יועץ, שלדור

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

חברי הועדה להסדרה

	שם	תפקיד
יו"ר הוועדה	תא"ל (מיל.) ניצן נוריאל	ראש המטה ללוחמה בטרור, המטה לביטחון לאומי
מזכירת הוועדה	שירית פלמון	רמ"ח טכנולוגיות, המטה ללוחמה בטרור, המטה לביטחון לאומי
חברים בוועדה	תא"ל איילה חכים	מפקדת היחידה לתקשוב ולטכנולוגיות המידע, צה"ל
	ארז ק.	ראש הרשות הממלכתית לאבטחת מידע
	רם לוי	עמית מחקר, סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב מזכיר המיזם הקיברנטי
	דני שטייר	מ"מ רח"ט טכנולוגיות, המטה ללוחמה בטרור, המטה לביטחון לאומי
	בוקי כרמלי	משרד הביטחון
	פרופ' דני דולב	האוניברסיטה העברית יו"ר הוועדה להגנה ניטור ובקרה
	אילן דוידי	רח"ט שליטה ומודיעין, רשות החירום הלאומית
	שוקי פלג	מנהל אבטחת מידע, תהיל"ה
	יניב הראל	מפא"ת, משרד הביטחון ומטה הסייבר, צה"ל
	עו"ד דבורה האוסן-כוריאל	עמיתת מחקר, סדנת יובל נאמן למדע, טכנולוגיה וביטחון, אוניברסיטת תל אביב יו"ר הוועדה למדיניות וחקיקה
	סנ"צ ג'קלין לוי	רמ"ד אבטחת מידע, משטרת ישראל
	אורן שיב	רמ"ח ביטחון ותקשורת, משרד הביטחון
	גיל ארז	לשכת המדען הראשי, משרד התמ"ת
	דניאלה פרטס	רפרנטית ביטחון, אגף התקציבים, משרד האוצר
	סא"ל עומר דגן	צה"ל

לא להפצה לשימוש רישמי בלבד - גירסה 03 להתיחסות

נציגי חברת שלדור שלקחו חלק במיזם

שם	תפקיד
סאמי פרידריך	מייסד ומנכ״ל
עומר טפר	סמנכ״ל
צביקה בנדט	סמנכ״ל
ג׳ון דיוויס	יועץ בכיר
נועם מני	יועץ בכיר
ענת אסטה	מידענית