חדשנות ישראלית בסייבר

נייר מסכם לדיון שהתקיים במסגרת כנס הרצליה ה-14

דוברים במושב:

יו"ר: אלוף (מיל.) פרופ' **יצחק בן ישראל**, יו"ר המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל; ראש סדנת יובל נאמן, אוניברסיטת תל אביב

תא"ל **איתן אשל**, ראש מו"פ, המנהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית (מפא"ת), משרד הבטחון

פרופ' **יובל אלוביץ'**, מנהל מעבדות Deutsche ekomTel, אוניברסיטת בן-גוריון בנגב

ד"ר **טל שטיינהרץ**, CTO, מטה הסייבר הלאומי, משרד ראש הממשלה

מר **רביב רז**, מנכ"ל, Security Hybrid

גב' **אסתי פשין**, ראש מינהל מערכות סייבר, תע"א-אלתא

מר **רם לוי**, יועץ לביטחון סייבר, הוועדה הלאומית לסייבר, המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל

מדי שנה מקדיש כנס הרצליה במסגרת שיתוף הפעולה עם סדנת יובל נאמן והמולמו"פ מושב או דיון "שולחן עגול" לנושא הקשור בתחום הסייבר. במסגרת זו נדונו היבטים שונים של התחום והעיסוק בו: משפט, רגולציה, מערכות תשתית לאומיות, טכנולוגיה, צבא ומודיעין. הדיון בכנס השנה הוקדש לתחום המו"פ בענף הסייבר, לאיפיון המערכת המשולבת שהתפתחה בשלוש השנים האחרונות הכוללת שילוב ומעבר של רעיונות, הון, חוקרים, מומחים ויזמים בין האקדמיה, התעשייה ופרויקטים לפיתוח יישומים ראשוניים. מדובר ב"אקו-סיסטם" ייחודי במסגרתו פועלים במשולב הממשלה, המערכת הביטחונית, האקדמיה, התעשייה הוותיקה וחברות סטרט-אפ. התפתחות זו נובעת מהנסיבות המיוחדות המאפיינות את ישראל בכל הנוגע ליזמות ופיתוח טכנולוגי אך גם כתוצאה מהכוונה ועידוד ממשלתיים שיצרו יחד הצלחה המזינה ומניעה את עצמה. ענף הסייבר הישראלי הוא כיום בעל נתח שוק המוערך כנע בין 5 ל-10 אחוזים (תלוי באופן המדידה) משוק הסייבר העולמי שהיקפו הכולל מוערך בכ-60 מיליארד דולר. חלקן של חברות ישראליות בהשקעות חדשות במו"פ עמד השנה על 11-13% מכלל ההשקעות שהתבצעו בעולם.

התפתחות ה"אקו-סיסטם" הישראלי מתרחשת על רקע השתכללות האופן בו נתפש איום הסייבר בעולם מאז אירוע ה"סטוקסנט" באיראן ב 2010 . אירוע זה המחיש את הפגיעות הרבה של כל המערכות המכניות והאלקטרוניות המקיפות את חיינו לסיכוני סייבר. הרבה מעבר לרמת הפגיעות שנתפשה עד לאירוע זה, פגיעות שיוחסה בעיקר להיבטים של בטחון מידע. מערך הצנטריפוגות במתקן האיראני להעשרת אורניום נפגע בלא שהיה קשור לאינטרנט או לכל רשת מחשב חיצונית. תולעת ה"סטוקסנט" שהושתלה בו מקורה בחלקים מבוקרי מחשב שהיו משולבים בציוד עצמו, כשהפגיעה אינה פגיעה במידע אלא פגיעה פיזית משמעותית בציוד.

ההתפתחות של תחום הסייבר בארץ ניכרת הן ברמת המשאבים ותשומת הלב הממשלתיים המוקדשים לו, והן בהיקף העיסוק האקדמי ובפעילות בסקטור העסקי. מטה הסייבר הלאומי, הפועל במסגרת משרד ראש הממשלה, הוא ייחודי מבחינת תפקידו כמקדם התפתחות הפעילות בתחום. מדובר במבנה פעילות ייחודי שבניגוד למדינות אחרות בעולם איננו אחראי על התגוננות מפני איומי סייבר אלא הוא בעל תפקיד מכוון ומתאם של הפעילות בענף, פעילות בעלת היבטים ביטחוניים מובהקים וכן היבטים מסחריים ואזרחיים. תפישה זו הותוותה במסגרת חזון ראש הממשלה משנת 2011 למיזם קיברנטי. חזון השואף לשמר את המובילות של ישראל בתחום ולהפוך אותה למעצמת סייבר באמצעות השקעות במחקר בסיסי ויישומי ופיתוח תכניות עידוד להקמת מיזמים עסקיים ולהכשרת כח אדם ייעודי.

לצד ה"חזון הקיברנטי" הלאומי פועלת במסגרת המועצה הלאומית למחקר ופיתוח וועדת סייבר המורכבת משמונה עשר חברים, נציגים של הגורמים השונים המעורבים בתחום הסייבר בהיבטיו השונים. מדובר בוועדה מייעצת שעוסקת באבחון וניטור התפתחות התחום, זיהוי בעיות והזדמנויות וכן עידוד הקשר ושיתוף הפעולה בין הגורמים השונים. הוועדה מסייעת בהכוונת המדיניות הכוללת לצורך ההתפתחות של אקו-סיסטם בר-קיימא בתחום הסייבר.

אחד המרכיבים העדינים ב"אקו סיסטם" הכלכלי-טכנולוגי הוא המקום והתפקיד של הממשלה, כשתפקיד פעיל מדי של הממשלה עשוי להפריע לתהליכים הקשורים בפיתוח חדשנות ובפיתוח עסקי. במקרה הישראלי מדובר באתגר קשה במיוחד מאחר ומדובר בתחום שהוא גם בעל ממדים ביטחוניים מובהקים. מתוך התחשבות ברגישות זו מכוון המטה הקיברנטי הלאומי מדיניות שתכליתה הוא איזון בין היבטים הגנתיים הקשורים בביטחון המדינה ובין מובילות טכנולוגית שהיא גם מנוף צמיחה כלכלי. מדובר על קשר בעל שני צירים מקבילים. הציר הראשון מתייחס לתנאים המאפשרים פיתוח חדשנות מחוץ למערכת הביטחון במטרה להגדיל את היצע הפתרונות העומדים לרשות המדינה וייתכן שלא היו יכולים להתפתח במוסדותיה, הן מסיבות הנובעות ממגבלות של אנשי מחקר ופיתוח והן מתוך הכרה ביכולת של מסגרות חוץ ממסדיות, דוגמת חברות "סטרט אפ", להניב חדשנות. ציר שני נוגע להיותה של הגנת סייבר חלק מהתנאים המאפשרים התפתחות של הכלכלה הלאומית.

בכל הנוגע למו"פ פועל המטה הקיברנטי להקצאת משאבים נדרשים לפיתוח המחקר הבסיסי והיישומי באקדמיה. במסגרת זו הוקמה בשיתוף משרד המדע והות"ת קרן מחקר לאומית וכן קרן דו לאומית ישראלית-בריטית. המטה משקיע מאמץ מיוחד בהקמתם של מרכזי מחקר ייעודיים לתחום הסייבר באוניברסיטת תל אביב ובאוניברסיטת בן גוריון, וזאת מתוך מטרה ליצור "מסה קריטית" של ידע ופעילות שתניב רעיונות והתנסות. שני מרכיבים שהם בסיס להתפתחות של כלים יישומיים ותעשייה. חלק מהפעילות במסגרת זו מוקדשת למחקר סביב בעיות או צרכים שזוהו כצרכי ביטחון לאומי כלליים, דוגמת פיתוח הקשור במאגר ביומטרי שיקנה הן מענה לצרכים ביטחוניים והן רמה גבוהה של הגנה על הפרטיות. צורך נוסף שאופיין על ידי המטה, ושסביבו מתבצעת עבודה מחקרית-אקדמית, הוא פיתוח שיאפשר למכונות עצמאיות לזהות התקפות סייבר בעת התרחשותן, וזאת בלא תלות באמצעי ניתוח חיצוניים למכונה.

בישראל פועלות כיום כ 200 חברות סטרט-אפ העוסקות בתחום הסייבר, מתוכן כ 100 הוקמו במהלך השנה החולפת. מעבר להן פועלים בארץ 20 מרכזי פיתוח של חברות רב-לאומיות זרות העוסקים בתחום הסייבר, חטיבות סייבר ייעודיות במספר חברות ותיקות (כולל בחברות ביטחוניות גדולות דוגמת התע"א, אלביט ורפאל) וחברות סייבר בינוניות וגדולות שהבולטת בהן היא צ'ק פוינט. יצוא מוצרי ושירותי סייבר מישראל עומד על היקף שנתי של 3-5 מיליארד דולר. הממשלה מקצה כספים לתמיכה והשקעה בחברות בעיקר באמצעות תכניות שונות של לשכת המדען הראשי במשרד הכלכלה, בהן קרן יעודית בשם "קרן קידמה" וקרן יעודית נוספת, משותפת למדע"ר ולמפא"ת, קרן מסד. גם פעילותן של חברות במסגרת קריית הסייבר בבאר שבע, סייברפרק, היא בגדר מסלול תמיכה אותו מעמידה המדינה לרשותם של יזמים וחברות. מפא"ת מסייעת כיום במימון פעילותן של 30 חברות סייבר

ומעבר לכך הייתה שותפה במיסוד שיתוף פעולה למחקר ופיתוח בתחום הסייבר עם ממשלת סינגפור. מדינה בה פועל גם מרכז פיתוח סייבר של התעשייה האווירית.

מהדיון בכנס עלה גם כי בראייה כוללת הבעיות שזוהו כקריטיות למימוש החזון הקיברנטי אינן דווקא בתחום המימון הראשוני אלא ביכולתן של חברות ופרויקטים מסוג "סטארט אפ" להתפתח לכיוון של חברה בוגרת. קושי המאפיין את כלל הסטארט-אפים הישראליים. בהקשר זה נאמר כי בכדי להגדיל את הזדמנויות הצמיחה עבור חברות הזנק ישראליות מתקיימים מאמצים להוריד חסמי יצוא, בעיקר בכל הנוגע למגבלות על העברת ידע.

אפיק סיוע נוסף, שגם מדגיש מאד את היווצרות ה"אקו סיסטם" המקומי, הוא שת"פ וקשר עם האוניברסיטאות ועם תעשיות וותיקות. הסוציולוגיה היחודית של החדשנות הישראלית באה לידי ביטוי, בין היתר, בהיכרות אישית ובאופי משותף של היזמים, אנשי האקדמיה, התעשייה ומערכת הביטחון. ההיכרות והאופי היזמי המשותף של הגורמים במערכות השונות באים לידי ביטוי בנכונות וביכולת לבחון רעיונות חדשים, לייעץ ולהתייעץ וכן ליטול סיכונים בכל הנוגע להתקנה וניסוי של מוצרים הנמצאים בשלבי פיתוח במערכות פעילות בחברות עסקיות, באוניברסיטאות ובמערכת הביטחון. בהקשר זה הוצג הקשר כדו-כיווני גם בכל הנוגע למעבר של רעיונות מהתעשייה הוותיקה לתחום הסייבר, למשל השאלה של אסטרטגיות מתחום העקיבה אחר עצמים והסבתן לתחום הסייבר.

האפשרות העומדת בפני יזמים ואנשי פיתוח לקבל גישה לסביבה של "תעבורת רשת" חיה היא מנוף לשכלול ולשיפור של המוצר מול תנאי אמת וכן משמשת כ"תו-איכות" עבור לקוחות פוטנציאליים שיחששו פחות מהתקנת המוצרים במערכותיהם. לצד השת"פ עם גופים ציבוריים הוצג גם אפיק השת"פ עם התעשייה הבוגרת. בהקשר זה הוצגה התעשייה כ"מבוגר אחראי", כמקור ליכולת וניסיון ארגוני וטכנולוגי העשויים להשלים ולקדם משמעותית לכיוון של מוצר או פתרון כולל שיזכה לאמון מצד הלקוח. שיתוף הפעולה ההדוק שנוצר בארץ מאפשר תגובה מהירה לבעיות קונקרטיות "בזמן אמת" ואפילו גופים ישראלים הנחשבים -מסיבות מובנות -כשמרנים, דוגמת בנקים וחברות ביטוח, מוכנים לשלב במערכותיהם מוצרי סייבר ישראליים הנמצאים בשלבי פיתוח.

הטענה העיקרית שעלתה מהדיון נגעה למגבלות בירוקרטיות המכבידות בעיקר על פעילות היצוא של חברות מתחום הסייבר. בהקשר זה נטען כי קצב השגת היתרי יצוא עומד בממוצע על שנה וחצי והוא איטי ביחס לצרכי הסקטור העסקי. טענה נוספת הועלתה ביחס לקושי של מעבר רעיונות מהאקדמיה, רעיונות הנכללים תחת נורמות של פומביות הידע, לתעשייה. בהקשר זה הוצע כי יש לפתח מנגנון שיקנה יתרון לתעשייה המקומית לשימוש בידע בטרם יהפוך לידע ציבורי פומבי. בתוך כך צוין כי הממשלה נמצאת בשלבי ארגון והקמה של קרן גדולה לתמיכה במחקר אקדמי-יישומי שבמסגרתה יוקנה לתעשייה המקומית יתרון בכל הנוגע לשימוש יישומי בארץ.

במסגרת הדיון זוהו מספר אפיקי פעולה בעלי פוטנציאל רב בתחום הסייבר ובכללן: שינוי בכללי הזיהוי והחתימה של פעילות ברשת. פעילות שבתנאים הקיימים מאפשרת שימוש קל מאד בזהויות בדויות ;שינויים במבנה המערכת כך שתשתנה ה"חתימה" הנייחת של מערכות ורכיבים ;התאמת התפתחות פתרונות הסייבר להתפתחויות צפויות בתחום המחשוב.

תמונות מהמושב חדשנות ישראלית בסייבר

מימין לשמאל: יו"ר: אלוף (מיל.) פרופ' **יצחק בן ישראל**, יו"ר המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל; ראש סדנת יובל נאמן, אוניברסיטת תל אביב

תא"ל **איתן אשל**, ראש מו"פ, המנהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית (מפא"ת), משרד הבטחון

פרופ' **יובל אלוביץ'**, מנהל מעבדות Telekom Deutsche, אוניברסיטת בן-גוריון בנגב.

ד"ר **טל שטיינהרץ**, CTO, מטה הסייבר הלאומי, משרד ראש הממשלה

מר **רביב רז**, מנכ"ל, Security Hybrid

גב' **אסתי פשין**, ראש מינהל מערכות סייבר, תע"א- אלתא

מר **רם לוי**, יועץ לביטחון סייבר, הוועדה הלאומית לסייבר, המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל.

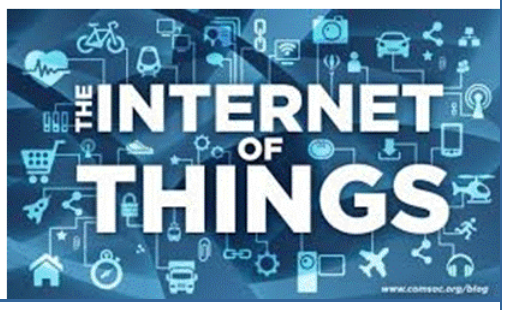
תא"ל **איתן אשל**, ראש מו"פ, המנהל למחקר, פיתוח אמל"ח ותשתית טכנולוגית (מפא"ת), משרד הבטחון

מגמות בסייבר

- אנחנו "מחברים עצמינו לדעת"

Internet of things (IOT) –

Bring your own device (BYOD) –



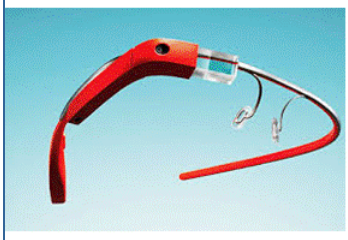
מגמות בסייבר

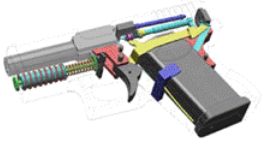
- כמויות המידע בענן רק הולכות וגדלות...

- הסייבר הופך למרחב לחימה

מגמות בסייבר

- חיבור של חדשנות טכנולוגית וסייבר מצית את הדמיון...
  - מציאות רבודה (Google glass –
  - Bitcoin –
  - הדפסת תלת מימד –





בעיות בשיטות ההגנה הקיימות

- הגנה מבוססת "מניעה" ו"הגנת גבול"
  - "גדרות" ו"חומות" מול כמות עצומה של "החורים".
  - תוקף שיחדור פנימה ישהה תקופה ממושכת.
- הגנה מבוססת "ניטור", "גילוי" ו"התמודדות"
  - קשה מאד לנטר "הכל" ולגלות את כל סוגי האיומים.
  - התוקפים מנצלים את "הרעש הטבעי" הקיים ברשת ופועלים מתחת ל"סף הרעש".

מאפייני האיום

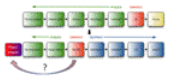
- אין משמעות למרחק הגיאוגרפי
- קלות ופשטות מימוש
- א-סיטמריה בין התוקף למגן

האיזורים בהם פועלים האיומים:

- אפליקציות
- מערכות הפעלה
- חומרות – מרכיבי הרשת, Mobile (BYOD), (IOT) מכל סוג שהוא...
- הגורם האנושי

דרכי התמודדות מתקדמות

- **שימוש בכלי מודיעין** לטובת הגנה
  - רתימת טכנולוגיות כריית מידע – מה **כוונת** התוקף?
  - unknown-unknown



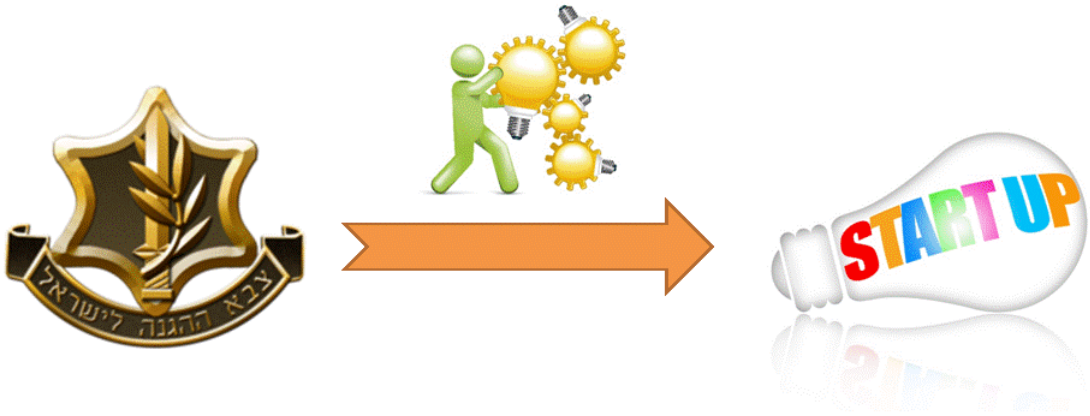
- **שימוש בכלי הונאה לטובת הגנה**
  - תמרון לא מותנה.
  - הסתגלות כתגובה להתקפה.

האתגרים

- ניהול רשת המשתנה דינאמית.

פרופ' **יובל אלוביץ'**, מנהל מעבדות Telekom Deutsche, אוניברסיטת בן-גוריון בנגב.

Source of Cyber Security Innovation



Mostly Cyber Security innovation is generated by startup-companies based on knowledge the founders acquired in the IDF

Ben-Gurion University of the Negev
המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

The Role of the Academia in Promoting Cyber Innovation

June, 2014

Yuval Elovici, Prof.
Director of Telekom Innovation Laboratories
Head of BGU Cyber Security Labs

Academic contribution to cyber innovation

The increase in cyber security attack sophistication will intensify the demand for academic support.

IDS
- Anomaly detection Algorithms
- Honeypots

Malware
- Static analysis based on ML techniques
- Dynamic analysis

Crypto
- New cryptographic algorithms
- Analysis of security protocols

Academia is Faster than industry

Research conducted by Prof. Lior Rokach and Prof Yuval Elovici

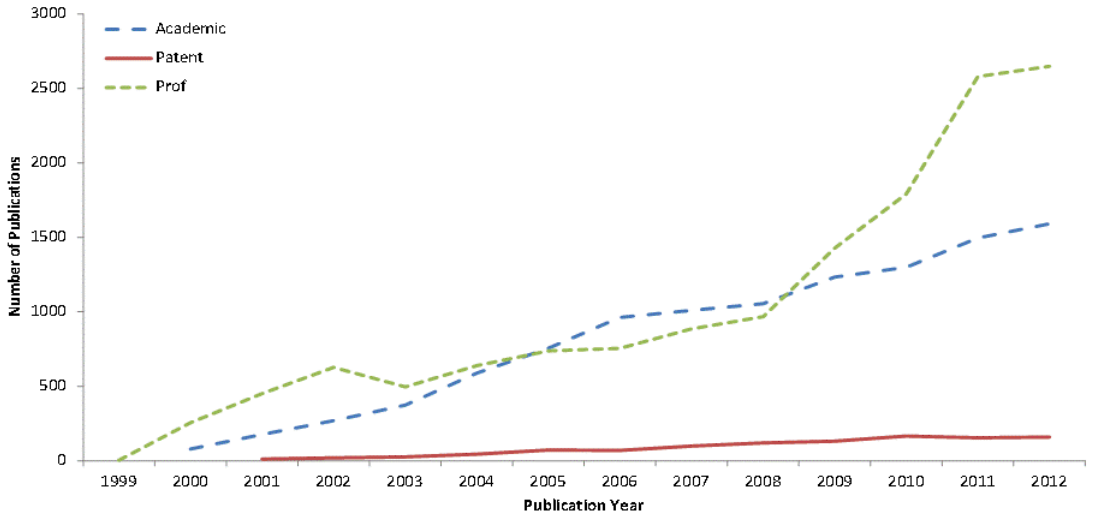
Distributed Denial of Service
- Attacks
- Mitigation technologies

Botnet
- Platform for launching cyber attacks
- Detection is based on detecting C&C

Advanced Persistent Threat
- Launched by advanced attackers
- Very hard to detect

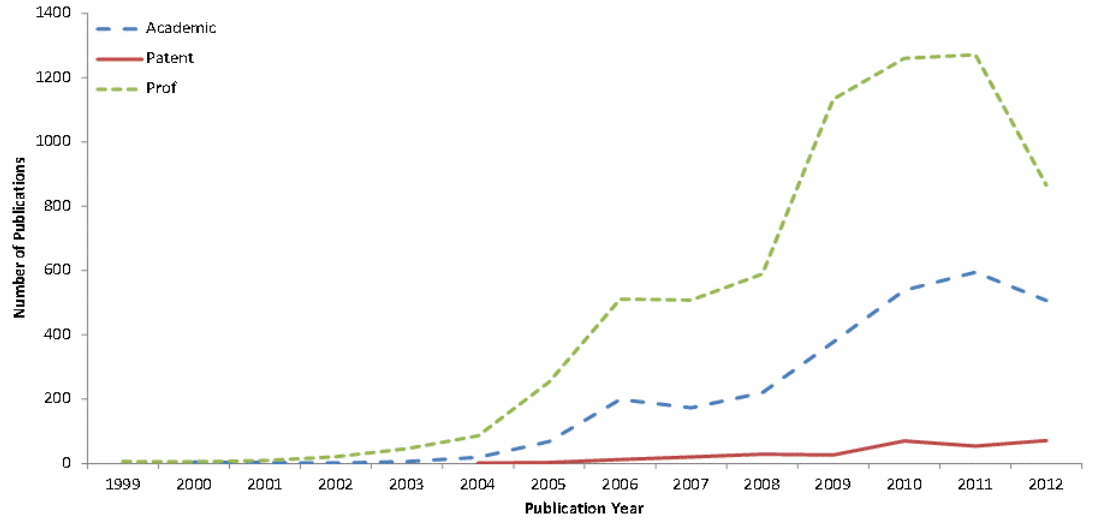
DDoS

First reported (year)	First mentioned in a professional article	First scientific publication	First patent application
1999	1999	2000	2001



BotNet

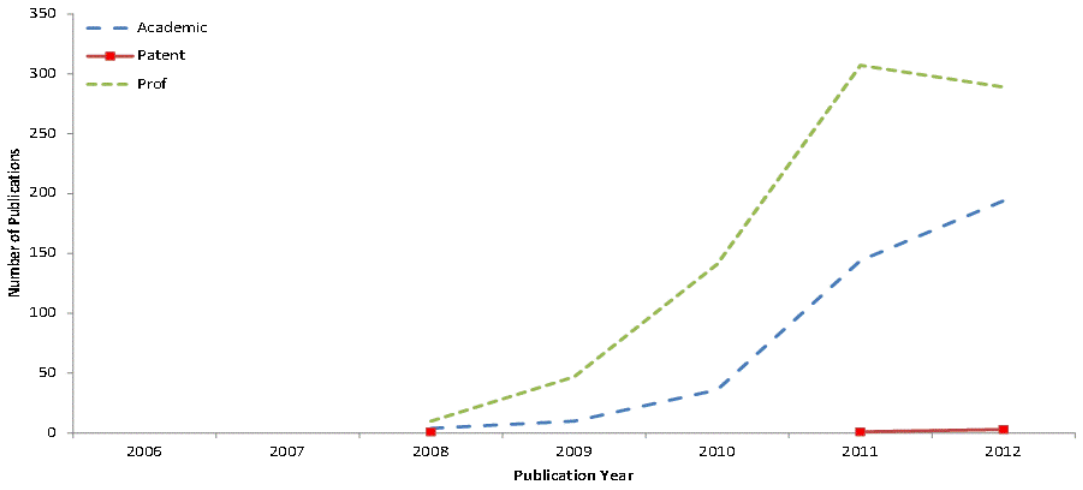
First reported (year)	First mentioned in a professional article	First scientific publication	First patent application
1999	1999	2000	2004



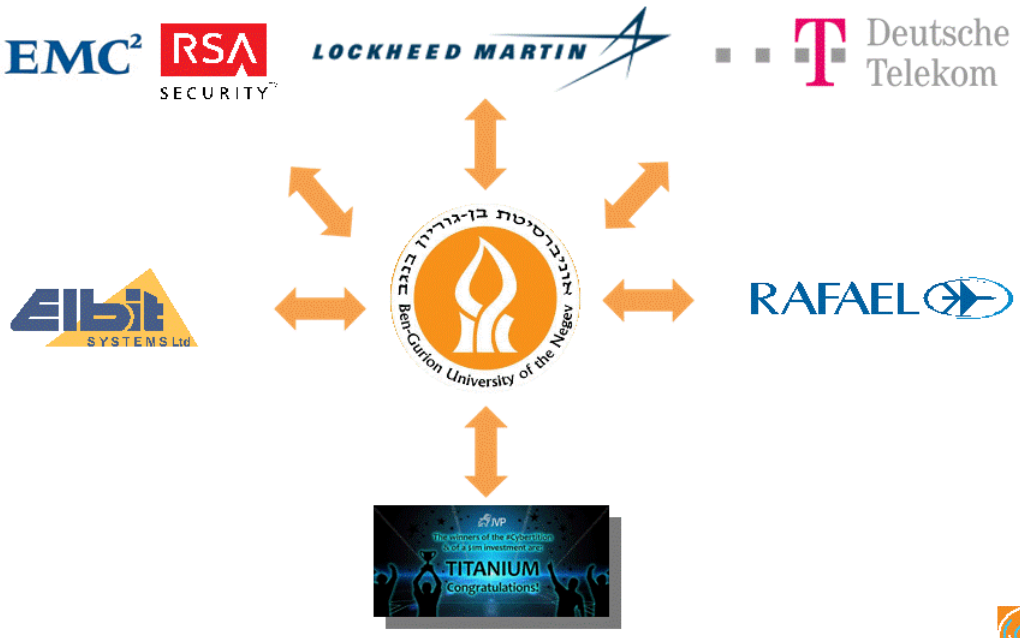
Academia's contribution to cyber innovation

APT

Threat class	First reported (year)	First mentioned in a professional article	First scientific publication	First patent application
APT	2006	2008	2008	2008



Transfer of Innovation from BGU to Industry



Ben-Gurion University of the Negev
המכון לחקר ביטחון החברה והמדינה
Homeland Security Research Institute

Thank You!

Yuval Elovici, Prof.
Director of Telekom Innovation Laboratories
Head of BGU Cyber Security Labs

ד"ר **טל שטיינהרץ**, CTO, מטה הסייבר הלאומי, משרד ראש הממשלה

משרד ראש הממשלה
המטה הקיברנטי הלאומי

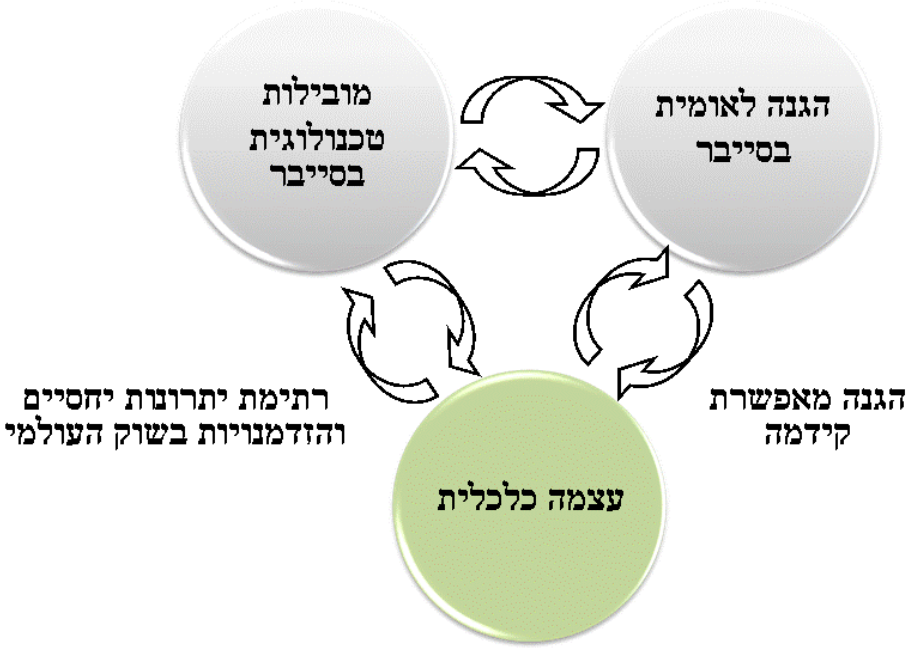
מובילות ישראלית בסייבר

תפקידה של המדינה בעידוד החדשנות

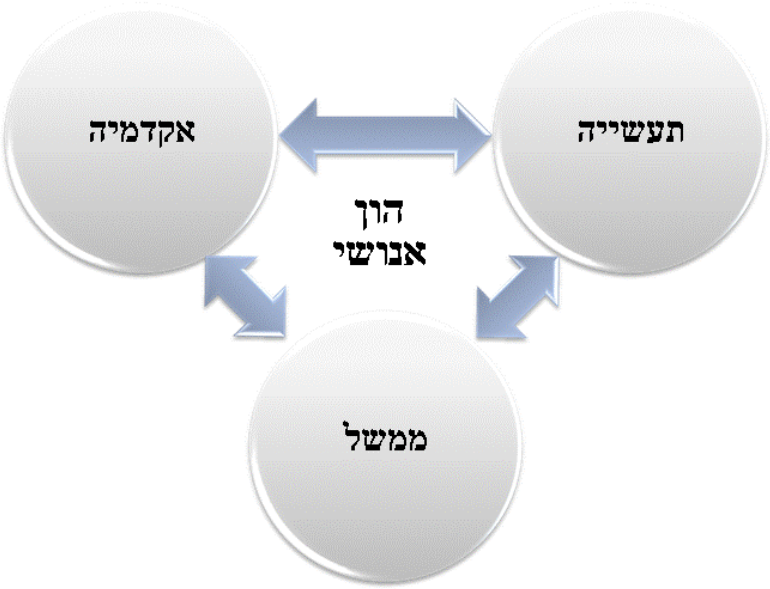
יוני 2014

סיוון התשע"ד

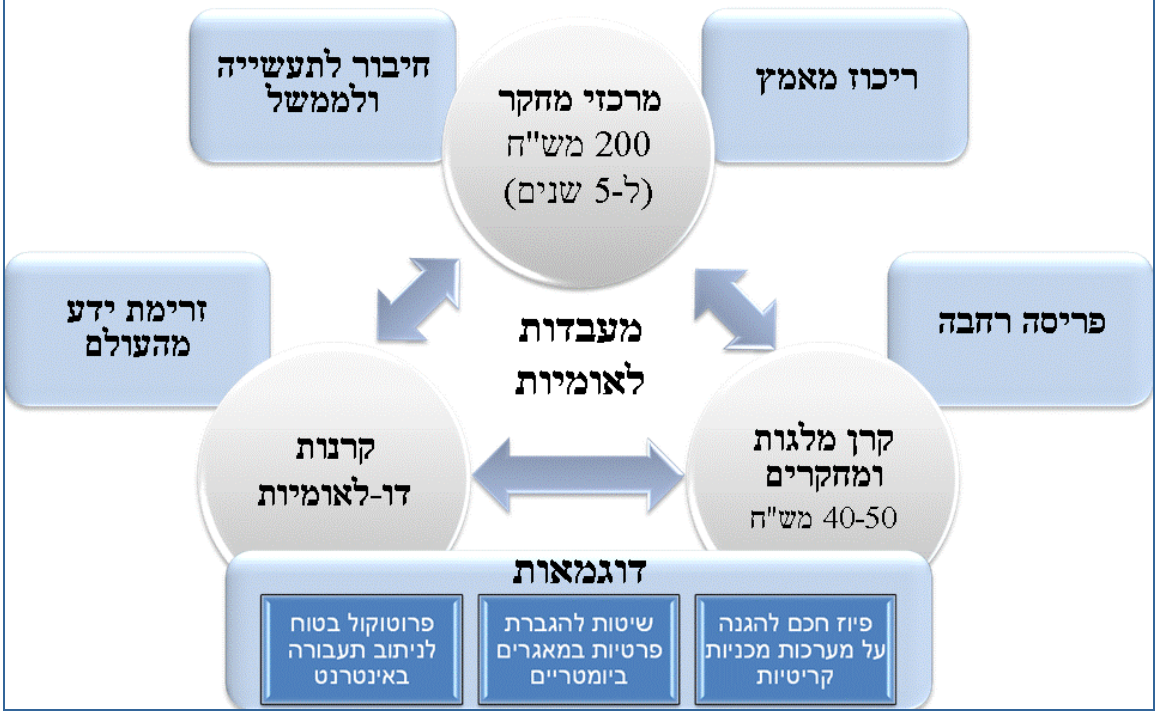
איום גלובאלי – הזדמנות לוקאלית



מובילות טכנולוגית בסייבר

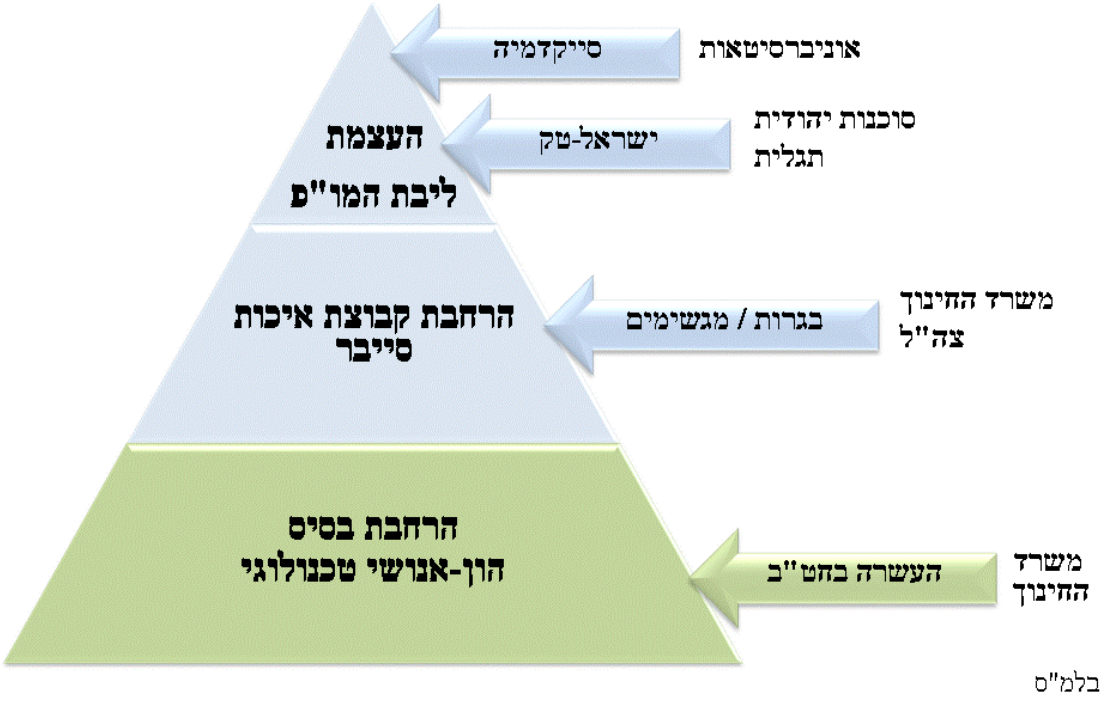


מחקר אקדמי בסייבר –
תשתית הידע לטווח הארוך



העצמת תעשיית הגנת הסייבר בישראל

תכנית אסטרטגית לבניין הון אנושי ייחודי



בלמ"ס

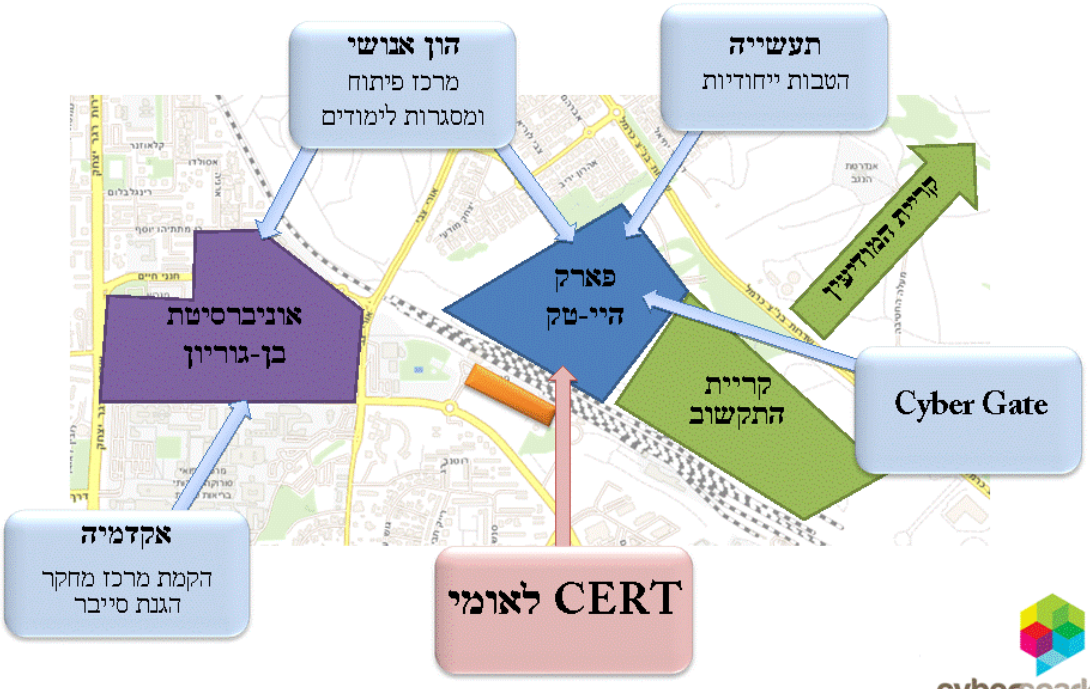
קריית סייבר לאומית

cyberspark

ISRAELI CYBER INNOVATION ARENA

7

המתווה להקמת קריית סייבר לאומית



cyberspark

ISRAELI CYBER INNOVATION ARENA

המדינה כלקוח ומובילת דעה

מר **רביב רז**, מנכ"ל, Security Hybrid

Cyber Innovation Israel

HYBRID SECURITY

HYBRID SECURITY

- Founded 2011 - Midreshet Ben-Gurion incubator
- Artificial Intelligence detects bad website users
- "Smart approach that advances the traditional signature based identification" - IDC
- "Heuristics as the next step in security" - Barclays

AI Learning to Identify Cyber Attacks

An Israeli company has developed a system capable of locating suspicious behaviors on the Web. The system has already been installed in several Israeli infrastructures

Moriya Ben-Yosef | 17/12/2012 | Recommend

The Israeli company Hybrid Security has developed a system called Telepath, which makes use of artificial intelligence for spotting suspicious behaviors in Web and intranet systems. The company is presently launching a second version of the system, which was installed last year in several national infrastructures in Israel in the framework of an operational pilot program.

The system includes more than ten algorithms developed by the company, which examine the user's surfing process and the various aspects of his behavior. The AI studies the surfers behaviors, learns what to expect and to locate the abnormalities in the framework of his network activity.

iHLS
Israel's Homeland Security Home

Home | News | Tech » | Security » | Cyber » | Intelligence » | Unmanned » | iHLS TV »

Cyber Threats: Net Psychology

Posted by Natalie Novitski

Artificial intelligence researchers are constantly trying to teach machines to think like humans. Despite all their efforts, though, there's a massive gap between human and machine psychology. An Israeli startup recently began using these differences to form a new, refreshing model of information security.

So… you have a great idea?

HYBRID SECURITY

Funding

Chief Scientist

- Incubator program
- Kidma

Matimop

- Starting entrepreneurs
- Bilateral R&D

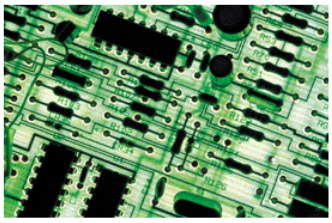
Ministry of Defense (MAFAT)

- Cyber warfare R&D

HYBRID SECURITY

R&D

- **Inter-University Computation Center**
- **Prime Minister Office**
  - Government offices
  - Academic programs
- **Early adopters / critical infrastructure**
  - Banks
  - Telecoms
  - Utility companies



HYBRID SECURITY

Marketing

- **Ministry of Foreign Affairs**: foreign delegations
- **Ministry of Economy**: commercial attachés
- **Export Institute**: global marketing
- **Chambers of Commerce**: international partnerships
- **Prime Minister Office**: foreign governments

HYBRID SECURITY

גב' **אסתי פשין**, ראש מינהל מערכות סייבר, תע"א- אלתא

ISRAEL AEROSPACE INDUSTRIES

Israeli Innovation in Cyber Technology

Unclassified

This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

Meet Mr Hacker!

Fake Identity
Huge Amounts of Data
Encryption

Unclassified

This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

The (Black-Hat) Hackers are Winning !

US cybercrime: Rising risks, reduced readiness
Key findings from the 2014
US State of Cybercrime Survey

pwc

This year, three in four (77%) respondents to the US State of Cybercrime Survey detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected increased over the previous year. So it's no surprise that more than 59% of respondents said that they were more concerned about cybersecurity threats this year than in the past.

http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Unclassified
This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

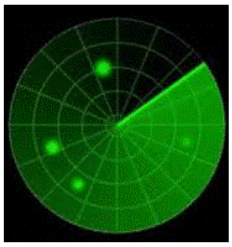
IAI Cyber Innovation Drivers

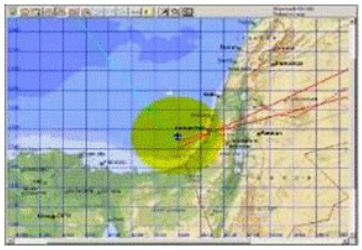
- Cyber as an EVOLUTION and not (only) a REVOLUTION
  - Adapting legacy Radar, Electronic Warfare, C4I and Comm. Capabilities
  - Diverse competencies
- Collaborating with Israeli (& other) Start-Up companies
- Establishing Cyber Innovation, Research & Development Centers
- Protecting IAI's IP, firmware, network & systems
  - A test-bed for IAI's Cyber capabiltie

Unclassified
This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

Cyber as an EVOLUTION and not (only) a REVOLUTION
Utilizing Radar and EW Techniques in Cyber

- The Challenge in Creating a Radar Situation Picture

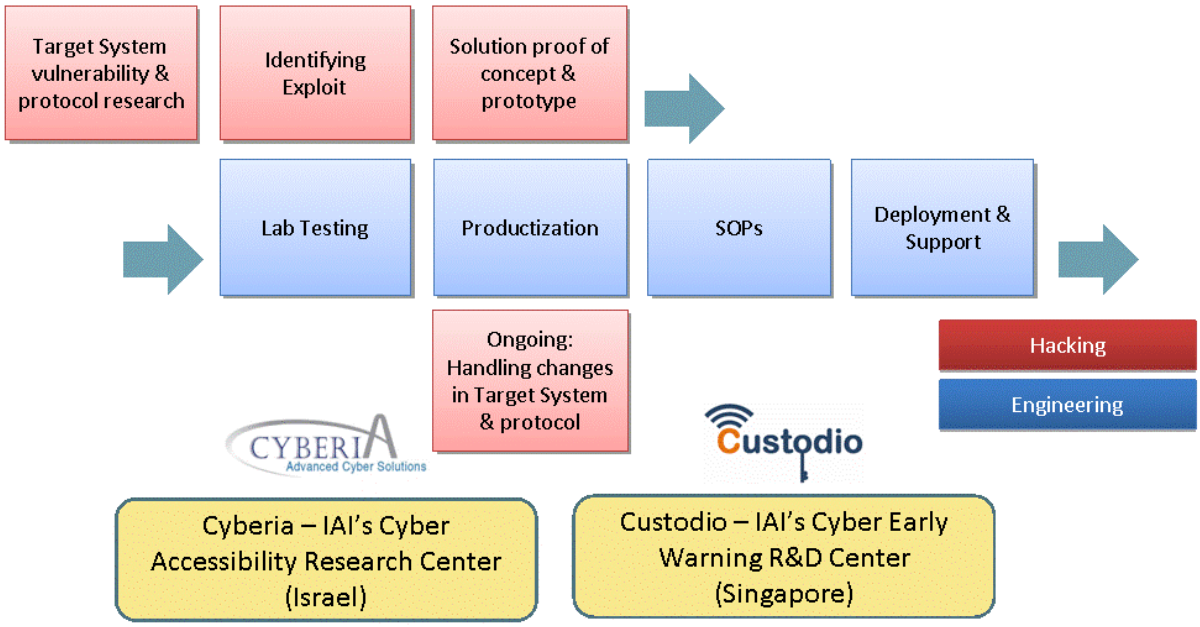




- Similar practices in Cyber Analytics – The Identity challenge

This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd

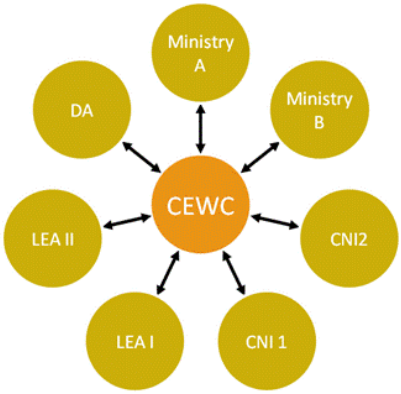
IAI's Cyber R&D Centers
Combining White Hat Hackers, Researchers and Engineers



This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

Ensuring Innovation with a Cyber Early Warning Center - A Service Oriented Approach

- Government offices and CNIs as subscribers
- Centralized Handling of Cyber Threat Monitoring
- Forming a national database and forensic center capabilities for Cyber threats
  - *Populating news, threats and security measures*
  Ability to perform forensics at the national level
- Bi-Directional relationship with subscribers
  - *To CEWC: Collection, information, new threats/virus/malware*
  - *From CEWC: intelligence, new threats/virus/malware, policies and procedures*



Unclassified
This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

Thank you

Unclassified
This document contains proprietary information of Israel Aerospace Industries Ltd. and may not be reproduced, copied, disclosed or utilized in any way, in whole or in part, without the prior written consent of Israel Aerospace Industries Ltd.

מר **רם לוי**, יועץ לביטחון סייבר, הוועדה הלאומית לסייבר, המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל.

כנס הרצליה 2014

יוני 2014

רם לוי, יועץ הסייבר של המולמ"פ

כנס הרצליה
המכון למדיניות ואסטרטגיה | הבינתחומי הרצליה

הרקע להקמת הוועדה

- ממשלה והחלטת הקיברנטי המיזם 3611 (אוג' 2011)
- מחשוב תשתיות על וגדלה הולכת הישענות
- פגיעות מערכות מחשבים להתקפות סייבר
- חזון לאור הישראלית העולמית המובילות הבטחת הממשלה ראש

ייעוד

- **להביא לתרומה משמעותית ומתמשכת לשגשוגה וחוסנה של ישראל בהיבטי הידע, הכלכלה, הביטחון והחברה באמצעות התוויית מדיניות ומימושה בתחום מו"פ הסייבר**
- להציג תוכנית שתסייע בשמירת מעמדה של ישראל כמובילה עולמית בתחום הסייבר

רם לוי, כנס הרצליה 2014

חברי הוועדה

18 חברי וועדה
12 גופים שונים

- **תא"ל (מיל.) ד"ר דני גולד – יו"ר הוועדה**
- ד"ר טל שטיינהרץ - המטה הקיברנטי הלאומי, משרד ראש הממשלה – מרכז הוועדה
- מר אילן פלד- מנהל מגנ"ט - המדען הראשי במשרד התעשייה, משרד הכלכלה
- מר רן שרמן, ראש הרשות הממלכתית לאבטחת מידע, שירות הביטחון הכללי
- פרופ' אסף שוסטר - הפקולטה למדעי המחשב, הטכניון
- פרופ' נפתלי (תלי) תשבי - האוניברסיטה העברית
- פרופ' יובל אלוביץ' - מעבדות דויטשה טלקום, אוניברסיטת בן גוריון
- ד"ר ליאת מעוז - המועצה להשכלה גבוהה / הועדה לתכנון ולתקצוב
- עו"ד מילי בך - ראש מחלקת חקירות ואכיפה הרשות למשפט וטכנולוגיה, משרד המשפטים
- אל"מ משה גולני - המנהל למחקר, מפא"ת
- מר רם לוי - המועצה הלאומית למחקר ופיתוח, משרד המדע, הטכנולוגיה והחלל
- סא"ל ניר פלג – ראש אגף מחקר ופיתוח, המטה הקיברנטי הלאומי, משרד ראש הממשלה
- מר גל שמואלי – המטה הקיברנטי הלאומי, משרד ראש הממשלה
- מר שוקי פלג - מנהל אבטחת מידע, הבנק הבינלאומי
- מר אבי זרוק – ממשל זמין
- מר ארז קריינר – לשעבר ראש הרשות הממלכתית לאבטחת מידע, שירות הביטחון הכללי
- עו"ד יום הכהן – לשעבר ראש הרשות למשפט וטכנולוגיה, משרד המשפטים
- מר אבי שביט – המדען הראשי, משרד הכלכלה

תפקידי הוועדה

- להמליץ לממשלת ישראל על מדיניות לאומית כוללת, רב שנתית, לקידום המחקר והפיתוח האזרחי בתחום הסייבר
- להמליץ על תשתיות מו"פ ופרויקטים לאומיים הדרושים כדי לקדם את המו"פ האזרחי בתחום הסייבר
- להמליץ על התקציבים הנדרשים לפיתוח מערך המו"פ האזרחי בתחום הסייבר
- למפות את מוקדי הידע האזרחיים בתחום הסייבר בישראל (בתעשייה, באקדמיה ובמגזרים אחרים)
- לבחון ולהמליץ על דרכים לעידוד שיתוף הפעולה בין כלל הגורמים הממשלתיים, האקדמיים והפרטיים העוסקים במו"פ אזרחי בתחום הסייבר
- לבחון ולהמליץ על אופן הכשרת כוח האדם המדעי והטכנולוגי בישראל בתחום המחקר והפיתוח סייבר באקדמיה ובתעשייה

תמונת מצב של תעשיית אבטחת הסייבר

	חברות מוצרים	חברות שירות	חברות שמבצעות פרוייקטי Turnkey גדולים	מרכזי מו"פ באבטחת סייבר
סטארטאפים וחברות קטנות (עד 100 איש)	188	5	N/A	10-12
חברות בינוניות (100-1000 איש)	8	1	N/A	5-7
חברות גדולות (מעל 1000 איש)	1	---	--- (אין מסה קריטית*)	

המחסור העיקרי כיום וגם המנוף המרכזי לצמיחה משמעותית בעתיד של תחום אבטחת הסייבר הוא בהצמחת וישימור חברות גדולות ובכניסה לתחום של החברות הגדולות הקיימות

מקור: שלדור, עבור המולמו"פ

האתגרים המרכזיים בתעשייה

א לא נוצרות חברות גדולות מתוך הסטארט-אפים

ב חברות גדולות בתחומים משיקים לא נכנסות לאבטחת סייבר

ג נוכחות דלה של חברות ישראליות בתחום השירותים (Managed Services)

ד היעדר שחקן עם יכולות לפרוייקטי Turnkey בשוק הביטחוני/ממשלתי

ה אי מיצוי הפוטנציאל של מרכזי המו"פ

ו מחסור גדל בכח אדם

מקור: שלדור, עבור המולמו"פ

מחסור בכח אדם בתחום הסייבר

מחסור בכח אדם מקצועי בסייבר

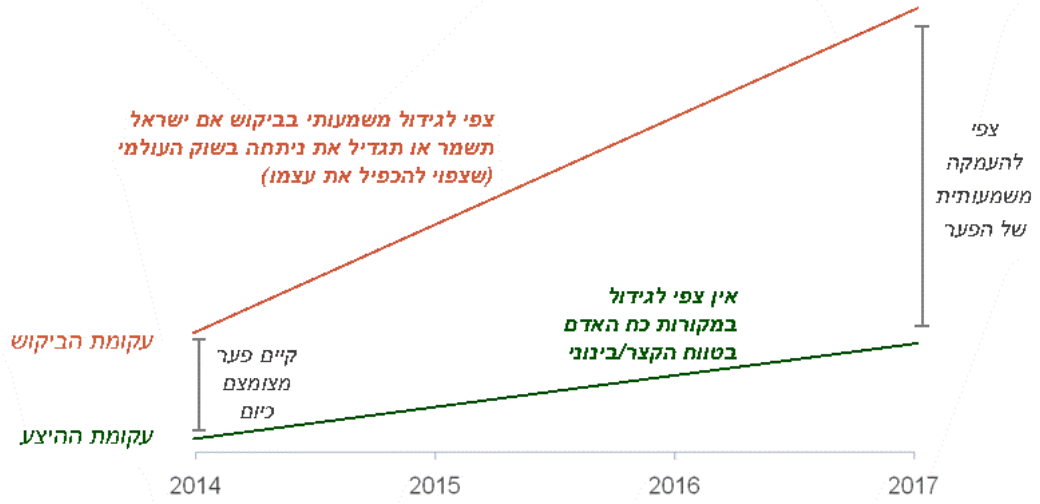
יוצאי צבא	• כמות נמוכה של אנשי סייבר שיוצאים מידי שנה לשוק... • ...רק חלקם נכנסים לתעשיית הסייבר • חלקם עוזבים לחו"ל...
בוגרי אקדמיה	• מחסור בהכשרה אקדמית מתקדמת (תואר שני ומעלה) שתייצר ידע משמעותי בסייבר
אנשי תעשייה	• חלקם יוצאים לחו"ל לעבודה בחברות סטארט אפ או חברות מובילות • חלקם חוזרים אך מאזן ההגירה שלילי

מחסור באנשי Execution בסייבר (מנהלים, שיווק, מכירות,...)

- חוסר במנהלים בישראל עם Track-record של הבשלת חברות
- פער באנשי Product שיכולים להפוך טכנולוגיה למוצר
- חוסר באנשי מכירות בסייבר שיודעים למכור לשווקים הגדולים (רב החברות הישראליות מעבירות את ה-HQ שלהם לארה"ב בגלל סיבה זו)

מקור: שלדור, עבור המולמו"פ

פער הכח אדם צפוי להעמיק עם התפתחות התעשייה



מקור: שלדור, עבור המולמו"פ

רם לוי, כנס הרצליה 2014

משרד המדע, הטכנולוגיה והחלל
המועצה הלאומית למחקר ופיתוח
הוועדה הלאומית לקידום המחקר והפיתוח בתחום הסייבר

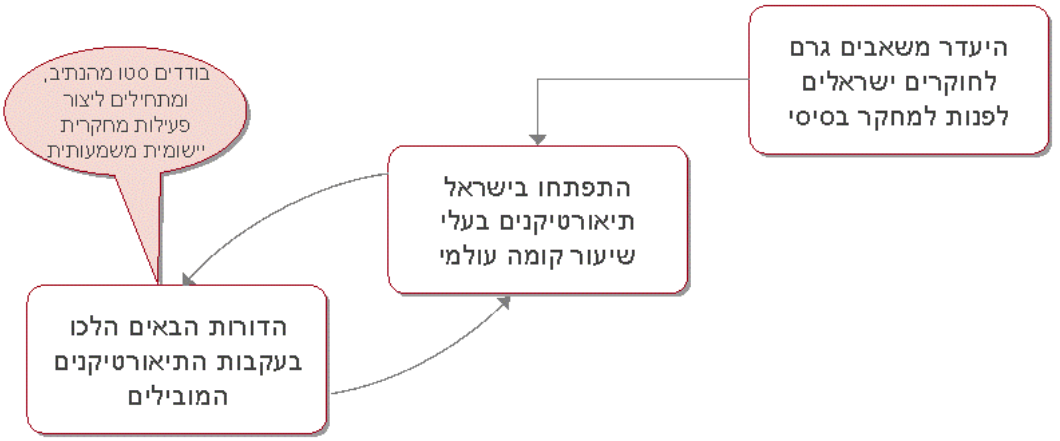
סטארטאפים - שני סוגים של חומר גלם - פסי ייצור שונים

	הרעיון העסקי	היכולות הנדרשות מצוות ההקמה
חומר גלם לייצור אקזיטים קטנים ומהירים	• רעיון לפתרון נקודתי של בעיה כואבת • בנתיב הקריטי של חברות גדולות בתחום.	• צוות פיתוח איכותי שיודע לפעול בסביבה חסרת אמצעים
חומר גלם לייצור חברות גדולות	• חזון משמעותי, בתחום בתול (אפשרות להתרחב למספר מוצרים) • ROI ברור בטווח הארוך	• יכולת ניהולית מרשימה ומוכחת • ניסיון שיווק ומכירות לחברות גדולות • יכולת גיוס סכומי כסף גדולים

מקור: שלדור, עבור המולמו"פ

רם לוי, כנס הרצליה 2014

מסיבות היסטוריות לאקדמיה בישראל
יש נטייה חזקה למחקר בסיסי על פני מחקר יישומי



"בפקולטה טיפוסית במדעי המחשב בארה"ב תמצא 30 פרקטיקנים ו-2 תיאורטיקנים. בישראל היחס הוא בדיוק הפוך, רב החוקרים הם תיאורטיקנים"

פרופ' אבישי וויל, אוניברסיטת ת"א

מקור: שלדור, עבור המולמו"פ

משרד המדע, הטכנולוגיה והחלל
המועצה הלאומית למחקר ופיתוח
הוועדה הלאומית לקידום המחקר והפיתוח בתחום הסייבר

האתגרים המרכזיים באקדמיה

1 מחסור בכמות ופער במצויינות באבטחת סייבר מחוץ לקריפטוגרפיה

- כמות קטנה של חוקרים ללא מסה קריטית
- ללא אימפקט משמעותי על המחקר העולמי

2 מחסור במחקרים בין תחומיים ומחקרים בתחומים רכים באבטחת סייבר

- רב המחקרים בישראל מבוצעים ללא שת"פ בינתחומיים
- תחומי המשפט, כלכלה ופסיכולוגיה לא מפותחים בתחום הסייבר בישראל

3 חסמים ב"הבשלת" מחקרי סייבר לכדי סטארטאפ או פרוייקט בתעשייה

- קיים פער גדול בין מה שחוקר מגדיר יישומי לבין מה שהתעשייה יכולה לנצל
- אין כיום מנגנונים שיודעים לגשר על פערים אלו
- גם כאשר ישנו רצון לשת"פ מדיניות ה-IP מקשה על שת"פ

מקור: שלדור, עבור המולמו"פ

המחקר מאוד בינתחומי, דרוש שת"פ חוצה פקולטות בדגש על שילובים של משפט, כלכלה, מדעי המוח וטכנולוגיה

	Attack	Security management	Risk Management Economics & Policy Making	Response & Recovery	Attack prevention Detection & monitoring	Privacy	Access Management, Identity & Trust	Secure Design & Engineering
מדעי המחשב	✓	✓	✓	✓	✓	✓	✓	✓
מקצועות ההנדסה			✓	✓	✓			✓
מתמטיקה				✓	✓	✓	✓	✓
קריפטוגרפיה		✓		✓		✓	✓	✓
משפטים	✓	✓	✓	✓	✓	✓	✓	
כלכלה	✓		✓	✓	✓			✓
ניהול	✓	✓	✓	✓				
פסיכולוגיה/ סוציולוגיה/ קרימינולוגיה / מדע המדינה	✓	✓	✓	✓	✓	✓	✓	

מחקר בסייבר כיום בישראל מתבצע בבודדים, עם מעט מאוד שת"פ בין חוקרים בכלל ושת"פ בינתחומיים בפרט

תחומים שבהם לאקדמיה תרומה משמעותית לפיתוח התעשייה

תחומי מחקר באקדמיה לפי תרומתם לתעשייה

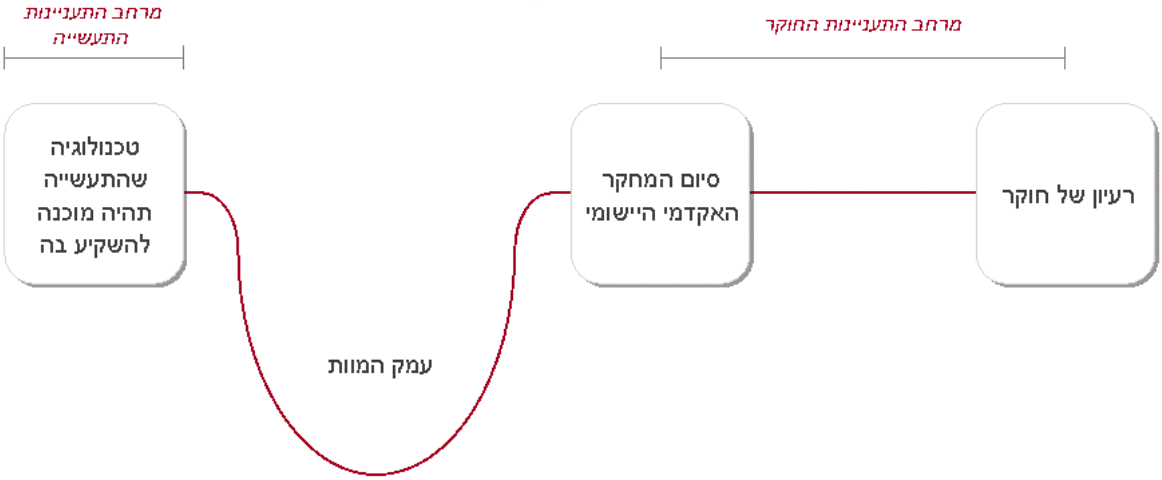
התקפה	מוכנות וניהול האבטחה			מניעה וזיהוי				
Attack	Security management	Risk management Economics & Policy Making	Response & Recovery	Attack Prevention, Detection & Monitoring	Network and end point protection	Privacy	Access management, Identity & Trust	Secure Design & Engineering
Reverse Engineering	Security information and event management	Vulnerability assessment & risk management	Forensics	Malware	Network protection	Usable Privacy & Security	Access Management & Authentication	Secure Operating Systems
Other attack	Fraud Management	Cyber Security Economics	Computer Security Incident Response (CSIR)	Bot-nets	Endpoint Protection	Privacy & Anonymity	Managing Identities	Language Based Security
Legal guidelines for offensive cyber attack	Organizational Procedures	Cyber Insurance	Incident Recovery	anomaly detection	Mobile devices and operating ystems	Data Confidentiality	Trust delegation & management	Testing Systems
	Policies for data & Information management	Regulation and policy making	Incident Management	Data & commerce Protection	Cloud protection			
				Cybercrime/ Cyber terrorism				
				Social Engineering				

תחומים בהם לאקדמיה היה אימפקט משמעותי על התעשייה

תחומים שבהם הייתה התעשייה מובילה על האקדמיה

מקור: cyber security research agenda – U.S, U.K, Netherlands – Shaldor analysis

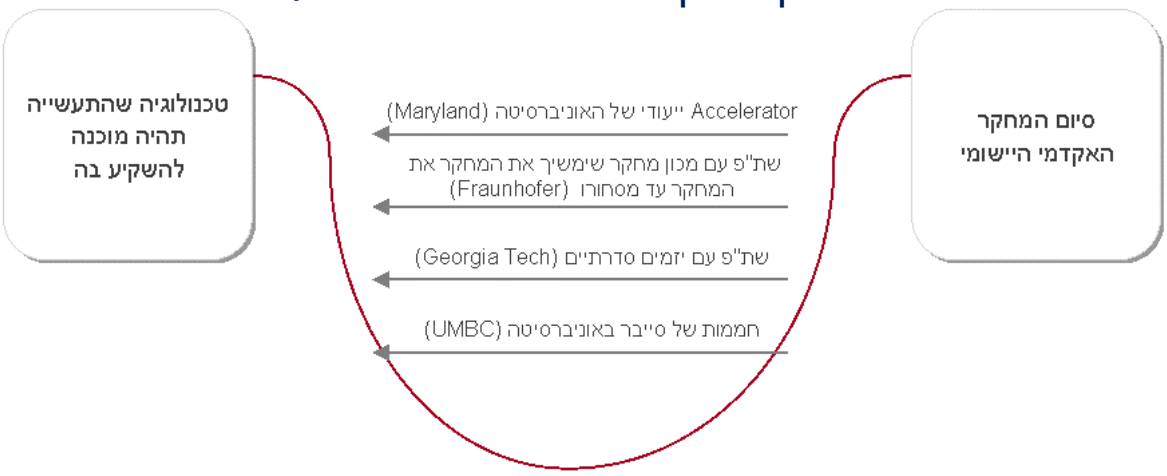
המחקר היישומי באקדמיה מסתיים לרב בשלב שהוא מקדמי מידי עבור התעשייה, ולכן הוא לא ממומש



- אין עניין לחוקר
- אין לתעשייה מה לעשות עם זה
- אין כסף
- חסר יכולות

משרד המדע, הטכנולוגיה והחלל
המועצה הלאומית למחקר ופיתוח
הוועדה הלאומית לקידום המחקר והפיתוח בתחום הסייבר

בעולם פיתחו מספר מנגנונים שיגשרו על 'עמק המוות' שמפריד בין האקדמיה היישומית לתעשייה



בישראל אין כיום מנגנון יעיל שמצליח לגשר על עמק המוות

הצעדים הבאים

הצגה ואישור המלצות בממשלה

המלצות למכלול המהלכים הנדרשים לקידום התחומים שזוהו.
המלצות לתשתיות ופרויקטים לאומיים
המלצות להכוונת משאבים לאומיים ופרויקטים קיימים במידת הצורך
המלצות ארגוניות, נהלי עבודה, מדיניות וחקיקה
מדדים להצלחה.

קידום ושיפור מעמדה של מדינת ישראל במו"פ בתחום הסייבר והצבתה בחמישיה הפותחת בעולם

רם לוי, כנס הרצליה 2014

כנס הרצליה 2014

יוני 2014

רם לוי, יועץ הסייבר של המולמ"פ

כנס הרצליה
המכון למדיניות ואסטרטגיה | הבינתחומי הרצליה