<u>סייבר כמימד בלוחמת היבשה</u>

אלוף במיל' פרופ' י. בן ישראל, יו"ר סוכנות החלל ויו"ר המועצה הלאומית למו"פ

אני מאמין שבעוד 20 או 30 או 40 שנה תחום הסייבר יהיה מרכיב שלא ניתן לפעול בלעדיו. היום הוא מרכיב בשולי הלחימה; אבל היום אני שואל איפה לוחמת הסייבר? אני מדבר על לוחמת סייבר - לא לוחמת מידע, **information warfare** באנגלית, אלא תחום יותר צר. היכן תפקידה של לוחמת הסייבר בלוחמת היבשה כיום? רק במחשבה, כמעט שלא בחיים. ולכן זו דברי יהיו כוללניים יותר, ויתייחסו ללוחמת סייבר בכלל.

מדינת ישראל עוסקת בסייבר, מזה כ-15 שנה. מובן שהחלו הישר מהשורשים. פותחו כל מיני יכולות שלחלקן אפילו יכולות שיש להן משמעות מבצעית, וראש הממשלה כשהדגימו בפניו לפני קצת יותר משנה מה מדינת ישראל יכולה לעשות בתחום הסייבר, הוא שאל מיד: אם זה מה שאנחנו יכולים לעשות לאחרים, מה האחרים יכולים לעשות לנו?

כתוצאה מכך הוקם צוות שעמדתי בראשו בהיותי יו"ר המועצה הלאומית למו"פ, צוות שישב שנה על המדוכה והגיש דו"ח שאומץ לפני שלושה שבועות כהחלטת ממשלה.

אפתח ביסוד התפיסתי: הטכנולוגיה משתנה במהירות עצומה, לפעמים איננו שמים לב לקצב השינוי ולמהפכה שבה אנחנו נתונים ומתעוררים באיחור, וחייבים להתאים את התרגולות והאימונים כמו גם תורת הלחימה לטכנולוגיות החדשות.

אנחנו נמצאים בעיצומו של עידן שאפשר לקרוא לו עידן המידע. בשליש הראשון של המאה ה-20 ובמיוחד לאחר מלחמת העולם השנייה, היו אנשים שהבינו לא רק שהטכנולוגיה מאפשרת לנו לעשות את הכל יותר מהר, לחשב יותר טוב, יותר רחוק, יותר מדויק וכל הדברים שכולנו מכירים, אלא שאנחנו עומדים בפני שינוי קונספטואלי בגלל כמה סיבות.

הפילוסוף אלווין טופלר שאני מניח שהוא סוציולוג עתידן, כתב באמת את ספרו "מלחמה ואנטי מלחמה" ב-1950 בערך, (חלק גדול מהאנשים שמוכרים לי פה קראו אותו) והוא טוען בו

שעברנו מעידן שבה התרבות הייתה חקלאית, אי שם במאה ה-17 - 18 לעידן שבו התרבות היא תעשייתית. באמצע המאה ה-20 שבו התרבות סובבת סביב המידע. כשאני אומר תרבות אני מתכוון לכלכלה, בעבר העשיר היה בעל האדמות; בעידן התעשייתי היה זה התעשיין, בעידן העכשווי זהו ביל גייטס או סטיבן ג'ובס. העשירים האלה מה הם עושים בעצם? הם מאפשרים לנו להתעסק בידע שהם פיתחו. עברנו לעידנים האלה בכלכלה וגם במלחמה.

בעבר כלי המלחמה היה חרב ומגל היה הכלי החקלאי: אלה שני שימושים שונים באותה טכנולוגיה. מלחמת העולם השנייה שהתחוללה בעיצומו של העידן התעשייתי הוכרעה בסופו של דבר באמצעות קווי ייצור תעשייתיים, מי ייצר יותר מטוסים? מי ייצר יותר טנקים? מי ייצר יותר אוניות? אנחנו עוברים מבלי משים לעידן שבו הכל סובב סביב האינפורמציה, מבלי לשים לב שאינפורמציה אינה זהה למטוסים, טנקים או חרבות. זהו משהו אחר.
מבחינה פילוסופית זה איננו חומר, גם לא חוויה מנטלית; כולנו יודעים פילוסופית שהדברים הם או בגוף או בנפש, כלומר - או חומר או חוויה מנטלית, ואילו ידע אינו זה גם לא זה. הוא דומה לחוויה מנטלית במובן זה שלא היה קיים אלמלא היו בני האדם יוצרים אותו, אבל הוא דומה לחומר בהיותו אובייקטיבי ולא סובייקטיבי.

משפט פיתוגרס או כל משפט אחר במתמטיקה אינו משפט סובייקטיבי:הוא משפט אובייקטיבי. בכלכלה העניין יותר בעייתי, משום שכל הכלכלה בנויה על הרעיון שאם אני מוכר לך איזשהו מוצר הוא כבר לא שלי, ז"א שאני יכול להשתמש ב-50% ואתה ב-50% אם אמכור לך 50%, אבל אותם 50% שאני מוכר לך כבר לא יהיו לי. לא כן הידע. אני יכול למכור לך את הידע שלי ולמכור למדינה שלישית את הידע שלי ולמכור לכל אחד את הידע שלי והוא עדיין בלתי נדלה, והוא כלל לא נעלם.

ואם אנחנו אומרים שכל התרבות כולה, כולל המלחמה, עוברת להיבנות על איזושהי מניפולציה בידע, אנחנו צריכים לשנות מושגים יסודיים מאוד.

כאשר מחברים את כל הדברים האלה אנחנו מבינים שאנחנו נמצאים בעידן חדש שבו המקור העיקרי כמעט לכוח - וכשאני אומר כוח אני מתכוון גם כוח צבאי וגם כוח כלכלי - הוא איזשהו סוג של ידע.

מה זה אומר לגבי תורת המלחמה שלנו? מה זה אומר לגבי האפשרויות החדשות? הנה נוצר הדבר הזה שאנחנו קוראים לו סייבר ספייס, שהוא לא בדיוק מוגדר; כשאומרים סייבר ספייס מתכוונים בעצם למחשבים, לתוכנות בתוך המחשבים, לקווי התקשורת בין המחשבים האלה, ולכל דבר שקשור למניפולציה של אחסון מידע, העברת מידע, עיבוד מידע, כל הדברים שקשורים למניפולציה במידע שאגור במחשבים הללו.
אלה יוצרים הזדמנויות אדירות ללחימה, כל מערך האסופה שהוזכר קודם על ידי האלוף גרשון הכהן התאפשר בשנות ה-90 משום שהמחשבים הלכו וקטנו, קטנו עד כדי כך שאנחנו מסוגלים להכניס אותם היום לא רק לפלטפורמות של לחימה, אלא להכניס אותם לתוך החימוש עצמו, לתוך הפצצה, והרי כך נוצר מוצר שנקרא פצצה חכמה.
כאשר אנחנו יכולים להפוך אותם לעצמים כל כך קטנים, אנחנו מסוגלים לראשונה בהיסטוריה לפגוע במטרה בקליע אחד. לא צריך לעשות מה שהיינו עושים בעבר - להפעיל הרבה אש כדי לפגוע במשהו.

בכל אחד משלושת האלמנטים שיוצרים את הרעיון של תקיפה מדויקת, החימוש עצמו, מודיעין המטרות והשליטה והבקרה שמחברות את החימוש הנכון למטרה הנכונה בזמן הנכון, כל אחד מהאלמנטים האלה לא היה מתאפשר בלעדי מחשבים.

ההתפתחות הזאת מקנה לנו אפשרויות עצומות, אבל גם יוצרת נקודת תורפה אדירה. מעניין שנקודת התורפה הזו איננה רק צבאית. הרי ברור שאם כל מערך הלחימה שלי מבוסס על מחשבים, ואם מישהו יודע כיצד אפשר להיכנס באיזשהו אופן לתוך המחשבים האלה, כמו הוירוסים שיש לנו בבית השכם והערב, הוא יכול לפגוע בי בצורה שלא התאפשרה קודם, אפילו בדברים הטריוויאליים.

תארו לכם שעכשיו קורה משהו ורוצים להזעיק את המילואים ומישהו פוגע ברשומות שבהן שמות אנשי המילואים מוחזקות. במקרה כזה אפשר כמובן להודיע לכולם ברדיו להגיע ליחידותיהם; נקווה שיבואו. אגב, אפשר גם לפגוע ברדיו באמצעות המחשבים. וכך לצד היכולות החדשות, נוצרות גם נקודות תורפה חדשות. ובכל מקום שבו קיימת נקודת תורפה, מיד יש גם מי שמתפרנסים מזה, ולכן יש איומים במרחב הסייבר.

יש איומים קלים: כל בוגר, אם הראש שלו מספיק טוב, יכול לשבת ולהיות 'האקר' ולחדור למערכות, לעתים גם למערכות מאובטחות מאוד. זו לא בעיה גדולה. 'האקרים' רציניים יודעים להיכנס כמעט לכל אתר מחשב, אלה איומים מטרידים אבל אינם איומים שיש בהם כדי לאיים על הביטחון הלאומי של המדינה.

מנגד, בקצה השני של הספקטרום, יש איומים ממשיים, איומים שמונעים על ידי מדינות; והרי למדינות יש סבלנות, הן יכולות להרשות לעצמן להשקיע בכך אלפי שעות אדם, הן יכולות לחכות חמש שנים. חדירה למחשב אינה 'זבנג וגמרנו'. אתה עושה משהו, אתה מנצל את מה שעשית, אח"כ מישהו נכנס כדי לשפר את האחיזה שלך, ובינתיים המחשב שנכנסת אליו מחליף גרסת תוכנה, ואתה צריך להתארגן ולהתמודד עם הגרסאות החדשות, ולאט-לאט אתה מפתח יכולת ובסוף אתה יכול לקטוף את הפירות.

כמה דוגמאות מדברים שהתפרסמו בעיתונות. יש התקפות שנמשכות חמש שנים, יש שלבים בהתקפה אבל מהשלב הראשון ועד האחרון עברו חמש שנים.

האיום שאנחנו רוצים לדבר עליו הוא איום שמונע או נתמך על ידי מדינות, ומשהו שמאוד דומה לו, קצת פחות חמור, אבל לא רחוק מזה, ונפוץ מאוד כיום בעולם, וזה האיום של ארגוני פשע גדולים. לזה כמעט שלא אתייחס, אבל דעו שכל מה שאמרתי על מדינות, יש גם לארגוני פשע גדולים; אפשר להרוויח הרבה כסף מטרנסקציות במחשב. יש ארגונים שזו מטרתם עלי אדמות והם נוהגים לגנוב מידע ולמכור אותו, או להכנס ולהעביר בבנקים כסף מחשבון לחשבון, וההתנהגות הזאת דומה מאוד להתנהגות של מדינות.

ברשת ה-**CNN** עשו הדמייה, הזמינו אנשים שהיו בעלי תפקידים בכירים בממשל האמריקאי, והושיבו אותם לשחק את התפקיד שלהם, ואז הטילו עליהם בזמן-אמת איזשהו סיפור של מתקפת סייבר על ארה"ב. בתחילה נתקלים בבעיות בתקשורת הסלולארית במרכז ארה"ב, פתאום הטלפונים לא פועלים, ולאט לאט הכשל הולך ומתרחב והמלוהקים לתפקידים מתבקשים לפתור את הבעיות ואז מתגלה להם, כמובן, שארה"ב לא ערוכה לזה. לא מבחינת הכלים האופרטיביים, ולא מבחינת החוקים. לעניין יש מימדים רבים שצריך להתכונן לקראתם לפני שתהיה מסוגל באמת להפעיל איזושהי הגנה אפקטיבית.

לפי דוגמאות שהתפרסמו בעיתונות בשנים האחרונות, כמה מההתקפות הבולטות ביותר בתחום הסייבר החלו לפני כעשר שנים. הדוגמה הראשונה שהעירה את העולם היתה השיתוק שתקף את אסטוניה. האסטונים עשו טעות והזיזו איזו מצבה של החייל האלמוני שהרוסים השאירו שם לפני שעזבו, למקום שנחשב לא-מכובד בעיני הרוסים והם התעצבנו.

אסטוניה היא מדינה ממוחשבת מאוד, מרבית הפעולות הבנקאיות שאנשים עושים מתבצעות דרך הרשת, לא באופן ישיר, כך גם מצביעים בבחירות דרך הרשת, קונים בסופרמרקט דרך הרשת. ואז נעשתה נגדם מתקפה מאוד פרימיטיבית, מה שנקרא **denial of service**, זו התקפה שרק גורמת לעומס על הרשת ומפילה את השרתים. במשך שלושה שבועות המדינה הייתה משותקת ופתאום העולם תפס שאפשר לעשות משהו בעל אופי מלחמתי מבלי לירות ולו כדור אחד. בלי טנקים ובלי מטוסים.

הדבר חזר בשנייה בצורה קצת יותר חלשה במלחמה בין רוסיה לגיאורגיה; שם היעד היה בעיקר מערכות הממשל של הגיאורגים, מערכות שליטה ובקרה, ולפתע התברר שזה חלק ממלחמה. כשמדובר בפגיעה במערכי השליטה והבקרה, השו"ב של האויב, אפשר לעשות זאת בפצצות, או על ידי ל"א, או באמצעות חסימות של קשר וכך הלאה, ואתה יכול לעשות את זה גם בכך שאתה נכנס למחשבים שלהם עם הוירוסים המתאימים. זה מחייב, כמובן, הכנה מראש, מישהו צריך להתכונן לזה לפני המלחמה: זו אינה פעולה שאתה מחליט עליה ומבצע אותה בזמן אמת.

האירוע הגדול האחרון שעורר את תשומת הלב הוא הסיפור על הסטקסנט. בעיתונות נכתב על וירוס מאוד מתוחכם שפגע במערך הצנטריפוגות באיראן וירוס שהתפשט במערכת והגיע לכל מקום. אחרי שהוא נתגלה ונחשף, בדקו ואז התברר שהוא מצוי באיזה 100 אלף מחשבים בכל מיני מקומות. אבל כשהוא מגיע לאיזשהו מקום הוא בודק איפה הוא נמצא. אם הוא נמצא בסביבה של צנטריפוגה, הוא מעלה את המהירות שלה ופוגע בה. אם הוא נמצא בסביבה שאינה צנטריפוגה הוא הולך לישון.

הסיפור הזה אינו מה שעורר את מי שעוסקים בתחום ברחבי העולם הזה וגרם לכך שכל הנורות האדומות ניצתו, אלא העובדה שמיתקן הצנטריפוגות בנאתנז האיראני מבודד, אינו מחובר לשום רשת, בוודאי לא לאינטרנט וגם לא לרשת פנימית איראנית; אם כך, איך הוירוס נכנס לשם? ההשערות בספרות הגלויה ציינו את האפשרות שאחת מהמדיות, כמו דיסק-און-קי,

למשל, שהיא דרך טובה להזריק, וירוס למחשב גם כשאיננו קשור לרשת, או לחלופין דרך מערכי התחזוקה.

מה הדבר המעניין מבחינתנו? הדבר המעניין מבחינתנו הוא שהאיראנים הודיעו, ואין במדינת ישראל מי שלא מאמין להם, שאם יקומו בבוקר יום אחד ויראו שמישהו הפציץ את המערכים לייצור אורניום, הם יתקפו בתגובה את ישראל ואת הבסיסים האמריקאיים במפרץ: הם לא ישאלו מי זה. ברור להם שאלו הן שתי המדינות שמעוניינות בפגיעה ביכולת הזאת והם יגיבו באש.

יש מישהו שאף אחד לא יודע מיהו, שתקף את הצנטריפוגות שלהם, שהתרסקו בגלל הוירוס הזה, והם לא פתחו באש. הם חושבים גם לגבי הפעולה הזאת שארה"ב או ישראל הן שעשו זאת, כי זו המחשבה הטבעית, כי אלו שתי המדינות שמעוניינות שלא יהיה להם נשק גרעיני.

אבל הם לא יודעים; איש לא יודע בתחום הסייבר הזה מנין התקיפה מגיעה באמת. אפשר להעלות השערות, אבל אי אפשר לדעת ממש. נשיא ארה"ב הכריז לפני כמה חודשים שמתקפה על המערכות הקריטיות בתחום הסייבר של ארה"ב, תיחשב כמלחמה. מבחינת ארה"ב, זאת אומרת שארה"ב חופשית להגיב באש.

קל להכריז על כך כמדיניות, אבל לא פשוט לבצע זאת כשאתה לא יודע בדיוק מי התקיף אותך ואתה לא יודע אם זה הוא או מישהו אחר, כי אפשר לנצל שרתים של מישהו אחר כדי להגיע ולבצע את המתקפה.

יש סיפורים גם על סין: התקיפה על לוקהיד מרטין שנמשכה חמש שנים. כדי להיכנס ללוקהיד מרטין נדרשו להם קודים. בלוקהיד מרטין המחשבים מוגנים על ידי חברה שנקראת **RSA**, **RSA** הם ראשי תיבות של ריבד-שמיר ואדלמן, הרעיון פותח פה במדינת ישראל, והיום זהו הקוד הנפוץ ביותר בעולם להגנה על מערכות מחשבים. כדי לפרוץ למחשבים של לוקהיד מרטין ביצעו פריצה שנה קודם לכן, ל-**RSA** על מנת להוציא את הקודים. וכדי לפרוץ ל-**RSA**

הנסיונות החלו חמש שנים לפני כן, וכולם אומרים שסין עשתה זאת, כי כשאתה מסתכל לאחור מתברר שזו תקיפה שנמשכת חמש שנים, שהתוכנות שמעורבות בה, התוכנות המזיקות, הוירוסים האלה למיניהם, נכתבו על ידי אלפי אנשים; זו אינה תוכנה ששלושה אנשים יושבים וכותבים, ואתה שואל את עצמך מי יכול להקדיש חמש שנים, להפעיל אלפי אנשים ומעוניין בדברים שהוציאו מלוקהיד מרטין, ובסופו של דבר אתה מגיע לסין.

ברור שלכך נוספים סימנים אחרים. ישבתי עם הצוות של מקאפי שכתב את הדו"ח הזה, בין היתר הם אמרו לי שבחלק מהסקריפטים שבהם הפעילו את הוירוס, נמצאו שגיאות כתיב אופייניות לסינים. הסינים מתקשים להבדיל בין הצליל **R** ו-**L**, ומופיעות שם שגיאות כתיב אופייניות וגם סימנים רבים אחרים, ובסופו של דבר זו עבודת בילוש יותר מאשר ידיעה של ממש, כי כולם משתמשים במחשבים של אחרים. השאלה למי אני מייחס את ההתקפה, היא לב ליבו של תחום הסייבר הזה.

לנוכח הדברים האלאה החליט ראש הממשלה להקים צוות, שצריך להסתכל על הסייבר במובן הרחב ביותר, לברר לא רק איך אנחנו מגנים על עצמנו, אלא איך אנחנו מגנים על עצמנו לאורך זמן, איך זה נעשה בעל ערך? כלומר, עלינו להפעיל בעניין זה לא רק את המומחים שיש לנו ברגע זה בסייבר, אלא את שלושת הגורמים עליהם מושתת כמעט כל דבר במדינת ישראל, הממשלה בכלל, אבל בעיקר הביטחון, התעשייה והאקדמיה.

אלה שלושת המגזרים עליהם בנויים כל ההייטק וכל תעשיית הביטחון שלנו. העבודה שקיבלנו על עצמנו התרכזה לא רק בשאלה כיצד מגנים, אלא איך בונים את כל הסביבות הללו. הקמנו צוות, בן שמונים איש, שנוהל על ידי צוות מלמעלה, ואני הייתי יושב הראש שלו, ומלמעלה היו גם ראש מפא"ת, המדען הראשי בתמ"ת וראש הות"ת פרופ' עמנואל טרכטנברג.

הקמנו 8 תת וועדות, אחת מהן עוסקת בתשתית. אי אפשר לעשות שום דבר בסייבר בלא תשתיות מסוימות שהעיקרית שבהם היא חישוב מהיר, כולם מגנים על מערכות המידע שלהם בעזרת צפנים ואם אתה רוצה להגן על עצמך אתה חייב להיות בעל כושר גדול בהצפנה, ואם אתה רוצה לחדור פנימה עליך להיות בעל כושר גדול בשבירת ההצפנה, וכל אלה לא יכולים להיעשות בחישוב נורמאלי, המחשב הרגיל לא די מתקדם לצרכים האלה, צריך חישוב מהיר מאוד.

למה אני מתכוון בחישוב מהיר? מהירות המחשב הרגיל שלפני בערך 5 גיגה, והוא מבצע 5 מיליארד פעולות בשנייה. המחשבים שאנחנו מדברים עליהם מהירים בערך פי מיליון. זאת אומרת 10 בחזקת 18 פעולות בשנייה. קל להגיד את המספר הזה, קשה לתפוס עד כמה הוא גדול.

כאמור, הצופן חשוב ביותר, בלעדיו אין עבודה בסייבר, וכך הוקמה וועדה שעסקה בהגנה, וועדה שעסקה בצד השני של הדבר, שבראשה עמד פנחס בוכריס.

היו ארבע וועדות רוחביות, שעסקו בהיבטים הכלכליים, בהיבטים האקדמיים, ברגולציה וכמובן במה שאנחנו קוראים הסדרה שזה הכאב ראש הכי גדול, מי יהיה אחראי על מה, ובישראל זו שאלה קשה מאוד.

הכוונה היא לחולל סינרגיה בין שלושת הגורמים התעשייה, הממשלה עם דגש על הביטחון, והאקדמיה. אך מה מצאנו? קודם כל, שאין לישראל מדיניות סייבר וצריך שתהיה. שנית, יש תחומים מסוימים שבהם אנחנו בפיגור גדול, כמו למשל באקדמיה, וצריך לתגבר את התחום. לעומת זאת יש תחומים באקדמיה שבהם ישראל היא מקום ראשון בעולם, כמו למשל הצפנים, הרי הקוד העולמי, ה-**RSA** העולמי, פותח באקדמיה הישראלית.

אנחנו חייבים להכניס את התעשייה פנימה וזה אומר שמוכרחים לאפשר לה למכור את המוצרים, לייצא אותם. זו בעיה ישראלית, לא בעיה אמריקאית, השוק בישראל כ"כ קטן שאין שום סיכוי בעולם שאיזו תעשייה תחיה רק על השוק הפנימי.
אם אנחנו רוצים שהתעשייה הישראלית תיכנס, תשקיע השקעות, עלינו לנהוג כמו תעשיית הביטחון שלנו שבה 80% מהתוצרת מיוצאת, 20% נמכרת לשוק הפנימי, כך צריך להיות גם בסייבר. קל לומר זאת, אבל קשה לעשות כי הסייבר הזה רגיש ביותר, יש לו כל מיני יכולות, האם נמכור אותן? נייצא אותן?

לתעשיית הביטחון שלנו יש יכולות רגישות מאוד ולא עולה על דעתנו למשל לפתח ל"א בתוך צה"ל. יש, כמובן, קציני פרויקט בצבא אבל הפיתוח עצמו נעשה בשתי תעשיות, אחת מהן ממשלתית ואחת פרטית לגמרי: חברת אלישרא. אבל בנינו את המנגנונים הנכונים. איך מאשרים את הייצוא הזה? מהם הכללים? כל אחד יודע בדיוק מה יתאפשר לו לייצא ומה לא, ואת הדברים האלה צריך לבנות גם בתחום הסייבר.
בנינו כלים שיעודדו את שיתוף הפעולה בין האקדמיה, התעשייה והביטחון, ובהם דברים שבעבר לא נהגו לעשות, כולל מיקור חוץ גדול הרבה יותר של תחום התוכנה.
האיום אינו וירטואלי, בישראל יש מערכות מוגנות זה כמה שנים. ב-2002 באנו ואמרנו לממשלה: כל היכולות שאנחנו מפתחים מחייבות הגנה גם על תשתיות אזרחיות, שלא ברור מי מגן עליהן, מי מגן על חברת החשמל למשל? הרי כולה נשלטת על ידי מחשבים.

בתרגיל שנעשה לפני כמה חודשים, חדרנו לתוך מחשבי חברת החשמל, הגענו למצב שבו ניתן בלחיצת כפתור להגביר את מהירות הסיבוב של הטורבינה באחת מתחנות הכוח שלנו למהירות כזאת שהמהנדס של חברת החשמל אמר לי שאילו היו מעלים אותה ממש למהירות זאת היא הייתה ניתקת מהבסיס ומגיעה בערך לקפריסין מעוצמת הסיבוב. תיקון טורבינה בחברת

החשמל אורך כמה שנים. כל זה בלחיצת כפתור דרך חדירה למערכות המחשבים של חברת החשמל.

ב-2002 נתקבלה החלטת ממשלה לפיה לצורך תשתיות מסוימות שסומנו כחשובות לביטחון המדינה הוקמה הרשות לאבטחת מידע בשב"כ, שתהיה אחראית על התשתיות הללו. כשאתה מסתכל היום ב-2012, מערכות רבות שפעם לא היו ממוחשבות ולא נחשבו כקריטיות, היום נכללות באותה קטגוריה. הדוגמא הפשוטה ביותר שאני יכול להעלות על דעתי היא מערכות הבורסה. בבורסה המסחר מתחיל ונפסק באופן אוטומטי אם המחשבים של הבורסה מגלים שהירידה גדולה מדי. הם בודקים את קצב הירידה, ומפסיקים את המסחר ל-45 דקות, או ליום שלם, תלוי בירידה. אין שום בעיה להיכנס למחשבים האלה ולהתחיל לשנות את שערי המטבע בישראל ואת מניות הבורסה. הפגיעה הכלכלית במדינה יכולה להיות אדירה. מבלי לירות אפילו כדור אחד. מי אחראי על המערכות האלה?

מהמערכות שאנחנו מגינים עליהן אנחנו יודעים שמספר ההתקפות בישראל מגיע למספר של מאות ביום רגיל, ובעיתות מצוקה יכול להגיע לכמה מאות בשעה. בסופו של דבר איתרנו תחום גדול, שהוא הסקטור העסקי הפרטי, הלא ממשלתי, הלא ציבורי, שבו יש בעיה גדולה, גם חוקית, גם התנהגותית, מי מגן עליו?

בארה"ב הבעיה אינה פתורה, הוקמו שני מרכזים להגנת סייבר, אחד בביטחון, זה ה-**NSA**, ה-**National Security Agency** ואילו האחר, המשרת את שאר הרשויות של הממשל,ה-**CSS** או **Central Security Service** שייך ל-**Homeland Security**, ומה לגבי התחום הפרטי? יש בעיה חוקית, האם בכלל רשאים להגיד לאיזה עסק פרטי מה לעשות ומה לא לעשות ואיך להגן על עצמו.

בישראל הבעיה יותר קלה מאשר במדינות אחרות; בגלל המצב שבו אנחנו חיים יש איומים כל הזמן, אני לא יודע אם באמריקה אפשר להכריח בנאדם לבנות ממ"ד בבית. מה פתאום אתה בתור ממשלה תאמר לי שאסור לי לבנות בית חדש אלא אם אתקין בו חדר מוגן בסטנדרט כזה וכזה שנקבע על ידי אנשי הצבא? בישראל זה אפשרי, העניין החוקי מוסדר, אבל צריך לשפר אותו.

לצורך ההצפנה יש צורך במחשבים מהירים, יש גם סימולטורים, כל ההתפשטות ברשת היא דבר בעל חיים משל עצמו, לעשות סימולטור לרשת אינו דומה לסימולציה רגילה שאני עושה מול המחשב שלי, זוהי תשתית, וזה עולה הון.

כבר לא מייצרים מחשבים מהירים על ידי התקנת מעבד יותר ויותר מהיר, אלא לוקחים ענן של מעבדים, שמים אותם באולם אחד, מחברים אותם זה עם זה וכשאני אומר הרבה אני מתכוון ל-10,000 או 20,000 מעבדים, שכל אחד מהם מעבד מהסוג שאפשר לקנות בחנות או הישר מהיצרנים, אבל כשיש לך 20 אלף כאלה, מתקבלת יכולת חישוב במספרים שהזכרתי.

נקודת התורפה היא התקשורת ביניהם, זו מערכת תקשורת מהירה מאוד שמקבלת מכל אחד מהם את האינפורמציה, מעבירה לשני ומנהלת את העניין הזה, גם ברמת החומרה תקשורת מהירה, וגם ברמת התוכנה.
לפני ההחלטה לבנות מחשב מהיר בישראל, בדקנו אם יש לנו יכולת כזאת. יש בעולם רשימה של 500 המחשבים המהירים ביותר בעולם, היא מתעדכנת כל הזמן, ברשימה האחרונה שיצאה אין מחשב ישראלי. המחשב הישראלי שהיה ברשימה לפני שנה, נמצא במקום ה-490 ומשהו. ברשימה האחרונה לא הופענו כלל. אז אולי אנחנו לא יודעים לבנות מחשב? ולעומת

זאת, אסור למכור לנו מה שמוגדר כמחשב מהיר. אנחנו לא חתומים על האמנה לאי-הפצת נשק גרעיני, על ה-**NPT**, ולכן לא מוכרים לנו. לעשות לבד לא עשינו, ולמכור לא מוכרים לנו.

בדקנו את העניין ואז התברר לנו ש-43% מהמחשבים המהירים בעולם נבנו על ידי חברות ישראליות.ארבעה מבין השבעה המהירים ביותר. ברמת התקשורת היו שתי חברות ישראליות שאחת קנתה את השנייה וכך נשארה אחת, זה מלנוקס, וברמת התוכנה זו חברת סקלנפי, והן בעצם בונות את המחשבים לכולם. למה לא עשינו את זה עד היום? כי לא היינו ערניים לעניין הזה.

ההמלצה הראשונה שהנחנו על שולחן הממשלה היתה למנות יועץ לאומי לסייבר שיעמוד בראש מטה לאומי לסייבר: הוא יהיה כפוף ישירות לראש הממשלה, היה ויכוח אם יוכפף ישירות לראש הממשלה או דרך המועצה לביטחון לאומי, והוחלט שלפחות בשלוש השנים הראשונות הוא יהיה כפוף ישירות לראש הממשלה ויהיה דיון בעוד 3 שנים, היועץ יקבל מספר סמכויות. מתפקידו קודם כל לעקוב אחרי המדיניות ולהגדיר. עליו לעשות מה שעשינו פה באופן חד פעמי 24 שעות ביממה. הוא ישרת את מוסדות הממשלה והוא יעשה את זה באמצעות כסף. היו לנו הרבה המלצות על תוכניות, צריך לפתח, לבנות, אבל כשאתה צובר את כל התוכניות האלה זה משהו כמו 2.5 מיליארד שקל לחומש, ז"א חצי מיליארד שקל לשנה. מתוך ה-500 מיליון האלה הוא יחזיק בכ- 100 מיליון, יש עוד 200 מיליון שהגופים השותפים לעניין הזה, קרי: הות"ת, המפא"ת והמדען הראשי בתמ"ת הסכימו להעביר, אם הוא יעביר את ה-100 שלו הם יעבירו את ה- 200 שלהם, ביחד יש 300 מיליון, וחסרים עוד 200 מיליון, ואנחנו מאמינים שנוכל להשיג אותם בגיוס מהתעשייה הפרטית, אם באמת נאפשר להם לעשות את הדברים שהזכרתי.

,החברות העולמיות הגדולות כמו **HP IBM** צ'ק פוינט, שיש להן מרכזי מו"פ בארץ רוצות להיות חלק מהסיפור הזה, הן מוכנות להשקיע כסף, בהנחה שה-300 מיליון שקל השנתיים מהממשלה עליהם כבר הוחלט אכן יועברו.

זו ההמלצה המרכזית הראשונה; הרשות לאבטחת מידע בשב"כ הסכימה, וראש השירות הסכים לקבל על עצמו את הרחבת הסמכות של רא"ם לא רק לאותן 19 תשתיות אזרחיות שנקבעו ב-2002, אלא לכל המרחב האזרחי כולו, מה שמחייב כל מיני תיקוני חקיקה שעובדים עליהם עכשיו. יש לדאוג להקמת מרכזי מצוינות באקדמיה, הקמת מרכז לחישוב-על, כי בניית מחשב כזה היא עניין אחד, אבל איך ננצל אותו ואיך נבנה את האלגוריתמים הראשונים, זה לפרק בעיה שעד היום עשינו אותה במעבד אחד, לעננים רבים של מעבדים, לשם כך צריך ידע אקדמי שעלינו ליצור, והשקעות גדולות יותר בהכשרת כוח אדם, גם באקדמיה וגם במשרד החינוך.
משרד החינוך היקצה 50 מיליון שקל משום שאי אפשר להכשיר בני אדם באוניברסיטה אם אין להם 5 יחידות בגרות במתמטיקה, פיזיקה, במקצועות הקשים.
אשר לרגולציה, ז"א, כל המנגנון של סיב"ט, על הזרועות המפקחות על הייצוא, האם מתאימים אותו לתחום הסייבר? עובדים על זה עכשיו. מה יקרה אם כבר הותקפנו? גיבויים, התאוששות ופיתוח מעטפת הגנה לאומית. לישראל יתרון בכך שאנחנו כמו אי במובן מסוים; זה חיסרון בהרבה מובנים אחרים, אבל בתחום הסייבר זה יתרון, כי כל המידע שמגיע, מגיע אלינו במספר סופי וקטן מאוד של כבלים, ואפשר להושיב עליהם מערכת הגנה לאומית שתחסום בכניסה לישראל את מרבית האיומים. אך זה לא מספיק, צריך להציב גם בקצה את מערכות ההגנה למיניהן וזה מחייב, בין היתר, פיתוח של הרבה יותר מערכות כחול לבן מכפי שאנחנו עושים היום, כי בסוף זה לא יעזור אם אני אגן על המחשב הזה ואם אני אכניס לתוכו את תוכנת ההפעלה של מיקרוסופט, אם אין לי את הקוד שלה ואני לא יודע בדיוק מה הכנסתי פנימה. או למשל השביב שאני קונה - הרי מרבית הצ'יפים היום בעולם מיוצרים בסין, אני קונה

אותו מסין ואני לא יודע מה הוכנס לצ'יפ. לכן הדבר מחייב שיתוף פעולה יותר גדול עם כל החברות האלה וגם פתיחות רבה יותר לגבי הקודים ובתוכנות שהם נותנים לנו, ובצד השני יש הבנה ובמערכות הקריטיות לנו ביותר הם מוכנים להשתמש מוצרים כחול לבן.