

הוא דיבר על הקשר שבין הגנת גוף האדם באמצעות מערכות אלקטרוניות להגנת סייבר. "נכון לסוף 2013, בגוף האדם היו 15 מערכות מצילות חיים, לא רק קוצב לב", אמר. "עד סוף העשור הנתון יצמח לכדי 800 מערכות. ברחבי העולם קיימים 20 אלף מיזמי פיתוח של מערכות תוך-גופניות, חלקם הרב נעשה באוניברסיטאות ובמסגרת מחקרים המבוצעים בישראל. מכלל הדברים הללו ניתן להבין שאייזיק אסימוב לא היה כלל סופר מדע בדיוני, מאחר שאנחנו נמצאים בעידן בו מותקנות או יותקנו על גופנו מערכות קולטות ומשדרות. יש לכך משמעות מבחינת אבטחת הסייבר. הוא הופך להיות מרכיב רביעי בצריכה האנושית. לא דחק היום בו המקור שלנו יזמין עבורנו חמאה שנגמרה".

פעילות נוסף של המטה הוא "העלאת המודעות של ארגונים ועובדים לתחום. עלינו להיערך ולהתגונן טוב יותר לסייבר".  
"הכנס הזה מוכיח שיש בישראל תעשייה שיודעת לתת פתרונות לתחום הסייבר. הרבה אנשים בארץ שעוסקים בתחום חושבים מחוץ לקופסה. יש פה הזדמנות לקדם משמעותית את נושא הגנת הסייבר, ברמת התעשייה והמדינה", ציין.

### "הסייבר הוא אב המזון הרביעי"

וייסמן אמר כי "אנחנו מצויים בעידן החדש. עד היום האדם נהג לצרוך מים, מזון ואוויר. כעת אנחנו מתחילים לצרוך גם סייבר באופן שוטף".

## השתלטות על מכונית מרחוק - בפעם הראשונה בישראל

אם חשבתם שכדי להשתלט על מערכות של רכב צריך בן אדם, הרי שבכנס הוצג איך הטכנולוגיה מאפשרת לעשות זאת בלעדינו

סלולרי. הוא הדגים איך מכשיר טלפון של מתנדב מהקהל הפך להיות "מפעיל" סלולרי, ושניים נוספים - "למנויים", והראה איך הוא יכול להאזין לכל תעבורת הקול שלהם ולגנוב נתוני מידע שנמצאים על המכשירים המשוחרים. שטרנברג הסביר, כי כדי להפוך את המכשיר ל"מפעיל" סלולרי, כל מה שצריך זה לשלם על חומרה עלות בסיסית של מאות דולרים בלבד, רדיו שניתן לתכנת אותו ותוכנה לעיבוד אותות. "אז ניתן להרים כל דבר", אמר.

הוא ציין כי גם בהשתלטות שכזו יש יתרונות: היא יכולה לבצע איכון לניצולים, לפצועים ולנעדרים באירועים רבי נפגעים, דוגמת רעידות אדמה, להרים רשתות תקשורת אזרחיות ומבצעיות, ולהפוך את הרשת ה"גנובה" לרשת חירום לכל דבר ועניין. **יוסי הטוני. צילום: קובי קנטור**



דוד שטרנברג

השתלטות מרחוק ניתן לאתר רכבים, למנוע שכחה של תינוקות בתוך כלי רכב, לעצור מכוניות אם חלילה נוסעיהן נחטפו ועוד שימושים חיוביים שונים. אחרי ש"עזב" את המכונית הראה שטרנברג כיצד הוא משתלט על רשת סלולרית והפך מכשיר טלפון נייד ל"מפעיל"

כדי להפעיל מערכות של מכונית צריך שאדם ייכנס לתא הנהג, ישם את המפתח בסוויץ' ויתניע. נכון? אז זהו שלא. דרכים חדשות מאפשרות לעשות זאת מרחוק, באמצעות השתלטות על מערכות המכונית, בלי לגעת בה פיזית.

**דוד שטרנברג**, חוקר סייבר, עשה זאת במסגרת הכנס, בפני מאות מקצועני אבטחת מידע וסייבר. שטרנברג השתלט מרחוק על מכונית מסוג מוסטאנג, ככל הנראה באמצעות פריצה למערכות לווייניות המקושרות למכונית. הוא הסביר שיש שתי דרכים נוספות לעשות זאת, שתיהן פיזיות. לדבריו, תעשיית הרכב הכניסה מערכות מיחשוב למכוניות כבר לפני קרוב ל-20 שנה, אולם לא פיתחה להן במקביל מערכות הגנה ואבטחת מידע. כך, נוצר מצב בו ניתן להשתלט על המערכות לפתיחת הדלתות, החלונות ועוד. לשאלת המנחה אמר שטרנברג כי לפני שהחל להשתלט על מכוניות, הוא עצמו חקר את הנושא במשך כמה חודשים, כאשר לאחר מכן נדרש לו יום-יום וחצי על מנת לחדור ולהשתלט על מכוניות מסוגים אחרים.

אל מול הקהל המשתאה הראה שטרנברג כיצד הוא יכול לגרום לכך שהמכונית "חושבת" שהמנוע שלה התחמם ובאמצעות זאת להפעיל את מערכות הקירור. עוד הוא הראה כיצד הוא מגדיל את מהירות סיבובי המנוע או מהירות הנסיעה, מפעיל את האיתות ומבצע השתלטויות על מערכות נוספות ברכב. שטרנברג אמר כי יש לכך אמנם צדדים שליליים, אולם גם יתרונות: באמצעות



אבי וייסמן מדגים כיצד הוא משתלט על המכונית