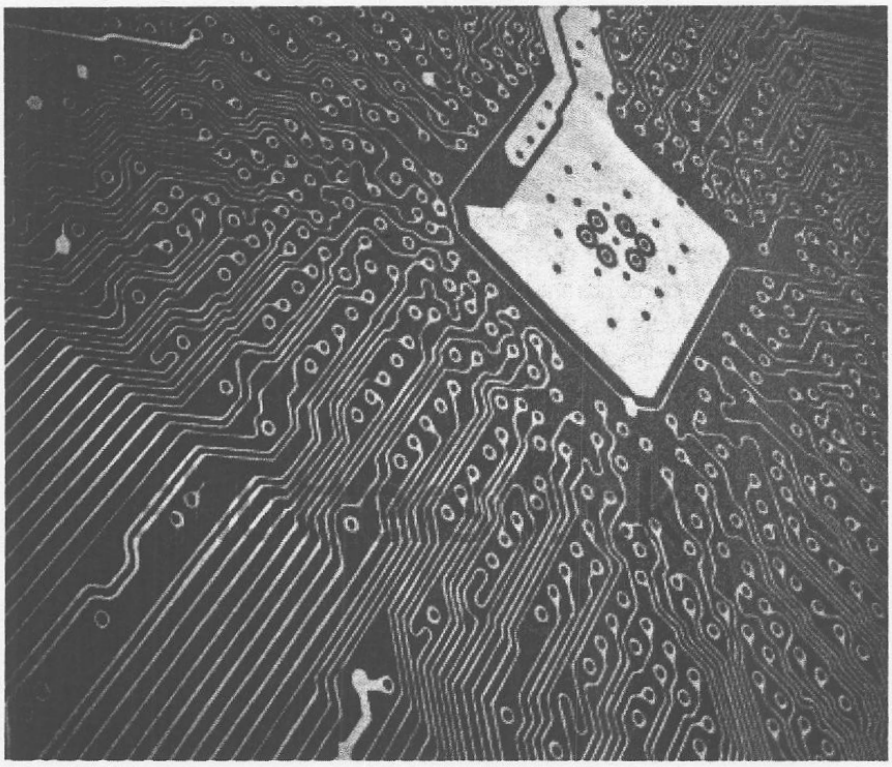
דרוש: מהנדס ייעודי להגנת התעשייה

התשתיות הלאומיות מוגנות על ידי המדינה מפני מתקפות סייבר - אבל מה לגבי התעשייה? גבי סיבוני מאמין שצריך לייסד בישראל מקצוע חדש - כזה שיוכל להתמודד עם המציאות הקיברנטית

מאת ד"ר גבי סיבוני



איור: Shutterstock

תומה שפיצוץ צינור הגז טרנס-סיביר ביוני 1982 הייתה המתקפה הקיברנטית המתועדת הראשונה. תיעוד המופיע בספרו של תומס ריד, מי שהיה בשנים ההן יועץ מיוחד לבטחון לאומי של הנשיא האמריקני רונלד רייגן.

תומס ריד טוען שסוכני ה-CIA הצליחו לטפל בציוד בקרה קנדי עליו הניחו הסובייטים את ידם ובו עשו שימוש לצרכי ניהול ובקרת הפעלת צינור הגז. הפעולה שיבשה את מערך בקרת הלחצים בצינור וכתוצאה ארע פיצוץ רב עוצמה שאף נצפה על ידי לווייני הריגול האמריקנים.

אם בשנים ההן היה השימוש במערכות בקרה מבוקרות מחשב נחלתן של מדינות וארגונים מעטים, הרי שעתה ועם התפתחות כוח המחשוב ותקשורת הנתונים, רובן המכריע של המערכות התעשייתיות נשלט ומבוקר באמצעות מערכות בקרה ממוחשבות.

התפתחות זו גרמה למדינות להיות חשופות לפגיעה במרחב הקיברנטי שלהן על ידי גורמים שונים ומגוונים בהם: מדינות עוינות, ארגוני טרור, גורמים פלילים ואף פרטים הפועלים מתוך אתגר אישי או מתוך מניעים אנרכיסטיים. למעשה רוב המערכות בחברה מפותחת תלויות בתשתית מחשוב ומידע. התלות ההולכת וגדלה בטכנולוגיית מידע ותקשורת גורמת לכך שפגיעה במערכות מחשוב ובקרה של תהליכים ומתקני תעשייה עלולים לגרום לפגיעה פיזית של ממש. ניתן להעריך כי פני איומים אלה ילכו ויתגברו בעתיד ללא היכר.

חשופים בשטח

עד לפני שנים לא רבות התעשייה (הפרטית והציבורית) הייתה מוגנת על ידי המדינה, למשל: תחנת כוח, מתקן התפלה, או כל מתקן תעשייתי אחר היו חשופים לפגיעה פיזית שלא בגין תאונה, רק באם המדינה הייתה נקלעת למלחמה פיזית של ממש, תפקידה של המדינה היה להבטיח את ההגנה על התשתיות, המוסדות הכלכליים, מפעלי תעשייה ועוד. מתקני התעשייה במדינה היו מוגנים באמצעות המערכות הצבאיות והבטחוניות שהגנו על המרחב (הטריטוריה) מפני מפגעים בעלי כוונות זדון.

עתה, עם התפתחות הסביבה הקיברנטית, נפרצו הגבולות ואנו עדים לשינוי דרמטי.

מתקני תעשייה ותשתיות חיוניות שמוקמו הרחק מגבולות העימות, חשופים לפגיעה קיברנטית חסרת גבולות הן במערך המחשוב הארגוני, וחמורה מספר מונים, לפגיעה במערך הבקרה של התהליכי הייצור. לראשונה ניתן לפגוע בתעשייה וביכולות הכלכליות ללא הפעלת כוח פיזית.

מדינת ישראל הקימה רשות ייעודית להגנה על תשתיות לאומיות קריטיות. אלה כוללות מספר עשרות בודד של מתקנים ותשתיות חיוניות. אף שזו אינה עוסקת בכלל בהגנת כלל מתקני התעשייה, הרי קיימת מגמה להגדיל את הרגולציה ולחייב את הסקטור התעשייתי לספק פתרונות בתחום הבטחון ואבטחת תהליכי הייצור מפני פגיעה בזרון. לאור זאת, מתפתחת ההבנה שהסקטור העסקי והתעשייתי יידרש לעסוק לא רק בהיבטים המקצועיים הטהורים של העשייה, אלא שעליו לעסוק גם בהגנה ובבטחון תהליכי הייצור ושימור היכולת להמשכיות עסקית מול תרחישי ייחוס רלבנטיים.

דיסציפלינה חדשה

בתחומי הידע ההנדסי-מדעי התעשייה התפתחו במהלך השנים שתי דיסציפלינות ידע שונות ומקבילות אחת בהקשר לתחום ההנדסי תעשייתי שהכשיר מהנדסים שהתמחו בתהליכי ייצור בתעשייה, בבקרה של תהליכים, בייעול תהליכי וניהול רצפת הייצור, ועוד היבטים של המערך הייצור התעשייתי. והשניה הנה דיסציפלינה שהתפתחה מתחום מדעי המחשב ונוגעת בעיקר להיבטים של אבטחת מערכות מידע. מהנדסים או מומחים אלו באו בדרך כלל מתחום מדעי המחשב והתמקדו בטיפול באבטחת המידע במחשוב הארגוני. אלה לא עסקו ברוב המקרים באבטחה של תהליכי הייצור ומערך הבקרה המפגר באופן משמעותי אחרי אבטחת מערכות ה- IT הארגוניות.

תמונת המצב שתוארה, מייצרת צורך לדיסציפלינה עדכנית שתוכל לספק הכשרה למהנדס מסוג חדש. כזה שיוכל להיות בעל ידע הנדסי בתחום התעשייה והייצור מצד אחר, ובעל ידע בתחום האבטחה של מערכות בקרה תעשייתיות מצד שני. כיום, מהנדסים כאלה אינם קיימים לא רק בארץ אלא בעולם, שהרי מגמת התפתחות האיום האמור הנה מגמה חדשה יחסית. בישראל, מהנדסים אלה יוכלו להשתלב במאות חברות תעשייתיות וחברות ייעודיות שיספקו שרות לחברות תעשייתיות נוספות. לדוגמה: חברות בתעשיית המזון, התרופות, הכימיקלים, חברות תחבורה, ייצור אנרגיה, מתקני טיפול במים, התפלה, שפכים, ובכלל כל מתקן ייצור תעשייתי יידרש למענה בתחום הבטחון וההגנה על מערך הייצור שלו מפני תקיפה קיברנטית.

הכשרת מהנדסים בדיסציפלינה בין תחומית הנה אתגר לא מבוטל והיא שונה מכל מתכניות הנדסה המוכרות בישראל ואף בעולם. היכולות הטכנולוגיות של מדינת ישראל, לצד הצורך להוביל את תחום הגנת הסייבר בשל איומים מפציעים, מאפשרים מצע ייחודי לפיתוח תחום הנדסי חדש ועדכני אותו יש לפתח ולשכלל.

הקמה של תכניות אקדמיות, פיתוח של ידע חדש והכשרת מהנדסים בתחום, יספקו תרומה משמעותית למדינת ישראל על ידי מתן מענה לצורך אקוטי מתפתח, חדשני וארוך טווח. פעולה זו אף תקבע את מיצובה של ישראל כמובילה עולמית בתחום הסייבר. ◉

"היכולות הטכנולוגיות של מדינת ישראל, לצד הצורך להוביל את תחום הגנת הסייבר בשל איומים מפציעים, מאפשרים מצע ייחודי לפיתוח תחום הנדסי חדש ועדכני אותו יש לפתח ולשכלל"

ד"ר גבי סיבוני הינו ראש תכנית: צבא ואסטרטגיה וראש תכנית לוחמת סייבר במכון למחקרי בטחון לאומי