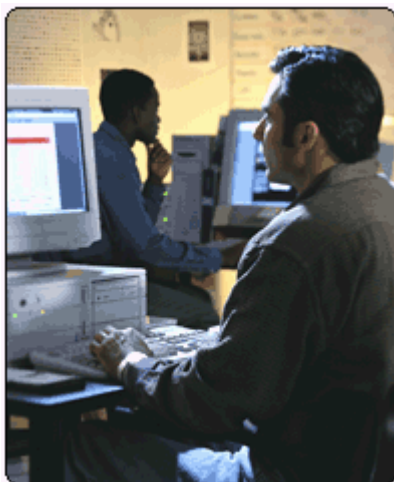


- עבירות המחשב וחדירה לאתרי האינטרנט הם רק היבט אחד של עידן המידע, שבו מערכות מחשב שולטות כמעט על כל אירוע בחיינו.
- היבט נוסף עוסק בפגיעה במערכות החיוניות לקיום חברה מודרנית.
- האופי הגלובאלי של תקשורת בין מחשבים מאפשר חדירה מכל מקום בעולם למערכות מחשב חיוניות, וגרימת נזק רב בגלל "אפקט הדומינו".

רב-פקד מאיר זוהר, ר' צוות עבירות מחשב

כיום קיימים באינטרנט מאות אתרים, שבהם ניתן לקבל הסבר מקצועי, תוכנות וכלי פריצה, המאפשרים כמעט לכל אחד לפרוץ למחשבים. קיים חשש, כי לא רק "האקרים" מקצועיים יפרצו למחשבים אלא גם נערים וילדים תמימים שעשו זאת מתוך סקרנות ואתגר אינטלקטואלי. כאשר עסקאות כספיות רבות מאוד נערכות באמצעות האינטרנט, טרנסאקציות בין גופים מסחריים ופינאנסיים מבוצעות ברשת קניות בכרטיסי אשראי, ומידע פינאנסי ומסחרי נשמר במדיה האלקטרונית, קיים חשש, כי גורמים עבריינים, המתחילים להבין את הפוטנציאל הגלום ביכולת המיחשוב, ינצלו את אותם צעירים, וירתמו את יכולתם הטכנולוגית לביצוע מעשי פשע. ה-F.B.I מסר, כי לא רק החברה צועדת לקראת עידן טכנולוגי ממוחשב אלא גם עולם הפשע, אשר משתמש במחשבים ליצור קשר עם שותפים לפשע, לגנוב מספרי כרטיסי אשראי, לשדוד בנקים



ולהצפין מידע על עסקיהם האפלים. האינטרנט והעידן הטכנולוגי נותנים לפושעים כלים חדשים לביצוע עבירות קלאסיות כמו מרמה, גניבה וזיוף, וכן כלים לביצוע פשעים כנגד מערכת תשתית, חיונית, המסכנת את החברה כולה.

החדירה אינה פעולה המתבצעת סתם כך בעולם וירטואלי. תוצאותיה יכולות להיות כואבות וממשיות מאוד, כמו גניבה, הרס ושינוי מידע ארגוני. לפעולות אלו יכולות להיות גם תוצאות מוחשיות, המסכנות חיי אדם, כמו במקרה של ההאקר מאיטליה ששיתק את מערכות בקרת הטיסה של שדה התעופה במסאצ'וסטס או האקר ששיתק את מרכזיות החירום של המשטרה בפלורידה.

## < משאבים חיוניים

עבירות המחשב וחדירה לאתרי אינטרנט הם רק היבט אחד של עידן המידע. היבט נוסף ורחב יותר דן בפגיעה במערכת החיוניות לקיום חברה מודרנית. בעידן המידע, שבו מערכות מחשב שולטות כמעט על כל אירוע בחיינו, ניתן לשתק מדינה שלמה ע"י הפלת מערכות מחשב חיוניות ו/או שיבוש המידע האגור בהן. טכנולוגיות המידע הביאו לעלייה דרמטית באפקטיביות ובתפוקה של כל ענפי המשק. עם זאת, התלות במחשבים יצרה חולשות וסכנות

חדשות. כל מערכות התשתית החיוניות תלויות במחשבים ובתקשורת בין מחשבים.

טלפוניה - תקשורת קולית, תקשורת נתונים ותשדורות פקס חיוניים לחברה מתקדמת. שירותי חירום כמו משטרה, צבא ומכבי אש תלויים בקווי התקשורת.  
חשמל - אספקה שוטפת של חומרי גלם (גז, פחם, מים), אספקת חשמל סדירה לבתים, לעסקים, למוסדות ולארגונים, טיפול שוטף ממוחשב, סנסורים ממוחשבים.  
מים - אספקת מים, מערכות סינון וטיהור, מערכות ביוב, טיפול שוטף ממוחשב, סנסורים ממוחשבים.  
מערכות פיננסיות - בנקים, בורסה, כרטיסי אשראי, כספומטים - כולם מוכוונים מחשב.  
תחבורה - כבישים, מסילות ברזל, נמלים ושדות תעופה - ראדר ובקרת טיסה, תאורת כבישים ורמזורים כולם מוכוונים מחשב.  
ממשל תקין - שירותי ממשלה וגופים ממשלתיים: ביטחון, משטרה, מיסים, שירותי עירייה בתי-ספר וגנים.  
מידע חיוני - רשומות בתי-חולים, רשומות חיילי מילואים ובעלי תפקיד בעתות חירום.

## סכנות

האופי הגלובאלי של תקשורת בין מחשבים מאפשר חדירה למערכות מחשב חיוניות מכל מקום בעולם, וגרימת נזק רב בגלל אפקט ה"דומינו" של המערכות הללו, התלויות אחת בשנייה. מיכאל וואטיס, סגן המנהל הכללי של ה-F.B.I בטענתו בפני ועדת הכלכלה של הקונגרס לפני כשנה ציין, כי עיקר הסכנה אורבת מצד טירוריסטים, מדינות עימות ומודיעין זר, אך העלייה בשיעור מפעילי המחשב ושכיחות הכלים לגרימת הרס (וירוסים, סוסים טרויאניים, תולעים, פצצות לוגיות, רחרחנים, גלי רדיו, גלים אלקטרומגנטיים) מאפשרת גם להאקרים, לעובדים ממורמרים, לאנשי הפשע המאורגן ולקבוצות פוליטיות קיצוניות לגרום נזק רב.  
קבוצת האקרים שמושב בדאלס, טקסס, חדרה למערכות מחשב של מספר חברות תקשורת מקומיות, ושלפה פרטים על לקוחות, על מספרי כרטיסי אשראי ועל מספרי טלפון חסויים, וגרמה נזק של 500 מיליון דולר. ההאקרים שתלו רחרחנים וביצעו האזנות סתר על קווי התקשורת. מומחיות ההאקרים הללו לא נפלה מזאת של מומחי החברות עצמן, והם יכלו לבצע פעולות פליליות גם בקווי התקשורת הלאומיים.  
לאחרונה פורסם, כי עברייני מחשב השתלטו על לווין של צבא בריטניה, הסיטו אותו ממסלולו, ושיגרו באמצעותו איומי סחיטה.  
כן פורסם, כי האקרים מרוסיה פתחו במתקפה על מחשבי הפנטגון.

מאמר שפורסם בחודש יוני בעיתון JERUSALEM REPORT העלה תסריט דמיוני של יום כיפור אלקטרוני, ולפיו ארגוני טירור ו/או האקרים להשכיר מפילים את מערכות המחשב החיוניות בישראל. לפי תסריט זה, נפגעו המחשבים של חברת החשמל, של המוביל הארצי ושל חברות הטלפוניה. גם מחשבי בקרי הטיסות החלו להשתולל, ולווייני הריגול של ישראל וארה"ב החלו לשדר שירים. באותה שעה פתח אלמוני באזור הקריה מזוודה, שהחלה להקרין גלים אלקטרומגנטיים, שהפילו את כל מערכות המחשב בבניין משרד הביטחון הסמוך. לטענת העיתון, אין מדובר בתסריט דמיוני, אלא באפשרות למלחמת אינפורמציה, העלולה להתממש ע"י גורמים עוינים. ישנן שמועות באינטרנט, שלאחר פלישת עירק לכווית, רכשו האמריקאים מרומניה מערכת ראדר מרכזית שנמצאת בשימוש הצבא העירקי, ולאחר לימוד המערכת שתלו ירוס למדפסות (באמצעות קווי הטלפון או גירסת עדכון נגועה) ששיבש את קריאות הראדר. שמועה עקשנית אחרת טוענת, כי הצרפתים שתלו באג במערכות הממוחשבות במטוסי המיראז' שנמכרו לעיראקים, ומטוסי האוייב לא זיהו את מטוסי בעלות הברית במלחמת המפרץ.

לטענת העיתון, מתקפה כזאת על מדינת היי-טק כמו ישראל, עלולה לגרום נזק גדול יותר מאשר הטילים של סאדם חוסיין ו/או כל נשק קונבנציונאלי אחר. באופן פראדוקסאלי, דווקא מדינה מפותחת פגיעה יותר למתקפה בגלל התלות הגבוהה במחשבים.  
לטענת וואטיס אין מדובר בתרחישים בדיוניים, והסטטיסטיקה מדגימה את חולשות מערכות אלה בפני לוחמת המידע:

● מחקר משנת 1998 של COMPUTER SECURITY INSTITUTE-CSI ציין עלייה של כ-16% (משנת 1997) בחדירות למערכות מחשב של חברות מסחריות, אשר גרמו לנזקים של מיליוני דולרים (136 מיליון בשנת 1998 לעומת 100 מיליון דולר בשנת 1997).

● דיווח של COMPUTER EMERGENCY RESPONSE TEAM-CERT מלמד, כי רוב החדירות למחשבים נעשו לאחרונה באמצעות SCRIPT אוטומטי, המאפשר תקיפה של מספר גדול של מחשבים בעילות רבה יותר.

● מחקר שנערך על שלוש מאות חברות באוסטרליה דיווח על התנסותן של 37% מהחברות

בפגיעה כלשהיא באבטחת המידע שלהן בשנת 1997 כאשר 57% מכלל חדירות המחשב בוצעו כלפי בנקים ומוסדות פינאנסיים.

סקר שנערך בשנת 1996 ע"י AMERICAN BAR ASSOCIATION בקרב אלף חברות אמריקאיות הראה, כי כ-48% התנסו במעילות באמצעות מחשב במשך חמש שנים. החברות דיווחו על הפסד ממוצע של 2-10 מיליון דולר בחמש שנים.

לפי ההערכה של DEFENSE INFORMATION SYSTEM AGENCY - DISA משנת 1996 אירעו כ-25 אלף מקרי תקיפה וניסיונות חדירה למערכות ממשלתיות וצבאיות בשנת 1995. לפי ההערכה זו, מקרי התקיפה עלו בעקביות כל שנה, וצפוי שמגמה זו תימשך גם בשנים הבאות.

ה-F.B.I דיווח על עלייה משמעותית בחקירת מקרי חדירה למחשבים ובהעמדת עבריינים לדין. מספר התיקים עלה ב-133% מראשית 1997, מספר המעצרים עלה ב-950%, ומספר ההרשעות עלה ב-88%.

גופים ביטחוניים בארה"ב, בעידוד הנשיא קלינטון, השקיעו מיליוני דולרים בהקמת גופי חקירה, בפיתוח שיטות וכלים להתמודדות במלחמת המידע ובשיתוף פעולה בין סוכנויות החקירה והגופים האזרחיים העוסקים בנושא.