

## מאת שחר גייגר מאור

**גליון 40, מרץ 2013**

## האינטרנט



[מקור: [computers4business.com](http://computers4business.com)]

אי אפשר לדבר על תופעת ההאקרים ומניעיהם מבלי להתייחס לרשת האינטרנט, אותה קרקע פורייה עליה הם פועלים תוך ניצול חולשות אנושיות. בשנת 1945 פרסם ד"ר ואנבר בוש (Bush) מאמר בירחון אטלנטיק בו טען כי הבעיה הגדולה ביותר העומדת בפני מדענים היא עודף המידע. הפתרונות, לטענתו, היו שניים: המיקרופילם והשפופרת הקתודית. הראשונה מצמצמת מידע עצום לגודל קטן והשנייה מאפשרת

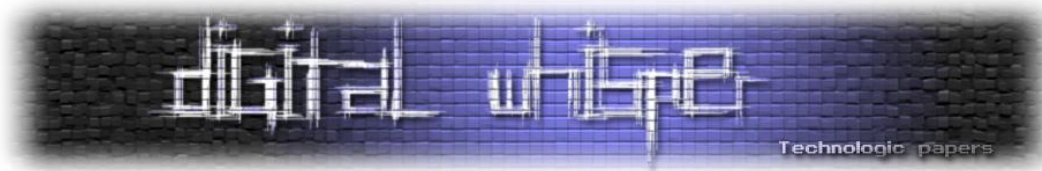
הצגת מידע על גבי מסך זכוכית. עוד כתב בוש, כי המשתמשים יוכלו לעבור ממסמך אחד לשני באמצעות "נתיבים" (trails). למערכת שהייתה אמורה לאפשר זאת קראו Memex אך היא לעולם לא נבנתה.<sup>9</sup> קל לראות שרעיון הנתיבים דומה להפליא לרעיון הרשת העולמית (WWW) שיעברו עוד שנים רבות עד שתופיע בחיינו. שנות החמישים והשישים של המאה ה-20 היו שנים של חשש ניכר מפני תוצאותיה של מלחמה גרעינית וחשוב יותר, המשכיות החיים לאחר מהלומה גרעינית. אחד הרעיונות המרכזיים שעניינו את הצבא האמריקאי היה תקשור ישיר בין יחידות צבאיות ללא מעבר דרך רשת שליטה מרכזית וזאת באמצעות טכנולוגיית "מיתוג חבילות" (Packet Switching) בניגוד לטכנולוגיית המעגלים האנלוגיים.<sup>10</sup>

בשנת 1968 החליטה ARPA, גוף השייך לפנטגון, לבנות רשת מחשבים שתקשר מספר פקולטות אוניברסיטאיות שעסקו במחקרים עבור משרד ההגנה. כך נוסדה ה-ARPANET שהייתה מבוססת על המצאת "מיתוג החבילות". בשנת 1973 החליטו ARPANET לחבר פרוטוקול חדש המתאר איך מחשבים ברשת צריכים לדבר אחד עם השני ונקבעו שני עקרונות מרכזיים: רשתות מחוברות = internetwork או בקיצור - אינטרנט. העיקרון השני: כל סוגי התקשורת יקבלו יחס זהה. מכאן, החלו לעבוד על שני תקנים מרכזיים: TCP & IP, שני פרוטוקולים הנחשבים עד היום למרכזים ביותר בתקשורת אינטרנט. על פי פרוטוקולים אלה, הרשתות השונות יחוברו באמצעות רכיבי חומרה הנקראים "שערים" (gateway). תוכנית זו הייתה גמישה דייה כדי לאפשר חיבור רשתות תקשורת שונות ועמידה מספיק כדי לאפשר גידול מהיר. מכאן הייתה ההתפתחות מהירה. בשנת 1971 ריי טומלינסון (Tomlinson), מהנדס בהכשרתו, המציא את תוכנת הדואר האלקטרוני הראשונה והשתמש בסימן "@" כדי להפריד בין השולח לכתובת הרשת שלו.<sup>11</sup> בשנת 1982 החלו לצמוח רשתות תקשורת מתחרות ל-ARPANET (שבצמחה פוצלה לרשת צבאית ולרשת אזרחית).

<sup>9</sup> The Atlantic Magazine, *As You May Think*, <http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/>

<sup>10</sup> Paul Baran: Introduction to Distributed Communications Networks (Rand Corporation, 1964): [http://www.rand.org/pubs/research\\_memoranda/2006/RM3420.pdf](http://www.rand.org/pubs/research_memoranda/2006/RM3420.pdf)

<sup>11</sup> About.com - Investors, History of Email & Ray Tomlinson, <http://inventors.about.com/od/estartinventions/a/email.htm>



בסוף שנות ה-80 של המאה ה-20 אישר הקונגרס האמריקאי תקציב לבניית רשת חדשה ומהירה (NSFNET). ב-1990 נסגרה ה-ARPANET ונושא האינטרנט הועבר לקרן הלאומית למדעים. לקראת סוף שנות ה-80 היו כבר כמה מיליוני מחשבים מחוברים לרשתות התקשורת והאינטרנט עצמו כלל יותר מ-800 רשתות ויותר מ-150 אלף משתמשים רשומים אך עדיין החיבור והשימוש ברשת היו מסורבלים ולא נגישים.

בשנת 1990 טים ברנרס לי החל לכתוב תוכנה שתהפוך את הדיאלוג והחיבור לרשת לפשוטים יותר. הוא נתן לה את השם World Wide Web הידוע בקיצור WWW. התוכנית הייתה פשוטה, ונועדה "לשבת" מעל האינטרנט ולהשתמש בפרוטוקולי תקשורת וטכנולוגיית החלפת החבילות שלה. מכאן יצר לי את הדפדפן הראשון, הפך את מחשבו למחשב מארח ויצר את אתר התוכן הראשון<sup>12</sup>. בתחילת 1993 נאסר ע"י ממשלת ארה"ב לערוך שימוש מסחרי ברשת (דבר הנראה דמיוני היום) והשימוש ברשת חייב קבלת היתר מיוחד שהיה שונה מהסכמי השימוש המוכרים לנו היום בהיותו נגד שימוש מסחרי.

בנובמבר 1991 הציעה הקרן לניהול מדעים בארה"ב הצעה לסגור את NSFNET ולהחליפה ברשתות מסחריות ומתחרות. באפריל 1995 נסגרה NSFNET והאינטרנט הפך למיזם של הסקטור הפרטי. ביוני 1990 כתב אל גור, סגן נשיא ארה"ב לשעבר, מאמר במדור Washington post @ outlook ובו קבע בפעם הראשונה את המונח information superhighway - אוטוסטדרת המידע<sup>13</sup>. עם הזמן הפכה הטכנולוגיה את הגלישה באינטרנט לפשוטה ונגישה ומכאן האינטרנט לא עצר. עד היום הוא מגלם בתוכו אפשרויות אין סופיות לרווחים כספיים והשגת מידע חיוני. את זה יודעים גם ההאקרים, אשר הפכו לאיום על מערכות החיים, הכלכלה, התשתיות והביטחון<sup>14</sup>.

## מהי חדירה למחשב?

בדיון על מניעי חדירה למחשבים צריך להתחיל בלהגדיר מהי חדירה למחשב ואיך מתייחס אליה החוק. המונח "האקר" לא היה מונח שלילי בשנות האינטרנט והמחשוב המואץ של המאה הקודמת, אפשר לומר שרק עם התפתחות המסחר, הפצחנים גילו את הפוטנציאל הכלכלי "בפשיעה הנקייה" כביכול ולצידם הפכה גם מלחמת הסייבר לכלי מרכזי בפעילותן של מדינות, ארגוני טרור, אנשים פרטיים וכו'.

עבירות בעולם המחשוב העמידו בפני החברה צורך להגדיר מהו פשע ממוחשב ומהו איום ממוחשב ובלשונה של השופטת ברלינר: "לאחר החדירה למחשב לא נותרים סימנים, אין רסיסי זכוכית או מנעולים

<sup>12</sup> CERN, The website of the world's first-ever web server, <http://info.cern.ch/>

<sup>13</sup> Netvalley, Roads and Crossroads In The Internet History, [http://www.netvalley.com/internet/history\\_of\\_internet.pdf](http://www.netvalley.com/internet/history_of_internet.pdf)

<sup>14</sup> John Cassidy: Dot.com (Convention on Cybercrime- council of Europe, Budapest, 23.11.2001), <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

מעוקמים, ובהעדר סימנים לפריצה גילוי עבירות כגון אלה מחייב מיומנות טכנית גבוהה ומוחות מתוחכמים לא פחות מאלה של מבצעי העבירה<sup>15</sup>. בשורות הבאות נבאר את ההגדרות למונח חדירה למחשב וכן מספר מושגי יסוד במלחמת הסייבר.

בשנת 1995 נחקק חוק המחשב ובו הוגדרו סנקציות פליליות לעבירות מחשב אשר חולקו ל-3 סוגים ומגדיר מושגים מרכזיים לעניין זה<sup>16</sup>:

- עבירות רגילות בהן נעשה שימוש במחשב (כגון זיוף, מרמה וכדומה).
- עבירות בהן נפל בעל מחשב קורבן לעבירה פלילית בה נעשה שימוש במחשב שלו (דוגמאות: שיבוש והפרעה לפעולת המחשב, אחסנת מידע כוזב, הפצת וירוסים, חדירה לדואר אלקטרוני).
- עבירות בהן המחשב הוא אמצעי לביצוע העבירה ומהווה הראייה המרכזית נגד חשודים בעבירה פלילית מכל סוג.

בשנים האחרונות נוסף מימד נוסף לחדירה למערכות מחשב והוא "מלחמת הסייבר" שלמרות שמקבלת לגיטימיות מגופי ממשל (תלוי מי התוקף ומי המגן כמובן) הרי היא פעילות האקרית לכל דבר. המושג Cyberspace אינו חלק מהטבע ומורכב מכל הרשתות הממוחשבות בעולם ומכל נקודות הקצה שמחוברות אל אותן רשתות ונשלטות באמצעות פקודות העוברות בהן<sup>17</sup>.

## הגדרת מושגי הייסוד החשובים בהקשר של חדירה לא חוקית למחשבים

דיון על פריצה למערכות מחשב מחייב אותנו לעשות סדר ולהגדיר בצורה ברורה מספר מושגי יסוד שיחזרו ויעלו כאן בעמודים הבאים משני צידי המתרס: מי הם הפורצים? ולכן?

חשוב לציין כי במסגרת סקירה קצרה זו נתייחס למושגים נבחרים בלבד בעולם הפריצות למחשב. יודגש, כי עולם תוכן זה עתיר במושגים ובביטויים ייחודיים לו ויש חשיבות רבה לקריאה נוספת לצורך הבנה טובה יותר של הגורמים והאמצעים שבאמצעותם ניתן לפרוץ למחשבים. כמו כן חשוב להרחיב ולהכיר את סוגי ההתקפות אשר מבוצעות כנגד רשתות מחשבים יום יום ברחבי העולם.



ה"פריקר", ה"קראקר" וה"האקר":

**Phreaking**<sup>18</sup> - אומנות הפריצה למערכות ומרכזיות טלפוניה. על פי הגדרה רחבה יותר מדובר בפריצה למערכות תקשורת כלשהן. היו זמנים בהם פריקינג

[מקור: [dearestscooter](http://dearestscooter)]

<sup>15</sup> עפ 071227/01, מדינת ישראל נגד אהוד טנבאום, עמ' 6.

<sup>16</sup> חוק המחשבים, התשנ"ה - 1995.

<sup>17</sup> ליאור טבנסקי - לחימה במרחב הקיברנטי: מושגי יסוד - צבא ואסטרטגיה / כרך 3 / גיליון 1 / מאי 2011

<sup>18</sup> The Free Dictionary, **Phreaking**, <http://encyclopedia2.thefreedictionary.com/Phone+phreaking>

נחשב לפעילות כמעט מכובדת בקרב ההאקרים. הסכם ג'נטלמני לא חתום בין הפורצים למיניהם התיר פריצה למערכות טלפוניה לשם הסקרנות האינטלקטואלית, אך אסר גרימה של נזק ממשי. מצב זה לא שרד יותר מדי זמן עם הופעת קבוצות פריקרים פרועות אשר פגעו פרצו למערכות טלפוניה לשם השגת רווח וגרמו, אגב כך, לנזק ללקוחות, לעצמם ולעמיתיהם. דוגמא לכך ניתן למצוא בנוף המקומי בפרשת האחים באדיר, אשר הורשעו בבית משפט בתחילת שנות האלפיים בפריצה למרכזיות טלפוניה וגניבת שיחות בסכום כולל של כ-20 מיליון שקלים.<sup>19</sup>

**Cracker**<sup>20</sup> - אדם שפורץ את מעגל האבטחה על מערכת מסוימת. הביטוי הומצא על ידי האקרים בשנת 1985 כדי לתאר התייחסות לא נכונה אליהם מצד עיתונאים. הביטוי מכיל בתוכו בוז וסלידה מהצורה הוונדליסטית שבה נעשית הפריצה למחשב. האקרים מציבים עצמם מעל לקראקרים ומצפים מעצמם וחבריהם "ליותר" מאשר "סתם" פריצה גסה למערכות.



**Hacker**<sup>21</sup> - מקור המילה באנגלית הוא בעל מקצוע, "המבקע" (hack) עצמים או משטחים באמצעות גרזן. בעולם המחשבים והתכנות מדובר באדם אשר נהנה לחקור את גבולות התוכנה ומערכות המחשב. המושג הוכנס לשימוש בתחום מדעי המחשב ככל הנראה

בשנות ה-60 של המאה העשרים במכון הטכנולוגי של מסצ'וסטס (MIT), אשר בה תוארו שני טיפוסים של סטודנטים: "tool" - סטודנט רגיל אשר מגיע לשיעורים ולומד בצורה סבירה, "hacker" - סטודנט שהוא בדיוק ההיפך. האקר לפי MIT העביר את רוב לילותיו בפריצה למחשבים וחקירה שלהם.<sup>22</sup> האקר מתואר כמתכנת בעל יכולות גבוהות מהממוצע ואף כמומחה אשר נהנה מחיפוש דרכים יצירתיות לגלות את דרכי הפעילות של מערכות המחשב. לעתים המושג "האקר" ניתן כשם תואר לאנשים חקרניים וניתן למצוא אותו בהשאלה גם בעולמות תוכן שאינם קשורים למחשב. ההקשר בו מתואר האקר הוא חיובי ברובו. על פי "מילון ההאקרים החדש" בעריכת אריק ריימונד (שממנו מצוטטים המושגים "האקר" ו"קראקר"). האוריינטציה שיש להשתמש במונח "האקר" צריכה להיות חיובית, בעוד שהמונח "קראקר" מתייחס לצד השלילי והנחות של פריצה למחשבים.

חשוב לציין כי רובנו חוטאים בהתייחסנו לכל פורצי המחשבים המזיקים כ"האקרים" ולא "קראקרים". מכיוון שאין מטרטנו במאמר זה לשנות את התפיסה הרווחת בתחום, נתייחס בביטוי "האקר" כשם כללי לכל פורץ למחשב באשר הוא ללא תלות במהות הפריצה.

<sup>19</sup> הארץ, האחים בדיר הורשעו בחדיירה למחשבים, <http://www.haaretz.co.il/misc/1.731648>

<sup>20</sup> Eric S. Raymond, The New Hacker's Dictionary, 163, (The MIT Press, VERSION 4.2.2, 20 AUG 2000)

<sup>21</sup> Eric S. Raymond, The New Hacker's Dictionary, 310, (The MIT Press, VERSION 4.2.2, 20 AUG 2000)

<sup>22</sup> Brian Harvey, Computer Hacking and Ethics -Appendix A: What is a Hacker? (University of California, Berkeley, 1985)



## סקירה היסטורית של אירועים חשובים בתחום הפריצה למחשבים

אירועי פריצה וחבלה במחשבים או ברשתות תקשורת, בין אם אמצעי המחשוב משמשים כמטרה מרכזית ובין אם הם משמשים כאמצעי לפגיעה במערכת אחרת, החלו לצוץ לאחר הופעת אמצעי המחשוב עצמם. בעוד שמחשב המודרני הומצא, לפי חלק מהגרסאות, עוד בשנת 1936<sup>23</sup>, חדירות וחבלות מחשב החלו לצוץ מאוחר יותר, כשמחשבים נעשו נפוצים ומוכרים גם מחוץ למעבדות הפיתוח וזמינים, למעשה, כמטרות.

### ההתחלה

ההתקפות הראשונות על מחשבים היו התקפות פיסיות על מקום מושבם של מחשבים אלה. בין השאר אפשר למנות מקרים מוכרים כדוגמת המקרים הבאים:

- הסופר Thomas Whiteside אסף מספר אירועים המתארים התקפות על ציוד מחשב<sup>24</sup>. בעוד שחלק מההתקפות כונו ישירות במטרה לפגוע בציוד, חלק אחר הביא לנזק רק בצורה עקיפה:
- 1970, אוניברסיטת ויסקונסין בארה"ב. פצצה שמתפוצצת בקמפוס הורגת עובר אורח אחד, פוצעת שלושה נוספים וגורמת לנזק של 16 מיליון דולר למידע המאוחסן על מחשבים באתר.
- 1972 בניו-יורק. אדם תוקף ליבה מגנטית של מחשב מסוג Honeywell<sup>25</sup> באמצעות חפץ חד וגורם לנזק של 580 אלף דולר.
- 1974, שארלוט ארה"ב. מפעיל מתוסכל יורה במחשב שעליו עבד בחברת ביטוח החיים Charlotte Liberty Mutual Life Insurance.
- 1978, בסיס ח"א ונדנבורג בקליפורניה. פעיל שלום משחית בעזרת פטיש, מקדחה וכלי עבודה נוספים מחשב שאינו בשימוש כמחאה נגד פרויקט מערכת הניווט הלוויינית NAVSTAR.

פגיעות פיסיות במחשבים המשיכו לרכז חלק מתשומת הלב הציבורית גם בשנים שלאחר מכן. אך, עם זאת, למרות שפגיעה פיסית בציוד מחשב נחשבה במשך שנים למאוד אפקטיבית, מהר מאוד החלו לצוץ אירועים שמטרתם פריצה לוגית למחשבים במטרה להוציא מהם מידע או להזיק להם.

### שנות ה-70 - הופעת התוכנות הזדוניות הראשונות

בשנת 1971 נולדת לה תוכנת מחשב מיוחדת במינה בשם Creeper על ידי בחור בשם בוב תומאס מ-BBN Technologies<sup>26</sup>. התוכנה יועדה להעתיק עצמה על גבי מערכות הפעלה מסוג TENEX<sup>27</sup> ולהציג על גבי

<sup>23</sup> About.com, **Inventors of the Modern Computer**, <http://inventors.about.com/library/weekly/aa050298.htm>

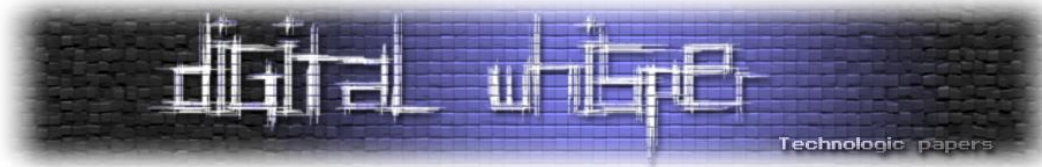
<sup>24</sup> Thomas Whiteside, **Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud**, 73-76 (Ty Crowell Co; 1st edition April 1978)

<sup>25</sup> Computer History, **Honeywell**,

<http://archive.computerhistory.org/resources/text/Honeywell/Honeywell.H632.1968.102646107.pdf>

<sup>26</sup> Physorg, **The Virus Turns 40** <http://phys.org/news/2011-03-virus.html>





המסך את המסר: "אני שרץ (creeper), תפסו אותי אם תוכלו!". תוכנה זו שהייתה ניסיונית, לא כוונה במטרה לגרום נזק ממשי אלא כדי לבדוק את פעילותה על גבי המערכות. כדי להסירה, פותחה תוכנה אחרת בשם Reeper.

תוכנת זדונית וויתקה אחרת היא ה-Wabbit. תוכנה (או יותר נכון משפחה של תוכנות) אשר נחשפה גם היא באמצע שנות ה-70 של המאה העשרים שכפלה עצמה במהירות על המחשבים שהודבקו על ידה ומכאן גם שמה.<sup>28</sup> השכפול המהיר הביא בדרך כלל לקריסת המערכת המארחת.<sup>29</sup> ה-Wabbit חשפו לעולם שני זרמים נוספים של תוכנות זדוניות: "פצצות לוגיות" - תוכנות שמופעלות תחת תנאים מסוימים, לדוגמה תאריך מסוים, רצף הקלדות על מקלדת מחשב וכן הלאה. "התפוצצות" הפצה מביא להפעלת וירוס או תוכנה זדונית אחרת.<sup>30</sup> סוג נוסף הוא התקפת מניעת שירות או DoS<sup>31</sup> שהיא ורסיה נוספת של תוכנות Rabbit או Wabbit אשר מריצות אפליקציה מסוימת פעמים רבות עד אשר המערכת קורסת. התקפות מניעת שירות קיימות עד היום ונחשבות לאפקטיביות מאוד.<sup>32</sup>

תוכנה נוספת אשר הופיעה בשנות ה-70 של המאה העשרים היוותה השראה לז'אנר שלם של תוכנות זדוניות אשר מוכרות כיום בכינוי "סוס טרויאני". התוכנה "Animal" תוכנה על ידי ג'ון ווקר ונכתבה בשפה ותיקה בשם UNIVAC. מטרת התוכנה המקורית היה משחק מחשב פשוט שניסה לנחש - על ידי סדרת שאלות - איזה בעל חיים המשתמש בחר. בינתיים, מאחורי הקלעים, רצה תוכנה אחרת שהפיצה את ה-Animal, בצורה שלא פגעה במחשב, לכל ספריה או מחיצה שאפשר תחת מגבלות מערכת ההרשאות. סביב תוכנה זו התפתחו לא מעט סיפורים ואגדות אורבניות אשר ייחסו לה תכונות רעות, כאשר בפועל היה מדובר במשחק תמים לגמרי עם מנגנון הפצה חדשני.<sup>33</sup>

## ראשית שנות ה-80 - "משחקי מלחמה"

המחשוב מתפתח במהירות ובתחילת העשור מופיעים עוד ועוד דגמים של מחשבים אישיים.<sup>34</sup> המחשב האישי (Personal Computer - PC) הופך לכל כך משפיע מבחינה טכנולוגית, עד אשר תופעה זו נבחרת ב-1982 ל"איש השנה" של המגזין Time.<sup>35</sup>

<sup>27</sup> Tenex, **Origins and Development of TOPS-20**, <http://tenex.opost.com/hbook.html>

<sup>28</sup> מעין שיבוש אותיות של המילה ארנב (rabbit) כפי שנהגתה על יריבו של "באגס באני", הצייד "אלמר פדס":  
<http://jazz.he.fi/jargon/html/W/wabbit.html>

<sup>29</sup> Infocarnivore, **The very first viruses: Creeper, Wabbit and Brain**, <http://www.infocarnivore.com/2010/05/30/the-very-first-viruses-creeper-wabbit-and-brain/>

<sup>30</sup> TechTarget, **Logic Bomb (Slag Code)**, <http://searchsecurity.techtarget.com/definition/logic-bomb>

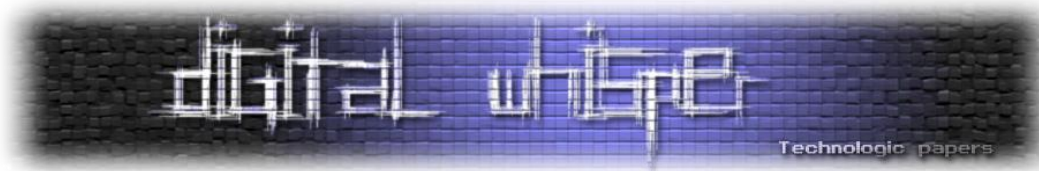
<sup>31</sup> Denial of Service

<sup>32</sup> Go4Expert, **How to make a Fork Bomb(rabbit virus)?**, <http://www.go4expert.com/forums/showthread.php?t=11213>

<sup>33</sup> Fourmilab, **The Animal Episode**, <http://www.fourmilab.ch/documents/univac/animal.html>

<sup>34</sup> Low and Mac, **Personal Computer History: The First 25 Years**,  
<http://lowendmac.com/lowendpc/history/index.shtml>

<sup>35</sup> Time Magazine, **The Computer Moves In**, <http://www.time.com/time/magazine/article/0,9171,953632,00.html>



גם עולם הפשיעה והחבלה הטכנולוגית מתפתחים ובעשור זה אנו עדים לעלית מדרגה ברמת התחכום של הפורצים. בחור צעיר בשם איאן מרפי (Ian Murphy) מצליח לפרוץ למחשבים של חברת הטלפוניה AT&T ולשנות את מנגנון השעות, כך שלקוחות שיבצעו שיחות טלפון בשעות היום יקבלו תעריף מוזל של שעות השפל.<sup>36</sup> מרפי, או בכינויו "קפטין זאפ", הוא פורץ המחשבים הראשון שהורשע כתוצאה מעבירה מהסוג הזה.<sup>37</sup> פרשיית קפטין זאפ נחשבת לאבן דרך בהיסטוריה של הפשיעה הקברטית. מכאן ואילך הולכים ומתרבים מקרי הפריצה למחשבים או באמצעות מחשבים. כמו כן עולה מספר ההתארגנויות העברייניות והקבוצות האידאליסטיות בתחום.

**קבוצת Warelords**<sup>38</sup> - נוסדה בשנת 1981 בארה"ב על ידי האקר בשם Black Bart. הקבוצה הורכבה ממספר בני נוער ו"גאוני מחשב" אחרים ונדעה בשל מספר פריצות למערכות מחשב של ארגונים ומוסדות, ביניהם "הבית הלבן", מעבדות Southwestern Bell, מרכזיות טלפוניה ועוד.

הופעת הסרט "**משחקי מלחמה**" בשנת 1983 הביאה לחשיפה רחבת היקף את תופעת הפריצות למחשבים בארה"ב. הסרט מספר על גאון מחשבים משועמם אשר מנסה לפרוץ לחברה למשחקי וידאו, אך פורץ, ללא כוונה, למערכת מסווגת של צבא ארה"ב וכמעט מביא למלחמה גרעינית.<sup>39</sup> הסרט מציג את ההאקרים בצורה מאוד אוהדת והדמויות והאירועים בו מבוססים, לפי חלק מההשערות,<sup>40</sup> על אירועים ואנשים אמיתיים, הם מה שהצית את דמיונם של צעירים רבים לאחר מכן.

**קבוצה 414**<sup>41</sup> - שמה של קבוצה זו לקוח מקידומת הטלפון בעיר מילווקי במדינת ויסקונסין, ארה"ב. קבוצה זו יוסדה על ידי מספר נערים צעירים בגילאים 16-22 אשר תוארו בתקשורת באותם זמנים של לאחר צאת הסרט War Games (ראו לעיל) כ: "גברים צעירים ואינטליגנטים בעלי מוטיבציה ואנרגיה". אחד מאותם צעירים, אשר זוהה כדובר של החבורה, היטיב לתאר את רוח פעילות הקבוצה וקבוצות דומות לה בתחילת שנות השמונים. לטענתו, המוטיבציה היחידה של הקבוצה הייתה "לפרוץ למקומות שהם לא היו אמורים להיות בהם ולהישאר בהם בלי שיבחינו בהם". באופן כללי לא מדובר בקבוצה שגרמה לנזקים גדולים מדי. ברוב המקרים הם ניצלו חולשות ידועות במערכות ההפעלה של מחשבים שטרם הוטלאו וכן בסיסמאות ברירת מחדל שלא הוחלפו. עם זאת, העיתוי ואופי הפעילות של הקבוצה הם שהכניסו אותם להיכל התהילה של ההאקרים.

<sup>36</sup> Wired, The Greatest Hacks of All Time,

<http://www.wired.com/science/discoveries/news/2001/02/41630?currentPage=all>

<sup>37</sup> Hack Story, Captain Zap, [http://www.hackstory.net/index.php/Captain\\_Zap](http://www.hackstory.net/index.php/Captain_Zap)

<sup>38</sup> Wikipedia, Timeline of computer security hacker history ,

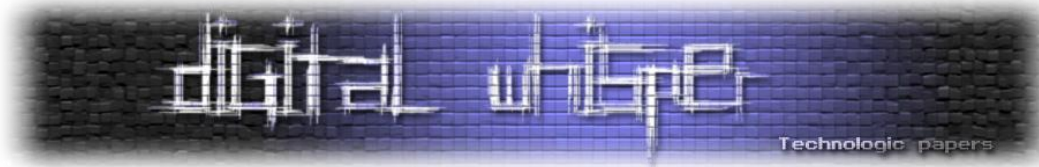
[http://en.wikipedia.org/wiki/Timeline\\_of\\_computer\\_security\\_hacker\\_history](http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history)

<sup>39</sup> IMDb, Plot Summary for WarGames, <http://www.imdb.com/title/tt0086567/plotsummary>

<sup>40</sup> WebCitation, A Q&A that is 25 years late: David Scott Lewis, the mystery hacker who inspired the film "War Games", <http://www.webcitation.org/5v9y5REPI> "

<sup>41</sup> Wikipedia, The 414s, [http://en.wikipedia.org/wiki/The\\_414s](http://en.wikipedia.org/wiki/The_414s)





**Phrack** - נקודת ציון חשובה בשנות ה-80 היא הוצאת המגזין <sup>42</sup>**Phrack** ב-17 בנובמבר 1985 והיא מסמלת שלב נוסף בהתמסדות תחום ההאקינג והפריקינג. המגזין נחשב לפעיל עד היום והוציא כבר יותר מ-68 כרכים על נושאים שמעניינים את קהל קוראיו הנאמן.

## MOD ו-LOD

לקראת סוף שנות ה-80 הולכות ומתגבשות קבוצות אידאולוגיות של האקרים ברחבי העולם ובארה"ב. בשנת 1987 מייסדים מספר צעירים קבוצת האקרים בשם MOD (Master of Deception) קבוצה זו אשר מקום מושבה בניו-יורק ארה"ב מתמחה בפריצות לכרטיסי אשראי וגניבת פרטים אישיים של מפורסמים.<sup>43</sup> בערך באותן שנים קמה במדינת טקסס בארה"ב קבוצה בשם LOD (Legion of Doom).<sup>44</sup> קבוצה זו נוסדה על ידי ההאקר Lex Luthor וחבריה מנו מספר מומחים לפריצות למערכות טלפוניה (<sup>45</sup>Phreakers) ומחשבים. ייחודה של קבוצה זו הוא בהפצה של מספר חוברות טכניות ללימוד עצמי, אשר הביאו להעשרה של הידע בקרב קהילת ההאקרים בעולם מבלי שהקבוצה עצמה גרמה ליותר מדי נזק למערכות שעליהן השתלטה.<sup>46</sup> בסקירה של החוברות הטכניות של ה-LOD ניתן לראות כי תחומי הידע של חברי הקבוצה בהחלט נרחבים והם שלטו בכל תחומי התקשורת ומערכות המידע הרלוונטיות בשנות הפעילות שלהם, החל במרכזיות טלפוניה, דרך מערכות UNIX וכלה במערכות Mainframe שריכזו את רוב המידע המחשובי בשנות ה-90 של המאה העשרים.<sup>47</sup>

שתי הקבוצות (MOD, LOD) זכו לתהודה גדולה בקרב קהילת ההאקרים בארה"ב ונחשבו ליריבות. בין השנים 1990-1991 הפכה יריבות זו למלחמה קברטית של ממש במה שכונה **מלחמת ההאקרים הגדולה**. הכל החל לאחר שגורם אנונימי מקרב קבוצת LOD כינה את אחד מחברי MOD <sup>48</sup>"Nigger" ומכאן והלאה במשך יותר משנה ניסו הקבוצות לתקוף אחת את השנייה, לפרוץ למחשבים ולמרכזיות אחת של השנייה ובעיקר לנסות להביך את היריבים.

גורמים מסוימים מתוך עולם ההאקרים ניסו להשכין שלום בין הניצים אולם ללא הצלחה. רק בסוף 1991 הצליחו גורמים שונים להביא להפסקה של מובילי הקבוצות (Chris Coggans מ-LOD ו-Mark Abene מ-MOD) ולהרגעת הרוחות. הרגיעה במתחים בין הקבוצות פינתה לחברים מספיק זמן להמשיך במלוא המרץ בפעילות הלא חוקיות שלהם עמוק לתוך שנות ה-90 ואף מעבר לזה. מצד שני, חברי שתי הקבוצות

<sup>42</sup> Phrack, Issue #1, <http://www.phrack.org/issues.html?issue=1&id=1#article>

<sup>43</sup> HackDigital, 5 Most Notorious Hacking Groups Of All Time, <http://www.hackdigital.com/5-most-notorious-hacking-groups-of-all-time/>

<sup>44</sup> ZoneAlarm, Famous Hacker Groups, <http://blog.zonealarm.com/2011/08/famous-hacker-groups.html>

<sup>45</sup> Telephone Tribute, Phone Phreaking, <http://www.telephonetribute.com/phonephreaking.html>

<sup>46</sup> DocDroppers, Legion of Doom (hacking), [http://wiki.docdroppers.org/index.php?title=Legion\\_of\\_Doom\\_\(hacking\)](http://wiki.docdroppers.org/index.php?title=Legion_of_Doom_(hacking))

<sup>47</sup> Textfiles, Electronic Magazines: The Legion of Doom/Hackers Technical Journal, <http://www.textfiles.com/magazines/LOD>

<sup>48</sup> Michelle Slatalla and Joshua Quittner, Masters of Deception: The Gang That Ruled Cyberspace, 64, (Harper-Collins, 1995)

סבלו מרדיפה של רשויות החוק האמריקאים, אשר החלו להקדיש מאמצים למיגור תופעת ההאקרים כבר מתחילת שנות ה-80 ואחדים מהם אף הורשעו בבתי המשפט בגין עבירות שונות.<sup>49</sup>

### האקר ושמו קווין מיטניק

רוב הציבור נחשף בדר"כ להאקר כמושג ולא ממש לדמות מוחשית שעומדת מאחוריו. רוב ההאקרים פועלים במחשכים, כך הם יכולים להימנע מחיכוכים מיותרים עם מוסדות רשמיים וגורמי אכיפת החוק. מעטים הם המקרים בהם הציבור הרחב נחשף בצורה ישירה להאקר בעל שם ופנים. קווין מיטניק היה אחד מאותם מעטים ששמו הפך שגור בפיהם של רבים בארה"ב של שנות התשעים.

מיטניק לא רק היה מוכר, אלא הוא הפך במרוצת השנים לידוען של ממש. למיטניק מיוחסות פריצות לאתרים ומוסדות שונים בשנות ה-80 וה-90 בארה"ב, ביניהם: Pacific, Sun Microsystems, Motorola, Bwll ואחרים. באוגוסט 2011 התארח מיטניק בתוכנית פופולארית בשם The Colbert Report ובה הוא סיפר על שנותיו הפרועות.<sup>50</sup> בראיון סיפר כי בשל עבירות שונות הוא בילה 5 שנים בכלא פדראלי ועוד שנה אחת במעצר בית מיוחד ללא גישה לטלפון מחשש שהוא מסוכן לציבור. עוד הוא סיפר על התקופה בה הוא נרדף על ידי ה-FBI טרם מעצרו, על פי הריאיון, הוא הצליח לפרוץ למכשירי הטלפון הסלולרי של רודפיו ולדאוג להישאר במרחק רב מספיק מהם.

בשנת 1995 נעצר מיטניק על ידי ה-FBI לאחר מרדף שנמשך יותר משלוש שנים. אחד האנשים שסייעו ללכידתו הוא חוקר ומומחה אבטחה בשם Tsutomu Shimomura שמיטניק פרץ למחשבו.<sup>51</sup> אורח חיו, "הישגיו המקצועיים" והנסיבות הפכו אותו לאחר ישיבה לא קצרה בכלא פדראלי למודל של האקר מחשבים ובהמשך אף ליועץ, לסופר ומרצה מבוקש בכל רחבי העולם.<sup>52</sup>

### התמקצעות - כנסים ותערוכות



שיתוף ידע הוא הבסיס להתפתחות טכנולוגית. תחום ההאקינג אינו שונה במובן זה משום תחום טכנולוגי אחר. הזכרנו כבר למעלה את הופעת המגזין Phrack והמגזינים שהופיעו בעקבותיו וכן את החבורות הטכניות שחברי LOD נהגו להפיץ בקרב קהילת ההאקרים. בשנת 1993 עולה הענף מדרגה נוספת בכינונו של הכנס שיהפוך במרוצת השנים לשם דבר בקהילה, DefCon.<sup>53</sup> כנס זה נולד כהתכנסות חד פעמית של מספר קהילות האקרים לחגוג מעבר של אבא של אחד מהם למקום עבודה אחר. השם, אגב, מקורו בצמד המילים "con" -

<sup>49</sup> Textfiles (Originally by The NY Transfer News Service), New York Computer Crime Indictments , <http://www.textfiles.com/news/modbust.txt>

<sup>50</sup> Colbert Nation, The Colbert Report Videos-Kevin Mitnick, <http://www.colbertnation.com/the-colbert-report-videos/395003/august-18-2011/kevin-mitnick>

<sup>51</sup> The New-York Times, A Most-Wanted Cyberthief Is Caught in His Own Web , <http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html>

<sup>52</sup> <http://mitnicksecurity.com/company.php>

<sup>53</sup> DefCon, The DefCon Story, <http://www.defcon.org/html/links/dc-about.html>

תחילת של המילה האנגלית כנס ו-"def" שמסמל את הספרה שלוש על לוח מקשים סטנדרטי של טלפון (כמחווה לפורצי הטלפונים). לשילוב המילים יש משמעות צבאית וכן משמעויות נוספות. כנסי DefCon נערכים מדי שנה במשך כארבעה ימים בחודשי הקיץ בלאס וגאס, ארה"ב.

כנסי Defcon מורכבים מהרצאות מקצועיות של אנשי מקצוע מהתעשייה וכן מתחרויות פריצה שונות הנערכות תוך כדי הכנס ומזמינות את קהל ההאקרים להשתתף בחגיגה. לצד כנס זה קיימים כנסים חשובים נוספים ובראשם RSA ו-BlackHat. כנס RSA נוסד בשנת 1991 ומתקיים מדי שנה בסוף פברואר בסן-פרנסיסקו, ארה"ב. בשנים האחרונות נוספו כנסי משנה גם באירופה, יפן ואף בסין. למרות שהכנס מופק על ידי חברה ציבורית מתחום אבטחת המידע, התכנים בכנס נקבעים בצורה מקצועית על ידי פאנל של מומחים<sup>54</sup>. גם בכנס זה מוצגות הרצאות מקצועיות ומתקיימת תערוכה גדולה של יצרני פתרונות אבטחת מידע. כנס RSA ידוע כבמה מצינית להכרזות על מוצרים חדשים ורבים מהיצרנים מתזמנים הוצאת גרסאות חדשות בהתאם.



אחיהם הצעיר, אך המצליח, של כנסים אלה הוא כנס BlackHat המדובר. הכנס נוסד בשנת 1997 והפך מכנס בן יום אחד בלאס וגאס לאירוע מתגלגל בן כמה ימים. הכנס נערך כיום מספר פעמים בשנה במספר אתרים בעולם (בנוסף ללאס-וגאס) כמו אבו-דאבי, וושינגטון וברצלונה. מארגני הכנס והקהל הרחב מעידים עליו כי מדובר בכנס נטרלי, ללא נטיות ליצרן כזה או אחר. בכנס ניתן לצפות במצגות של טובי המומחים בתחום וכן להתנסות בסדנאות מקצועיות לפי תחומי עניין באבטחת מידע. כנס זה משמש אכסניה להעברת קורסים מקצועיים בני כמה ימים ורבים מגיעים אליו כדי לעבור הסמכות מקצועיות<sup>55</sup>. בדומה לכנסים דומים בתחום מורכב צוות ההיגוי של BlackHat ממומחים מהשורה הראשונה בעולם אבטחת המידע אשר מקפידים על הצגת תכנים איכותיים ולא שיווקיים<sup>56</sup>. יו"ר הכנס ומייסדו הוא ג'ף מוס, האקר המוכר בכינוי Dark Tangent, אשר ייסד גם את כנס DefCon לעיל<sup>57</sup>. חשוב לציין כי ברחבי העולם ובמיוחד בארה"ב מתקיימים מדי שנה עשרות כנסים מקצועיים אחרים אשר תורמים מאוד להעשרת אנשי המקצוע ולקידום תחום אבטחת המידע.

## נוזקות ידועות

וירוסים, תולעים, פצצות לוגיות, סוסים טרויאנים ונוזקות אחרות הפכו במהלך השנים לסממן מרכזי של פגיעה במחשבים. למרות שמחקר זה נוגעת בשינויים שחלו במהלך השנים במניעי פריצה למחשבים, קשה יהיה להתעלם מנוזקות המחשב<sup>58</sup> המוכרות והמפורסמות ביותר שהיוו בחלק ממקרי הפריצה אמצעי

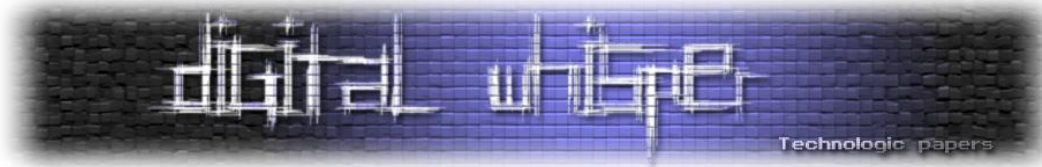
<sup>54</sup> RSA Conference, **About RSA Conference**, <http://www.rsaconference.com/about/>

<sup>55</sup> Black-Hat, **About Black-Hat**, <http://www.blackhat.com/html/about.html>

<sup>56</sup> kBlack-Hat, **Black-Hat Review Board**, <http://www.blackhat.com/html/review-board.html#Butler>

<sup>57</sup> CNN Tech, **Meet Dark Tangent, the hacker behind Black Hat and DEF CON**, [http://articles.cnn.com/2011-08-03/tech/jeff.moss.black.hat\\_1\\_lulzsec-hacker-moss?\\_s=PM:TECH](http://articles.cnn.com/2011-08-03/tech/jeff.moss.black.hat_1_lulzsec-hacker-moss?_s=PM:TECH)

<sup>58</sup> Computer malware



חשוב לביצועה. חלק מהנוזקות המוקדמות הופיעו במקור ממניעים תמימים וחלקן, בעיקר המאחרות, נכתבו במטרה לשמש כלי נשק קיברנטי.

ברור, כי ככל שמערכות מחשב ותקשורת הפכו נפוצות יותר, כך התפשטו להן הנוזקות וזכו להתהודה רבה יותר. אפשר להגיד בוודאות, כי עם תחילתה של המאה ה-21, קיבלו הנוזקות את מרכז הבמה הקיברנטית. אם בעבר הכיר כל ילד את השם קוין מיטניק, כיום אין אדם בעולם המערבי שלא נחשף לשמות Flame, Stuxnet ו"חבריהם" המסתוריים. את הסקירה הזו נתחיל באמצע שנות ה-90 של המאה העשרים, עם הופעת הווירוסים הראשונים למערכת ההפעלה "חלונות" של חברת מיקרוסופט.

### Concept

וירוס המאקרו הראשון למערכות WINDOWS שהתפרץ בצורה חסרת שליטה במחשבים בעולם הוא הווירוס Concept אשר התגלה ביולי 1995. יש לציין כי לא מדובר בווירוס המאקרו הראשון שהתגלה אי פעם, אולם זהו הווירוס הראשון מסוגו שהתפרץ פרא<sup>59</sup>. Concept פעל על מספר פקודות מאקרו אשר היו נפוצות בעיקר במעבדי תמלילים מסוג Word במערכות הפעלה Windows NT, Windows 95. עבודה עם פקודות מאקרו חסכה לכותבי הווירוסים כתיבה מסובכת יותר בשפת Assembly. כותבי וירוסים המבוססים על הווירוס הזה ניצלו לרעה יכולות מאקרו להעתקה של קבצי Word, אשר הפכו לקבצים פופולאריים בשנות ה-90 של המאה העשרים, וכך עברו ממחשב למחשב<sup>60</sup>.

### Melissa

מי שיווע בנפשו במרץ 1999 שפתיחת מייל ב-Outlook מאיש קשר מוכר, אשר מכיל צרופת Word, עשויה להפוך אותו קורבן לנוזקת מחשבים חדשה בשם "Melissa". Melissa שמקור שמה הוא רקדנית אקזוטית מפלורידה, תוכננה לנצל חולשות במערכות ההפעלה של מיקרוסופט (גרסאות 95, 97 ו-2000 של Windows) ולהפיץ עצמה לרשימת אנשי הקשר של הקורבן. הנוזקה פעלה על מסמכי Word 97 ו-2000. במידה והנוזקה הצליחה להפעיל עצמה על מחשב הקורבן, היא פנתה לפתוח Outlook ולשלוח עותק עם קובץ Word נגוע לחמישים אנשי קשר קיימים<sup>61</sup>. הנוזקה התפשטה מהר מאוד ברשת האינטרנט ופגעה במיליוני מחשבים, חלקם מחשבי רשויות פדראליות אמריקאיות. הנוזקה דחפה את ה-FBI לבצע מצוד שבסיומו נתפס, הודה והורשע יוצר הנוזקה, אדם בשם דיויד סמית<sup>62</sup>. סמית' אומנם הודה בגרימת נזק למיליון מחשבים בעלות כוללת של כ-80 מיליון דולר, אך הנזק המדויק שנגרם קשה לאמידה.

<sup>59</sup> Flashing Cursor, **The Concept Virus**, <http://www.chebucto.ns.ca/~af380/ConceptMacro.html>

<sup>60</sup> F-Secure, **Virus:W32/Concept**, <http://www.f-secure.com/v-descs/concept.shtml>

<sup>61</sup> Melissa.com- Home, <http://www.melissavirus.com/>

<sup>62</sup> FBI, Testimony, <http://www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks>

## ILOVEYOU

נוזקה זו, אשר כונתה גם Love Letter הופיעה לראשונה בפיליפינים במאי 2000. הנוזקה הופיעה על מחשב הקורבן בשיטה דומה לשיטה שבה Melissa פעלה: מכתב שכותרתו ILOVEYOU ואליו צורף קובץ בשם "LOVE-LETTER-FOR-YOU.txt.vbs". הסיימת vbs, המייצגת את שפת התכנות Visual Basic, היוותה אינדקציה לשיטה שבה הופעלה הנוזקה. חשוב לציין כי הסיימת הוסתרה בדרך כלל, כך שמי שראה את הצרופה חשב שבפניו עומד קובץ טקסט (txt) תמים<sup>63</sup>. על פי הערכות שונות, הנזק שנגרם כתוצאה מהנוזקה הזו עומד על כמה מיליארדי דולרים ופגיעה במיליוני מחשבים של משתמשים ברחבי העולם, ביניהם רשויות ומוסדות ממשלתיים שונים בארה"ב ורחבי העולם. גם במקרה הזה פעלו רשויות הביטחון ביעילות והצליחו לאתר בתוך מספר ימים שני סטודנטים פיליפיניים בחשד כי הם אלו שפיתחו את הנוזקה והפיצו אותה<sup>64</sup>.

## Conficker

תחילתו של העשור הראשון במאה ה-21 הביאה ל"פריחה" של ממש בהתפשטות הנוזקות והוירוסים אשר השפיעו בצורה קשה על מיליוני מחשבים ברחבי העולם. וירוסים ונוזקות כמו MSBlast, Code Red ואחרים גרמו על פי חלק מהערכות לנזקים בהיקפים של מיליארדי דולרים עד שנת 2004<sup>65</sup>. המייחד את כולם הוא ניצול חולשות במערכות Windows של חברת Microsoft שהגדילה משמעותית את נתח השוק שלה בשוק המחשוב הפרטי והארגוני באותן שנים והיוותה מטרה עסיסית מצד מפתחי הנוזקות. החברה עצמה הבינה - יש שיאמרו באיחור מה - את חומרת הבעיה ואף קידמה מתודולוגיות לפיתוח מאובטח של מוצריה<sup>66</sup>. כיום מתודולוגיות אלה עומדות בחזית המאבק בנוזקות המנסות ללא הרף לחפש חולשות ביישומים אינטרנטיים ובמערכות הפעלה. החשיבות של פיתוח מאובטח לא נעלמה גם מארגונים ומוסדות בישראל והיא מרכזת עניין רב בקרב מנהלי פיתוח ואבטחת מידע<sup>67</sup>.

נוזקה בשם Conficker היא דוגמא שממחישה בצורה מצוינת את ההחרפה באיום מצד תוכנות זדוניות כלפי מערכות הפעלה. הנוזקה דווחה לראשונה לחברת Microsoft ב-21 בנובמבר 2008 והיו לה בסה"כ חמישה וריאנטים בין סוף 2008 עד אפריל 2009<sup>68</sup>. התוכנה הפיצה עצמה באמצעות ניצול חולשה במנגנון RPC של מערכת ההפעלה ובאמצעות כוננים נתיקים (כמו Disk-on-Key) וגרמה לנזק רב למערכות

<sup>63</sup> ZDNET, 'ILOVEYOU' e-mail worm invades PCs ,

[http://web.archive.org/web/20081227123742/http://news.zdnet.com/2100-9595\\_22-107318.html?legacy=zdn](http://web.archive.org/web/20081227123742/http://news.zdnet.com/2100-9595_22-107318.html?legacy=zdn)

<sup>64</sup> מתוך עדותו של עוזר התובע הראשי במשרד המשפטים של הפיליפינים,

<http://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana,Phillipine.html>

<sup>65</sup> Catalogs, Top 10 worst computer viruses, <http://www.catalogs.com/info/travel-vacations/top-10-worst-computer-viruses.html>

<sup>66</sup> Microsoft, Security Development Lifecycle, <http://www.microsoft.com/security/sdl/default.aspx>

<sup>67</sup> פיני כהן ושחר גייגר מאור, פיתוח ממרס אבטחה ממאדים - אבטחת מידע בפיתוח מערכות ב-IT, (מאי 2011) <http://shaharmaor.blogspot.co.il/2011/05/blog-post.html>

<sup>68</sup> Safety & Security Center, Protect yourself from the Conficker Worm virus, <http://www.microsoft.com/security/pc-security/conficker.aspx>

המחשב שאליהם פלשה, תוך שהיא עוברת מוטציות שהקשו מאוד על בידוד והסרתה ממערכות המחשב. הנוזקה הצליחה להדביק מיליוני מחשבים ברחבי העולם והתפשטות שלה כללה את רוב המדינות הממוחשבות על פני כדור הארץ. כדי להתמודד עם הנוזקה ועם ההשלכות שלה הוקם בשנת 2009 צוות משימה מיוחד שהורכב מנציגי יצרניות אנטי וירוס מובילות, גופים פדראליים ואנשי מקצוע ואקדמיה כדי להיטיב את הטיפול והמניעה של נזקה זו. צוות משימה זה פעל באופן שוטף עד יוני 2010, כשקצב ההדבקה ירד באופן דרמטי ורוב מערכות המחשב חוסנו בצורה אפקטיבית נגד אחרוני הווריאנטים של הנוזקה<sup>69</sup>.

### Stuxnet

"Stuxnet הוא הנשק הקיברנטי המתוחכם ביותר שהופץ מעולם" כך פורסם במאמר מערכת בניו-יורק טיימס ב-15 בינואר 2011 בעקבות החשיפה של תוכנה עלומה שעל פי התיאור גרמה לנזק לפרויקט הגרעין האירני. על פי המאמר נוסה כלי הנשק החדשני הזה ראשית על מתקני דמה שהוצבו בכור הגרעיני בדימונה וזאת במטרה לדמות עד כמה שניתן את סביבת היעד האמתית של ה-Stuxnet - מתקן הצנטריפוגות בנתנז, אירן<sup>70</sup>. דוח של חברת Symantec אשר חקרה את הקוד של Stuxnet מתאר אותו כ-"אחד מהאיומים המתוחכמים ביותר שאי פעם חקרנו". בדוח מתואר תוואי הפעולה של הנוזקה ורמת המקצועיות הרבה שניכרת בפיתוחה. הערכות החוקרים מדברות על כמה עשרות מפתחים שכתבו קוד ל-Stuxnet. עוד עולה כי מפתחי התוכנה הצליחו למצוא ארבע חולשות חדשות במערכות ההפעלה שנגדן פעלו ולזייף שתי תעודות דיגיטליות. כותבי הדוח מסכמים אותו במשפט המדהדד הבא: "למרות האתגר המרגש שבחקירתו ובניסיון להבין את פעולתו, Stuxnet הוא מסוג האיומים שאנחנו מקווים לא לראות יותר לעולם"<sup>71</sup>. נזקה זו מהווה פריצת דרך של ממש ביכולת החדירה למחשבים ולמערכות תעשייתיות ומהווה פתח לדור חדש של נזקות. סנונית נוספת לנוזקות אלה היא הנוזקה Flame שנחשפה ב-2012.

<sup>69</sup> Conficker Working Group, Home\Infection Distribution, <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionDistribution>

<sup>70</sup> The New-York Times, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, [http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?\\_r=3&hp](http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&hp)

<sup>71</sup> Symantec Security Response, W32.Stuxnet Dossier, [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)





## מי פורץ ולמה?

פרק זה מתאר מה הם הגורמים השונים שעומדים מאחורי פריצות למחשבים ומערכות מחשב. ננסה לברר מי פורץ לנו למחשב ומה הן מכלול הסיבות שמביאות את אותם גורמים לבצע את הפריצה.

### הסיבות לפריצה

בתחילת מסמך זה תוארו האקרים כמתכנתי מחשב מוכשרים מעל הממוצע, אך מה גורם לאנשים מוכשרים לנסות לפרוץ למחשב? פול טיילור מצא בספרו Hackers - Crime and the Digital Sublime שישה סוגים שונים של מוטיבציות בקרב האקרים: התמכרות, סקרנות, שעמום, שיכרון כוח, הכרה בקרב חבריו ואידאולוגיה.<sup>72</sup>

### הבסיס הסוציולוגי - הסקרנות והאתגר

במגזין "מחשבים ואבטחה" במהדורת אוגוסט של שנת 1991 תיאר בלדן מנקוס במאמרו האקרים כאנשי מקצוע בעלי סקרנות אין סופית ורצון להבין בצורה מיטבית את המערכות מולם. למרות שכל האקר פועל ממניעים שונים, הרבה מהסיבות ניתנות לתיאור במסגרת מכנה משותף צר יחסית והוא הרצון להשביע סקרנות בלתי נגמרת. במהדורת 28 באוקטובר 1988 של המגזין הבריטי "גארדיאן", צוטט האקר בשם אדוארד סיין בהתייחסו למניעים שהביאו אותו לפרוץ למחשבים: "ההתרגשות היא קודם כל אינטלקטואלית. זה מתאים לאותם אנשים שאוהבים לפתור פאזלים... אני אף פעם לא הרסתי נתונים כלשהם ולא התעניינתי במידע עצמו". אלמנט משלים לאותה סקרנות הוא האתגר הגדול בפריצה. פריצה מוצלחת למערכת כמוה כפתרון לתעלומה. ככל שהאתגר נעשה גדול יותר, כך הוא מושך אליו את ההאקר.

האקר אחר בשם פול בדוורת' מצוטט בעיתון סאן שיצא לאור ב-18 במרץ 1993 כאומר שכשהוא התחיל לפרוץ למחשבים זה לא נחשב לפעילות לא חוקית. "כולם עשו את זה. העניין הוא שזה ממכר. אתה רוצה להמשיך עוד ועוד. קשה לעצור. לא ניסיתי לגרום לנזק. הדבר המרכזי הוא האתגר".<sup>73</sup> פריצה למערכות מחשב מונעת בראש וראשונה על ידי האתגר עצמו שבפריצה.

### זאבים בודדים

"צרעה" הוא כינוייה הקיברנטי של ליזבת סלאנדר, פורצת מחשבים מיומנת בטרילוגיית "מילניום" של הסופר השבדי, סטיג לארסן. "צרעה" היא טיפוס מופנם ומתבודד אשר מוצאת נחמה בכישורי המחשב יוצאי הדופן שלה. גם שאר "חבריה" הקיברנטיים מורכבים משורה של אנשים בודדים ומופנמים אשר מוצאים דרור בזירה היחידה שאינה דורשת מהם לחשוף עצמם באמת בפני הזולת.<sup>74</sup>

<sup>72</sup> Paul A Taylor, Hackers- Crime and the Digital Sublime, 46, (Routledge, 1999)

<sup>73</sup> Peter Hoath and Tom Mulhall, Hacking Motivation and Deterrence, Part I, 16-19, (Computer Fraud & Security, April 1998)

<sup>74</sup> Stieg Larsson, Millennium (trilogy), <http://www.stieglarsson.com/Millennium-series/>

## הגיל והתרגיל

לא בכדי מוצגים ההאקרים בספרות כגורמים מסתוריים ובודדים. אופי הפעילות של האקר הרי מכיל אלמנטים רבים שאינם חוקיים. גם מצבו החברתי ופעילותו הלילית בדר"כ מוסיפים נימה של אפלוליות ומסתוריות, אשר משווים לו קווי דמיון נוספים לאופי הפעילות של "גנב בחשכת ליל". לרוב עושה רושם שהאקרים הם צעירים. ברוב המקרים בהם אנו נחשפים בתקשורת להאקרים שנתפסים מדובר בחתך גיל שנע בין 17 לתחילת שנות השלושים.

גם הספרות תומכת בהשערה הזו: ספרו של רוג'ר בלייק Hackers in The Mist משנת 1994 מנסה לבחון את תופעת ההאקרים מזווית אנתרופולוגית. עבודה זו, כמו חלק ממחקרים אחרים בתחום, טוענת כי ההאקרים ברובם מונעים משיקולי רווח, כוח ותהילה. את הרווח הם משיגים כתוצאה מהמידע שברשותם, כמו מספרי כרטיסי אשראי. גם הכוח נגזר מהמידע שהם מצליחים להשיג מהמערכות שאליהן הם פורצים ובעקבותיו - גם התהילה. הנתון המעניין ביותר בעבודה של בלייק הוא גילם של ההאקרים. לפי המחקר מדובר בצעירים בין הגילאים 12 ל-28, רובם גברים בעלי אינטליגנציה גבוהה מהממוצע. רבים מהם סיפרו כי החברה לא מבינה אותם וכי הם אוהבים מאוד טכנולוגיה. נתון נוסף שעולה מבדיקת סיפוריהם של ההאקרים על ידי בלייק הוא העובדה כי הם נסחפים על ידי תפיסה עצמית של עצמם כ"עילויים" ומחפשים כל הזמן הכרה בקרב עמיתיהם המקצועיים.<sup>75</sup>

גם במחקרה של אורלי טורגמן-גולדשמידט מ-2005 שבו ביצעה ראיונות עומק עם 54 האקרים ישראלים כדי לנסות ולהתחקות אחריהם ואיך הם תופסים את עצמם ואת הסביבה, ניכר שאוכלוסייה זו מורכבת מתמהיל דומה: קבוצת הגיל העיקרית נעה בין 20 ל-30; 78% מהם רווקים ו-51 מתוך 54 הם גברים. עוד היא גילתה כי 41% מהם הם בעלי השכלה על-תיכונית ול-74% מהם הכנסה הגבוהה מן הממוצע.<sup>76</sup>

## הפורצים

### (Skiddies) Script Kiddies

למרות שרוב ההאקרים תופסים עצמם כגורם מקצועי וחיובי יחסית, קשה שלא להתייחס לצדדים הפחות חינוכיים של תחום הפריצה למחשבים. "ילדי סקריפטים" הוא כינוי שרווח מאוד בתחילת שנות ה-2000. ילדי סקריפטים הם צעירים אשר עושים שימוש בתוכנות ופקודות מוכנות מראש (סקריפטים), אשר ניתנות להורדה מהאינטרנט, על מנת לתקוף מחשבים אחרים. בדו"ח אשר פורסם על ידי המכון להנדסת מחשבים באוניברסיטת קרנגי-מלון בארה"ב עבור משרד ההגנה בשנת 2005, מתוארים אותם ילדי סקריפטים כ-"לא בשלים, אך לא פחות מסוכנים". בהמשך מתוארת מידת המודעות הנמוכה שלהם

<sup>75</sup> Roger Blake, Hackers in the Mist, 48-60 (Chicago, IL: Northwestern University, 1994)

<sup>76</sup> Orly Turgeman-Goldschmidt, Hackers' Accounts : **Hacking as a Social Entertainment** (Social Science Computer Review, 2005)

להשלכות הפריצה למחשבים: "...אין להם הבנה או עניין לגבי הנזק שהפעילות שלהם עלולה לגרום למערכות מחשב"<sup>77</sup>.

הכינוי מכיל בתוכו את תמצית סיפור הפריצה למחשבים בעידן שלנו: הזמינות הרבה של תוכנות מוכנות מראש לתקיפת מחשבים והקלות הרבה שמיוחסת להפעלת תוכנות. כמו כן, ניתן להתרשם מקלות הדעת שמאפיינת בעיקר צעירים בעלי נגישות למחשבים וידע מתאים בעת פריצה למחשבים אחרים. כבר בתחילת שנות ה-2000 היו זמינות יותר מ-100 תוכנות מוכנות מראש לפריצה למחשבים, כך מצוטט ג'ון קלארק מחברת Network Associates בשנת 2001 במאמר של ג'ון ליידין על תרבות ילדי הסקריפטים<sup>78</sup>.

ילדי הסקריפטים אינם מתאימים לאתוס ההאקרים הרומנטי שעשוי לעיתים להצטייר מהפרסומים בתקשורת. הרמה הטכנולוגית הנדרשת לצורך ביצוע תקיפה נמוכה יחסית, מכיוון שכל האמצעים מסופקים או נרכשים על ידי הפורץ באינטרנט ואין חשיבות לדמיון, ליצירתיות ולחקרנות אשר מאפיינים את ההאקרים המתוחכמים יותר. כל שנותר לו הוא להגדיר בצורה פשוטה את מערכת התקיפה ולצאת לדרך. הזמינות והקלות בכלי הפריצה המוכנים מסייעות מאוד להעלאת הנגישות של פריצות למחשבים לאוכלוסיות שלמות אשר עד אז יכלו רק להתגרות מהסיפורים אשר הציפו את העולם בשנות התשעים של המאה העשרים ולהביא לעליה בפריצות למערכות מחשב לאורך כל שנות האלפיים.

במחקר של חברת Tuffin הישראלית, אשר פורסם בשנת 2010, נשאלו כ-1000 סטודנטים ניו-יורקים לגבי דעתם על פריצה למחשבים (האקינג). תוצאות המחקר מראות כי כ-50% חשבו כי מדובר במשהו "מגניב" והן בהחלט מאששות את העלייה בפופולאריות של פריצה למחשבים בקרב צעירים חסרי ייחוד ומיומנות מיוחדת במחשבים. גם מחקר מקביל שנערך על אוכלוסיית סטודנטים אקראית בלונדון חשף ממצאים דומים. במחקר זה העידו כ-28% כי "פריצה למערכות מחשב היא מטלה קלה", בעוד ש-23% טענו כי פרצו בפועל למערכות מידע<sup>79</sup>.

### קבוצות מאורגנות

בסקירה ההיסטורית לעיל הוזכרו מספר קבוצות האקרים ופריקרים מאורגנות. שמען של קבוצות אלה האפיל בדו"כ על ההאקרים העצמאיים של אותן תקופות. עם זאת, הזכרנו כי ההאקרים הם טיפוסיים מתבודדים, או לפחות נתפסים ככאלה. למה, אם כן, מתקבצים האקרים לקבוצות מאורגנות? להצטרפות של פרטים לקבוצות יש הסברים סוציולוגיים מורכבים. התפיסה הרווחת היא כי האדם הוא ייצור חברתי במהותו. האקרים אומנם נתפסים כטיפוסים פתולוגיים ולא כייצורים חברתיים, אך גם הם מוצאים מקום

<sup>77</sup> Nancy R. Mead et al.: Security Quality Requirements Engineering Methodology (Carnegie Mellon University, 2005)

<sup>78</sup> The Register, Virus toolkits are s'kiddie menace,

[http://www.theregister.co.uk/2001/02/21/virus\\_toolkits\\_are\\_skiddie\\_menace/](http://www.theregister.co.uk/2001/02/21/virus_toolkits_are_skiddie_menace/)

<sup>79</sup> FastCompany, IT Security Firm: Fear Students, <http://www.fastcompany.com/1690541/it-security-firm-fear-students>

בקהילות משל עצמם אשר מספקות להם תמיכה, ניסיון, אימון ומסגרות מקצועיות מתאימות. מה שמושך אותם לעבוד ביחד זה במקרים רבים היא מטרה משותפת, אידאולוגית או אחרת כדוגמת רווח כספי.<sup>80</sup>

### ארגוני פשע

אחת הסיבות הנפוצות ביותר להתאגדות של קבוצות האקרים היא למטרות ביצוע פשעים קיברנטיים. רוב הפשיעה הקיברנטית כיום מקורה בקבוצות פשע מאורגנות. המוטיבציה הבלעדית של קבוצות אלה היא רווח כספי גרידא. בעדות של גורדון סנאו, סגן מנהל מחלקת הסייבר ב-FBI בפני הוועדה לפשיעה וטרור של הסנאט האמריקאי באפריל 2011 תואר עולם הפשיעה הקיברנטית כעסק כלכלי ומאורגן לעילא: "הפושעים הקיברנטיים בונים עסקים שלמים סביב פיתוח, תחזוקה ומכירת בוטנטים (botnets).<sup>81</sup> לקבוצות פושעים אלה יש מתכנתים אשר בונים את מערכות הפריצה, אנשי מכירות אשר מוכרים או משכירים את התוכנות הזדוניות שמפעילות את הבוטנטים ובמקרים מסויימים אף אנשי תמיכה לתקלות ושירות לקוחות. פושעים אלה עובדים במשותף כדי לייצר מערכות קלות לתפעול על ידי הלקוחות וקשות לזיהוי על ידי הרשויות".<sup>82</sup>

בדו"ח נוסף של ה-FBI ממרץ 2010 מפורטים לפרטי פרטים עשרת בעלי התפקידים העיקריים בשרשרת האספקה של ארגוני הפשע הקיברנטי. תפקידים אלה כוללים את אותם מתכנתים אשר בונים את מערכות המחשוב (כן כן) לצורכי פשיעה קיברנטית; יש סוחרים וספקים של מידע גנוב שנאסף במערכות; אנשים טכניים אשר מתחזקים את מערכות המחשוב ומפקחים על "העקבות" של המערכות בקרב ספקיות האינטרנט כדי לצמצם את האפשרות שיתחקו אחריהן; האקרים - אשר מאתרים פגיעויות במערכות מידע אזרחיות לפי רשימות מסודרות וסדרי קדימויות; אנשי ההונאות - אלה אותם פושעים אשר עוסקים באיסוף מידע אשר נחוץ להוצאת התקפות. בדו"ח מדובר בפעולות הכוללות הונאות "הינדוס חברתי"; "המארחים" הם אותם גורמים אשר ממונים על בניית רשת שרתים לגיטימיים שמחוברים בשירותי הפניות (proxy) לתשתית הפשיעה, כך שאלה לא יזוהו על ידי רשויות החוק; "פודי הכספים" (cashers) הם גורמים האמונים על רשת בקרת החשבונות והפקדות הכספים של הלקוחות. הם גם אלה שמספקים מעטפת מנהלתית שלמה לבלדרים (money mules); הכספרים (tellers) - כשמן כן הם: אחראים על העברת כספים והמרה של מטבעות מהעולם הדיגיטלי.<sup>83</sup> לעולם האמיתי וחזרה; בעלי התפקיד האחרונים בשרשרת על פי דו"ח ה-FBI הם "המנהיגים". אלה הם מנהלי הפרויקטים אשר בוחרים את האנשים ומצוותים את אנשי המקצוע למשימות. הם בוחרים את המטרות ומגדירים יעדים. במקרים רבים אין מדובר באנשים בעלי יכולות טכניות, אולם הם "המושכים בחוטים".<sup>84</sup>

<sup>80</sup> Tim Jordan and Paul Taylor: A sociology of hackers (The Editorial Board of The Sociological Review 1998)

<sup>81</sup> רשתות מחשבים משותפים אשר מסייעים לפעילות לא חוקית ללא ידיעת בעליהם החוקיים.

<sup>82</sup> FBI, Testimony: cybersecurity responding to the threat of cyber-crime and terrorism,

<http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism>

<sup>83</sup> למשל bitcoins המוכרים כאמצעי תשלום ברשת ה-Darknet (ראו הרחבה בהמשך המסמך).

<sup>84</sup> The FBI, Speech: The Cyber Threat, Who's Doing What to Whom, <http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom>

## ברוכים הבאים לרשת האפלה



פשיעה קיברנטית אינה מוגבלת רק לעבירות בין מחשבים כפי שהן מוגדרות בחוק המחשבים, תשנ"ה-1995, אלא גם לעבירות בהן המחשב ורשת התקשורת המוצפנת מהווים תווך בלבד לביצוע הפשע. אחת הדוגמאות המפורסמות ביותר לשימוש ברשת האינטרנט כמקלט לעבירות מכל הסוגים והמינים היא "הרשת האפלה", ה-Darknet. הרשת האפלה היא אומנם שם כולל לפעילות מחתרתית שנעשית באינטרנט על ידי גורמים שונים ומשונים, אולם את שיטת ניתוב הבצל (TOR - The Onion Routing), השכיחה ביותר לקיום הרשת, פיתח במקור הצי האמריקאי כדי להצפין מידע מסווג על פעולותיו ברשת האינטרנט<sup>85</sup>. TOR זמינה כיום להורדה לכל דורש והיא ממשיכה להתפתח באדיבות קהילת הגולשים והמפתחים ברחבי העולם<sup>86</sup>. לצד פעילי זכויות אדם, עיתונאים ושאר גורמים העושים שימוש ברשת האפלה מתוך כוונה לשמור על פרטיותם, פועלים ברשת זו פושעים מסוגים שונים הנהנים מחיסיון וחוסר אונים של המשטרה ומרגישים חופשיים להגשים את האפלים שבפשעיהם<sup>87</sup>.

### פריצה אידאולוגית

אידאולוגיה היא מרכיב חשוב מאוד בהמרצת ההתנהגות של הרבה האקרים. לא מעט פריצות למערכות מחשב יוחסו לאורך השנים להאקרים אשר פעלו על רקע אידאולוגי.

בין השאר ניתן למנות את תולעת המחשב הראשונה שיוחס לה מימד פוליטי. מדובר בתולעת WANK (Worms Against Nuclear Killers) אשר הוחדרה למחשבי NASA בשנת 1989 כנראה על ידי שני האקרים אוסטרליים מחאה נגד שימוש לכאורה בפלוטוניום במערכות הדלק של החללית גלילאו<sup>88</sup>.

פריצות שבוצעו באמצע שנת 2001 על ידי גוף בשם סייבר ג'יהאד. גוף זה התקיף את אתר משטרת אינדונזיה כדי להפעיל עליה לחץ לשחרר פעיל פוליטי<sup>89</sup>. גופים ואירועים אקטואליים יותר ניתן למצוא בפרשיות הקשורות בפעילות של גופים כמו Anonymous אשר להם יוחסו פעולות כמו התקפת מניעת שירות נגד ארגון IFPI<sup>90</sup> וספקיות אינטרנט שונות בפרשת סגירת אתר The Pirate Bay<sup>91</sup> והתקפה דומה

<sup>85</sup> The TOR Project, About Tor, <https://www.torproject.org/about/overview.html.en>

<sup>86</sup> NRG, מדורי גיהנום: כך פועל גן העדן לפדופילים ופושעים באינטרנט,

<http://www.nrg.co.il/online/1/ART2/370/929.html?hp=1&cat=402&loc=1>

<sup>87</sup> רועי גולדשמידט, שימוש ברשתות תקשורת אנונימיות על גבי האינטרנט למטרות פשיעה (הכנסת, מרכז המחקר והמידע (2012)

<sup>88</sup> Dreyfus, Suelette, Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier, Mandarin Australia, 1997

<sup>89</sup> Antarksa, 2001. I am a thief, not a hacker: Indonesia's electronic underground. Latitudes Magazine, 12- 17 (July 2001)

<sup>90</sup> [http://www.ifpi.org/content/section\\_about/index.html](http://www.ifpi.org/content/section_about/index.html)

<sup>91</sup> ZDNET, The Pirate Bay criticizes Anonymous for DDoS attack, <http://www.zdnet.com/blog/security/the-pirate-bay-criticizes-anonymous-for-ddos-attack/12072>

נגד משרד המשפטים האמריקאי לאחר סגירת אתר Megaupload<sup>92</sup>. קבוצה נוספת היא Lulzsec אשר לה מיוחסים, בין השאר, פעולות כנגד חברת Sony, גופים שותפים של ה-FBI, חברת ייעוץ לאבטחת מידע בשם HBGary<sup>93</sup> ופעולות נוספות. שני חברים בריטים מהקבוצה אף נעצרו והודו בהתקפות כנגד גופים אלה ואחרים.<sup>94</sup>

Wikileaks הוא אתר הדלפות פוליטיות שזכה לתהילת עולם לאחר הדלפת ענק של יותר מ-250 אלף



תשדורות ומסמכים השייכים למשרד החוץ האמריקאי. אומנם, לא הוכח כי חברי אתר זה ובראשם ג'וליאן אסאנג' המייסד פרצו וצותתו בעצמם למערכות פדראליות ובינלאומיות, אולם בחלק מהמקרים הורשעו גורמים שונים אשר השיגו מידע שהועבר לאחר מכן לפרסום באתר. אחד המקרים המפורסמים יותר הוא מעצרו של ברדלי מאנינג, חייל אמריקאי בשירות משרד החוץ, אשר העביר, על פי החשד, קבצים רבים ל-Wikileaks<sup>95</sup>. האקרים, הפועלים על רקע אידאולוגי, פועלים בשם מטרות פוליטיות שונות. בשעה שחלק מהאקרים האידאולוגים פועלים בהתאם למדיניות פוליטית לאומנית שעומדת בקנה אחד עם מדיניות הממשלה שלהם, אחרים פועלים נגד הריבון שלהם.<sup>96</sup>

### האקטיביזם

ד"ר אלכסנדרה סמואל הגדירה את ההאקטיביזם כ"חתונה בין אקטיביזם פוליטי לפריצה של האקרים"<sup>97</sup>. סמואל מאפיינת שלושה טיפוסים עיקריים של האקטיביסטים: כאלה הפועלים כפורצים פוליטיים (political hacktivists). דוגמאות לפעילויות מהסוג הזה הן השחתת אתרים על רקע לאומני ופריצה לאתרים המזוהים עם ישויות פוליטיות או לאומיות אשר ההאקר נמצא עמן בקונפליקט. הטיפוס השני של האקטיביסטים מכונה Performative Hacktivism. אלה האקרים שפועלים על רקע אנרכיסטי יותר. הם יהיו אלה שמתנגדים לגלובליזציה, לבעלי הון וידאגו לזכויות אדם (או לפחות לחלק מהן).



קבוצות מוכרות הן אותן קבוצות שהוזכרו כבר למעלה (Anonymous, Lulzsec ואחרות). הטיפוסים האחרונים שמתוארים על ידי סמואל הם העוסקים ב-Political Coding. הכוונה היא להאקרים "מפוכחים" או בשלים יותר שכבר צברו ניסיון חיים ומאופיינים במצפון חברתי מפותח יותר מחבריהם הצעירים והנמרצים.

<sup>92</sup> RT, Internet strikes back: Anonymous' Operation Megaupload explained , <http://rt.com/usa/news/anonymous-barrettbrown-sopa-megaupload-241/>

<sup>93</sup> <http://www.hbgary.com/>

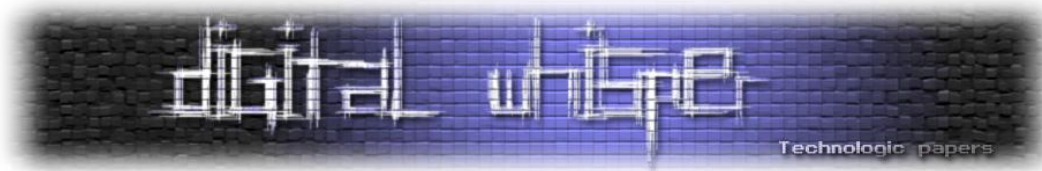
<sup>94</sup> Forbs, Two Members Of Hacker Group LulzSec Plead Guilty To Cyber Attacks, <http://www.forbes.com/sites/parmyolson/2012/06/25/two-members-of-hacker-group-lulzsec-plead-guilty-to-cyber-attacks/>

<sup>95</sup> Bradley Manning, Free Bradley Manning, <http://www.bradleymanning.org/>

<sup>96</sup> Nir Kshetri, Pattern of global cyber war and crime: A conceptual framework, Journal of International Management 11 (2005)

<sup>97</sup> Alexandra Whitney Samuel: **Hacktivism and the Future of Political Participation** (Harvard University 2004)





האקטיביסטים אלה נתפסים כסייבר-ליברטריאניסטים ברמה הפילוסופית. פעילות האקטיביסטית שמיוחסת לטיפוסים אלה היא הפצת קוד בשם DeCSS שמסוגל לפתוח את ההצפנה של תקליטורי DVD וכך לאפשר צפייה בהם באופן חופשי על מחשבים המריצים מערכות הפעלה מסוג Linux. פרויקט נוסף שיוחס לפעילות של political coders מקבוצה בשם CDC (Cult of the Dead Cow) הוא פרויקט "האקטיביסמו" לשמירה על רשת האינטרנט נקייה מצנזורה וחופשית לכולם.<sup>98</sup>

יש לציין כי משתי הדוגמאות האחרונות ניתן להתרשם כי עיקר הפעילות של כותבי הקוד הפוליטיים היא פעילות במרחב הציבורי (חוקית יותר או פחות) ופחות בפריצה למערכות מחשב.

## לאומנות ופריצה למחשבים

אפשר להתייחס ללאומנות ופטריוטיזם כתת-משפחה בפריצות אידאולוגיות. כישראלים, זהו הצד המוכר יותר של האקטיביזם שאליו אנו נחשפים מדי כמה חודשים. הסכסוך הישראלי-פלשתיני הגיע גם הוא לעולם הווירטואלי. מאז פריצתה של האינתיפאדה השנייה (29 ספטמבר 2000) והירידה הדרסטית בהכנסה הממוצעת של האוכלוסייה הפלשתינית בשטחי יהודה ושומרון, חלה עליה חדה באחוז התושבים המחוברים באופן קבוע לאינטרנט (28.5% נכון ל-2009<sup>99</sup>). הרבה מהצעירים הפלשתינים גילו, כמו צעירים בכל מקום אחר בעולם, את נפלאות ויכולות הרשת העולמית. לצד תקשורת בין צעירים פלשתינים למורים ולמוסדות החינוך שלהם, הלכה והתבססה רשת האינטרנט כמדיום חדש למאבק בישראל.<sup>100</sup>

### מלחמת לבנון השנייה - קיץ 2006

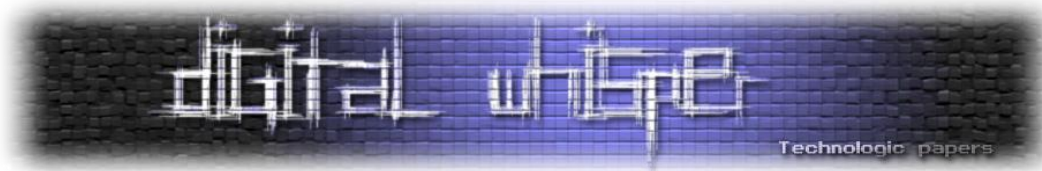
לאורך כל העשור הראשון של שנות האלפיים נרשמו התנצחויות קיברנטיות בין האקרים ישראלים לשכניהם במזרח התיכון. בעולם הרחב לא קשה למצוא גורמים פרו פלשתינים אשר מוכנים ויכולים לבצע התקפות קיברנטיות על אתרים ישראלים ויהודיים. גורמים פרו ישראלים מצדם לא נשארו חייבים והחזירו מלחמה שארה כנגד אתרים המזוהים עם מוסדות ומדינות ערביות. "כלים טכניים הפכו להיות כלי נשק מרכזיים בסכסוכים פוליטיים וחברתיים"<sup>101</sup>. המרחב הקיברנטי אכן אינו מוגדר בגבולות שלפיהם אזרחים מתייחסים לתוכן כלשהו על פי הלאומיות שלהם. במרחב כזה לחימת סייבר מוגדרת כלחימה א-סימטרית. השימוש במרחב הקיברנטי בעת לחימה מטשטש מאוד לא רק את העולם הפיסי עם העולם הווירטואלי, אלא גם את העולם האזרחי עם העולם הצבאי. בעימותים כמו העימות הקיברנטי בין ישראל לחיזבאללה בזמן מלחמת לבנון השנייה בקיץ 2006 רואים כי אזרחים ומומחים מחשב משני צידי המתרס נטלו חלק

<sup>98</sup> Cult Dead Cow, FAQs, [http://www.cultdeadcow.com/cDc\\_files/HacktivismoFAQ.html](http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html)

<sup>99</sup> PCBS, Palestine in Figures 2009, <http://www.pcbs.gov.ps/Portals/PCBS/Downloads/book1661.pdf>

<sup>100</sup> Makram Khoury-Machool: Palestinian Youth and Political Activism the emerging Internet culture and new modes of resistance (Policy Futures in Education, Volume 5, Number 1, 2007)

<sup>101</sup> Timothy Jordan: Technopower and its cyberfutures (Living with Cyberspace, Technology and Society in the 21st Century. Continuum 2003, pp 120-131)



פעיל במאמצי הלחימה כ"חילים וירטואליים". גם תומכים יהודים וגורמים אנטי ישראלים הצטרפו מהר מאוד למערכה ותרמו, כל אחד בתחומו, למאמץ הכללי<sup>102</sup>. בתקופת המלחמה עשו שני הצדדים שימוש מאסיבי בכלים טכניים לצרכי פגיעה, השבתה וסילוף מידע במערכות היריב.

## המשטים לעזה

בשנים 2010-2011 נעשו מספר ניסיונות לשבור את הסגר על רצועת עזה ולהעביר סיוע הומניטארי באמצעות ספינות של מתנדבים מארצות אירופה והמזרח התיכון. אחד המשטים הסתיים בהתנגשות חריפה בין כוחות צה"ל לפעילים על ספינה טורקית בשם "מרמרה" ב-31 במאי 2010. כחלק מגל המחאה האנטי ישראלי בעקבות המשט התרבו מאוד מקרי ההתקפות על אתרים ישראלים רשמיים בידי פעילים פרו פלשתינים/טורקים ברחבי העולם. בנובמבר 2011 הופלו מספר אתרי ממשלה ואתר המוסד ככל הנראה על ידי פעילים של ארגון אנונימוס כתגובה על עצירת משט נוסף כמה ימים לפני כן<sup>103</sup>. לפני ההתקפה פרסם הארגון סרטון ב-YouTube ובו הוא תיאר את עצירת המשט כפשע נגד האנושות, הדמוקרטיה, השלום וחוקי הימאות. הארגון איים כי מדינת ישראל חייבת להפסיק לעצור משטים חוקיים, לדבריו, בשם המאבק בטרור ולהפסיק לעצור אנשים חפים מפשע אשר מנסים לסייע לתושבי עזה. במידה ולא יעצרו הפעולות הללו, לארגון לא תיוותר ברירה והוא יתקוף פעם אחר פעם עד אשר הפעילות של ישראל תיפסק. הקריין בסרטון חותם את דבריו במשפט: אנחנו אנונימוס. אנחנו לא סולחים ולא שוכחים. מדינת ישראל, צפי לנו"<sup>104</sup>.

## ההאקר הסעודי

"למעלה מ-400 אלף פרטים מלאים של ישראלים, ביניהם עשרות אלפי פרטי כרטיס אשראי, נגנבו על ידי האקרים סעודים. ההאקרים מתכוונים לפרסם עד כמיליון כרטיסי אשראי", כך זעקה הכותרת הראשית באתר Ynet ב-2 בינואר 2012 במה שנודע מאוחר יותר כפרשת "ההאקר הסעודי"<sup>105</sup>. ההאקר (או קבוצת האקרים) תחת הכינוי 0xOmar העלתה לאתר בשם Pastebin רשימה שכללה כמה מאות אלפי רשומות ובהן פרטי כרטיסי אשראי של לקוחות ישראלים.

בימים הראשונים שלאחר התפוצצות הפרשה שררה אווירת פאניקה בקרב רבים בציבור. הציבור הרחב נחשף בפעם הראשונה לתופעה מוכרת וותיקה בעולם הפשיעה הקיברנטית, אך הפעם מזווית לאומנית. התבטאויותיו של מי שטען כי הוא ההאקר הסעודי, הן באתרי אינטרנט שונים<sup>106</sup> והן לכלי תקשורת

<sup>102</sup> Sabrine SAAD et al.: **Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield** (WebSci'11 2011)

<sup>103</sup> Haaretz, Israel government, **security services websites down in suspected cyber-attack**, <http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042>

<sup>104</sup> YouTube, **Anonymous- A Message to the State of Israel**, <http://www.youtube.com/watch?v=Z3l1wDWYQwk&feature=related>.

<sup>105</sup> YNET, **אלפי כרטיסי אשראי ישראלים נגנבו על ידי האקרים**, <http://www.ynet.co.il/articles/0,7340,L-4170430,00.html>

<sup>106</sup> Pastebin, **group-xp credit cards update**, <http://pastebin.com/13nJQQ9p>

ישראלים<sup>107</sup>, הצביעו בבירור כי המניע לפעולה היה לאומני. למרות שהסתבר בדיעבד כי מספר כרטיסי האשראי שנחשפו בפועל היה קטן בהרבה מהמספר הראשוני שפורסם<sup>108</sup>, פרשת ההאקר הסעודי העלתה לכותרות נקודה מעניינת נוספת: הוספת מימד קיברנטי לעורף הלאומי. הקלות שבה ניתן לבצע מניפולציות ולפגוע בביטחון האישי של כל אחד מאתנו הודגמה ביתר פשטות בפרשה הזו. כואבת לא פחות הייתה התגובה הלא מקצועית, לא מידתית ולא אחראית של חלק מאנשי המקצוע שהתראיינו לכל כלי תקשורת בשטח וגרוע מכך - אנשי ציבור שנהגו כך<sup>109</sup>. שירות חשוב מאוד שפרשת ההאקר הסעודי ופרשת הפלת אתרי אל-על והבורסה שהתלוותה אליה סיפקו לנו, הוא הצורך החיוני העלאת המודעות הלאומית והאישית של נושא אבטחת המידע באינטרנט.

### ארגוני טרור - החיזבאללה

הלחימה בין צה"ל לחיזבאללה מתרחשת כבר יותר משני עשורים במקביל בכל הזירות המוכרות לנו: יבשה, ים ואוויר. הצהרות הצדדים וכן הניסיון מלמדים אותנו ששני הצדדים עושים שימוש מרובה גם במרחב הקיברנטי כדי להתיש את הצד השני ולהשיג הישגים גם בחזית זו. לחיזבאללה מוטיבציה ברורה לפעול במרחב זה ממספר סיבות: ראשית מדובר בזירה שבה "נעלם" היתרון לגודל. האסימטריות של המרחב הקיברנטי מעמידה ארגון כמו החיזבאללה בשורה אחת עם המתקדמות שבמדינות העולם. מוטיבציה נוספת נעוצה באופי של הארגון השיעי ובהיותו ארגון המאמץ טכניקות וטכנולוגיות חדשות בכל רבדי הלחימה<sup>110</sup>. ארגון זה מחבר את תפיסת הלחימה הקיברנטית שלו עם פעילות בממדים אחרים ובמיוחד מול הציבור הרחב.

גיוס דעת הקהל היא, כמובן, אחד הפרמטרים החשובים ביותר בפעילות של כל ארגון טרור. החיזבאללה מראה כי כבר באמצע שנות האלפיים הוא היה חדשני מספיק כדי להבין את החשיבות של תחזוקת אתר אינטרנט עשיר בתכנים. הארגון הפך מהר מאוד את אתר האינטרנט שלו מדף חיוור ואינפורמטיבי לאתר דינמי ועשיר בתכנים כמו סרטוני וידאו, מידע על פעולות הארגון ברחבי העולם, העלאת תכנים של גולשים ועוד<sup>111</sup>. השימוש באינטרנט על ידי החיזבאללה נועד בראש וראשונה למטרות התמודדות והגנה בפני האמצעים העדיפים של צה"ל. רוב יכולותיו הטכנולוגיות של הארגון הוסבו להגנה על התשתיות הקריטיות שלו ובראשן - ערוץ השידור העצמאי "אל-מנאר". מאמצים אלה הוכחו כמוצלחים ואל-מנאר הצליח לשדר בצורה טובה יחסית בכל ימי הלחימה<sup>112</sup>.

<sup>107</sup> YNET, **ההאקר הסעודי ל-ynet: "זו רק ההתחלה"**, <http://www.ynet.co.il/articles/0,7340,L-4171895,00.html>  
<sup>108</sup> הכנסת ה-18 - פרוטוקול מס' 116 משיבת ועדת המדע והטכנולוגיה (10 בינואר 2012):

[www.knesset.gov.il/protocols/data/rtf/mada/2012-01-10.rtf](http://www.knesset.gov.il/protocols/data/rtf/mada/2012-01-10.rtf)

<sup>109</sup> גלובס, **ההיסטוריה הסעודית**, <http://www.globes.co.il/news/article.aspx?did=1000713182>

<sup>110</sup> Hasan M Al-Rizzo - **The undeclared cyberspace war between Hezbollah and Israel** (Contemporary Arab Affairs, v1, Issue 3, 2008)

<sup>111</sup> M J Warren - **Terrorism and The Internet** (chapter 4), in Lech Janczewski- Cyber Warfare and Cyber Terrorism (electronic recourse) [http://www.google.co.il/books?id=6CJ-aV9Dh-QC&printsec=frontcover&source=gbs\\_ge\\_summary\\_r&cad=0#v=onepage&q&f=false](http://www.google.co.il/books?id=6CJ-aV9Dh-QC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)

<sup>112</sup> David A. Acosta-**THE MAKARA OF HIZBALLAH DECEPTION IN THE 2006 SUMMER WAR** (Naval Postgraduate School, June 2007) <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469918&Location=U2&doc=GetTRDoc.pdf>

## ממשלות

אבטחת מידע באינטרנט הפכה בשנים האחרונות מכלי טקטי יומיומי לקונספט אסטרטגי. השילוב של התלות ההולכת וגדלה של העולם במחשבים ובתקשורת אינטרנט ביחד עם היכולות המתפתחות של התוקפים וכניסה של גורמים מוסדיים לתחום, הם שמאיימים כיום על מדינות וארגונים בינלאומיים.

מדינות רבות החלו עושות צעדים במימוש יכולות מתקדמות במרחב הקיברנטי מתוך הבנת חשיבות מרחב זה על שדה המערכה העתידית<sup>113</sup>. כמו שמלחמות העולם הראשונה והשניה הביאו עמן תנופה טכנולוגית משמעותית בכלי הלחימה, כך עידן המידע הביא עימו יכולות חדשות בתחום הלחימה הקיברנטית. מערכות המידע נוגעות בכל המערכות שאנו מכירים ולכן מהוות בסיס רחב לפעילות סייבר של מדינות. באופן אירוני, דווקא אותן מעצמות שהכרנו מהעולם הפיזי כבלתי מנוצחות, הפכו פגיעות מאוד להתקפות קיברנטיות בשל התבססותן על מערכות מידע<sup>114</sup>.

בשנים האחרונות אנחנו עדים למגוון דוגמאות לפעילות קיברנטית אינטנסיבית של מדינות העולם. בשנת 2007 הוסר פסל "חייל הברונזה" מאנדרטת הזיכרון לחיילים סובייטים במרכז בירת אסטוניה, טאלין. בתגובה פתחו גורמים עלומים בהתקפה קיברנטית חריפה כנגד מוסדות השלטון האסטוניים. על פי ההערכות, מדובר בגורמים רוסיים רשמיים שפעלו במסווה כנגד ההחלטה להסיר את הפסל<sup>115</sup>. גם סין היא אחת מהמדינות הפעילות ביותר בתחום. על פי הדיווחים, ענק זה הקים יחידה מיוחדת של לוחמי סייבר אשר משמשת את צבא העם הסיני במטלות שונות<sup>116</sup>. יש לציין, כי מזה מספר שנים קיימים חשדות לגבי פעילות סינית במרחב הקיברנטי. מדינה זו נודעה במספר פעולות מטרדות כמו למשל ניתוב לא חוקי של כ-15% מתעבורת האינטרנט בעולם למשך 18 דקות. פעולה זו לא ממש פוענחה על ידי גורמים במערב, אך היא בהחלט מוכיחה שיש מה לחשוש ממנה בכל הקשור ליכולות קיברנטיות<sup>117</sup>.

בסוף 2009 פתחה סין, על פי החשד, בהתקפה מתוכננת ומשולבת כנגד מספר חברות וגופים בינלאומיים ובראשם גוגל. על פי עדויות של גורמי מקצוע שחקרו את ההתקפות עולה, כי רמת התחכום ובעיקר טשטוש העקבות מוכיחים מעל לכל ספק כי מדובר במדינה. המתקפה, אשר נודעה בשם הקוד Aurora הביאה לחשיפת סודות וקניין רוחני מגוגל וכן לחשיפת פרטי משתמשים בשירות המייל שלה, תוך שימוש בקוד עזר שלא מוכר ליצרניות האנטי-וירוס ומימוש טכנולוגיות הצפנה מתקדמות<sup>118</sup>. התקפה

<sup>113</sup> Kenneth Geers - Strategic Cyber Security ( NATO Cooperative Cyber Defense Centre of Excellence June 2011), [http://www.ccdcoe.org/publications/books/Strategic\\_Cyber\\_Security\\_K\\_Geers.PDF](http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF)

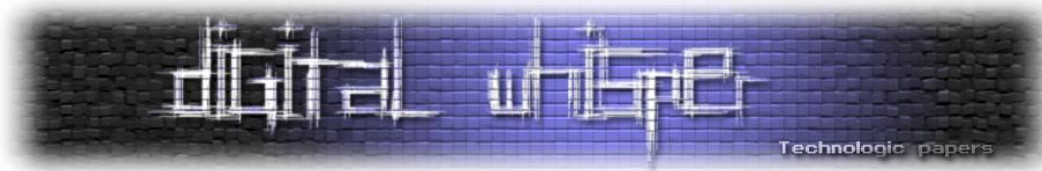
<sup>114</sup> James Adams - **Computers Are the Weapons & the Front Line Is Everywhere** (Simon & Schuster; 1'st edition (August 10, 1998))

<sup>115</sup> The Guardian, **Russia Accused Of Unleashing Cyberwar To Disable Estonia**, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>

<sup>116</sup> Channel 4, **China admits cyber warfare unit**, <http://www.channel4.com/news/china-admits-cyber-warfare-unit>

<sup>117</sup> U.S.-China Economic And Security Review Commission, Report to Congress (One Hundred Eleventh Congress, Second Session, November 2010): [http://www.uscc.gov/annual\\_report/2010/annual\\_report\\_full\\_10.pdf](http://www.uscc.gov/annual_report/2010/annual_report_full_10.pdf)

<sup>118</sup> Wierd, **Google Hack Attack Was Ultra Sophisticated, New Details Show**, <http://www.wired.com/threatlevel/2010/01/operation-aurora/>



נוספת שיש המייחסים אותה לסין, אירן או רוסיה היא ההתקפה על חברת RSA במרץ 2011 שבמסגרתה נפרצו אמצעי ההגנה של החברה ונגנבו פרטים רגישים הקשורים למוצר בשם SecureID, המשמש כאמצעי להזדהות חזקה.<sup>119</sup> מתקפה זו הייתה, ככל הנראה, יריית פתיחה למתקפה קיברנטית אחרת שבוצעה על תשתיות חברת Lockheed Martin (יצרן מערכות הביטחון וההגנה הגדול בארה"ב) מתוך כוונה לגנוב מידע ביטחוני רגיש הקשור לאחד ממוצריה.<sup>120</sup>

ישראל וכמובן ארה"ב הן שחקניות דומיננטיות נוספות במרחב הקיברנטי ועל פי גורמים מקצועיים הן אף פיתחו כלי נשק קיברנטיים למטרות שונות.<sup>121</sup> לשם המחשה, את "יצירת הפאר" הקיברנטית Stuxnet, שכבר הוזכרה לעיל, פיתחו על פי הערכות ארה"ב וישראל במשותף מתוך כוונה לפגוע בתוכנית הגרעין האיראנית. תוכנה זו היא חלק מפרויקט בשם "המשחקים האולימפיים" אשר החל בימי הנשיא בוש הבן וכלל, שוב, על פי הערכות, אמצעים טכנולוגיים שונים שנועדו לחבל בתוכנית הגרעין האיראנית.<sup>122</sup> מדינות נוספות שידועות בשל הפעילות הענפה שלהן בממד הקיברנטי הן צפון קוריאה,<sup>123</sup> רוסיה וצרפת.<sup>124</sup>

## התמודדות חוק המחשבים והתמורות בעולם הטכנולוגי

חוק המחשבים נחקק בשנת 1995 וחלק מההגדרות שבו נלקחו מתזכיר החוק משנת 1987 (תזכיר שלגי). עם זאת, ההגדרות שבו אינן מתאימות לעידן האינטרנט המהיר, הטלפונים החכמים והמכשירים הרבים המחוברים היום לרשת המידע. השלב הבא של האינטרנט IOE (Internet On Everything) יחבר כל מכשיר פיזי לרשת, החל מהדור הבא של התקנים ניידים, דרך Google Glasses וכלה במכוניות, שעונים וכדומה.<sup>125</sup>

אין לנו ספק כי ההגדרות לחוק המחשבים יהיו חייבות לעבור רענון על מנת להתמודד עם שינויים אלו. אחד האתגרים הגדולים העומדים בפני מערכת המשפט הוא בעיית האכיפה הבינלאומית של עבירות מחשב ועבירות חדירה, רבים המקרים בהם העברין נמצא מחוץ לגבולות השיפוט של מדינת ישראל.

<sup>119</sup> Gartner, **RSA SecurID Attack Details Unveiled They Should Have Known Better**, <http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-secrid-attack-details-unveiled-they-should-have-known-better/>

<sup>120</sup> InformationWeek, **Lockheed Martin Suffers Massive Cyberattack**, <http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151>

<sup>121</sup> McAfee, **McAfee Inc. Warns of Countries Arming for Cyberwarfare**, <http://www.mcafee.com/de/about/news/2009/q4/20091117-01.aspx>

<sup>122</sup> The New-York Times, **Obama Order Sped Up Wave of Cyberattacks Against Iran**, [http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?\\_r=0](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0)

<sup>123</sup> James L. Lewis - **The "Korean" Cyber Attacks and Their Implications for Cyber Conflict** (Center for Strategic and International Studies, Oct. 2009): <http://dspace.cigilibrary.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20The%20Implications%20for%20Cyber%20Conflict.pdf?1>

<sup>124</sup> McAfee, **McAfee Inc. Warns of Countries Arming for Cyberwarfare**, <http://www.mcafee.com/de/about/news/2009/q4/20091117-01.aspx>

<sup>125</sup> Cisco Blog, **Internet of Everything: Fueling an Amazing Future #TomorrowStartsHere**, <http://blogs.cisco.com/news/internet-of-everything-2/>

בשנת 2001 נחתמה אמנה בינלאומית למלחמה בעבירות מחשב ואינטרנט על ידי 26 מדינות אירופאיות וארה"ב. ישראל אינה חלק מאמנה זו. שיתוף פעולה עם מדינות אחרות יהיה עשוי להיות הכרחי בהווה ובעתיד<sup>126</sup>. חוק המחשבים מאפשר פרשנות רחבה להגדרה של מה זה "עבירות מחשב" ומתייחס ברצינות רבה לאפשרויות הרבות שפותחת טכנולוגיית המחשוב בפני העבריינים הפוטנציאליים. המחוקק מודע לכך שפעולות מחשב רבות ושגרתיות עלולות להוות עבירה פלילית (לדוגמא: פס"ד מזרחי - אליו נתייחס בהמשך).

ההבדל הדק בין פעולה שגרתית או בדיקה לבין פריצה/חדירה ואיסוף מידע לא חוקי מחייב את בית המשפט לערוך הבחנה בין סוגי העבירות ולאתר מתוך כלל הראיות את כוונת המבצע על מנת להכריע האם בעבירה פלילית עסקינן או בפעולה לגיטימית. אחד המפתחות לפתרון הוא פירוש המונח "שלא כדין" ומכאן העברת נטל ההוכחה אל התביעה. כוונת המחוקק במקרה כזה הייתה לחייב את המשתמש לקבל רשות לביצוע הפעולה הנחשדת כעבירה ובמקרה של חריגה, הרי שלפנינו מעשה שנעשה "שלא כדין".

חדירה למחשב הוגדרה במדינות רבות בעולם כעבירה פלילית בעיקר כי החדירה היא השלב ההכרחי בדרך לביצוע עבירות נוספות באמצעות המחשב, בפס"ד מזרחי<sup>127</sup> ציין השופט טננבוים כי אין הגדרה בהירה למונח "חדירה למחשב". הנאשם זוכה מחדירה לאתר האינטרנט של המוסד לאחר שבית המשפט שוכנע כי ביקש אך ורק לבדוק את אבטחת האתר.

ניתן ללמוד ממקרה זה שלמרות שהחדירה למחשב אסורה לכאורה ניתן, לדעתנו, להבין כי זהו שלב הכרחי בכל פעולה בין מחשבים והשאלה הנשאלת היא מה מטרת החדירה? לאחר שענינו על שאלה זו, יש לקבוע האם זו עבירה או פעולה לגיטימית. עוד מציין השופט טננבוים כי חקיקת אינטרנט יש לפרש בצורה שתעזור לעולם האינטרנט להמשיך ולהתפתח קדימה לטובת הציבור ולא בצורה שתגביל, תפריע ותעכב התקדמות זאת. לנושא פרשנות המונח "שלא כדין" התייחסו עו"ד נעמי אסיא ועו"ד רחל אלקלעי<sup>128</sup>.

בהסתמך על הפסיקה הקיימת לגבי פירוש מונח זה, נראה כי הכוונה היא לקיום אלמנט של ידיעה לגבי העדר הרשות לביצוע המעשה (ביצועו שלא ברשות לפי כל דין), ואלמנט נפשי של פזיזות לגבי התוצאה העלולה להיגרם בעקבותיו; אין הכוונה כאן לפעולה המתבצעת מתוך רשלנות גרידא. עוד הציעו עו"ד הנכבדות בישיבת וועדת המשנה להצעת חוק המחשבים, שבכל מקום בו כתוב "שלא כדין" יש לכתוב אף "בזדון".

<sup>126</sup> Council Of Europe, **Convention on Cybercrime** (Budapest, 23.11.2001):  
<http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>127</sup> ת"פ 3047/03 מ"י נ' מזרחי אבי. ניתן בבית משפט השלום בירושלים ע"י השופט טננבוים ביום 29.2.2004

<sup>128</sup> אסיא נעמי, ואלקלעי רחל, "עבירות מחשב בעשור החולף", שערי משפט, כרך ד' 2, 2006, ע' 397



כדברי השופטת ברלינר בפס"ד טנבאום 4:

**"הצורך הוא לשדר מסר ברור כלפי אותו פלח צבור שממנו יכולים לבוא העבריינים הפוטנציאליים, קרי אנשים צעירים, נורמטיביים, שרקע חייהם תקין, ובמרבית המקרים כישוריהם השכליים למעלה מן הממוצע. נגד עיניהם של אלה צריכה להידלק נורה אדומה בכל פעם שהפיוי הקל והזמין לפורץ למחשב יעבור במוחם."**

אם כך, אנו רואים שמהות הענישה היא להרתיע בעונשים יחסית כבדים על מנת לנסות ולהתמודד עם הפיתויים הרבים שעולם המחשוב מעמיד בפני המשתמשים. הרי פשעי מחשב הם "נקיים": אין נפגעים פיזיים, אין צורך באלימות מוכחת כדי להשיג הישגים ולעיתים האקרים שפוגעים במערכות ממשל, מערכות פיננסיות וכו' אף נתפשים כגיבורים (כגון ארגון Wikileaks ו Anonymous לדוגמה). לכן הרתעה, חינוך והטמעה של מה מותר ומה אסור חשובה והכרחית כבר משלבים מוקדמים של חשיפה למחשוב. בחוק המחשבים ביקש המחוקק לנסות ולהסדיר את השימוש בטכנולוגיה. מחשבים וטכנולוגיה נתפשים, כאמור, כדבר חיובי הנועד לפיתוח החברה האנושית ומחיקת פערם.

מכאן פרשנות המונח חדירה צריך להיות כפוף לשינויים הטכנולוגיים הדחופים. הרי לפני בואה של Facebook רוב הדיונים ברשת היו על שמירת הפרטיות וכיום שימוש בפייסבוק, אינסטגרם ודומיהם משנה את הגדרת הפרטיות. לדעתנו מדובר בשינוי במונח "חדירה למחשב" כי הרי שימוש גובר ותכוף ברשתות חברתיות מזמין סוג של חדירה למחשב ללא רשות אך ללא כוונה פלילית מצד החודר. ניתוח שנעשה ע"י פרופסור קר (Kerr) לביטוי "Unauthorized Access" מצביע על היעדר אחידות בפירוש לביטוי ומציע להבחין בין גולש שניגש למחשב תוך הפרת תנאי החוזה שבינו לבין מפעיל אתר למשל לבין גישה לחומר מחשב הכרוכה בעקיפת מנגנונים טכנולוגיים.

לשיטתו העבירה הפלילית היא במצב השני, פרשנות זו מאזנת בין שני ערכים מנוגדים: חירות השימוש ברשת מול פרטיות הגולשים שמידע עליהם מוחזק אצל התארים בהם הם גולשים, כך אנו רואים שיש העברת מידע בצורה "התנדבותית" של אנשים וארגונים לצד שלישי שלא תמיד ברור מה הם עושים במידע זה וכיצד הם שומרים עליו<sup>129</sup>.

האם מכירת מידע כזה לצד שאינו קשור לגולש המקורי מהווה חדירה למחשבו של התובע? אנחנו לא בטוחים כי ניתן להחיל את חוק המחשבים במקרה כזה וזהו עניין הנתון לפרשנות רחבה. לסיכום דיון זה יש לדעתנו לפרש את חוק המחשבים על פי התמורות החלות בעולם הטכנולוגי ולתת פרשנות מצומצמת ככל הניתן למונח חדירה למחשבים.

<sup>129</sup> Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", 78 NYU L. Rev. 1596 (2003).

הקשר בין טכנולוגיה למשפט מחייבת העמקת הידע אצל העוסקים בשפיטה על מנת לסייע להם בהבנת התמורות המהירות בעולם המחשוב ( אין לדעתנו מקום להתייחסות למחשב כיחידה בודדת). בהקשר זה נבקש לסיים עם דבריו של ד"ר מיכאל בירנהק<sup>130</sup>: "את חוק המחשבים יש לפרש על רקע עקרונות אבטחת המידע המקובלים אצל מפעילי מערכות מידע, כלומר על פי עקרונות טכנולוגיים. הדיאלוג בין המשפט לטכנולוגיה צריך להתנהל תוך תשומת לב לטכנולוגיה, לאפשרויות ולקשיים הגלומים בה, תוך ערנות לקשיי אכיפה אפשריים ולתגובה הטכנולוגית האפשרית".

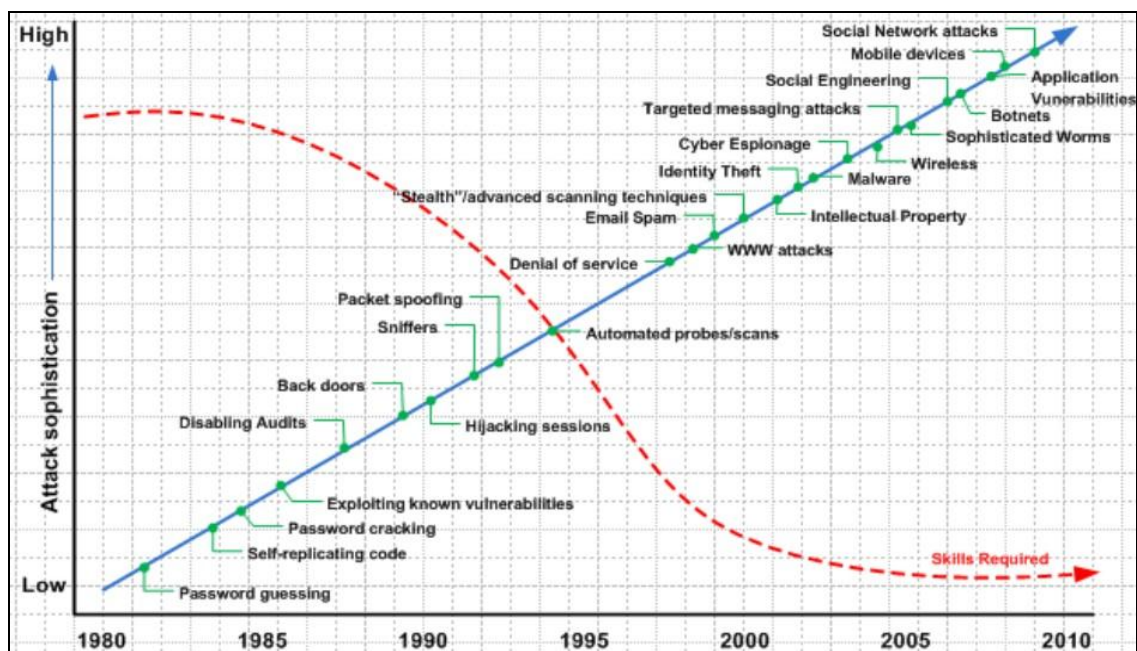
## סיכום ומסקנות

קנת' גירס (Kenneth Geers) מ-NATO Cooperative Cyber Defense Centre of Excellence בחן בעבודת מחקר שביצע בשנת 2011 ארבע אסטרטגיות אופציונאליות להתמודדות מדינות עם איומים קיברנטיים. אחד מהם היה טכנולוגי (יישום הדור הבא בפרוטוקולי הניתוב ברשת האינטרנט - IPv6). השני, אסטרטגיית המלחמה המוצגת בדוקטרינה של סון טסו (Sun Tzu) "אומנות המלחמה" היא מנגנון מלחמתי. השלישי, מנגנון הרתעה בעולם הסייבר, הוא שילוב של אמצעים פוליטיים צבאיים וכמוהו הרביעי: מנגנוני פיקוח על נשק.

גירס מוצא במחקרו כי אופי האיומים לא השתנה בהרבה ברבות השנים. השינוי המהותי הוא במהירות, בהיקף ובעוצמה של ההתקפות. כתוצאה מכך, הסיק, תשתיות קריטיות מצויות בסיכון רב לא רק בימי מלחמה, אלא גם בעיתות שלום. גירס סבר במחקרו כי במלחמות העתידיות צפוי משקל רב לאלמנט הקיברנטי. משקל שקשה מאוד לאמוד אותו כיום. מסקנתו הייתה כי מוטב למדינה להסתמך על אמצעים טכנולוגים עד כמה שניתן כדי להתמודד בצורה מיטבית עם האיומים הקיברנטיים. אמצעים טכנולוגים כדוגמת יישום IPv6 מושפעים במידה מועטה יחסית מהפרעות חיצוניות והם נותנים מענה טוב לאחת הבעיות הכאובות ביותר במרחב הקיברנטי: אנונימיות<sup>131</sup>.

<sup>130</sup> ד"ר מיכאל בירנהק, משפט המכונה: אבטחת מידע וחוק המחשבים - 13.12.2006 ציטוט מאתר דיני רשת, [http://netlaw.co.il/it\\_itemid\\_3595.html](http://netlaw.co.il/it_itemid_3595.html)

<sup>131</sup> Kenneth Geers - **Strategic Cyber Security** (NATO Cooperative Cyber Defense Centre of Excellence June 2011), [http://www.ccdcoe.org/publications/books/Strategic\\_Cyber\\_Security\\_K\\_Geers.PDF](http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF)



כשבוחנים את האבולוציה שעבר העולם הטכנולוגי מול האבולוציה של פריצה וחבלה במחשבים ומערכות תקשורת, ניתן לתאר את יחסי הגומלין בין השניים על פי התרשים הבא<sup>132</sup>:

מעיון בתרשים עולה המסקנה הבאה: רמת התחכום של ההתקפות ואפשרויות הפריצה למערכות מחשבים ותקשורת עולה באופן עקבי עם השנים (קו מגמה זה מסומן בכחול רצוף)<sup>133</sup>. בראשית שנות השמונים, עת הפך המחשב האישי לאביזר נפוץ בבתים רבים בארה"ב ולאחר מכן בשאר העולם, התפתח "מקצוע" לוואי חדש לתעשיית המחשבים, הפריצה הלא חוקית למערכות תקשורת ולמחשבים. אומנם, ראינו כי חלק מפעילות הפשיעה במחשבים החלה מוקדם יותר. עם זאת, שנות השמונים בהחלט זימנו צמיחה משמעותית בתחום והפכו את המחשב מכלי אוניברסיטאי למערכת ביתית. התרשים לעיל מראה מגמה חשובה נוספת בהתפתחות עולם המחשבים והפריצה למחשבים: תהליך הספיגה של הטכנולוגיה בקרב הציבור הרחב הוא תהליך שלוקח זמן (קו מקווקו אדום).

בתחילת שנות השמונים הנגישות למערכות מחשב עדיין הייתה מצומצמת יחסית. שפות הכתיבה והתכנות היו נחלתם של מעטים והשליטה בהן הפכה את המתכנתים לציבור קטן וייחודי. גם היכולת לגרום נזק למערכות, תוך פיתוח כלים ייעודיים לשם כך היו מוגבלים מאוד באותה תקופה. פריצות למערכות מחשב באותה תקופה מאופיינות ברצון לעמוד באתגרים טכנולוגיים, לזכות בתהילה ובמקרים מאוחרים יותר - גם ברווח כלכלי.

<sup>132</sup> המקור לתרשים אינו ידוע לנו. אנחנו מצאנו אותו בקישור הבא:

<http://itsecguru.blogspot.co.il/2009/11/information-security-threatscape.html>

<sup>133</sup> אין להניח כי העלייה היא ליניארית, אך זוהי דרך מקובלת להראות בצורה טובה את המגמה הכללית.

במהלך **שנות השמונים** של המאה העשרים הלך והתפשט השימוש הפרטי במחשבים ואיתו - הניצול לרעה של מערכות אלה. מגוון השיטות והפרקטיקות לפריצה למחשבים הלכו וגדלו ביחד עם שפות התכנות והמגוון של מערכות המחשוב והיישומים שלהן. רמת המיומנות אשר נדרשה לפריצה למערכות מחשב ותקשורת בסוף שנות השמונים של המאה העשרים הייתה גבוהה ודרשה יכולות גבוהות יחסית של הפורץ. ההאקרים של אותה תקופה, כמו קווין מיטניק שהוזכר לעיל, הם אנשים שהחלו את דרכם כפריקים של מערכות טלפוניה ותקשורת והכירו בצורה מעולה את פרוטוקולי הניתוב, מערכות הטלפוניה והמרכזיות וכן את פרוטוקולי התקשורת שהחלו להתפתח עבור מערכות המחשב והאינטרנט.

**שנות התשעים** סימנו את תחילת עידן האינטרנט המסחרי והגדילו מאוד את האטרקטיביות של הקישוריות בין מחשבים מסחריים ופרטיים. עולם הפשע לא נותר אדיש לנוכח מגמה זו. שנות התשעים אופיינו בחבורות ובודדים רבים אשר ניצלו לרעה את הפתיחות שאפיינה את מערכות התקשורת והאינטרנט כדי לפרוץ, לגנוב ו"לרוץ לספר לחבר'ה". חבורות האקרים כמו MOD ו LOD חייבו את הממסד הפדראלי בארה"ב להתחיל להתייחס לעולם הפשע הקיברני ברצינות רבה ולהתחיל להפנים את השינוי שחל. בשנים אלה "האידאולוגיה" מצטרפת ללוח המשחק הקיברנטי. בפרק זמן זה אנו נחשפים לקבוצות וליחידים אשר רצו לשדר מסר לחבריהם ולעולם. מוטיבציה נוספת שכבר ראינו בשנות השמונים (פריצה לשם רווח כלכלי) תופסת תאוצה בין השאר בשל מחשוב מערכות תומכות לתהליכים עסקיים וכניסה של אמצעי תשלום אלקטרוניים באותן שנים.

**שנות האלפיים** נפתחו בסערה עם עליה חדה בכמות הנוזקות שהחלו להתפשט ברשת. ראשית המילניום אופיין בניסיון של הפורצים וכותבי הנוזקות להגיע למאסות גדולות של מחשבים. יותר ויותר גופים ופרטים החלו להישען על רשת האינטרנט ככלי עבודה וכמנוע עסקי. עוד ועוד מערכות ציבוריות החלו את ההתנסות האינטרנטית שלהם באותן שנים. הקישוריות והפתיחות היו לרועץ בכל הקשור להתפשטות נוזקות ברחבי העולם. כתיבת הנוזקות חייבה עדיין התמחות, אולם שימוש חוזר בנוזקות שמישהו אחר כתב הפך לנפוץ מאוד.

בשנים האחרונות (אמצע שנות ה-2000 ואילך) כבר לא צריך לדעת לכתוב קוד כדי לפרוץ למחשב של מישהו אחר. הכלכלה האדירה שמושכת את תחום הפשיעה הקיברנטית שיכללה כל כך את השיטה, עד שאדם ללא רקע טכנולוגי יכול לגלוש לאתר כלשהו באינטרנט, להוריד בחינם "ערכת פריצה" ומשם הדרך קצרה מאוד עד לביצוע הפעולה הלא חוקית. מצד שני, המגוון העצום של מערכות המידע והגופים שמחוברים לרשת, מגדילים מאוד את "בנק המטרות" שהפורץ יכול לבחור לעצמו. אין מוסד או גוף מסחרי שיכול להרשות לעצמו להתנתק מהאינטרנט, אשר בו נמצא המנוע לפעילות העסקית של העולם שלנו. המפגש בין מערכות מחשוב מורכבות לנגישות גבוהה לפורצים מביא לעליה מתמשכת בכמות ההתקפות והפריצות לאורך השנים. שנות האלפיים פרצו את הדרך לפריצות על רקע לאומני ופוליטי.

עידן "הפריצות בסמכות" ולוחמת הסייבר, אותן פריצות שמאחוריהן עומדת מדינה, ליווה אותנו מראשית ימי האינטרנט, אולם תחום זה זכה לתהודה תקשורתית רבה מאוד בשנים האחרונות. שאר המוטיבציות שהוזכרו בעשורים הקודמים (אתגר, תהילה, רוח כלכלי ואידאולוגיה) עדיין רלוונטיות: טכנולוגיות חדשות מביאות אתגר פריצה חדשים; הרצון להרשים הוא יסוד סוציולוגי בסיסי גם אצל האקרים; הכלכלה השחורה רק מגבירה את הפריצות על רקע כלכלי ככל שהשנים נוקפות ואידאולוגיות שונות מתחזקות נתח משמעותי מהפריצות המתקשרות של השנים האחרונות.

המסקנה מעבודת המחקר הזו היא שמה שהשפיע על מניעי הפריצה למחשבים בין ראשית שנות השמונים של המאה העשרים לימינו הוא המגוון הטכנולוגי והרחבת השימושיות במערכות מידע, מחשבים ותקשורת. הרחבת השימושים במחשבים לכל תחום בחיים המודרניים מרחיב את האפשרויות ליהנות מהטכנולוגיה, אך גם לנצל אותה לרעה. ראינו במאמר זה כי הרחבת השימושים בטכנולוגיה פתחה צוהר למוטיבציות חדשות לפריצה למערכות. מה שהחל כאתגר וסקרנות, הוביל לחיפוש אחר הרווח אישי מהפריצה, לפרסום פוליטי של רעיונות ודעות, להתנגחויות לאומניות וכיום - גם למלחמות קיברנטיות של ממש.

## על המחבר

שחר גייגר מאור הוא מבקר פנים ביחידה לביקורת מערכות מידע בבנק הפועלים. בשש השנים האחרונות שחר שימש כסמנכ"ל ואנליסט בכיר לשירותי תשתיות בחברת המחקר STKI ויש לו הכרות מעמיקה עם עולם מערכות המידע ובמיוחד עם שוק אבטחת המידע. בין עיסוקיו ב-STKI ניתן למנות: ניתוח מגמות, טכנולוגיות ואסטרטגיות בעולם אבטחת המידע והתקשורת הארגונית בשוק המקומי והעולמי; הובלת מאות פגישות עבודה מול גופים עסקיים ומוסדיים בתחומי אבטחת המידע ומערכות המידע בישראל ונציגי חברות גלובליות; הנחיית סדנאות לקבוצות של 20-30 משתתפים (מפגשי "שולחן עגול"); מתן הרצאות בכנסים מקצועיים וכתובת חוות דעת ואנליזות לפי דרישה. שחר מחזיק בתואר ראשון בכלכלה ומנהל עסקים מהאוניברסיטה העברית בירושלים, תואר שני במשפטים מאוניברסיטת בר-אילן וכן בהסמכות CISSP מארגון ISC2 ו-"ניתוח והנדסת מערכות מידע" מהטכניון.