מדינת ישראל
משרד האוצר - אגף החשב הכללי
ועדת האינטרנט הממשלתית
WWW.ITPOLICY.GOV.IL

שם המסמך : סקירה מקוצרת – מלחמת המידע
תאריך כתיבה : 16/01/01
גירסא : 1.0
מצב המסמך : להפצה
שם לאחזור: Internet Warfare.rtf
כותב המסמך : טל רפפורט, דודו רשתי, אופיר בן-אבי

מלחמת המידע

הקדמה

דמיינו את עצמכם מתעוררים בבוקר, משפשפשים את עיניכם וחושבים קפה, ניגשים לקומקום החשמלי ומפעילים אותו – אין תגובה, מסובבים את ברז מים – אין מים, בחוגת הטלפון – אין צליל חיוג, מערכת הרמזורים בדרך לעבודה במצב של כתום מהבהב, בתחנת הדלק מספר לך המתדלק (שתקוע שם מאתמול בלילה) שמערכת החיוב בכרטיסי אשראי קרסה, הכספומט בבנק מודיע שאין ביכולתו לספק שירות. האנדרלמוסיה ברחוב עולה על כל דמיון, מערכת החשמל, תעבורה, תקשורת, והבנקים משותקות, אנשים משוטטים ברחוב ללא מטרה, המשטרה לא נראית, פעולות ביזה מתחילות...

מה קרה? כנראה שאתם צופים בסצנה הוליוודית מרהיבה שבהמשכה נחשפים טרוריסטים מגלומנים החודרים באמצעות האינטרנט עמוק לתוך מערכות המחשב של מערכות צבאיות ואזרחיות, משתלטים עליהן תוך פריצת הגנות בקלי קלות, דורשים סכומים כסף גדולים למטרות נאצלות , וכל זאת אל מול עיניהם המשתאות של פוליטיקאים ואנשי צבא המתקשים להבין את הנעשה עד להופעתו של הגיבור...

הסבירות להתרחשות התסריט ההוליוודי הפשטני קיימת, אך התחום בכללותו של מלחמת מידע (I-War, IW, C4I, Cyberwar) נמצא כיום ברמת מורכבות גבוהה יותר.
ממשלות רבות מקצות משאבים לחשיבה והתארגנות בתחום, מכוני מחקר מתמחים אוספים נתונים, יוצרים פרדיגמות תיאורטיות ומנסים להבין את היקף התופעה, ארגונים עסקיים מפתחים שירותי אבטחת מידע והגנה על מערכות מידע ובקרה, מנגנוני צבא וביון עוסקים במלחמת מידע שנים רבות ומפתחים כלי מגננה ומתקפה. מנגד, בצידו השני של המתרס, מבינים מספר הולך וגדל של גופים אידיאולוגים, פוליטיים, עסקיים וכו' את הפוטנציאל הגלום במלחמת המידע להשגת מטרותיהם באמצעים "אלגנטיים" ומתוחכמים.

מאז תחילת אינתיפדאת אל-אקצה נרשמו בישראל ניסיונות חדירה של גורמים זרים באמצעות רשתות תקשורת (מטווחי אינטרנט או ישירות דרך רשת הטלפון).[1] אתר החדשות wirednews טוען כי נערכה התקפה על מוסדות ישראלים רבים, ביניהם בנק ישראל, הבורסה, ספקי אינטרנט, בנק לאומי ועוד. הערכה היא שלא כל ניסיונות החדירה זוהו, כמות מסוימת של חדירות מתבצעות ללא השארת עקבות או יכולת הערכת נזקים.

מכל זאת עולה כי התסריט הקטסטרופלי שתואר לעיל אמנם עדיין לא התרחש, אך על מקבלי ההחלטות להפנים יותר ויותר את העובדה שהסבירות לביצוע "מבצע מידע" (IO–Information Operation) עולה ככל שמערכות תשתית עסקיות וממשלתיות מבוקרות ומופעלות באמצעות רשתות תקשורת ומערכות מידע.

[1] http://www.wirednews.com/news/politics/0,1283,40030,00.html

 / כל הזכויות שמורות, מדינת ישראל.

מטרת מאמר זה היא:

- סרטוט מסגרת התייחסות למלחמת המידע
- תיאור סוגי נשק ותיאורי מקרה במלחמה זו
- תיאור התארגנויות ממשלתיות בעולם בתחום זה
- תיאור המצב בארץ

הגדרה ומסגרת תיאורטית:

"מלחמת מידע היא השימוש ההתקפי או הגנתי, במידע ומערכות מידע, על מנת למנוע, לנצל, להשחית או להרוס מידע, תהליך עיבוד המידע, מערכות מבוססות מידע ומערכות תקשורת מבוססות מחשב. מטרת פעולות אלה היא להשיג יתרון על יריב צבאי או עסקי."

דר' איוון גולדברג (ראש המכון ללימודים מתקדמים של מלחמת מידע IASIW[2])

בספרו המפורסם של אלווין טופלר – "הגל השלישי" (The third wave), מגדיר המחבר את החברה שלנו כ"חברת ידע" שבה כל המערכות המרכזיות (פוליטיות, כלכליות, חברתיות..) נשענות על מערכות מידע ותקשורת מתקדמות החודרות לכל תחום בחיינו (דמיינו עולם ללא טלפון). הישענות זו על מארגי מידע ותקשורת מאפשרת לנו מחד, לבצע פעולות שבעבר תוארו רק בספרי מדע בדיוני, אך מאידך חושפות רגישויות חדשות מתחום הפרט, ועד לפעולות הבסיסיות של מדינות וארגונים מבוססי תקשורת. רגישיות אלה מוגברות כתוצאה מכך שמערכות תקשורת וידע מתחברות זו לזו ומפתחות יחסי גומלין (אני נופל = אתה נופל).

המודל הטוב ביותר כדי להבין את המכאניזם של מלחמת המידע הוא המודל האבולוציוני. על מנת לשרוד במשחק הקיום, מסתגלים אורגניזמים לשינויי סביבה. מיקרו אורגניזמים מפתחים הסוואה כימית להשתלטות על מערכות חיסוניות, טורפים ונטרפים מפתחים מערכות הטעייה בכל פינה בממלכת החי, כך, שכאשר מפתחים דיון ציבורי מורכב בנושא מלחמת המידע, צריך לזכור שהמכאניזם בבסיס הדברים הוא פשוט.

כאמור, היות והעולם עדיין מחולק ל"טובים" ו"רעים" (בנושא זה לא נצפתה כל התקדמות), מפתח כל אחד מהשחקנים בתחום, אסטרטגיות פעולה שונות התואמות את מטרותיו.
מקובל לחלק אסטרטגיות פעולה של שחקנים ל – 4 סוגים:[3]

1. מניעת מידע (Denial Of Information) – השימוש בהצפנה והסתרה על מנת למנוע מקבוצות ויחידים לא רצויים להשיג מידע בו הם מעונינים (דוגמא, מערכת הרשאות וסיסמאות).
2. הסוואה וחיקוי (Deception and Mimicry) – השגת מידע מהמערכת תוך הסוואת זהות החודר.
3. שיבוש והרס מערכות (Denial of Service, Disruption & Destruction) – החדרת מידע למערכת הגורם להטעיית נתונים או חוסר תפקוד של מערכות היריב עד הרס טוטלי ([4]התקפות PING, פצצות EMP).
4. חתרנות – (subversion) – החדרת מידע המפעילה תהליך השמדה עצמי במערכת היריב (פצצות לוגיות, וירוסים, סוסים טרויינים...).

---

[2] http://www.psycom.net/iwar.1.html

3 Carlo Kopp –(2000) Information Warfare Part 1 A Fundamental Paradigm of Infowar

[4]תוכנות המופעלות מרחוק ליצירת עומס מלאכותי על השרת עד לשיתוקו.

 / כל הזכויות שמורות, מדינת ישראל.

ווין שוורצו (Winn Schwartau), תאורטיקן מרכזי בתחום מגדיר כמה סוגיות עיקריות להתייחסות למלחמת המידע כיום:

1. התמודדות עם כשלי אנוש בתחום (Human Factors).
2. התמודדות עם בעיות תחיקה בנושא.
3. מציאת פתרון לבעיית הערכת הנזקים.
4. בידוד אפקט הנזק כדי לצמצם נזק משני (collateral damage).
5. התמודדות עם השאלה - כיצד מקצים כוחות למלחמת מידע?

הקושי העיקרי בתחום נעוץ בכך שמסגרת חשיבה המתאימה לעידן המידע הדיגיטלי, נמצאת עדיין בחיתוליה. רבים ממקבלי ההחלטות אינם ערים לשינוי הערכים המתחייב ממהפכת המידע. בזמן שביל גייטס הפך להיות האיש העשיר בעולם, מערכת הערכים החברתית המקובלת לא עברה במלואה מהעידן התעשייתי לתפיסה מלאה של המציאות הדיגיטלית בה אנו חיים כיום. תאורטיקנים טוענים שעד שלא נזכה לחוות את ה"פרל- הרבר" של עידן מלחמת המידע, הנושא לא יקבל את הדגש המתאים.

כלי נשק במלחמת המידע:

כדי להבין את רגישות המערכת מומלץ להכיר את כלי הנשק הפעילים בתחום[5]:

1. וירוסים (Computer Viruses): רסיס מידע המשעתק עצמו לתוך תוכניות מחשב ומשנה אותן. ככל שמחשב "בא במגע" עם יותר מחשבים, כך הוא חשוף יותר להידבקות. וירוס יכול להרוס מידע, תוכנות וחומרה. הוירוס הוא הכלי הנפוץ ביותר במלחמת מידע, אלפי וירוסים רשומים בעולם וישנם מקרים רבים בו הם הופעלו וגרמו לשיתוק מערכות. וירוס הוא כלי נשק בעזרתו אפשר לשתק מערכות מכל סוג ואף להרוג אנשים (שיתוק בתי חולים, נמלי תעופה...). קשה מאוד להלחם בוירוסים שכן במקרים רבים כדי לפתח נוגדן, צריך לזהות את הוירוס לפני תחילת הפעולה. וירוסים גרמו לנזקים גדולים בעבר וימשיכו לעשות זאת בעתיד.

2. סתימה אלקטרונית (Electronic Jamming): היכולת לסתום את מערכת התקשורת ברעש כך שלא ניתן יהיה לקבל בה מידע ואף לשלוח בה מידע מוטעה.

   ב-1996[6] דווחו לפחות 4 סתימות אלקטרוניות באתרי ה-FBI שגרמו לקריסתו. השיטה החביבה אל האקרים היא יצירת תכנה הגורמת לאתר לחשוב כי מיליוני קבצי דואר אלקטרוני נשלחים אליו.[7] שיטה אחרת אותה נקטו האקרים ישראלים ופלשתינאים באירועי אוקטובר 2000 היא יצירת שרשרת פקודות הגורמת לשרת האתר לטעון את האתר מחדש בהפרשי זמנים קצרים שגורמים לקריסת האתר.

   ידועה כפופולרית גם שיטת התקפות "פינג" (PING), בו שולח משתמש בקצב מהיר הודעות מיוחדות בעלות נפח גבוה המחייבות את שרת האתר לקבל אותן ולהשיב תשובה. הקצב המהיר של ההודעות מאט את תגובת האתר עד לשיתוקו.

3. סוסים טרויינים (Trojan Horses): תכנה המציגה עצמה לשימוש מסוים אך מטרתה האמיתית היא הרס המערכת. קל יותר להלחם בסוסים מאשר בוירוסים, שכן לרב הסרת התכנה תפתור את הבעיה, אולם, קשה יותר לגלות אותם מפני שתוכנות אנטי-וירוס אינן מזהות אותן.

---

[5] http://www.seas.gwu.edu/~reto/infowar/

[6] http://www.wired.com/news/politics/0,1283,19934,00.html

[7] http://www.wirednews.com/news/politics/0,1283,40030-2,00.html

4. תולעת (Worms): פועלת בדומה לוירוס אך בעלת כושר ניידות עצמאי ברשת. ב - 1988 שיתק רוברט מוריס, סטודנט אמריקאי, בתוך כמה שעות את מערכות המחשב המרכזיות בארה"ב וגרם נזקי חומרה במיליוני דולרים. מוריס שלח תולעת ניסיונית לרשת, אך ביצע טעות תיכנותית שגרמה לתולעת להתרבות בקצב אקספוננציאלי. שיקום הרשתות והסרת התולעת מהן לקחה זמן רב. מוריס נשלח לכלא.

5. פצצות לוגיות (Logic Bombs): אלמנט המצורף לתכנה תמימה שניתן להפעיל אותה כאשר מעוניינים לעשות כך. הפצצות בנויות כך שניתן להפעיל אותן מרחוק. ב – 1996 ידוע כי נשדדו 4 בנקים בריטיים בסכומים של עד 12 מליון פאונד לאחר שקבוצת טרוריסטים הוכיחה להם כי השתילה פצצות לוגיות שהפעלתן תגרום להרס מערכות המחשב והמידע של הבנקים. כמובן שגופים עסקיים הנפגעים בצורה כזו מעוניינים להשתיק את הפרשה.[8]

6. דלת ממולכדת (Back Door ,Trap Doors): מכאניזם המושתל בתוכנה על ידי המתכנת ומאפשר גישה חופשית דרך מערכת ההגנות. ב- 1998 הפיצה קבוצת האקרים בשם "פולחן הפרה המתה"[9] תוכנת חלונות BACKDOOR בשם 'Back Orifice' (BO). בכל מקום בו התקין משתמש את תוכנת החלונות, יכלו חברי הקבוצה לבצע פעולות באופן חופשי על המחשב האישי או השרת.

7. השתלת צ'יפים (Chipping): יצרנים מסוגלים להשתיל מנגנוני חמרה חבויים במחשב ולהפעיל אותם בשעת הצורך. ניתן באמצעות ההשתלה להרוס מערכות, לעקוב אחר פעילות, לנתר מיקום וכו'. השתלת צ'יפים נחשבת כנשק נדיר יחסית.

התארגנות ממשלתיות בתחום מלחמת המידע:

ב-1997 הוגש לנשיא קלינטון דוח בנושא מלחמת המידע (PPCIP[10]). המסקנה העיקרית בדוח, היא שמלחמת המידע מסכנת את תשתיות המידע של ארה"ב וכתוצאה מכך יש להקצות מיידית משאבים להגנתן. לצורך כך הוקם ב 1998 ב- FBI גוף מיוחד - NIPC[11] (National Infrastructure Protection Center) המרכז את כל הפעילות בנושא זה.

ב-NIPC מיוצגים כל הסקטורים המפעילים מערכות מידע, הסקטור העסקי, האקדמי והממשלתי. תפקידה של NIPC הוא:

- לאתר ולהעריך גורמי סיכון[12].
- לבצע חקירות לאיתור ותפיסת עבריינים.
- להגיב על התקפות על תשתיות מידע בארה"ב.

על מנת להגביר את שיתוף הפעולה בין הסקטורים האמורים יוסדה ב NIPC תכנית מיוחדת (Infragard) שבמסגרתה הוקם בכל סניף מקומי של ה- FBI (56 סניפים) משרד

---

[8] http://news.cnet.com/news/0-1005-200-311444.html?tag=

[9] :http://xforce.iss.net/alerts/advise5.php

[10] http://www.epic.org/security/infowar/epic-cip.html

[11] http://www.nipc.gov/

[12] http://www.fbi.gov/pressrm/congress/congress99/nipc10-6.htm

אחראי לנושא בו שותפים כל הסקטורים האמורים (518 חברים בכל ארה"ב). המשרד המקומי מספק לקהילה במסגרתה הוא פועל 4 שירותים עיקריים:

- אזעקת חדירה למערכות מידע.
- אתר מאובטח להעברת מידע על חשדות לפעילות עוינת.
- מרכז פעילויות לקהילה.
- מרכז מידע לקהילה.

במקרה של חשד לחדירה עוינת ניתן להעביר את המידע באופן מאובטח ל FBI במטרה לפתוח בחקירה, ולהעביר את המידע למטה הארצי של NIPC לצורך ניתוח המידע. אופן פעולה זה יוצר שיתוף מידע ופעולה בין גופים אזרחיים וגופי אכיפת החוק. ההנחה שהתארגנות משותפת תגביר את יכולת העמידה הביאה ליוזמות רבות נוספות בתחום, כמו זו של [13] משרד המשפטים האמריקאי שהקצה לאחרונה משאבים להתארגנות מדינתיות בתחום שמטרתן לרכז פעילות כנגד גורמים בתוך ארה"ב. [14]באריזונה לדוגמא, החליטו מספר סוכנויות במדינה לנצל את שיתוף הפעולה שנוצר בפרוייקט באג אלפיים לצורך מלחמת המידע. בועידה שהתכנסה בנובמבר 2000 הוחלט להקים מרכז שיטפל בנושא, תפקיד המרכז הוא לגבש תכניות למצבי חירום ולהוות מרכז מידע בשעת חירום לגופי ממשל. בכל פעם שתותקף סוכנות ממשלתית המידע ישלח למרכז ושם יוחלט איך לטפל במשבר.

גם מדינות הנמצאות בדרגת רגישות נמוכה מארה"ב שמות דגש על נהלים והתארגנות בתחום הבטיחות.

[15]בקנדה הנהיג ה – ITC יעוץ חובה בנושא הערכת סיכונים והערכות אליהם (Threat Risk Assessment) במערכות מחשב של סוכנויות ממשלתיות.

[16]באנגליה קיים גוף ממשלתי (CESG) שתפקידו לרכז את כל הפעילות הממשלתית בנושא אבטחת מידע ונוהלי הגנה בנושא. גוף זה מספק הנחיות גם לארגונים פרטיים.

באופן כללי, ההמלצות וההנחות תחתן פועלות ממשלות בעולם לטיפול בנושא הן[17]:

- יצירת מתודולוגיה להערכת סיכונים.
- יצירת קונצפטואליזציה של סביבת המידע.
- הגברת נהלי בטיחות.
- הגדרת דרישות בטיחות מיצרנים.
- ייסוד שיתוף פעולה ממשלתי\פרטי בתחום.
- הגברת חינוך בתחום ברמות שונות.
- שימוש בהאקרים כמשאב לאומי.
- יצירת שיתוף פעולה בין-לאומי.

הערכה היא שאם מכסים את כל התחומים הנ"ל ניתן להוריד באופן משמעותי את הן את הנזקים והן את התפשטות הנזקים כתוצאה ממלחמת מידע.

בישראל:

[13] http://www.gcn.com/archives/sl/1999/January/17a.htm

[14] http://www.govtech.net/news/news.phtml?docid=2000.11.02-2030000000000635

[15] http://www.cse.dnd.ca/cse/english/other.html

[16] http://www.cesg.gov.uk/

[17] Matthew G. Devost (1995) National Security In The Information Age

ביחס לעולם המערבי נמצאת ישראל בפיגור מסוים בהגנה על תשתיות מידע אזרחיות.

באירועי אוקטובר 2000, שימשה ישראל כשדה קרב של Cyber terrorist ממגוון גופים, בעיקר בניסיון להפיל באמצעות האינטרנט שרתי מידע חיוניים. למרות שלא נגרמו נזקים כבדים במתקפות אלה, הן מוכיחות כי יש להיערך בהקדם כדי להוריד את הסבירות לנזקים עתידיים קשים.

מסוף שנות ה-60, נמצאת האחריות בתחום האזרחי לאבטחת מידע אזרחי רגיש בידי השב"כ. כתוצאה מההתפתחות הטכנולוגית של השנים האחרונות, המליצה המועצה לביטחון לאומי להקים רשות מיוחדת לאבטחת מידע שתהייה כפופה לשב"כ או תפעל

באופן עצמאי. תפקידה של הרשות יהיה (בדומה לזה של NIPC האמריקאי) לפתח תורה בנושא, לעסוק בהערכת סיכונים, לגבש הנחיות מחייבות לגופים אזרחיים ולהוות מטה חירום. המלצה זו לא הגיע עדיין לשלבי ביצוע כתוצאה מעיקוב בתהליכי חקיקה.
בינתיים עד שתוקם הרשות, בעיצומם של ההתקפות על אתרים ישראלים, הציעה תהל"ה – (**ת**שתית **ה**ממשלה **ל**עידן **ה**אינטרנט, גוף האחראי לפיתוח תשתיות אינטרנט למערכת הממשלתית בראשות משרד האוצר) להקים מטה חירום שיורכב מנציגי כל הגופים בתחום. המטה ירכז את הפעילות, יאתר פרצות במערכת, ירכז מידע על התקפות, יהווה מוקד לשיתוף מידע בין גופים, יהיה מסוגל לצייר תמונה עכשווית של המצב ועוד. הקמה מטה מעין זה תיתן מענה מהיר למתקפות בהן עומדת ישראל בשדה הקרב החדש. הטיפול בהקמת המטה נמצא עדיין בדיון.

רשימת לינקים בנושא מלחמת מידע:

פורטלים ומכוני מחקר:

פורטל למלחמת מידע – מאמרים, חדשות, מוצרים...
http://www.infowar.com/

מכון מחקר בתחום מלחמת המידע – האתר מכיל רשימת קישורים בנושא.
http://www.psycom.net/iwar.1.html

פורטל מאמרים של ממשלת ארה"ב.
http://www.terrorism.com/infowar/index.shtml

http://netsecurity.miningco.com/compute/netsecurity/mbody.htm
פורטל מאמרים מקוטלגים לפי נושאים המספק מידע מקוצר על מושגים בתחום.

http://www.gcn.com/search/index.html
פורטל חדשות על ביטחון בממשל – מאמרים בנושא הקצבות והתארגנות ממשלתית.

מאמרים וספרים:

מאמר מבוא מצויין לנושא – מפרט מסגרת התייחסות לא טכנית, ראייה הסטורית ,סוגי נשק ועוד.
http://www.seas.gwu.edu/~reto/infowar/
ספר מקוון בנושא – כיצד להגן על מערכות מידע מהאקרים.
http://www.ods.com.ua/win/eng/security/Max_Security/index.htm

קרלו קופ - תזה בנושא מלחמת מידע והאיום על ארה"ב, סוגי נשק ומניעה (בסוף)

עבודת דוקטורט מקוונת בנושא מ-1995.
http://www.devost.net/mgd/documents/devostthesis.pdf

המלצות של מחקר של דר' ג'ון היוורד מ 1995 – נושא המחקר – ניתוח של מקרים ברשת 1989-1995. פרק 14
http://www.info-sec.com/internet/howard/table_of_contents.html

מאמר ב TIME MAGAZINE בנושא מלחמת מידע
http://www.time.com/time/magazine/archive/1995/950821/950821.cover.html

רשימה של 56 ספרים בחיפוש תחת INFORMATION WARFARE בחנות הספרים BARNES&NOBLE
http://shop.barnesandnoble.com/booksearch/results.asp?userid=1LOHO2PDDF&mscssid=&sourceid=&keyword=information+warfare&match=exact&options=and&srefer=&pcount=0

אתר המרכז מאמרים בתחום.
http://www.ndu.edu/inss/siws/ch7.html

http://www.psycom.net/iwar.2.html
מילון מונחים בנושא

http://secinf.net/info/misc/harmless/gtmhh/3_7_1.html
מאמר מבוא לוירוסים – סוגים, מניעה...

התארגנות ממשלתיות :

אתר ה NIPC : מטה הממשל האמריקאי המרכז פעילות לאומית בנושא.
http://www.nipc.gov/

אתר של גוף המייעץ לממשל הבריטי בנושאים של IW
http://www.cesg.gov.uk/

אתר של ממשלת קנדה בנושא IW
http://www.cse.dnd.ca/cse/english/home_1.html

כתבות וחדשות

מלחמת אינטרנט באינטיפדת אל-אקצה.
http://www.wirednews.com/news/politics/0,1283,40449,00.html
http://israel.internet.com/news/cyberterror1.html

תקציר ראיון עם ראש ה CIA בנושא – מספק רקע לנושא

http://www.infowar.com/class_2/class2_121498a_j.shtml

מאמר בעיתון על וירוס חדש בשם PAPA – האקרים נגד הממסד
http://www.internetnews.com/bus-news/article/0,,3_89541,00.html

כתבה על וירוס חדש התוקף דרך האוטלוק וגורם לקריסת מערכות.
http://www.info-sec.com/viruses/99/viruses_033099c_j.shtml

דוגמא לשימוש בתכנת BACK DOOR (1998) :
http://xforce.iss.net/alerts/advise5.php

כתבת חדשות על סחיטת בנקים באנגליה.
http://news.cnet.com/news/0-1005-200-311444.html?tag=

התקפות האקרים על ה FBI.
http://www.wired.com/news/politics/0,1283,21725,00.html

כתבה על קטגוריות של פשעי מחשב.
http://nsi.org/Library/Compsec/crimecom.html

 / כל הזכויות שמורות, מדינת ישראל.