שיקולים בפיתוח והפעלת נשק קיברנטי

מאת יובל סיני

הקדמה

עידן המידע, יצר עבור רבים כר של הזדמנויות חדשות, דבר אשר כלל בין השאר את לידתה של כלכלת המידע, האצת הגלובליזציה והחדשנות. לצד היתרונות הגלומים בעידן המידע, נוצרה תלות מלאה של מרבית הציבור ומדינות העולם בטכנולוגיה ובזמינות תשתיות קריטיות (Critical Infrastructure), כדוגמת תשתית החשמל והתקשורת, אשר בתורן משמשות כבסיס לתשתיות מידע קריטיות (Critical Infrastructure Information).

המרחב הקיברנטי (Cyber Space)[1], אשר בהתאם להגדרת מאמר זה כולל בחובו את העולם הווירטואלי אשר האדם יצר באמצעות טכנולוגית מידע ותקשורת (Information and Communication Technology), מאפשר לשחקנים (קואליציות, מדינות, ארגונים[2], קבוצות, ופרטים) לבחור באסטרטגיות פעולה מגוונות ודינמיות. הבחירה של שחקן באסטרטגיה נגזרת משורה של קריטריונים, כדוגמת צרכים עסקיים-פוליטיים, זמן ותמונת המצב הקוגניטיבית אשר כל שחקן בונה לעצמו. הבחירה במונח "תמונת המצב הקוגניטיבית" אינה מקרית, אלא היא באה לחדד כי אין לשחקן אפשרות לקבל תמונה מצב מלאה וריאלית, ולפיכך בעת הבניית העולם השחקן נאלץ להסתמך על מודלים הסתברותיים ו\או אקסיומות.

האסטרטגיה הדינמית אשר כל שחקן יבחר תשפיע על התנהלותו כלפי שחקן אחר, כדוגמת: שיתוף פעולה ויצירת בריתות, "ישיבה על הגדר", עימות גלוי, עימות עמום. כתוצאה מכך, כל שחקן בונה לעצמו את מטריצת ההתנהלות שלו כלפי השחקנים האחרים, כאשר שני היתרונות הבולטים במרחב הקיברנטי הינה היכולת לשנות את האסטרטגיה הנבחרת בקצב מהיר ובעלות נמוכה יחסית, וביכולת שחקן לאמץ בו זמנית מספר אסטרטגיות כלפי שחקן אחר, וזאת תוך צמצום האפשרות של השחקן שכנגד לחשיפתו של המשחק הכפול.

[1] ישנה סבירות גבוהה כי הגבולות בין המרחב הקיברנטי (Cyber Space), לעולם האלקטרומגנטי המופשט המוכר לנו כיום יטשטשו בעתיד.

[2] Non-State Entity

המונח נשק אינו חדש, ומטרתו להכליל את רשימת האמצעים שבהם צד יוכל להשתמש על מנת להטיל את מרותו החד צדדית של פלוני על האחר, וזאת לשם השגת מטרות כאילו ואחרות. המונח לוחמת מחשב (Cyber Warfare)[3] כולל בחובו שורה של פעולות התקפיות אשר שחקן יכול ליזום כלפי שחקן אחר במרחב הקיברנטי.

כניסתו של הנשק הקיברנטי לזירה הרחיב את מרחב ההזדמנויות והכלים אשר עומדים לרשות כל שחקן, ואין פלא כי המרחב הקיברנטי זכה להכרה בעיני רבים כמימד החמישי (The fifth dimension) של שדה הקרב המודרני. בהתאם לכך מאמר זה סוקר, על קצה המזלג את עיקר השיקולים בעת ההחלטה להפעיל נשק קיברנטי.

שיקולים בהפעלת נשק קיברנטי

עלות פיתוח ותפעול

עלות פיתוח אמצעי לחימה מסורתיים, עשויה להגיע למאות, אם לא לעשרות מיליארדי דולרים, כאשר זמן הפיתוח עשוי להגיע לא פעם אף לעשרות שנים . אף עלות הייצור עשויה להסתכם בסכומים לא נמוכים לפריט, כאשר ראוי לציין כי השימוש באמצעי לחימה מסורתיים עשוי להגיע בנקל לעלות של 10,000 - 30,000 דולר לשעה. אף אורך חיי אמצעי לחימה מסורתיים נמוך מעשור בממוצע, דבר המחייב חידוש מלאי באופן תקופתי.

בהתאם למספר מחקרים אשר בוצעו בשנים האחרונות, התגלה כי עלות פיתוח ה-Stuxnet מוערכת בכ-10-20 מיליון דולר, דבר אשר מציג כי ישנם מקרים רבים בהם ניתן לפתח ולהשתמש בנשק קיברנטי, וזאת ללא צורך בהשקעה תקציבית גבוהה. לאור העובדה כי מדובר בעלות לא גבוהה יחסית, מדובר בפתרון אידיאלי עבור גורמים רבים שאינם בעלי גב כלכלי ענף, כדוגמת ארגוני פשיעה וטרור.

אנונימיות הפיתוח, המכירה והשימוש בנשק קיברנטי

פיתוח נשק קיברנטי אינו תלוי מקום גיאוגרפי וזמן, ולפיכך ניתן לפתח אותו אף ללא קשר ישיר בין גורמי הפיתוח. הלכה למעשה, מרבית האמצעים לפיתוח נשק קיברנטי זמינים מזה שנים רבות למרבית הציבור, ואף גורמים בעל כישורים טכניים ממוצעים יכולים לפתח כיום נשק קיברנטי אפקטיבי.

אפשרויות תשלום מבוססות מטבע וירטואלי, כדוגמת ביטקוין מקלות על תהליכי מכירה ורכישה של נשק קיברנטי ב"שוק השחור", ולפיכך ניתן לזהות מגמה של מכירה ורכישה של נשק קיברנטי בין שחקנים שונים, כאשר למרבה ההפתעה התגלה לא פעם כי אף מדינות (כדוגמת אייזרביג'ן אשר שמה עלה לדיון בפרשת הפריצה ל-Hacking Team) רוכשות נשק קיברנטי ממקורות שונים ומגוונים.

[3] המונח Cyber Warfare זכה לתרגום עברי נוסף - "לוחמה קיברנטית".

המרחב הקיברנטי מקשה מטבעו על איתור פעילות השחקנים, ביחוד כאשר שחקנים אלו מאמצים טכניקות של חמקנות, עמימות והסוואה. לפיכך, לגורמי אכיפה וביטחון ישנו קושי ניכר לאתר ולפגוע בשחקנים המשתמשים בנשק קיברנטי, כאשר יש לזכור כי מרבית התקיפות הקיברנטיות מתבצעות תוך זמן קצר יחסית, דבר אשר מקטין את ההסתברות לאיתור יוזם התקיפה ע"י גורמי האכיפה והביטחון.

אורך חיים קצר של נשק קיברנטי

הצלחתו של הנשק הקיברנטי תלויה במספר פקטורים מהותיים, כדוגמת קיומה של פגיעות שלא תוקנה או לא ידועה (Zero Day Attack), כשל במעגל אבטחה אשר ניתן לניצול לרעה, אי מימוש מנגנוני אבטחה וכשל אנושי. הדינמיות בעולם המחשוב משאירה לשחקן "חלון הזדמנויות" צר יחסית, ועל כל שחקן לבחון האם הוא רוצה ומסוגל לנצל את "חלון ההזדמנויות" הצר, שלאחר סגירתו, הנשק הקיברנטי אשר ברשותו יהיה חסר תועלת.

התמקדות במטרות איכות

אחד היתרונות הבולטים של הנשק הקיברנטי הינו היכולת להתמקד (להתביית בעגה הצבאית) ב"מטרות איכות" לשם השגת מטרות מוגדרות, תוך צמצום ההשפעה הרוחבית על תשתית הארגון המותקף. רוצה לומר, שיטת פעולה זו מצמצמת את חתך החשיפה של הפעילות העוינת, דבר המקשה על איתורה. כמו כן, באמצעות התמקדות במטרות איכות, השחקן אשר בוחר להשתמש בנשק קיברנטי מגדיל את הוודאות כי במקרה כי התקיפה תצלח, הנזק אשר יגרם לשחקן המותקף יהיה גבוה. עם זאת, התמקדות במטרות איכות מחייבת מודיעין מדויק, ואף מעמידה רף קושי גבוה יותר לחציה, וזאת מכיוון שבארגונים רבים מוטמעות בקרות מפצות רבות לשם הגנה על ישויות אשר מוגדרות כמטרות איכות פוטנציאליות.

שיבוש פעילות ודיסאינפורמציה

לאור העובדה כי עידן המידע יצר תלות גוברת במחשוב, הנשק הקיברנטי מאפשר שיבוש של פעילות נורמלית של שירות עסקי, תוך יצירת אשליה למפעיל כי השירות עסקי פועל באופן תקין. יתרה מכך, באמצאות שינוי נתונים ו\או הזנת מידע כוזב (דיסאינפורמציה) במערכות עסקיות, כדוגמת Big Data, השחקן התוקף יכול להשפיע על תהליך קבלת ההחלטות בשחקן המותקף, דבר אשר עשוי לגרום לטעויות אסטרטגיות, כדוגמת קבלת החלטה על השקעה גבוהה בפתרון לא אפקטיבי ואופטימלי. דוגמא אחרת, הערכות לא נכונה מבחינת סד"כ לפעילות לחימה האמורה להתרחש במרחב הפיסי עשויה להוביל לתבוסה גורפת. וכדוגמא אחרונה אציין את היכולת ליצור אנדרלמוסיה כלכלית במדינה פלונית, וזאת ע"י הזנת מידע כוזב במערכות הפיננסיות ו\או המדיה.

ריגול, איסוף מידע ובניית פרופיל פסיכולוגי - התנהגותי

עידן המידע הביא עמו תלות גוברת והולכת בזמינות, סודיות, מהימנות ואמינות המידע. נדיר לראות כיום ארגון אשר אינו מאחסן מידע באופן דיגיטלי. יתרה מכך, שירותים עסקיים רבים תלויים באופן ישיר במערכות המחשוב. מטבע הדברים, במהלך השנים מערכות המחשוב נהפכו ליעד תקיפה מועדף, אשר באמצעותו ניתן להפיק מידע איכותי, וזאת כדוגמת גניבת תוכניות מטוס ה-F-35 האמריקאי ע"י סין[4]. בהתאם לכך, ניתן לראות כי נשק הקיברנטי (דבר הכולל לא פעם שילוב של תקיפות מסוג "הנדסה חברתית") מתמקד לא פעם במציאת דרכים לאיתור מידע איכותי והוצאתו ממתחם הארגון, ובכלל זה באיתור אנשי מפתח בארגון, והוצאת מידע איכותי מרשותם.

בנוסף, ניתן להשתמש במידע הדיגיטלי הטמון במרחב הקיברנטי לשם בניית פרופיל פסיכולוגי - התנהגותי של פלוני, ובכך להכין את הקרקע למימוש תקיפות קיברנטיות שכיחות, ובכלל זה ניתן להשיג יכולת חיזוי מסוימת לגבי התנהגותו של פלוני במצבים מסוימים. וכך לדוגמא, הסטארטאפ Crystal Project Inc. מציע שירות המציע יכולת בניית פרופיל פסיכולוגי - התנהגותי של פלוני, וזאת על סמך מידע דיגיטלי הטמון במרחב הקיברנטי.

מן הראוי אף לציין כי בהתאם לפרסומים זרים, ה-NSA (National Security Agency) פרץ לאלפי מכשירי טלפון ניידים, וזאת במטרה לאסוף מהם צילומים מזירות אירוע בהן התרחשו אירועי טרור, דבר אשר אפשר לממשלת ארה"ב למנף את תהליכי החקירה. לפיכך, ניתן לזהות מגמה שבה שירותי ביטחון מנצלים יכולות תקיפה קיברנטיות לשם איסוף מודיעני מאזרחי המדינה בה הם פועלים, דבר המעלה לדיון סוגיות מהותיות בנושא זכויות אזרח והגנת הפרטיות.

סחיטה ("כופר"), הונאה (Fraud) והלבנת הון (Money Laundering)

בשנים האחרונות החלו ארגוני פשיעה (בעיקר) להשתמש בתוכנת כופר (Ransomware) לשם סחיטת ארגונים ואנשים פרטיים, דבר הכולל הצפנת מידע חיוני, ודרישה לתשלום כופר לשם שחרור המידע הנמצא בחזקת התוקף. בנוסף, ניתן לראות מקרים שבהם בעלי אתרי אינטרנט (לדוגמא) נדרשים לשלם כופר לשם מניעת הישנות של תקיפות משביתות שירות, אשר פוגעות בפעילות העסקית של אתר האינטרנט.

כמו כן, באמצעות ניצול פגיעויות שונות, ארגוני פשיעה (בעיקר) משתמשים בכלים שונים לשם השתלטות על ציוד המחשוב ומכשירים ניידים, דבר המאפשר להם להפיק מידע אשר באמצעותו ניתן לסחוט את המותקף. דוגמא קלאסית לתקיפה מסוג זו היא הפעלת מצלמת המחשב באופן בלתי רצוני, וזאת לשם הכנת "סרט מביך" אשר יאפשר את סחיטת הצד המצולם. יוער כי שימוש בשיטות סחיטה מקובל מזה

[4] New Snowden Documents Reveal Chinese Behind F-35 Hack, Franz-Stefan Gady, 2015

אלפי שנים בעת גיוס מקורות מודיעין (כדוגמת "משתפי פעולה"), והנשק הקיברנטי מקל ברמה מסוימת על גיוס מקורות מודיעין, וזאת תוך מתן אפשרות להסתיר הפרטים האמיתיים של הגורם המפעיל.

באמצעות שימוש בזהויות בדויות, ואף באמצעות התחזות \ גניבת זהויות, גורמים שונים יכולים לבצע מעשי הונאה (Fraud) והלבנת הון (Money Laundering) אשר מטרתם להעשיר את הצד התוקף. ZeuS Trojan[5] מהווה דוגמא קלאסית לכלי תקיפה קיברנטי אשר מאפשר לתוקף לגנוב את פרטי האימות של חשבון הבנק של אדם פלוני, ובכך לאפשר לתוקף לבצע פעולות פיננסיות בשם הקורבן.

עמימות

ארסנל הנשק הקיברנטי ניתן להסתרה בקלות יחסית, ולפיכך ישנו קושי רב לדעת מהן היכולות הפרקטיות של גוף פלוני. לאור העובדה כי ניתן לייצר נשק קיברנטי ללא סממנים המזהים את המפתח המקורי, ואף ניתן להשתמש בנשק קיברנטי באופן אנונימי (כדוגמת הפעלת הנשק מכתובת IP הרשומה על שם מדינה זרה, גרימה לצד שלישי שאינו מעורב בסכסוך בין הצדדים להפעיל את הנשק קיברנטי), דבר המקשה על הצד המותקף להוכיח מיהו התוקף[6]. יתרה מכך, באמצעות שתילת סממנים מזהים כוזבים בנשק הקיברנטי ניתן לגרום לכך שהצד המותקף יחשוד בגורם צד שלישי, שאינו קשור כלל לתקיפה. לפיכך הנשק הקיברנטי יכול לסייע ביצירת חשדנות ומתיחות, ואף במקרים מסוימים לייצר עימות לא רצוני בין גורמים אשר במקור לא תכננו להחריף את מערכת היחסים ביניהם.

יצירת רשת דארקנט ("רשת אפלה") ומחשוב סריגי (Grid Computing)

באמצעות שימוש בנשק קיברנטי, גורמים שונים יכולים להקים רשת דארקנט ("רשת אפלה") פרטית, אשר עצם קיומה ופעילותה מוסתר וממוסך תחת פעילות לגיטימית של משתמשים. במאמר מוסגר יצוין כי מעבר להקמת רשת דארקנט ("רשת אפילה"), כלי הנשק הקיברנטים מאפשרים להשתמש בכוח מחשוב של משתמשים לגיטימיים לשם ביצוע פעולות הדורשות כוח עיבוד רב, כדוגמת כריית כסף וירטואלי ופענוח של מידע מוצפן.

הקדמה למלחמה מסורתית - "ערפל המלחמה" (The Fog of War)

הנשק הקיברנטי מאפשר לשחקן אשר מעוניין ליזום לחימה מסורתית לנקוט בשורה של צעדים מקדימים, כדוגמת שיתוק תשתיות קריטיות, פגיעה בשרשרת האספקה (Supply Chain) ובמערכות לוגיסטיקה, הסתרת שלבי ההכנה ליציאה לקרב וזריעת פאניקה בצד המותקף, דבר אשר מאפשר לצד היוזם להשיג עליונות על השחקן המותקף, ובכך לשנות את כללי המשחק בזירה[7]. דוגמא קלאסית לתקיפה קיברנטית מסוג זו הינה השבתת פעילות של מערכת המחשוב האחראית לזימון כוחות מילואים בחירום, המתבססת

[5] Kaspersky Lab Discovers Chthonic: A New Strain of ZeuS Trojan Targeting Online Banks Worldwide, 2014

[6] מושג שכיח המתאר את בעיה זו הינו "בעיית הייחוס" (Problem Attribution)

[7] Cyberwarfare and Information Warfare Shock Doctrine, Yuval Sinay

על ממשקים חיצוניים המאפשרים המצאת זימון אוטומטי לחייל המילואים באמצעות פנייה קולית ו\או דוא"ל ו\או SMS (מסרון).

חלופה למלחמה מסורתית

קרל פון קלאוזביץ, מאבות תורת הלחימה המודרנית הטביע את המשפט - "המלחמה אינה אלא המשך המדיניות באמצעים אחרים". עם זאת, השימוש במלחמה מסורתית מחייב את הצד היוזם ליטול סיכונים מרובים, ובכלל זה להשקיע משאבים רבים על מנת להיערך ללחימה, אשר זמן תחילתה ידוע, אך תאריך סיומה תלוי בערפל. יתרה מכך, קיומן של בריתות (כדוגמת "ברית נאט"ו") ואמצעי לחימה לא קונבנציונליים עשוי לגרור את הצד היוזם לעימות רוחבי, אשר בסופו עשוי להיגרם לצד היוזם נזק משמעותי, המקטין את כדאיות השימוש במלחמה מסורתית. כחלופה לכך, ניתן לזהות כי בשנים האחרונות גובר השימוש בנשק קיברנטי בין מדינות עוינות (כדוגמת העימות הנוכחי בין רוסיה לאוקראינה, והעימות בין איראן לאזרבייג'ן לפני שנים ספורות), וזאת כחלופה למלחמה מסורתית. היתרונות הגלומים בשימוש בנשק קיברנטי במקרה הנדון כוללים בין השאר את האפשרות להגביל את הפגיעה בצד המותקף (כדוגמת מניעת אובדן חיי אדם ופגיעה הרסנית בתשתיות פיסיות), אך עם זאת לשמר את היכולת לגרום לנזק מהות (כדוגמת השבתת פעילות תשתית האינטרנט אשר משמשת לטובת פעילות עסקית) לצד המותקף.

במאמר מוסגר יצוין כי דוגמא מעניינת לשימוש בעימות קיברנטי כחלופה למלחמה מסורתית הינו העימות אשר התקיים לפני פחות משנה בין ארה"ב לצפון קוריאה, אשר נסב אחר סרטה של חברת סוני - "ראיון סוף". במקרה הנדון נטען ע"י מקורות זרים כי מנהיג צפון קוריאה ("כוכב הסרט"), קים ג'ונג און נעלב מכך שהוא מוצג בסרט כאדם ילדותי ונלעג. עקב כך נטען כי צפון קוריאה יזמה מתקפה קיברנטית כנגד חברת סוני, דבר אשר כלל הדלפת מידע רגיש ממערכות המחשוב של החברה. בתגובה לכך נטען ע"י אותם מקורות, ארה"ב השביתה את פעילות האינטרנט של צפון קוריאה למשך יממה, וזאת מעבר לנקיטת שורה של צעדי ענישה נוספים כנגד צפון קוריאה.

בשנת 2011 אירן פרסמה כי היא הצליחה ליירט מל"ט (מטוס ללא טייס) אמריקאי, וזאת באמצעות שימוש בתקיפה מסוג GNSS-Spoofing[8]. צוות מחקר מאוניברסיטת טקסס באוסטין שחזר את מימוש תקיפה זו בשנת 2012[9], דבר המעיד כי המרחב הקיברנטי חשוף לשורה של תקיפות מתקדמות הכוללות בחובן אף תקיפות ל"א (לוחמה אלקטרונית), אשר מאפשרות לתוקף להשיג את מטרותיו בדרכים מגוונות ויצירתיות.

מן הראוי לציין כי למרות שלל היתרונות בשימוש בלחימה קיברנטית ביחס למלחמה מסורתית, הסיכון כי מלחמה במרחב הקיברנטי תזלוג למרחב הפיסי שריר וקיים, בייחוד במצבים בהם הפגיעה במרחב הקיברנטי תגרום לפגיעה בחיי אדם, וזאת כדוגמת פגיעה במערכות מחשוב רפואיות במתקני רפואה

[8] כיצד עלה בידי האיראנים ליירט מל"ט אמריקאי ומהי ההגנה הראויה?, חיים רביב, 2015

[9] חוקרים מאונ' טקסס "חטפו" מל"ט באמצעות זיוף אותות GPS, 2012

אזרחיים, גם אם בשגגה. ובמילים אחרות, הלחימה קיברנטית יכולה להסלים בקלות יחסית ללחימה מסורתית, ולפיכך ישנו צורך לבחון באופן מיטבי את ההשלכות האפשריות של תקיפה קיברנטית על הצד המותקף, ובהתאם לנקוט בצעדים הנדרשים לשם צמצום ההשלכות השליליות למינימום.

חדלון החוק הבינלאומי

דיני המלחמה מציגים שורה של חוקים והסדרים אשר מקובלים על מרבית מדינות העולם, ואף על ארגונים לא ממשלתיים, כדוגמת האו"ם. עם זאת, דיני המלחמה אשר שרירים ותקפים במלחמה מסורתית מתקשים לספק מענה הולם למלחמה במרחב הקיברנטי, דבר המקל על הצדדים לנהל "מלחמה וירטואלית", וזאת ללא הגבלות משפטיות של ממש. יתרה מכך, דיני המלחמה הנוכחיים מתקשים להתמודד עם שורה של סוגיות משפטיות-מעשיות, כדוגמת מהי התגובה הראויה שעל מדינה לאמץ במקרה שתוצאות תקיפה במרחב הקיברנטי שלה משפיעות על המרחב הפיסי שלה, וזאת עקב טעות אנוש מצדו של הצד התוקף. דוגמא אחרת הינה סוגיית אחריות מדינה אשר דרך מערכת התקשורת העוברת במרחב הטריטוריאלי שלה בוצעה תקיפה קיברנטית ע"י מדינה פלונית כנגד מדינה אלמונית. ודוגמא אחרונה הינה השאלה מהם הגבולות של זכות ההגנה העצמית של מדינה אשר חווה תקיפה קיברנטית אשר מקורה ביוזמה עצמאית של אזרח ממדינה פלונית.

יוער כי ניסיונה של ברית נאט"ו [10]להתאים את דיני מלחמה הנוכחיים למרחב הקיברנטי, תוך השגת הסכמה בינלאומית לא זכה להצלחה יתרה.

אקטיביזם

באמצעות שימוש בנשק קיברנטי, גופים שונים יכולים לנקוט בצעדים אקטיביסטים שונים, כדוגמת השתלטות על אתר אינטרנט מרכזי לשם פרסום משנתם, ואף לשם הענשת הגורם אשר לטענת אותם אקטיביסטים אינו פועל כמצופה ממנו. ולראיה פעילות קבוצת Anonymous המהווה דוגמא לסנונית הראשונה לפעילות אקטיביסטית "לא פוליטית" (כהגדרת חברי הקבוצה) במרחב הקיברנטי, אשר בהתאם למטרות המוצהרות של הקבוצה ברצונה לעורר מודעות חברתית לנושאים מהותיים, תוך חתירה לצדק.

טרור

יכולותיו של הנשק קיברנטי, ואופי השימוש בו, הופכים את הנשק הקיברנטי לפתרון אטרקטיבי עבור גופים המעוניינים להשליט טרור על מדינה ו\או ציבור מסוים. תוצאות פעולת טרור במרחב הקיברנטי יכולות לכלול בין השאר: פגיעה בתדמית, חשיפת מידע מביך אישים פוליטיים, חשיפת מידע אשר עשוי לגרום לסכסוך עם מדינה פלונית, פגיעה ביציבות המערכת הפיננסית ויצירת מצב של אי אמון בין העם לשלטון. מגבלות משפטיות ומעשיות (כדוגמת מגבלות טכנולוגיות) מקשות על גופי אכיפה וביטחון לספק מענה

[10] Tallinn Manual on the International Law Applicable to Cyber Warfare, Michael N. Schmitt, Cambridge University Press; Reprint edition, 2013

הולם לסוג איום זה, דבר המגדיל הסבירות להצלחת תקיפות קיברנטיות מטעם גורמים אלו, כאשר גורמים אלו מודעים לכך כי הסבירות כי הם יענשו בגין מעשיהם נמוכה.

במאמר מוסגר יצוין כי בשנים האחרונות התגלה קשר ישיר בין ארגוני טרור לארגוני פשע מאורגן, דבר הכולל בין השאר רכישת כלי נשק קיברנטים אשר פותחו ע"י ארגוני פשע מאורגן, אשר מאפשרים לארגוני טרור להשיג עצמאות כלכלית. סוגיה זו זוכה לחשיבות יתרה לאור העובדה כי היא מאפשרת ל"מפגע יחיד" להשיג גב כלכלי החיוני למימוש תקיפה פיסית מסיבית, וזאת תוך הסתרת עצם קיומו ופעילותו מגורמי אכיפה וביטחון.

הנשק הקיברנטי כמכפיל כוח

הנשק הקיברנטי מאפשר לכל גורם להכפיל את כוח הלחימה שלו, וזאת בהשקעה מינימלית. כמו כן, הגישה המקובלת בעת קיומו של מרוץ חימוש (Arms Race) בין גופים שונים היא שאם כלי נשק יכול להגיע לידי הצד האחר, אזי חלה חובה לפתח יכולות דומות. בנוסף, עקרון ההדדיות בלחימה מאיץ את השימוש בכלי נשק בעלי יכולות דומות בשלבי הלחימה הראשונים תוך מתן אפשרות לתוקף המפתיע את המותקף להשיג הישגים מהותיים כבר במערכה הראשונה, דבר ההופך את הנשק הקיברנטי לאטרקטיבי בעיני רבים.

השלם גדול מסך חלקיו

אחת היכולות היותר מעניינות בנשק קיברנטי היא היכולת לרתום את כוחם של אחרים, וזאת אף ללא ידיעתם והסכמתם, לשם מימוש המתקפה. וכך לדוגמא, ממשלת סין פיתחה נשק קיברנטי בשם Great Cannon. נשק זה מנצל פעילות של משתמשים לגיטימיים, אשר מפעילים ללא ידיעתם סקריפט מבוסס JavaScript המאפשר יצירת מתקפה משביתת שירות מסוג DDoS (Distributed Denial-of-Service) Attack כנגד אתר פלוני. דוגמא אחרת הינה מצב שבו גורם עוין משתלט על מערכות המחשוב של מטוס נוסעים ו\או מגדל פיקוח, ובאמצעות מתן הנחיות מרחוק הוא גורם לפיגוע המונים, נוסח פיגוע הטרור במגדלי התאומים בארה"ב מה-11 בספטמבר 2001.

שליטה על התודעה וצנזורה

הנשק הקיברנטי מאפשר למדינות וארגונים להחיל את משנתם במרחב הקיברנטי, וזאת באמצעות החלת ניטור ושלל הגבלות על פעילות המשתמשים. פתרון ה-Great Firewall אשר פותח על ידי ממשלת סין הוא דוגמא קלאסית למימוש פעולות ניטור והגבלת פעילות משתמשים. Edward Snowden חשף את קיומו של כלי נשק קיברנטי בשם QUANTUM אשר מטרותיו העיקריות כוללות בין השאר; לאפשר לממשלת ארה"ב לפצח מידע מוצפן, ולאפשר לממשלת ארה"ב לשתול Malware במיליוני מחשבים, וזאת תוך זמן קצר. למותר לציין כי אופי פעילות הכלי מעיד כי הוא תוכנן במקור להפצת בוטים, אך במקביל הוא מסוגל להתקין תוכנות מעקב במחשבים וטלפונים ניידים של קבוצות יעד גדולות. יוער כי לאחרונה אף הועלתה

טענה כי ה-FBI השתמש בסט הכלים של חברת ה-Hacking Team לשם השתלת [11]כלי מעקב במחשבים טלפונים ניידים של חשודים.

מישל פוקו[12], הוגה דעות צרפתי הציג את הפנאופטיקון כמודל הפיקוח אולטימטיבי, הגורם לאסיר להפנים את ההתנהגות הרצויה (הראויה), וזאת ללא שימוש באמצעי ענישה פיזיים. רוצה לומר, עצם העובדה כי אדם פלוני יודע כי הוא נתון למעקב פוטנציאלי בכל זמן נתון, דיה בכדי ליצור שינוי התנהגותי, ויכולת זו ניתנת להשגה במרחב הקיברנטי וזאת באמצעות שימוש בנשק קיברנטי.

מן הראוי אף לציין כי ישנו צפי כי השימוש בממשק אדם-מכונה יגבר בעתיד הקרוב, ולפיכך גורמים עוינים יוכלו את ממשק זה על מנת להפוך את "האדם" לממשק המקשר בין הנשק הקיברנטי למערכת המחשוב המותקפת. הדור הראשון של כלי הנשק אשר מאפשר השתלטות מוגבלת על אדם פלוני מרחוק זמין בשוק, והוא מוכר בשם "נשק אנרגיה ישירה" (Directed Energy Weapon). עם זאת, נכון לזמן כתיבת מאמר זה, ובכפוף למידע החשוף לנחלת הכלל, הדור הראשון אינו כולל יכולת לניצול לרעה של ממשק אדם-מכונה.

לחימה היברידית

אסטרטגיות ודוקטרינות הלחימה החדשות מציעות שילוב בין לחימה מסורתית לבין לחימה קיברנטית, וזאת בהתאם לצורך. וכך לדוגמא, לאחרונה פורסם כי חברת בואינג [13]מפתחת מל"ט (מטוס ללא טייס) הכולל רכיב חומרה בשם TNI (Tactical Network Injector) אשר מהווה יחידת אחסון לנשק קיברנטי (סביר להניח שיחידת האחסון מכילה Framework הדומה ביכולותיו ל-Metasploit), אשר ביכולתו לאפשר החדרת קוד זדוני לציוד המחובר לרשתות אלחוטיות (Wi-Fi), וזאת במטרה לאפשר מימוש למתקפת MiTM (Man In the Middle) וניצול Exploits. בנוסף, למל"ט ישנה יכולת לביצוע פעולות ריגול, ניטור ומעקב. למרות שלא פורסם מידע רשמי בנדון, סביר להניח כי המל"ט מצויד בראש נפץ אשר מקנה למל"א יכולת לפגוע בעת הצורך ב"מטרות איכות", כדוגמת מערכות תקשורת ומכ"ם (מגלה כיוון ומרחק), וזאת בנוסף לקיומו של מנגנון השמדה עצמי מובנה.

[11] FBI Used Hacking Team's Help to Track Tor User ,Adarsh Verma, 2015

[12]לפקח ולהעניש - הולדת בית הסוהר, מישל פוקו, רסלינג הוצאת ספרים, 2015 (גרסה בצרפתית ובאנגלית של הספר פורסמה בחו"ל בשנת 1975)

[13] Hacking Team and Boeing Built Cyber Weaponized Drones to Spy on Targets

סיכום

עידן המדע הפך את המרחב הקיברנטי לשדה לחימה, אשר שחקנים רבים יכולים לנצלו לשם השגת מטרותיהם. מאמר זה סקר על קצה המזלג את השיקולים העיקריים בפיתוח והפעלת נשק קיברנטי, כאשר יש לזכור כי לאור המציאות הדינמית, כניסתן של טכנולוגיות ומערכות אקולוגיות מתקדמות (כדוגמת IoT ו-IoE), סביר להניח כי רשימת השיקולים תגדל בעתיד. ניתן אף להניח כי בעתיד הקרוב השימוש בלחימה היברידית יגבר, וכי עידן חדש של מרוץ חידוש נכנס לזירה.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.", Richard A. Clarke

על המחבר

יובל סיני הינו מומחה אבטחת מידע, סייבר, מובייל ואינטרנט, חבר קבוצת SWGDE של משרד המשפטים האמריקאי. כמו כן, יובל סיני קיבל הכרה מחברת Microsoft העולמית כ-MVP בתחום Enterprise Security.

מילות מפתח

Armed Conflict, Critical Infrastructure Information, CII, Critical Infrastructure, CI, Cyber Conflict, Cyber Power, Cybersecurity, Cyber Space, Cyber Strategy, Cyber Warfare, Electronic Warfare, EW, Homeland Security, Hybrid War, Information and Communication Technology, ICT, International Law, Strategic Thinking

ביבליוגרפיה

ביבליוגרפיה בעברית

- כיצד עלה בידי האיראנים ליירט מל"ט אמריקאי ומהי ההגנה הראויה?, חיים רביב, 2015
- איום ארגוני הטרור במרחב הסייבר, גבי סיבוני, דניאל כהן, אביב רוטברט, צבא ואסטרטגיה, כרך 5, גיליון 3, דצמבר 2013
- מבוא ל-Web 3.0 Security, יובל סיני, Digital Whisper, 2013
- תפוצת נשק קיברנטי במרחב הסייבר, דניאל כהן, מבט על, גיליון 444, 08 יולי 2013
- חוקרים מאונ' טקסס "חטפו" מל"ט באמצעות זיוף אותות GPS, 2012
- מבט בינתחומי על אתגרי הביטחון בעידן המידע, יצחק בן-ישראל, ליאור טבנסקי, צבא ואסטרטגיה | כרך 3 | גיליון 3 | דצמבר 2011
- הגנה על תשתיות קריטיות מפני איום קיברנטי, ליאור טבנסקי, צבא ואסטרטגיה | כרך 3 | גיליון 2 | נובמבר 2011
- הוודאות האבודה של הטבע והאחדות הקוואנטית, צבי ינאי, מחשבות 55-56 | אפריל 1988

ביבליוגרפיה באנגלית

מאמרים:

- Police bust huge hacker black market
- China’s Great Cannon
- Cyber Strategy - United States Department of Defense
- Here's What a Cyber Warfare Arsenal Might Look Like
- New Snowden Documents Reveal Chinese Behind F-35 Hack, Franz-Stefan Gady, 2015
- 4 Arrested in Schemes Said to Be Tied to JPMorgan Chase Breach
- WATCH: Is Anonymous becoming the ‘modern-day technological Robin Hood’?
- Hacking Team and Boeing Built Cyber Weaponized Drones to Spy on Targets
- On Cyberwarfare, Fred Schreier, DCAF Horizon 2015 Working Paper Series (7)
- Critical Infrastructure Protection against Terrorist Attacks, Course Report, NATO COE DAT, Ankara Turkey, 3-7 November 2014 (Mon-Fri)
- Kaspersky Lab Discovers Chthonic: A New Strain of ZeuS Trojan Targeting Online Banks Worldwide, 2014

- Why cyber warfare is so attractive to small nations
- How the NSA Plans to Infect Millions of Computers with Malware, 2014
- A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, Louise Arimatsu, International Law Programme, Chatham House, London, UK, 2012
- Social Business Systems: Beyond Engagement
- Threat Assessment & Remediation Analysis (TARA), Methodology Description Version 1.0 , Jackson Wynn, Joseph Whitmore, Geoff Upton, Lindsay Spriggs, Dan McKinnon, Richard McInnes, Richard Graubart, Lauren Clausen, MITRE, October 2011
- Cyberwarfare and International Law, Nils Melzer, 2011
- The UK Cyber Security Strategy Protecting and promoting the UK in a digital world
- Civilians in Cyberwarfare: Conscripts, Susan W. Brenner - University of Dayton & Leo L. Clarke - Grand Rapids, Michigan, Vanderbilt Journal of Transnational Law, [Vol. 43:1011], 2010
- BEHIND THE GREAT FIREWALL: THE INTERNET AND DEMOCRATIZATION IN CHINA, Xiaoru Wang, University of Michigan, 2009
- CIP Program Discussion Paper Series, George Mason University, February 2007

ספרים:

- Understanding Cyber Warfare and Its Implications for Indian Armed Forces, Col R Tyagi, Vij Books, 2013
- Cyberpower and National Security, Ed by Franklin D, Kramer, Stuart H Starr and Larry Wentz, Vij Books, 2009
- Defense Strategies for Protection of People & Facilities against Bioterrorism, James Afshar, 2006