האומנם כל אחד הוא אויב בחלל הקיברנטי?

אריאל טי סובלמן

הקדמה

עבריינות וטרור בחלל הקיברנטי (cyber-space) הם מהחוליים הקשים של עידן המידע. בשנות ה-80, בתקופת הבום הגדול של המחשבים האישיים, רווחה הדעה, כי ניתן יהיה למנוע פריצות של האקרים למערכות מחשבים. אולם, עם העלייה במספר המחשבים ועם התרחבות רשת האינטרנט, הפכה בהדרגה אבטחת מערכות המחשב למשימה מורכבת ויקרה.

באמצע שנות ה-80 הוגדרה לוחמת המחשבים - המונח המציין התקפות שמקורן במחשבים ויעדן הוא מחשבים, או רשתות מחשבים - כיכולת לנצל את רמת הפגיעות הגבוהה של מערכות מידע. הלוחמה הזאת יכלה לבוא לידי ביטוי בצורות שונות, ולהצלחתה עלולות היו להיות השפעות הרסניות. ריגול, טרור, מעשים פליליים, ונדליזם, אנרכיה, או סתם מעשי קונדס של ילדים הם כיום מניעים להתקפות על מערכות מחשבים.

ממשלות וארגונים פרטיים ברחבי העולם הבינו את החומרה של האיומים, הנשקפים מלוחמת המחשבים, ולא חסכו במאמצים כדי להסתיר מהציבור מידע על היקף ההתקפות על מערכות מחשבים, הקשורות לתשתיות, לעסקים ולתעשייה. הסיבות לכך מגוונות: החל מרצונן של ממשלות להימנע מזעיעת פחד ובהלה בציבור, וכלה בעסקים (בעיקר ארגונים פיננסיים), המעדיפים שלא לחשוף את השיעור האמיתי של מעשי הגניבה וההונאה המתבצעים בחלל הקיברנטי, כדי שלא ייפגע האמון של הציבור במערכת. הסתרת המידע הזה גרמה לכך, שהציבור האמין, כי רמת האבטחה של המחשבים היא משביעת רצון, אולם, למעשה, המצב רחוק מלהיות כזה.

מערכות ותשתיות לאומיות קריטיות, חשופות באופן הולך וגובר, להתקפות קיברנטיות. ההערכה היא, כי מדי שנה נערכים עשרות מיליוני ניסיונות פריצה ברחבי העולם; חלק ניכר הם מעשי שובבות של בני נוער. רובם המכריע לא מתגלים לעולם. בתוך כך מעריכים, שעל המערכות של מחלקת ההגנה האמריקנית מתרחשות מדי שנה מאות אלפי התקפות. ההערכה האופטימית ביותר אומדת את שיעור ההצלחה של מחלקת ההגנה לאתר את ההתקפות האלה בלא יותר מ-5%.

קשה מאוד להעריך כמה התקפות נעשות בפועל, וחמור מכך, כמה מהן מצליחות בלי להתגלות. מעוררת דאגה במיוחד היא הקלות היחסית, שבה יכול יריב נחות להסב נזק גדול. לפיכך, מניעת התקפות על מערכות מחשבים והסתרת קיומן נחשבות לפעולות בעלות דרגת חשיבות עליונה ברוב המדינות המפותחות.

ארגונים וממשלות כמעט שאינם מצהירים על ההתקפות, שמבצעיהן השיגו את מטרתם, נגד מערכות המחשבים שלהם. אולם סביר להניח, כי נעשים ניסיונות חדירה מסיביים יותר למערכות מחשבים אזרחיים, בייחוד אלה של ארגונים פיננסיים, יותר מאשר למערכות של גופים צבאיים ומודיעיניים. הערכות גסות, שנעשו על-ידי האף-בי-איי והאינטרפול מצביעות על הפסדים שנתיים בסך מאות מיליוני דולרים, הנגרמים למוסדות פיננסים ולתעשיות היי-טק בשל התקפות וגניבות דרך מחשבים, כמו גם על עסקות פיננסיות לא-חוקיות, שמתבצעות באינטרנט.

קיימות כמה סיבות - השלובות זו בזו - לכך, שהמאמצים להתמודד עם העבריינות והטרור בחלל הקיברנטי לא עלו יפה. **ראשית**, יש נטייה להתייחס אל שני המונחים האלה כאל זהים.

שנית, קיימת נטייה להתייחס אל עבריינות וטרור בחלל הקיברנטי כאל סוגיות של ביטחון לאומי, הצריכות להיות מטופלות ככאלה על-ידי גופי הביטחון והמודיעין.

שלישית, הגנה סטטית - האסטרטגיה שאותה נוקטים כדי להתמודד עם התופעות הללו - הינה הגנתית טהורה.

רביעית, מכיוון שסוכנויות הביטחון במדינות השונות אינן מאמינות, כי ניתן להבחין בין אויב לידיד, הן נרתעות משיתוף פעולה ביניהן בכל הקשור למאבק בלוחמת מחשבים, ולכן אין באפשרותן להפיק תועלת מהידע ומהניסיון שהצטברו בידי כל אחת מהן.

ההבדל בין עבריינות קיברנטית וטרור קיברנטי

קיימת נטייה לבלבל בין טרור ועבריינות. כאשר דנים בהם בהקשר של החלל הקיברנטי מתייחסים אליהם כאל לוחמת מידע הכוללת פעולות כגון החדרת וירוסים, "תולעי אינטרנט" ותוכנות פגומות וכן אופנים שונים של פריצה למערכות מחשבים. אבל עבריינות קיברנטית וטרור קיברנטי הינם שני דברים שונים. טרור בחלל הקיברנטי מכוון לזרוע הרס ואף להרוג בני אדם באמצעות המרחב הקיברנטי, והוא מאפשר לתוקפים להישאר הרחק מהמטרה. בכך נמנעים עבריינו הטרור הקיברנטי מבעיות לוגיסטיות, הכרוכות בהעברת חומרי נפץ וציוד אחר וכן מקטינים את סיכויי ההיתפסות.

לעומת זאת, עבריינים קיברנטיים רוצים להרוויח, ולא רק להפגין את כוחם. הם עשויים למקד את מאמציהם בהעברות בלתי חוקיות של אמצעי מימון, בהלבנות כספים, בהונאות אינטרנט, בהעלמות מס ובתקשורת בין ארגונים פליליים.

האם יש להפקיד את הטיפול בטרור הקיברנטי בידי גופים העוסקים בביטחון לאומי?

הדמיון בין צורות שונות של התקפות קיברנטיות הוביל גופים העוסקים בביטחון

לאומי ליטול את האחריות על הטיפול בתופעות האלה. הנטייה להתייחס באופן מונוליטי לסוגים שונים של לוחמת מידע פגמה, לרוע המזל, ביעילות המאמצים. ברוב מדינות המערב הגורמים שטיפלו בלוחמת המחשבים היו הגופים שעוסקים בביטחון לאומי, רשויות אכיפת החוק ומערכת המשפט הפלילית. אבל הגופים הללו לא הצליחו לעמוד ביעדים שהציבו לעצמם. המוסדות המטפלים בביטחון לאומי נכשלו בניסיונותיהם לעצור את ההתקפות הקיברנטיות. לרשויות אכיפת החוק חסרו האמצעים לאתר את המתקיפים ולאסוף עדויות נגדם. כתוצאה מכך, מערכת המשפט הצליחה להשיג הרשעות בודדות בלבד של עבריינים קיברנטיים.

הנטייה לקשור בין טרור קיברנטי לעבריינות קיברנטית הובילה את הגופים האמריקניים העוסקים בנושאים של ביטחון לאומי – בייחוד את קהילת המודיעין – למסקנה, שיש ללחום בתופעות האלה באותם אמצעים. ארצות-הברית, שמסרבת לעשות את ההבחנה בין סוגים שונים של לוחמת מחשבים, טיפלה בכל אירוע – כולל מעשי קונדס, או משובה של נערים – כקשור לביטחון לאומי. הגישה הזאת התפשטה, ומדינות רבות נוספות מתייחסות כיום אל הפרות חוק בחלל הקיברנטי כאל נושאים של ביטחון לאומי. זוהי הסיבה לכך, שהרשויות האמריקניות חשדו באופן אוטומטי, כי הנער הישראלי אהוד טננבוים (הידוע כ"אנלייזר") שנעצר ב-1998 בחשד לפריצה לאתרי מחלקת ההגנה, הוא סוכן בשירות הריגול הישראלי.

הממשלות, בהתייחסותן לנושא זה כאל נושא רגיש באופן מיוחד, תרו אחר פתרונות משלהן ללוחמת מחשבים, סירבו לשתף פעולה עם גופים מקבילים במדינות אחרות ושמרו את פעילותן תחת מעטה כבד של חשאיות.

הגנה סטטית

הגנה סטטית היא **עמדה הגנתית** שאומצה על-ידי רוב המדינות המפותחות כדרך המאבק בלוחמת מחשבים. ההיגיון האסטרטגי שעומד מאחורי הגישה הזאת הוא, שהתקפות על החלל הקיברנטי הינן תכופות, אינן ניתנות לאיתור בדרך-כלל ומגיעות ללא התרעה מוקדמת. מעֵבר לכך, האנונימיות של המרחב הקיברנטי והקושי לזהות את מקור ההתקפה מצמצמות מאוד את יכולת ההרתעה נגד התקפות.

> הכללים לגבי שיתוף-פעולה בנוגע ללוחמת מחשבים טרם נקבעו. עד עתה, שיתוף-פעולה בתחום החלל הקיברנטי נראה כחלום רחוק. הרושם הוא שמדינות חושבות, כי בחלל הקיברנטי לא ייתכנו ידידים וכל אחד הוא אויב פוטנציאלי.

גורם נוסף המקשה על המצב, הוא הא-סימטרייה שהתפתחה בין מדינות מפותחות מבחינה טכנולוגית למדינות מפותחות פחות. הא-סימטרייה הזאת מאפשרת למדינות מפגרות מבחינה טכנולוגית לשתק את מערכות המחשבים של יריב מפותח מבחינה טכנולוגית בלי להיות פגיעות להתקפת נגד דומה.

הטענה שעומדת מאחורי ההגנה הסטטית היא אם כן, שמערכות הגנה מתקדמות הן האמצעי המעשי היחיד להתגונן מפני התקפות בחלל הקיברנטי. מערכת הגנה כזאת אינה תלויה בהתרעות מוקדמות, במודיעין על התקפות מתקרבות, או אפילו במודעות להתקפות. במקום זאת, הרעיון הדומיננטי באסטרטגיית ההגנה הסטטית הוא זה של קו הגנה יחיד ומסיבי, המורכב מביצורים וירטואליים ומערכות Firewall, המוצבים סביב נכסי המידע בעל הרגישות הלאומית ומערכות המחשב. כתוצאה מכך, סוכנויות מודיעין לא נאלצות לבזבז זמן בפיקוח על ניסיונות הפריצה למחשבים ובאיתור מקורות המימון והטכנולוגיה של הפורצים ושל עוזריהם.

"אין ידידים - כולם אויבים"

המציאות של לוחמת המחשבים מחייבת התנתקות ממושגים מסורתיים של אכיפת חוק, טרור וריגול. לדוגמה, תחום הטרור. רוב הממשלות מסוגלות להבחין בין ידיד לאויב, ומבינות את הקשר בין טרור לבין פשע מאורגן. הדבר הזה מאפשר מפגש אינטרסים ושיתוף פעולה בין מדינות בעלות הלך מחשבה דומה. לישראל ולארצות- הברית יש, למשל, אינטרס משותף בסיכול ניסיונות לחבל במטוסי נוסעים ישראליים על אדמת ארצות-הברית. ההנחה היא, שישראל תעשה אותו הדבר בשביל ארצות-הברית או כל מדינה ידידותית אחרת. האפשרות לריגול קיימת תמיד, אבל הניסיון הוכיח, שממשלות ידידותיות מתגברות על החשדנות שלהן ומתמקדות בשיתוף פעולה בנוגע לטרור נגדי ובהחלפת מודיעין.

אווירת האמון ושיתוף-הפעולה הזאת לא קיימת כשמגיעים לטיפול בחלל הקיברנטי. את מקומה תופסת התחרות העזה ששוררת בין מדינות לגבי מידע מהסוג הזה. הכללים לגבי שיתוף-פעולה בנוגע ללוחמת מחשבים טרם נקבעו. עד עתה, שיתוף-פעולה בתחום החלל הקיברנטי נראה כחלום רחוק. הרושם הוא שמדינות חושבות, כי בחלל הקיברנטי לא ייתכנו ידידים וכל אחד הוא אויב פוטנציאלי.

סיכום והמלצות

נראה, כי האופי המסווג של מאמצי ההגנה מוציא מכלל אפשרות אפילו דיאלוג מינימלי בין מדינות ידידותיות בנושא זה. חוסר היכולת להבחין בין נושאים של ביטחון לאומי להתקפות בעלות אופי פלילי מקשה על האפשרות לחלוק במידע הגנתי, טכנולוגי ומתודולוגי, בגלל הסיכון שבשימוש לרעה במידע. אולם הגישה הזאת מתעלמת מהצורך הדחוף בשיתוף-פעולה בין-לאומי. החסרונות הטמונים בגישה של "אין ידידים" רבים מהרווחים שניתן להפיק ממנה. הרמות הנוכחיות של האבטחה אינן נסבלות, משום שהפתרונות הקיימים כיום ברמה הלאומית אינם מספקים. הכישלון בשיתוף-הפעולה מונע את פיתוחם של פתרונות מוצלחים ומשאיר את הבמה פרוצה להתקפות. התשובה היחידה טמונה בבחינה ובהגדרה מחודשות של המדיניות כלפי ההתקפות הקיברנטיות.

על הקהילה הבין-לאומית ליצור מנגנון לשיתוף-פעולה בין-לאומי. שיתוף-הפעולה צריך להתייחס לנקודות הבאות:

1. הצורך להבחין בין סוגי האיומים: עבריינות קיברנטית וטרור קיברנטי אינם תופעות זהות. הן משאירות חתימה שונה וגורמות נזקים שונים. יש להגדיר את ההבדלים ביניהם ולהפיק תועלת מעשיית ההבחנה הזאת. מערכת הביטחון הלאומי תופקד על טיפול והתמודדות עם הטרור הקיברנטי ומערכת אכיפת החוק והשיפוט - על העבריינות הקיברנטית

2. אימוץ של דוקטרינת הגנה פרו-אקטיבית (proactive defense doctrine). הדבר הזה כולל איסוף מודיעין על קבוצות עבריניות ועל קבוצות טרור בחלל הקיברנטי. ממשלות חייבות להקצות משאבים לאיסוף מודיעין ולמחקר. יש לערוך מחקר אקדמי ומודיעיני לגבי הקבוצות הללו, האידיאולוגיה שעומדת מאחורי פעילותן, שאיפותיהן ומטרותיהן.

3. כינון מנגנונים של שיתוף-פעולה בין-לאומי: צעד כזה כולל את מוקד המחשבים הבין-לאומי לשעת חירום, את CERT (Computer Emergency Response Term), שיתוף-פעולה באכיפת החוק, החלפת מידע ושיתוף הדדי בידע טכנולוגי. סביר להניח, שהפעילויות האלה יחזקו את האמון בין המדינות ויגבירו את הפוטנציאל לאיתור מוקדם ולבלימת הגורמים המחבלים בחלל הקיברנטי.

עדכן אסטרטגי

עדכן אסטרטגי יוצא לאור על-ידי
מרכז יפה למחקרים אסטרטגיים, אוניברסיטת תל אביב, רמת אביב, תל אביב 69978.

•

עדכן אסטרטגי מתפרסם בעברית ובאנגלית
ותוכנו המלא מוצג באתר האינטרנט של המרכז.
כתובת האתר: http:www.tau.ac.il/jcss/quarterly.html