סדנת יובל נאמן למדע טכנולוגיה וביטחון

ISRAELDEFENSE

אוניברסיטת תל-אביב

המטרה: שיתוף פעולה גלובלי מול איומי הסייבר

האויב חשאי, האיומים דומים. מאמר מיוחד של ראש מטה הסייבר הלאומי, ד"ר אביתר מתניה, ושל טל גולדשטיין, לרגל כנס הסייבר הבינלאומי וגיליון הסייבר המיוחד

מאת ד"ר אביתר מתניה, טל גולדשטיין

איור: Shutterstock

כבר עם התפתחותו המואצת של עולם הסייבר לכדי מרחב פעולה של ממש, והיותו מנוע לשינוי וצמיחה עולמיים, גם הפעילות השלילית בו תופסת תאוצה – החל מונדליזם ומפשיעה מקומית, דרך ריגול מסחרי, פשיעה גלובלית וטרור, ועד לריגול מדינתי וללוחמה בין מדינות. כל אלו קיימים ומתגברים עם התרחבות הסייבר והשימוש בו, ומהווים איום ישיר על הכלכלה, על התעשייה ועל החיים המודרניים.

כמו בהתמודדות עם איומים אחרים מעשה ידי אדם (טרור, פשיעה בינלאומית, או נשק בלתי קונבנציונלי, למשל), כך גם בתחום הסייבר מהווים שיתופי פעולה בינלאומיים והסדרים בין מדינות מרכיב משמעותי בהתמודדות עם האיום. באופן טבעי, פונות מדינות העולם לחיפוש אחר שיתופי פעולה ומנגנונים, שיאפשרו התמודדות טובה יותר עם איום הסייבר.

גורם משמעותי העומד בבסיס הצורך בשיתופי פעולה בינלאומיים בהתמודדות עם תקיפות סייבר, אף יותר מאשר בהתמודדות עם איומים אחרים, הוא העובדה שלמרחב הסייבר יש יסודות גלובליים משותפים רבים. זאת, הן ברמת התשתיות עליהן הוא מבוסס והן ברמת תפוצת היישומים הרצים בו. מכיוון שהתשתיות הן גלובליות ומשותפות לכלל מדינות העולם, גם החולשות שלהן ודרכי המניעה של התקיפות הן דומות.

הגלובליות של הסייבר אינה באה לידי ביטוי רק בתשתיות המשותפות. פעמים רבות, האופי הפתוח וחסר הגבולות של מרחב הסייבר גורר מדינות וחברות שונות במהלכה של תקיפה אחת. כך, למשל, עשוי תוקף במדינה א' להפעיל תשתית תקיפה במדינה ב', כאשר הוא מקפיד לעבוד דרך פרוקסי במדינה ג', וכל זאת לצורך תקיפה של תשתית במדינה ד'.

מאפיין זה של הסייבר מעצים את החולשה המובנית של יכולות ההגנה, הנובעת מהאופי החשאי של תקיפות סייבר: הקושי ביכולת הזיהוי של התקיפות (עצם האבחנה שבוצעה תקיפה ואיך בוצעה?) ובעיית ייחוס התקיפה (מיהו הגורם המבצע?).

מכאן, שכדי לממש הגנה אפקטיבית, המתבססת על יכולות מחקר וזיהוי, ועל מנגנוני מניעה והרתעה של התוקפים, ישנה חשיבות לבנייה של שיתופי פעולה ומנגנוני הסדרה בינלאומיים.

מישורים לשת"פ גלובלי

לאיום הסייבר משרעת ורוחב מרשימים וייחודיים ביחס לכל איום אחר. מאיום טקטי של גניבה מקומית, או הדלפה של מידע, דרך ריגול מסחרי ומדינתי, הנע מהיקפים מקומיים ועד להיקפים גלובליים יוצאי דופן, איום פשיעה גלובלי, טרור, ועד למלחמה ואיום אסטרטגי.

משרעת רחבה ומגוונת זו מובילה לסוגים שונים של כלים גלובליים בהתמודדות עם האיום. בקצה אחד, שיתוף הפעולה מתמקד בשיתוף מידע וידע, בדומה להתמודדות העולמית עם פשיעה וטרור. בקצה השני, מתהווים תהליכים של הסדרה בין מדינתית לבניית מנגנוני יציבות למניעת הסלמה, בדומה לעיסוק בנשק בלתי קונבנציונלי. בתווך, ניתן לזהות מספר מגמות לשיתופי פעולה המשלבים בין השניים.

שיתוף מידע וידע

כאמור, לשיתוף מידע ברמה הבינלאומית יש חשיבות גבוהה, שכן המידע הנחוץ להתמודדות עם האיומים מפוזר בין מדינות וארגונים בכל העולם. שיתוף מידע עשוי לכלול עדכון הדדי לגבי תקיפות (שיטות, אמצעים, מטרות), חולשות שאותרו ודרכי התמודדות עם איומים ספציפיים ומתודות הגנה כלליות. בשונה מאיומים ביטחוניים מסורתיים, ובמיוחד איום הטרור, שמי שמשתפים לגביהם מידע הם גופי ביטחון מדינתיים, הרי

חלק ניכר משיתוף המידע בסייבר ניתן למימוש באמצעות מנגנונים לא מדינתיים.

מנגנון שיתוף המידע הראשון והפשוט ביותר, המוביל את שיתוף המידע כיום, הוא המידע שחברות אבטחה והגנה בינלאומיות חולקות עם לקוחותיהן. הן צוברות ידע ומידע מהתקיפות על הלקוחות, ומשקפות אותו בחזרה אליהם. מנגנון שיתוף המידע השני עובר באופן ישיר בין חברות וארגונים פרטיים, שיש ביניהם יסוד משותף הגורר איומים ורגישויות דומות (למשל במגזר הפיננסי או במגזר האנרגיה), הן בתוך מדינה והן בין מדינות. מנגנונים כאלה עשויים להתגבש כיוזמות ייעודיות במגזר (דוגמה טובה לכך הוא FS-ISAC המוביל את שיתוף המידע במגזר הפיננסי האמריקני), כמרכיב בשירות העסקי הניתן על ידי חברות האבטחה הגדולות או כמנגנון מדינתי.

לצד שיתוף ידע בין חברות ומגזרים, בתוך ובין מדינות, יש גם מקום רחב לשיתוף ידע בין מדינתי – בין גורמי ממשל, אך גם בתוך קבוצת מדינות. שיתוף מידע כזה מבוצע על ידי גופי CERT מדינתיים, חדרי מצב לאומיים וגופי ביטחון למיניהם.

הסדרה למניעת הסלמה

בדומה לנעשה גם בתחומים אחרים, כך גם בסייבר ישנה חשיבות גבוהה להסדרות בתחום הפעלת הכוח המדינתי. לצורך הסדרה זו, יש לשים לב לשני מאפיינים של איום הסייבר, המאתגרים מהותית את אופן ההסדרה הנדרש.

בשונה מההתמודדות עם התחמשות בנשק אסטרטגי, שם הדגש הוא על מניעת תפוצה של יכולות ועל ריסון בהתחמשות, הרי פיתוח יכולות התקפיות בסייבר נשען בעיקרו על ידע ויכולת אנושית. לכן, יש חשיבות בהתמקדות במניעה של המעשים ושל ההפעלה, ולאו דווקא בעצם ההתחמשות.

כאן נכנס מאפיין נוסף של איום הסייבר – חשאיות הפעולה והקושי בייחוס תקיפה לתוקף. אלו מצמצמים את יכולת הבקרה על ההפעלה ואת הריסון של מדינות. כתוצאה מכך, היכולת לממש הסדרה בין מדינות, שיש בה מנגנוני בקרה וריסון היא בעייתית, ונמצאת נכון להיום, עדיין בחיתוליה.

ניסיון ראשון מוביל לקידום שיח כזה ברמה הבינלאומית בוצע על ידי קבוצת חוקרים עצמאית במרכז המצוינות בתחום הסייבר של נאט"ו באסטוניה. הקבוצה ניסחה מסמך המכונה "מדריך טאלין", המתווה עקרונות למשפט בינלאומי

ד"ר אביתר מתניה

בתחום ניהול המלחמות במרחב הסייבר (מה נחשב כהפעלה מותרת ומתי, מה נחשב כפגיעה באזרחים ומה לא, וכדומה).

על אף שזהו מסמך ראשוני, לא רשמי וחסר קונסנזוס בינלאומי, יש לו חשיבות רבה כנקודת מוצא וייחוס לשיח עתידי שיתפתח בנושא.

כיוון אחר הנמצא בהתגבשות הוא הסדרות בילטראליות. ניסיון מרכזי להסדרה בתחום הפעילות ההתקפית של מדינות בסייבר, על אף שקשה ביותר בשלב זה לנבא את סופו ומשמעותו, הוא בשיח הישיר שמתחיל בימים אלו בין ארה"ב לסין, בעקבות תקיפות הסייבר המרובות בארה"ב המיוחסות לסין, והאמירות התקיפות של הממשל האמריקאי בנושא זה.

בנוסף, חשוב לציין בהקשר זה גם את השיח הבינלאומי לתיאום ולהסדרה של האופן בו מנוהלת ומתופעלת תשתית האינטרנט, בדגש על סוגיות חופש העברת המידע והשליטה של מדינות במרחב האינטרנט המדינתי. דיון זה היה במרכז ועידת ה-ITU (ארגון הטלקום העולמי של האו"ם) האחרונה, והוא חושף מתח פוליטי ואידיאולוגי בין מזרח ומערב.

על אף שליבת הדיון איננה בהתמודדות עם איום הסייבר, שיח זה מושפע ומשפיע על ההתמודדות ברמה הבינלאומית עם האיום, משום שהאופן בו מתופעל האינטרנט עשוי להשפיע גם על פוטנציאל התקיפות בו, והאופן בו מתמודדים עם תקיפות עשוי להשפיע על מדיניות השימוש באינטרנט.

מנגנונים המשלבים העברת מידע והסדרה

נושא מרכזי בו משולבים הן שיתוף מידע והן הסדרות בין מדינתיות, הוא בתחום ההתמודדות עם פשיעת סייבר, שהביטוי המרכזי שלו הוא האמנה על פשעי מחשב, "אמנת בודפשט", שגובשה על ידי מועצת אירופה. מטרת האמנה היא ליצור מדיניות פלילית משותפת בין חברותיה, למול פשיעה במרחב הסייבר, ולהסדיר שיתופי פעולה ומידע, בין היתר לטובת סיוע באיסוף ראיות, חקירה ואכיפת פשיעה בסייבר.

האמנה נוגעת הן בנושאי תקיפות סייבר והן בנושאי ניצול לרעה של הסייבר (עבירות פורנוגרפיה, זיוף ומרמה, הפרת זכויות יוצרים וכדומה).

מעבר לכך, ניתן להצביע על מגמה מטרידה המתפתחת כיום בסייבר, שבהתמודדות עימה נדרשים מיצוי הכלים בתווך שבין שיתוף מידע והסדרות: היווצרות של שחקנים לא מדינתיים, המחזיקים בידיהם יכולות סייבר הולכות ומתעצמות, המתקרבות בעצמותיהן ליכולות של מדינות.

מעבר לסיכון הישיר לכלכלה ולמדינות העולם כתוצאה מפעילות גורמים אלו, הם גם מהווים את אחד החסמים המרכזיים בגיבוש הסדרות בינלאומיות בתחום הסייבר. מצד אחד, מדינות מסתירות את פעילותן במסווה של פעילות של ארגון לא מדינתי ומכאן פוגעות באפקטיביות של מנגנונים בין מדינתיים. מצד שני, הן נמנעות משיתוף פעולה עם מנגנונים בינלאומיים להתמודדות עם איומים לא מדינתיים, מחשש שמנגנונים אלה יפעלו גם מולן ויצרו את צעדיהן. איום זה מחייב השקעת מאמץ בינלאומי מרוכז ועוצמתי לצורך התמודדות ישירה עם מקורות האיום. ניסיונות ראשוניים בתחום זה (אינטרפול, ITU-IMPACT) עדיין רחוקים ממיצוי הפוטנציאל בתחום, ולרוב יש פער בין ההצהרות בנוגע לפעילות הישירה מול האיום לבין המציאות. בשורה התחתונה, שיתוף פעולה בינלאומי בהתמודדות עם איום הסייבר הוא, ללא ספק, מרכיב חשוב בבניית הגנה במרחב הסייבר, במיוחד בהתחשב באופיין הגלובלי של תשתיות מרחב הסייבר ואופיו הגלובלי של האיום. על אף שההסדרה נמצאת כיום בחיתוליה, הרי שמנגנונים של העברת מידע, לצד ניסיונות ראשוניים להסדרות בין מדינות וכן הסכמים בינלאומיים (כדוגמת "אמנת בודפשט"), מתחילים כבר כיום לשרטט את קווי המתאר של אופי שיתופי הפעולה וההסדרות במרחב הסייבר, שרק ילכו ויתעצמו. ◉

ד"ר אביתר מתניה הוא ראש המטה הקיברנטי הלאומי במשרד רוה"מ, טל גולדשטיין הוא ראש תחום מחקר, תכנון וניתוח במטה.

מוסף סייבר מיוחד לרגל כנס הסייבר הבינלאומי מתפרסם בגיליון זה בעמודים 76-101