

הפעילות במרחב הסייבר בראי המשפט הבין-לאומי

יעל רונן

הדיון ברגולציה פנים-מדינתית של מרחב הסייבר שם את הדגש על הגנת מרחב זה. לעומת זאת, השיח בנושא הסייבר במשפט הבין-לאומי הינו היפוך גמור לכך, וזאת בשלושה מובנים: ראשית, המשפט הבין-לאומי עוסק בהסדרת יחסים בין מדינותיים; שנית, רגולציה היא פעולת ארגון, פיקוח ואכיפה, שמטרתה היא לכפות באופן חוקי כללי התנהגות מחייבים. הנחת היסוד של הרגולציה היא קיומם של כללי התנהגות כאלה. לעומת זאת, המשפט הבין-לאומי נמצא עדיין בשלב של ניסיון לברר מהם כללי ההתנהגות הקיימים והראויים במרחב הסייבר, כלומר, ניסיון לברר מה מותר ומה אסור לעשות בתחום זה; שלישית, בעוד שהרגולציה עוסקת בהגנת מרחב הסייבר, המשפט הבין-לאומי מתמקד בהשלכות של התקפות סייבר על הביטחון.

מרחב הסייבר מאתגר את המשפט הבין-לאומי בכמה היבטים: ראשית, המשפט הבין-לאומי, על כל ענפיו, עוסק בעיקר בהסדרת היחסים הקשורים לגופים מוחשיים (גוף, נכסים, קרקע). לעומתו, מרחב הסייבר אינו מוחשי. כתוצאה מכך מתעוררת השאלה אם הנורמות הקיימות במשפט הבין-לאומי מתאימות למרחב זה, או שיש צורך בעיצוב נורמות חדשות; שנית, המשפט הבין-לאומי מבוסס באופן ספציפי על חלוקה טריטוריאלית: הזירה העולמית מחולקת לשטחי אדמה – מדינות – ודגש רב מושם על חלוקת הסמכויות והזכויות – ריבונות. לעומת זאת, עולם הסייבר הינו במהותו חוצה גבולות; שלישית, המשפט הבין-לאומי מבוסס באופן מסורתי על עליונות המדינות כשחקניות בזירה הבין-לאומית: להן יש זכויות, והן נושאות באחריות. נדמה שבתחום הסייבר המדינות אינן השחקניות המרכזיות.

פרופסור יעל רונן היא פרופסור חבר במרכז האקדמי שערי מדע ומשפט בהוד השרון ועמיתת מחקר במרכז מינרבה לזכויות אדם, האוניברסיטה העברית בירושלים.

מאמר זה מתבסס על הרצאה בכנס של המכון למחקרי ביטחון לאומי, בשיתוף עם המרכז האקדמי שערי מדע ומשפט, שנערך ב-24 באוקטובר 2018 לרגל השקת המזכר "רגולציה במרחב הסייבר", שנכתב על ידי ד"ר אל"ם (מיל') גבי סיבוני ועידו סיון-סביליה

הבדלים אלה מעוררים שאלה בסיסית: האם המשפט הבין-לאומי חל במרחב הסייבר? העיסוק בשאלה זאת מתקיים בעיקר בזירה האקדמית. מדריך טאלין הראשון, מסמך שניסחה קבוצת אנשי אקדמיה והתפרסם בשנת 2013, התמקד בשאלה כיצד ניתן להחיל את המשפט הבין-לאומי על מרחב הסייבר, בראש ובראשונה בהקשר של פעולות המהוות הפרה של האיסור על שימוש בכוח ושל הזכות להגנה עצמית, או פעולות המתרחשות במהלך סכסוך מזוין. מדריך טאלין השני מ־2017 הרחיב את הדיון בסוגיה זאת לשאלת התחולה של המשפט הבין-לאומי על פעולות שאינן מגיעות לכדי שימוש בכוח או למצב של סכסוך מזוין בזירה המדינית. העיסוק של מדינות בתחולת המשפט הבין-לאומי במרחב הסייבר נותר מצומצם. אחת הסיבות לכך היא שהטכנולוגיה מאפשרת חדירה לתחומים רגישים, שבהם ממשלות נזהרות מלהתבטא. למרות זאת, יש כיום קונצנזוס שהמשפט הבין-לאומי חל גם על מרחב הסייבר. אחת ההתפתחויות הבולטות בהקשר זה היא ההסכמה שהושגה ב־2015 במסגרת קבוצת מומחים ממשלתיים שהתכנסה באו"ם, לפיה מגילת האו"ם חלה במלואה גם במרחב הסייבר. הקבוצה כללה, בין היתר, מומחים מארצות הברית, בריטניה, רוסיה וסין, שהן השחקניות הראשיות בזירה הבין-לאומית בתחום זה. להסכמה שהושגה ביניהם יש משמעות שונות, שכמה מהן יפורטו להלן.

מגילת האו"ם מעגנת את האיסור להשתמש או לאיים להשתמש בכוח נגד העצמאות או השלמות הטריטוריאלית של מדינות, וקובעת כי פעולה כזאת תהיה חוקית רק כהגנה עצמית, או בהסמכה של מועצת הביטחון ובנסיבות מיוחדות. השאלה היא, כמובן, מה ייחשב "שימוש בכוח" כשמדובר בפעולות סייבר. פעולות סייבר בהקשר זה היא פעולה נגד מערכת מחשבים במטרה לאסוף, להחדיר, לשנות או לשבש נתונים בדרכים אחרות, או כדי לעשות מניפולציה בפעולה של המערכת. יש הסכמה רחבה שפעולת סייבר יכולה להיחשב כ"שימוש בכוח" או כ"התקפה מזוינת", אם תוצאותיה הצפויות יהיו מסוג ברי-השוואה לאלו של התקפה קינטית, כלומר גרימת מוות או פגיעה של אנשים ופגיעה ברכוש. למשל, אם פעולת סייבר תביא להסטת רכבת מפסי המסילה או לפריצת סכר מים באזור מיושב, היא תיחשב להתקפה מזוינת, בדיוק כמו הפצצת המסילה מהאוויר.

דוגמה להתקפה מסוג זה היא פרשת Stuxnet. ב־2010 חדר פוגען ("סטקסנט") למערכות שעליהן התבססו הצנטריפוגות באחד המתקנים הגרעיניים של איראן. תולעת שהוחדרה למערכות במתקן הגרעיני גרמה לצנטריפוגות להסתובב, לצאת משליטה ולהיהרס. זו אחת הפעמים הראשונות שבהן נגרם הרס פיזי של רכוש על ידי פעילות סייבר. הפעולה הצביעה על הפוטנציאל של מרחב הסייבר כאמצעי להרס ולגרימת נזק ליריב, בדיוק כמו התקפה באמצעים קונבנציונליים.

לסיווג של מעשה כ"התקפה מזוינת" יש חשיבות, כי בהתקיים נסיבות מסוימות, "התקפה מזוינת" מקנה למדינה המותקפת זכות להגנה עצמית. אם פעולת סייבר יכולה להיחשב "התקפה מזוינת", אזי תיתכן גם תגובה כוחנית לה. לפי גישה זאת, ההתקפה על איראן באמצעות תולעת "סטקסנט" עשויה הייתה להקנות לה זכות להגנה עצמית. שאלה חשובה המתעוררת בהקשר זה היא כלפי מי קיימת זכות ההגנה העצמית. גורמים באיראן ובמדינות נוספות ייחסו את התקפת "סטקסנט" לארצות הברית ולישראל, אף שלא הוצגו ראיות של ממש למעורבות של מדינה מסוימת בייצור הפוגען או בהפצתו. שאלה נוספת היא איזו פעולת נגד תיחשב חיונית ופרופורציונלית, כנדרש על מנת שניתן יהיה לראותה כחוקית במסגרת זכות ההגנה העצמית.

הסוגיה המורכבת ביותר, לגביה עדיין אין קונצנזוס, קשורה לאותם מצבים שבהם פעולת סייבר גורמת פגיעה קשה ומשמעותית, אך ללא גרימת נזק פיזי לאדם או לרכוש. הפרשנות המקובלת היא שאיסוף מידע, גניבת מידע ואפילו השמדת מידע או שינויו אינם "התקפה מזוינת" בפני עצמם. כשאין מדובר ב"התקפה מזוינת", גם לא ניתן להגיב עליה במסגרת ההגנה העצמית. עם זאת, השפעתן המזיקה של פעולות כאלו יכולה להיות משמעותית מאוד. דוגמה אפשרית לכך היא התקפה על המערכת הכלכלית והפיננסית, למשל פעולת סייבר על הבורסה בניו יורק, שתגרום לה להתרסק בשל פגיעה באמינות המידע ובתשתית המחשבים. השאלה המתעוררת בהקשר זה היא אם מדובר בנזק כלכלי גרידא, או שהתוצאות הקטסטרופליות של הפעולה מצדיקות את התיוג שלה כ"התקפה מזוינת".

פעולת סייבר אחת כזאת עוררה את העניין הבינלאומי בתחולתו של המשפט הבינלאומי על מרחב הסייבר: באפריל 2007 הודיעה ממשלת אסטוניה על כוונתה להעביר אנדרטת זיכרון למלחמת העולם השנייה ממרכז עיר הבירה טאלין לבית קברות צבאי בפרברי העיר. בתגובה לכך החלו הפגנות אלימות של אזרחים אסטוניים ממוצא אתני רוסי. בהמשך בוצעו לאורך כחודש ימים התקפות על תשתיות אינטרנט ציבוריות וכלכליות באסטוניה. האינטרנט הוא כלי שימושי משמעותי ביותר באסטוניה: 95 אחוזים מהפעילות הבנקאית במדינה מנוהלת באופן דיגיטלי ו-98 אחוזים משטח המדינה היה מרושת, עד כדי כך שנאמר על אסטוניה כי האינטרנט חשוב בה כמעט כמו מים זורמים. ההתקפות על תשתיות האינטרנט באסטוניה כללו את האתרים של נשיא המדינה, ראש הממשלה, הפרלמנט, מפלגות, בנקים, אמצעי התקשורת ועוד. השפעתן הייתה משמעותית: שני הבנקים המרכזיים במדינה שותקו למשך מספר ימים, וחלק מסוכנויות החדשות המרכזיות נפגעו. קווי החירום במדינה נותקו למשך שעה, התקשורת הפרטית והציבורית נפגעה, ובעיקר נפגע האמון בכלכלת המדינה. מקובל לייחס את ההתקפות לרוסיה, וחלקן אכן בוצעו ממחשבים בשליטת מוסדות ממשלתיים רוסיים. עם זאת, עקבות

התוקפים הובילו ל-177 מדינות נוספות, ורוב ההתקפות בוצעו ממחשבים בעלי כתובת פרטית.

פוליטיקאים אסטונים השוו את ההתקפות לפלישה ולפעילות צבאית קונבנציונלית, אך הנזק הממשי שלהן היה מזערי, ובעיקרו כלכלי: לא הייתה פגיעה ברכוש או בנפש, חיילים לא נשלחו לחזית, ולא נעשה שימוש בתחמושת קונבנציונלית. מצד שני, הייתה פגיעה בתשתיות הכלכליות הבסיסיות של המדינה, דבר שהיווה פגיעה אנושה ביכולת התפקוד שלה.

קביעה אפשרית שמדינה שהייתה קורבן לפגיעה משמעותית באמצעות סייבר לא תוכל לנקוט צעדי הגנה עצמית בתגובה לכך, היא בעייתית מאוד. התעלמות מהתפתחויות טכנולוגיות עלולה להוביל לתוצאות אבסורדיות, וספק אם מדינות יצייתו לכלל שאינו עולה בקנה אחד עם צרכים מציאותיים. לכן, יש כיום מידה רבה של קונצנזוס בקרב אנשי האקדמיה שפעולות סייבר עלולות להוביל לתוצאות חמורות כל כך, עד שיהיה מוצדק להגדירן כ"התקפה מזוינת". השאלה היא מהן אמות המידה לכך. בתשובה לכך ניתן לבחון היבטים שונים, כמו השלכות על אינטרסים לאומיים חיוניים, מיידיות ההתממשות של התוצאות ומידת הישירות, החודרניות או המעורבות המדינתית.

עיקרון נוסף המעוגן במגילת האו"ם הוא האיסור להתערב בענייניהן הפנימיים של מדינות. איסור זה אינו מתייחס לאמצעים ספציפיים, ולפיכך כולל גם התערבות באמצעות הסייבר. האיסור על התערבות בעניינים פנימיים אינו בולט בדרך כלל בשיח הבין-לאומי, כי כאשר יש התקפה קונבנציונלית על מדינה, ה"התערבות" היא עניין שולי יחסית. דווקא כאשר אין שימוש באלמות, אלא נעשית מניפולציה חברתית או כלכלית, איסור ההתערבות הופך למרכזי.

ככלל, מעשה יחשב "התערבות" כאשר יש כפייה או לחץ, מפורש או אחר. למשל, ריגול ואיסוף נתונים ממחשבים במדינה זרה אינם בגדר התערבות אסורה, כי אף שיש בהם מרכיב של חדירה לרשת מחשבים זרה, כשלעצמם הם אינם מהווים כפייה או הפעלת לחץ על אותה מדינה. המצב שונה כאשר יש מניפולציה של תוצאות בחירות או של דעת קהל ערב בחירות באמצעות מחשבים. יש תחומים שבהם המחלוקת רבה עוד יותר: למשל, מה דין פגיעה באמצעות אתרי תוכן בקמפיין פוליטי של מפלגה מסוימת, או יצירת פעילות פיקטיבית שמטרתה היא הטיית דעת קהל? אפשר לטעון שבכל התחומים האלה יש התערבות בליבה של ריבונות המדינה – אמנם לא מבחינה צבאית, אלא מבחינה חברתית ופוליטית – שהשפעתה יכולה להיות חמורה מאוד. אין ספק שמעשים מסוג זה אסורים; מה שעדיין מהווה שאלה פתוחה היא איך רשאית המדינה הנפגעת להגיב עליהם.

מרחב הסייבר יוצר דילמות נוספות למשפט הבין-לאומי. אחת מהן קשורה למגבלות על שימוש בסייבר הנובעות מכללי המשפט ההומניטרי. דילמה נוספת

קשורה לסיכונים שהשימוש בסייבר מציב בפני הגנה על זכויות אדם. בתחומים אלה ונוספים נמצא המשפט הבין־לאומי רק בראשית דרכו. הצורך לעבד ולגבש נורמות בעקבות התפתחויות טכנולוגיות אינו ייחודי למשפט הבין־לאומי. עם זאת, אין ספק שמושכלות היסוד המשפטיות של המשפט הבין־לאומי שרירות וקיימות גם במרחב הסייבר.