מבט על, גיליון 1364, 13 באוגוסט 2020

סנקציות אירופאיות לראשונה בגין מתקפות סייבר – עליית מדרגה במאמצי ההרתעה של מדינות המערב בתחום?

*ורד זליכה**

ב-30 ביולי 2020 החליט האיחוד האירופי להטיל צעדים מגבילים על תשעה אנשים וגופים שמוצאם בסין, קוריאה הצפונית וברוסיה בגין אחריותם למתקפות סייבר או מעורבות בהן. הסנקציות כוללות הגבלות תנועה, הקפאת נכסים ואיסור על העברת כספים לאותם אנשים וגופים. ברמה הפוליטית נראה כי מדינות המערב הצליחו להגיע להסכמות בתחום זה ולפעול בשיתוף פעולה, על אף חילוקי דעות במישורים אחרים. מזווית המדיניות הבינלאומית בסייבר, על פניו מדובר בצעד משלים לצעדים קודמים שננקטו על ידי מדינות מערביות ועל ידי האיחוד האירופי עצמו, העשוי להשתלב היטב עם אסטרטגיית ההרתעה בסייבר, המקודמת בשנים האחרונות על ידי ארצות הברית. ייתכן, שהאיחוד האירופי שואף בין היתר לשגר מסר הרתעתי מפני תקיפות סייבר, בפרט בתקופת משבר הקורונה.

ב-30 ביולי 2020 הודיעה מועצת האיחוד האירופי על הטלת סנקציות ("צעדים מגבילים") על שישה אנשים ושלושה גופים שמוצאם בסין, קוריאה הצפונית וברוסיה בגין אחריות למתקפות סייבר וניסיונות לבצען, או מעורבות בהן. זאת, לפי הודעת שר החוץ של האיחוד (הממונה על נושא החוץ והביטחון בנציבות האיחוד) ג'וזף בורל, על מנת למנוע פעילויות זדוניות בסייבר, להרתיע מפניהן ולהגיב להן, וכך לקדם את היציבות והביטחון הבינלאומיים במרחב הסייבר.

הסנקציות החדשות הוטלו בהתאם למסגרת משטר הסנקציות בסייבר שאומצה על ידי האיחוד האירופי במאי 2019, כחלק ממדיניות תגובה דיפלומטית משותפת בסייבר ("סל כלים דיפלומטי") של האיחוד שפותחה החל משנת 2017.

בהתאם למשטר הסנקציות, הן יוטלו על אישים או גופים בגין אחריותם למתקפות סייבר בעלות השפעה משמעותית, או מעורבות בהן, או ניסיונות למתקפות כאמור, כאשר מדובר באיום חיצוני על האיחוד האירופי, או על חברותיו; חלופות נוספות הן מתקפות סייבר בעלות השפעה משמעותית על מדינות שלישיות או על ארגונים בינלאומיים, כאשר הדבר נחוץ להשגת יעדים משותפים במדיניות ביטחון וחוץ של האיחוד האירופי.

הצעדים שננקטו כוללים הגבלות על כניסה של האישים לאיחוד האירופי והקפאת נכסים שלהם ושל הגופים. כן נאסר על אנשים או גופים באיחוד האירופי להעביר כספים, במישרין או בעקיפין, לאותם אישים וגופים הנמנים ברשימת הסנקציות. כלפי נשואי הסנקציות נטען שהיו מעורבים באירועי סייבר מסוגים שונים, רובם התרחשו וזכו להד תקשורתי ובינלאומי בעיקר בשנים 2017–2018, כמפורט ברשימה:

(1) חברה צפון קוריאנית בגין מעורבותה, לפי הנטען, בסדרת תקיפות סייבר, בהן אירוע Wannacry, אשר שיבש מערכות מידע ברחבי העולם, לרבות מערכות מידע של חברות אירופאיות, ובכלל זאת פגע באספקת שירותים חיוניים ופעילויות כלכליות באיחוד;

(2) שני אישים סינים וחברה לפיתוח טכנולוגיה מסין שהעסיקה אותם, המעורבים על פי הנטען, בתקיפת מערכות מידע של תאגידים רב-לאומיים בשש יבשות, כולל תאגידים שמקום מושבם באיחוד האירופי, ובהשגת גישה בלתי מורשית למידע מסחרי רגיש תוך גרימת נזק כלכלי חמור ("Operation Cloud Hopper", APT 10);

(3) ארבעה אנשי שירותי המודיעין הרוסי בגין מעורבותם, לפי הנטען, בניסיון לגישה בלתי מורשית לרשת הארגון הבינלאומי OPCW (Organisation for the Prohibition of Chemical Weapons) הממוקם בהולנד, אשר לו הצליחה, הייתה פוגעת באבטחת הרשת והייתה עלולה לשבש את עבודת החקירה של הארגון; וכן המרכז לטכנולוגיות מיוחדות של הצבא הרוסי, בגין מעורבותו, לפי הנטען, באירוע NotPetya, אשר הביא לחסימת גישה למידע של חברות רבות בעולם, כולל באיחוד האירופי, וגרם נזק כלכלי רב, וכן בגין מעורבותו, לפי רשימת הסנקציות, בתקיפת תחנת הכוח באוקראינה בשנים 2015-2016.

יש לציין, כי ביחס למרבית האירועים המרכזיים הנזכרים בסנקציות ננקטו בעבר צעדי הוקעה פומביים מצד מדינות המערב. צעדים אלה כללו הודעות גינוי ו/או הגשת כתבי אישום בחלק מהמקרים, לעיתים תוך הטלת אחריות על פרטים או על גופים, ואף על מדינות. האיחוד האירופי עצמו גינה את מרביתם של אירועים אלה בהצהרות פומביות, והסנקציות החדשות בהקשר זה נראות כמהלך משלים ותואם לאותם צעדים.

בסמוך לפרסום ההודעה על הסנקציות, ארצות הברית, בריטניה, אוסטרליה וקנדה, לצד מדינות באיחוד האירופי, הביעו תמיכתן ובירכו על המהלך. בריטניה הודיעה כי הסנקציות הן בתוקף גם בבריטניה והזכירה את מנגנון הסנקציות הבריטי, התואם למנגנון האירופי, שיצרה בעקבות הברקזיט.

לפי הדיווחים בתקשורת, רוסיה וסין מתחו ביקורת על הצעד להטלת סנקציות על ידי האיחוד האירופי, תחת קיום דיאלוג. בין היתר, בהתייחסות משרד החוץ הרוסי, נאמר כי מדובר בצעד "חד צדדי" שאינו תואם את המשפט הבינלאומי, וכי "בדיפלומטיה הכל הדדי". עוד דווח, כי המשלחת הסינית לאיחוד האירופי הסתייגה אף היא מהצעדים, בציינה כי על הקהילה הבינלאומית לפעול על בסיס כבוד הדדי להבטחת ביטחון הסייבר הבינלאומי.

בחינה ראשונית של המהלך האירופי מצביעה על מספר תובנות מעניינות:

- ראשית, מהזווית המדינית הרחבה, הטלת סנקציות על ידי האיחוד האירופי בעת הנוכחית, בתמיכה של ארצות הברית, בריטניה ומדינות מערביות נוספות, יכולה להתפרש כביטוי לחזית מתואמת של מדינות המערב במדיניות סייבר בזירה הבינלאומית, חרף חילוקי דעות בסוגיות אחרות (ביניהן הסדרי הברקזיט, או ההתמודדות עם משבר הקורונה).

- שנית, ניתן לראות בסנקציות מהלך היכול להשתלב עם אסטרטגיית ההרתעה האמריקאית בסייבר, שפורסמה על ידי הבית הלבן בספטמבר 2018. עניינה של אסטרטגיה זו, בין היתר, בקידום פעולה מתואמת בקואליציה של מדינות Likeminded ל"גביית מחיר" מיריבים בגין מעשים זדוניים בסייבר, באמצעות מגוון צעדי תגובה הרתעתיים, כולל ייחוס והודעות פומביות. ניתן אפוא לראות בסנקציות האיחוד האירופי צעד תואם לתפיסה זו, בפרט בהתחשב בכך שלמהלך קדמו הודעות גינוי והוקעה על ידי מדינות המערב בתגובה למרבית האירועים הנדונים ברשימה.

נכון להבין את המהלך גם כחלק מתמונה מקיפה יותר של צעדי גינוי, הוקעה והטלת אחריות שנרשמו בחודשים האחרונים, בתגובה לאירועי סייבר אחרים, בהם: הודעות גינוי והתרעה מצד ארגונים בינלאומיים ומדינות בזמן משבר הקורונה ביחס לאירועי סייבר נגד מגזר הבריאות על זרועותיו השונות (בין הדוגמאות עליהן דווח בתקשורת - תקיפת מערכות מחשוב בבית חולים בצ'כיה; ניסיון לתקיפת ארגון הבריאות העולמי; ריגול מסחרי בחברות המפתחות חיסונים לקורונה); הגשת כתבי אישום בארצות הברית נגד שני אישים מסין בגין קמפיין ריגול מסחרי בסייבר ביחס לחברות ולגופים במדינות שונות; הוצאת צו מעצר בגרמניה נגד איש מודיעין רוסי החשוד במעורבות בתקיפת סייבר של הפרלמנט הגרמני (הבונדסטאג) בשנת 2015, שגרמה בין היתר לדליפת תכתובות רגישות.

- שלישית, החלטת הסנקציות מבטאת בכל מקרה "עליית מדרגה" בהוקעת פעילויות סייבר זדוניות מצד האיחוד האירופי. המהלך נועד לשדר מסר חד וברור כי האיחוד לא ישלים עם מעשים מסוג זה והוא נחוש להגן על עצמו ועל חברותיו. ייתכן, כי הטלת הסנקציות בעת הנוכחית משקפת בחירה אסטרטגית של האיחוד לפעול בתקיפות ולקדם הרתעה, בין היתר גם על רקע תקיפות סייבר שהתרחשו נגד מגזר הבריאות בתקופת הקורונה (ובהמשך להודעת גינוי בהקשר זה מטעם מועצת האיחוד האירופי מחודש אפריל 2020).

- רביעית, במהלכי האיחוד האירופי משתקפת גישה זהירה בסוגיית הטלת אחריות וייחוס כלפי מדינות ספציפיות, ככל הנראה מטעמים פוליטיים. הובהר על ידי האיחוד האירופי, כי צעדים מגבילים ממוקדים הם צעדים הרתעתיים, ויש להבחין ביניהם לבין ייחוס אחריות למדינה שלישית. ניתן להעריך, כי העובדה שבעבר הוצאו הודעות גינוי או התייחסויות אחרות מטעם האיחוד האירופי למקרים המרכזיים המוזכרים ברשימת הסנקציות, הקלה על חברות האיחוד את גיבוש ההסכמה להטיל על האחראים להם סנקציות קונקרטיות. יתר על כן, נראה כי בהחלטה להטיל מכלול סנקציות בבת אחת על קבוצת אירועי סייבר ומגוון גורמים ממדינות שונות, יש כדי לרכך את האפקט שהיה נוצר לו היו מכוונות לגורם אחד, ובד בבד לשגר מסר מרתיע בדבר נקיטת צעדים כלפי המעורבים במתקפות סייבר, ללא תלות במקור התקיפה.

לסיכום, הסנקציות מטעם האיחוד האירופי בגין אירועי סייבר מהוות מהלך נוסף בעיצוב "כללי משחק" ומדיניות הרתעה בסייבר, המצטרף לצעדי גינוי והוקעה הולכים וגוברים בתקופה האחרונה מצד מדינות מערביות בגין תקיפות סייבר, גם על רקע משבר הקורונה. יש לבחון כיצד יתפתחו הדברים בהמשך הדרך - מה תהיינה ההשפעות המיידיות של המהלך; האם יאומצו בקרוב סנקציות נוספות מצד האיחוד האירופי ובגין אילו מקרים; מה תהיה האפקטיביות לטווח ארוך של הצעדים האלה; האם וכיצד החלטת הסנקציות האירופית עשויה להשפיע על מהלכים אחרים בסייבר בזירה הבינלאומית.

** עו"ד ורד זליכה היא מומחית במשפט ומדיניות סייבר.*