מבט על, גיליון 1328, 2 ביוני 2020

מלחמת הסייבר בין ישראל לאיראן עולה מדרגה

דודי סימן טוב ושמואל אבן

תקיפת תשתיות אזרחיות חיוניות נחשבת דרגה חמורה בסולם תקיפות הסייבר. לפי דיווחים בתקשורת, איראן תקפה תשתיות מים וביוב בישראל, שהגיבה בתקיפת סייבר נגד תשתיות בנמל איראני בבנדר עבאס. הגם שתקיפות אלה אינן ראשונות, הן ממחישות שזירות העימותים בין שתי המדינות כוללת תשתיות אזרחיות חיוניות. ישראל הצליחה עד כה להתמודד עם תקיפות הסייבר נגד תשתיות כאלה בלי שנגרם לה נזק רב, אך היא עלולה להיות פגיעה יותר ככל שיואץ מרוץ החימוש בתחום הסייבר ואיראן תשכלל את יכולותיה. על ישראל להניח שיהיו ניסיונות תקיפה נוספים ומתוחכמים יותר מאלה שנרשמו עד כה.

מלחמות בסייבר מנוהלות בחשאיות ועמימות, למעט כאשר למי מהצדדים בעימות יש אינטרס בחשיפת מידע. המתקפות מבוצעות בדרך כלל ללא נטילת אחריות ותוך הכחשה, וברוב רובם של המקרים איתור מקורן אינו פשוט. תקיפות במרחב הסייבר נתפסות כמתאימות למערכה בין מלחמות (מב"מ) משום שהן מאפשרות לתוקף לפעול ממרחק, בחשאי, ולהימנע מפגיעה בנפש בשני הצדדים כדי למנוע הסלמה. מתקפות סייבר מאפשרות לאסוף מידע, לבצע לוחמת מידע תודעתית, להעביר מסרי הרתעה, להגביר לחצים על מערכות צבאיות ואזרחיות כדי להשיג מטרות ביטחוניות ומדיניות ולבצע פעולות סיכול. בתחום הסיכול הצבאי תוזכר תקיפת "סטוקסנט" נגד מתקני הגרעין באיראן, שנחשפה בשנת 2010 והייתה אירוע מכונן בתחום תקיפת תשתיות באמצעות סייבר. תקיפה על מערכות שליטה ובקרה של תשתיות אזרחיות חיוניות נחשבת לדרגה גבוהה בסולם דרגות החומרה של תקיפות סייבר, כשבין החמורות ביותר הן תקיפות המסכנות חיים של המוני אזרחיים, למשל בעקבות זיהום מים, או תאונות כתוצאה מתקיפת מערכות תחבורה.

לפי דיווחים בעיתונות אמריקאית, איראן וישראל מחליפות ביניהן מהלומות במרחב הסייבר, תוך תקיפת תשתיות אזרחיות קריטיות. לפיהם, ישראל ביצעה ב-9 במאי 2020 מתקפת סייבר בנמל איראני בבנדר עבאס (נמל שהיד רג'אעי) שבדרום איראן, כתגובה למתקפת סייבר איראנית נגד תשתיות מים ושופכין ("מערכת המים") בישראל.

התקיפה המיוחסת לאיראן נגד מערכת המים בישראל בוצעה במספר מוקדים במרחב המדינה ב-24-25 באפריל 2020 (לפני יום העצמאות ובתחילת השלב הראשון למתווה היציאה מהסגר הקורונה). באחת התחנות נרשמו חריגה בנתונים ו"אי-סדירות"; בתחנה אחרת, משאבה נותקה ממצב אוטומטי (מבוקר) ונכנסה לפעולה ללא-הפסקה, ובתאגיד מים אחר נרשמה השתלטות על מערכת התפעול (Ynet, 19 במאי). באחד המקרים, משאבת מים פסקה לפעול לזמן קצר. החשש, שהוצג על-ידי מערך הסייבר הלאומי, היה כי ישראל הייתה נאלצת להתמודד, בעת משבר הקורונה, עם מחסור זמני במים, או עם ערבוב של כלור או כימיקלים אחרים במינון לא נכון שיכול היה לגרום לנזק ולאסון.

לפי גורמים המקורבים לחקירת האירוע, מוערך שמקור תוכנות התקיפה הוא ביחידות הסייבר התקפיות של משמרות המהפכה של איראן (כך דיווח הניו-יורק טיימס, 19 מאי). בעקבות התקיפה פורסמה הודעה מטעם רשות המים ומערך הסייבר הלאומי בישראל, לפיה: "לאחרונה זוהה ניסיון למתקפת סייבר על מערכות שליטה ובקרה במגזר המים. ניסיון התקיפה טופל על ידי רשות המים ומערך הסייבר הלאומי. יודגש כי לא הייתה כל פגיעה באספקת המים והיא התנהלה ומתנהלת כסדרה". ראש מערך הסייבר של ישראל, יגאל אונא, הגדיר (28 במאי) את התקיפה כ"נקודת שינוי" בהיסטוריה של מלחמות הסייבר של ישראל. לדבריו, "הניסיון למתקפה על ישראל היה מתואם ומאורגן במטרה לפגוע במערכת המים ההומניטרית שלנו ואם היא הייתה מצליחה, היינו נאלצים להתמודד עם נזק לאוכלוסייה אזרחית ואף מחסור זמני במים שיכול היה לגרום לנזק ולאסון". אריק ברבינג, לשעבר ראש מערך הסייבר בשב"כ, העריך שהתקיפה מעידה על יכולת מדינתית, המתבססת על מודיעין מדויק. האלוף (מיל') פרופ' יצחק בן ישראל, ראש מרכז הסייבר באוניברסיטת ת"א, ציון שמדובר בניסיון שלישי לפחות לתקוף מערכות מים בישראל, שלא נחל הצלחה.

בנוסף, בחדשות ערוץ 12 דווח ב-25 במאי 2020, כי במהלך השבועות האחרונים נחשפו תקיפות סייבר, שנועדו לפגוע במכוני מחקר ישראלים, העוסקים בין היתר בפיתוח תרופות וחיסון נגד נגיף הקורונה. על פי הדיווח, מטרת התקיפה לא הייתה איסוף מידע אלא גרימת הרס. אם מדובר בעוד מהלך הקשור למלחמת הסייבר בין ישראל לאיראן, הרי שהיקף המתקפה האיראנית הינו רחב יותר.

עוד דווח בתקשורת בישראל, בהקשר לתקיפת הסייבר על המערכות המים, כי הנושא עלה לדיון בקבינט הביטחוני-מדיני ב-7 מאי 2020. ניתן להעריך ששם התקבלה החלטה להגיב. התקיפה המיוחסת לישראל בתקשורת אמריקאית יצאה לפועל ב-9 במאי 2020 והיא כוונה נגד תשתיות בנמל איראני בבנדר עבאס. התקיפה גרמה לקריסת המחשבים המכוונים את תנועת כלי השיט, המשאיות והסחורות, מה שגרם להשבתת הפעילות בו למשך מספר ימים. העיתון ישראל-דיפנס (15 במאי 2020) ציין כי מבחינת איראן מדובר בתקיפת הסייבר השלישית מאז דצמבר 2019 שגרמה להשבתת נמלי ים שלה. עם זאת, יצוין כי ישראל אינה היחידה שמיוחסות לה תקיפות סייבר באיראן.

ניתן להעריך, שישראל ראתה בתקיפת תשתיות מים אזרחיות שלה (במיוחד בעת מצב חירום לאומי בשל הקורונה) אירוע חמור, שלא ניתן לעבור עליו לסדר יום. וזאת בין אם מדובר באירוע חריג ובין אם מדובר באירוע שהגדיש את הסאה בשרשרת אירועים. לא מן הנמנע, שהעובדה שהתקיפה המיוחסת לאיראן נחשפה בתקשורת דרבנה את קברניטי ישראל להגיב. בכל מקרה, ישראל לא הופתעה אסטרטגית מההתקפה, הגם שהיא לא קשרה את איראן באופן פומבי למתקפה. ביוני 2019 אמר ראש מערך הסייבר הלאומי, יגאל אונא, כי "איראן ושלוחותיה ממשיכות להיות איום סייבר מרכזי על המזרח התיכון. ישראל ערוכה מול איומי סייבר, יש לנו את היכולת להגיב בעוצמה מול תוקפי סייבר, לא בהכרח באותו התווך בו תקפו". לפי נתונים שהציג, האיראנים פועלים באופן שוטף ולאורך זמן במתווה תקיפה רחב, הכולל תקיפות למטרת איסוף מודיעין, תקיפות המיועדות להשפיע על תודעה (כגון תקיפת אתרים ישראליים) ותקיפות שמטרתן פגיעה והרס של מערכות (Ynet, 26 ביוני 2019).

תקיפת הנמל האיראני, המיוחסת לישראל, נועדה כנראה להעביר מסר הרתעתי. הערכה זו נסמכת על רמיזות של בכירי מערכת הביטחון הישראלית בתקשורת. שר הביטחון, נפתלי בנט, הצהיר ב-18 במאי 2020 בטקס לסיום תפקידו: "התמנון האיראני שולח את זרועותיו ללפות אותנו מכל עבר [...] עלינו להגביר את הלחץ המדיני, הכלכלי, הצבאי, הטכנולוגי, ולפעול גם בעוד ממדים, זה אפשרי". הרמטכ"ל, ראי"ל אביב כוכבי, הצהיר ב-19 במאי 2020, שצה"ל "ימשיך לפעול בכלים צבאיים מגוונים ובשיטות לחימה ייחודיות לפגיעה באויב".

לוחמת הסייבר האיראנית היא חלק ממאבק אסטרטגי שמנהלת איראן במספר זירות, מול כמה אויבים ובראשם: ארצות הברית, ישראל וערב הסעודית. מבחינת איראן, מתקפות סייבר אינן תחליף לפעולות קינטיות, אלא יכולת נוספת להן. למשל, לאיראן יוחסו התקפות באיכות גבוהה יחסית נגד חברת הנפט הסעודית ארמקו, בבת עינה ומקור עושרה של הממלכה, שהיא ספקית נפט חשובה למשק העולמי וסייעה לארצות הברית לגשר על המחסור בנפט האיראני כתוצאה מהסנקציות שהוטלו על איראן. בדצמבר 2012 ביצעה איראן תקיפת סייבר נרחבת נגד "ארמקו", שבמהלכה נפגעו כ-30 אלף מחשבים של החברה ואילו בספטמבר 2019 הפתיעה איראן את העולם בתקיפות קינטיות מדויקות של מתקני החברה באמצעות מל"טים וטילי שיוט. בשני המקרים טהראן לא נטלה אחריות.

מול ישראל - תקיפות הסייבר האיראניות מהוות חלק ממאבק רב-חזיתות בין המדינות, הבא לידי ביטוי גם בקריאה להשמדת ישראל, התבססות צבאית בסוריה, תמיכה בחיזבאללה ובארגונים אסלאמיים פלסטינים, ובחתירה לנשק גרעיני. תקיפת סייבר נגד תשתית המים בישראל מעידה שאיראן אינה מהססת לעשות שימוש בנשק הסייבר נגד אוכלוסייה אזרחית. הסיבה לעיתוי הקונקרטי של ההתקפה של מתקני המים בישראל אינה ידועה. ייתכן שזו תגובת קונקרטית לתקיפות קינטיות המיוחסות לישראל נגד יעדים איראנים בסוריה, או שמדובר בעוד תקיפה איראנית, תוך ניצול הזדמנות, במערכה רב-זירתית (מב"ם) מתמשכת הכוללת גם לוחמת סייבר.

בזירת הסייבר, איראן נמצאת בנחיתות טכנולוגית וכלכלית מול ישראל ובוודאי מול ארצות הברית, בעלת-בריתה. ברם, במלחמת סייבר מול איראן עלולה גם ישראל לספוג נזקים, ולבטח לשאת בעלויות נוספות להגנה על מרחב הסייבר שלה, ובפרט שתלותה בממד הדיגיטלי הולכת וגוברת. למרות שאיראן טרם הצליחה לגרום לישראל נזקים משמעותיים במרחב הסייבר, ניתן לצפות להמשך המאמצים מצידה ולהתפתחות איכות התקיפות, כמו גם לתגובות ישראליות.