מבט על, גיליון 1190, 9 ביולי 2019

מוכנותה של ערב הסעודית להסלמה במרחב הקיברנטי

יואל גוזינסקי ורון דויטש

אחד הממדים שאליו גולשת ההסלמה האמריקאית-איראנית בשבועות האחרונים הוא המרחב הקיברנטי. העתקתו החלקית של העימות למרחב הסייבר מאפשרת לבצע פעולות תגמול תוך הפחתת התהודה שתחייב את הצד השני להגיב ולהסלים - כפי שניתן להבין את מתקפת הסייבר שביצעה ארצות הברית בתגובה להפלת המל"ט האמריקאי על-ידי איראן. עם זאת, בהתחשב בקצב ההתפתחות הגבוה של הידע והטכנולוגיה בתחום הסייבר, שילובו של תחום זה בעימותים בינלאומיים מעמידה בסכנה ממשית את המדינות המפגרות מאחור במרוץ הטכנולוגי. ערב הסעודית נמצאת במקום רגיש במיוחד בהקשר זה.

מתוקף היותה ב"קו האש" הקדמי של העימות בין ארצות הברית לאיראן, קרי כזו שעלולה לספוג מהלומה קינטית, יש לבחון את מוכנותה של ערב הסעודית לתרחיש שבמסגרתו ההסלמה בו תועתק באופן מוגבר למרחב הקיברנטי. ראשית, תוסבר רגישותה הרבה של ערב הסעודית בהקשר זה. בהמשך ינותחו האפשרויות השונות לפעילות הקיברנטית של איראן כלפי הממלכה, ולסיום תיסקר מוכנותה של ערב הסעודית להתמודדות עם פעילויות אלו.

למרות שערב הסעודית אינה מעורבת ישירות בהסלמה הנוכחית במפרץ, הנסיבות הגיאופוליטיות מציבות אותה ב"קו האש", גם בהיבט הקיברנטי. איראן לא בוחלת לתקוף מטרות אזרחיות-כלכליות אותן היא מזהה כפחות מוגנות ולכן פגיעות יותר מיעדים צבאיים. הממלכה היא אחת המדינות המותקפות ביותר בעולם בתחום הסייבר והערכה היא שמרבית ההתקפות עליה מקורן באיראן. כך לדוגמא, 42 אחוזים מהתקפות הסייבר שבוצעו על-ידי גוף הידוע בכינוי APT33 המזוהה עם איראן כוונו בשלוש השנים האחרונות כנגד יעדים סעודיים ו"רק" 34% מההתקפות כוונו נגד מטרות אמריקאיות.

הן ארצות הברית והן איראן מתמודדות עם דילמה אסטרטגית. מצד אחד, הן אינן רוצות בעימות כולל במפרץ (כפי שעולה מהתבטאויותיהם של הדרגים הבכירים ביותר משני הצדדים). לכן, לשני הצדדים יש אינטרס לא לנקוט צעדים שיסלימו את המצב. צריך לזכור שעימות במפרץ יכול להתפתח לא רק כתוצאה מתגובה לפעולות טרור מצד איראן אלא בהמשך למהלך כוח אמריקאי נגד יעדי הגרעין. מנגד, טהראן מוצאת שעליה להגיב לגל האחרון של הסנקציות שהוטלו עליה על ידי הממשל האמריקאי. ומבחינת ארצות הברית, הכלתם של צעדי ההתגרות האיראנים עלולה להתפרש כחולשה על ידי איראן ומדינות המפרץ, תערער את ביטחונן של בעלות בריתה של ארצות הברית באשר ליכולתה להגן על חופש השיט באזור, וכן תעודד את איראן להמשיך במעשי התוקפנות.

כבעלת הברית המרכזית של ארצות הברית במפרץ, ערב הסעודית נמצאת בסיכון גבוה. יכולותיה הגבוהות של ארצות הברית בכל הקשור להגנת סייבר אמורות להקשות מאוד על איראן להוציא לפועל מתקפה משמעותית ישירות נגדה, ולכן קיימת אפשרות שאיראן תבחר לפגוע דווקא בערב

הסעודית - "הבטן הרכה" של ארצות הברית באזור המפרץ - כדי לנסות ולכפות על הממשל להקל את מדיניות הסנקציות, ועדיין מבלי לחייבו לתגובה נרחבת. שכזאת. יכולותיה הנמוכות יחסית של ערב הסעודית בתחום הסייבר עושות אותה קלה יחסית לפגיעה. בהתחשב בחשיבותה הכלכלית והגיאופוליטית של הממלכה עבור הקהילה הבינלאומית, ולכן, פעילות סייבר כלפי יעדים סעודיים עשויה להשיג אפקט מכאיב בהרבה ממה שהייתה משיגה לו הייתה מכוונת כלפי ארצות הברית.

עקרונית, ניתן לתאר שני ערוצים פוטנציאליים מרכזיים לפעילות סייבר איראנית נגד ערב הסעודית: הראשון הוא הערוץ ה"ישיר", ובכלל זאת מתקפות על מתקנים ותשתיות סעודיות, צבאיות ואזרחיות כאחד, מה שעשוי לגרום נזק כלכלי רב ואף מספר גבוה של אבדות בנפש. דוגמה לפוטנציאל ההרסני של התקפה שכזו הומחשה ב-2017, בתקיפת סייבר שכוונה לאחד מהמפעלים הפטרוכימיים בממלכה. התקפה זו, שנכשלה משום שטעות בקוד התקיפה שיבשה את פעולתו, לא כוונה לגנוב מידע או לפגוע בבסיסי נתונים סעודים, אלא ליצור נזק קינטי של ממש ולהביא לפיצוץ באמצעות שיבוש מערכות המפעל.

לצד הערוץ הישיר, קיים גם ערוץ "עקיף" - שימוש בפלטפורמות אינטרנט פופולריות, כגון פייסבוק או טוויטר, גם תוך שימוש בחשבונות פיקטיביים, כדי להביע תמיכה בגורמים המתנגדים למשטר ולקדם תסיסה פנימית בממלכה. יתרונו של אופן פעולה זה בכך שהוא עשוי להתגלות כבעל חתימה נמוכה אף יותר מאשר מתקפות הסייבר הישירות על שום יכולתה של המדינה התוקפת להסתיר את פעילותה ולהציגה כמחאה פנימית אותנטית. כן אין להוציא מכלל אפשרות פעולה משולבת. בתסריט שכזה, פעילות סייבר בחתימה נמוכה תגרום אסון אזרחי רחב היקף, אשר יזעזע את החברה הסעודית. במקביל, פעילות מוגברת של חתרנות קיברנטית תנצל את המצב הפנימי הרגיש כדי לעודד התקוממות אקטיבית נגד בית המלוכה. לאיראן אינטרס לחזק את החשש בסעודיה כי יש בכוחה להניע חתרנות שיעית כנגד בית המלוכה. החשש הזה "סייע" בעבר לעצור צעדים סעודים נגד איראן.

יצוין שניכרת הבנה של בית המלוכה הסעודי את הסיכונים והסיכויים הטמונים בממד הקיברנטי והוא עמל על בניית אסטרטגיה קיברנטית בהתאם. ואולם, גורמים פנימיים מקשים על ההתמודדות. בראש ובראשונה, הפיצול המובנה בממשל הסעודי מחלק את הסמכויות הרלוונטיות בין מוקדי כוח רבים, המשתייכים למשרדים וגופים שונים. מצב זה, מקשה על גיבושה ויישומה של מדיניות סייבר אחידה, שתספק מענה ביטחוני לצרכיה המגוונים של הממלכה.

מכשול מרכזי נוסף הוא ניוונה הטכנולוגי היחסי של החברה הסעודית. בעיה זאת, שאינה ייחודית לסוגיית הסיבר, נוגעת בנקודות חולי עמוקות שמהן סובלת הממלכה. עושר הנפט ייתר במשך עשורים רבים את הצורך בפיתוח מגזרים כלכליים נוספים. יתר על כן, קניית "שקט תעשייתי" אזרחי באמצעות סובסידיות נדיבות, לצד פיזור מנופח של משרות ממשלתיות, לא המריצו את האוכלוסייה לעבודה מאומצת ולרכישת השכלה מתקדמת. כתוצאה מכך, ערב הסעודית חסרה את התשתית האנושית והטכנולוגית הדרושה ליכולות מתקדמות - גם בתחום הסייבר. תעשיית טכנולוגיות המידע תופסות נפח של כ-0.4 אחוזים בלבד מהתמ"ג הסעודי, והממלכה מסתמכת בעיקר על סיוע חיצוני לצרכים אזרחיים הקשורים בממד הקיברנטי.

במטרה להתגבר על קשיים אלו, הממלכה נקטה בשנים האחרונות מספר צעדים שהיטיבו מעט את מצבה בהקשר זה. כיום קיימות בה שלוש זרועות מרכזיות הקשורות לתחום הסייבר ופועלות במקביל. הראשונה היא "הרשות הלאומית להגנת הסייבר" (NCA). גוף זה, אשר הוקם במהלך שנת 2017 כפוף למלך סלמן ולבנו, יורש העצר, מחמד בן-סלמן, והוא אמון על ריכוז המדיניות, ההנחיות והאימון בתחום הגנת הסייבר עבור כלל הגופים הממשלתיים, כמו גם הפרטיים. למעשה, גוף זה הינו האחראי המרכזי על הטכנולוגיה ההגנתית עצמה בממלכה. אליו מתווספת הפדרציה הסעודית לביטחון קיברנטי ותכנות (SAFCAP). גוף זה כפוף לוועד האולימפי הסעודי והוא אחראי בעיקר על הכשרת כוח האדם והתשתית הטכנולוגית הדרושים עבור סקטור הסייבר והתכנות. כחלק מפעולתה השוטפת, הפדרציה מארגנת כנסים ותחרויות שמטרתם להגביר את המודעות לסוגיות ביטחון הסייבר ולעודד את הנוער הסעודי להתמחות בתחום ולהוות עתודה טכנולוגית. על שני גופים אלו נוספת זרוע שלישית, התקפית וחשאית יותר (שנוהלה לפחות עד פרשת רצח העיתונאי ג'מאל חשוקג'י) בידי יד ימינו של יורש העצר, מוחמד אל-קטאני. זרוע זו מעסיקה מאות סעודים המתפקדים כ"צבא טרולים" בערוצי המדיה החברתית ומנטרים מתנגדי משטר, מוחקים תגובות ביקורתיות בנושאים רגישים, ושותלים תגובות אוהדות למדיניות בית המלוכה.

למרות הצעדים שנקט בית המלוכה הסעודי, הממלכה נותרה פגיעה למדי. מחקר שהתפרסם באחרונה קבע כי רק ארבעה מתוך עשרה מנכ"לים סעודים דיווחו שארגונם מוכן להתמודדות מול מתקפות סייבר. זאת, על אף ניסיונות סעודים להוביל תהליכי למידה בתחום (כמו למשל, כנס בינלאומי בנושא הגנה קיברנטית שאירחה הממלכה בפברואר האחרון). ובנוסף, הממלכה טרם פיתחה טכנולוגיות התקפיות של ממש, כאשר גם המעט שברשותה נשען בעיקר על טכנולוגיות זרות.

כפי שעולה מההתפתחויות האחרונות באזור המפרץ, קיימת אפשרות סבירה בהחלט שההסלמה בין ארצות הברית לאיראן תקרין באופן גובר והולך גם על המרחב הקיברנטי. התפתחות שכזאת מסוכנת במיוחד עבור ערב הסעודית, עקב האפשרות שהממלכה תהיה עבור איראן אמצעי לפגיעה באינטרסים האמריקאים באזור. בחינת מצבה הנוכחי של הממלכה בתחום הסייבר מראה כי היא אינה ערוכה לתרחיש שכזה. צעדים רבים אומנם ננקטו בשנים האחרונות, אך הם צפויים לתת פירות רק בטווח הארוך. לכן, למען ביטחונה, על הממלכה למצוא פתרונות לטווח הקצר, למשל רכישה של טכנולוגיות וסיוע מחברות זרות, כדי לצלוח את המשבר עם כמה שפחות נזקים ניכרים. הפגיעות הרבה של מערך הפקה, זיקוק ושינוע הנפט בממלכה וחשיבותו למשק האנרגיה העולמי מחזק את הצורך שארצות הברית ואולי גם ישראל יתרמו מהידע ומהיכולת שלהם לשדרג את מערך המניעה הסעודי.