המרחב הקיברנטי: זירת העימות הסעודית-איראנית הבאה?

רון דויטש ויואל גוז'נסקי

השילוב של הערפול המובנה הגלום במבצעי סייבר נרחבים עם פוטנציאל הנזק הממשי הטמון בהם, הופך מרחב זה לאידיאלי לפעולה עבור ערב הסעודית ואיראן ותואם את ראייתן האסטרטגית ואת תפיסת הפעלת הכוח שלהן. הסיכון והסיכוי שמציב המרחב הקיברנטי בפני כל אחת משתי המדינות הופכים אותו למפתה, במיוחד כשהדבר נוגע להשקעת משאבים לטווח הארוך. נראה, לפיכך, שמרחב הסייבר צפוי להפוך לזירת התנגשות מרכזית עתידית נוספת עבור ערב הסעודית ואיראן, וזאת לאור מגבלות הכוח הקונבנציונלי שמנעו זאת מהן עד כה.

מילות מפתח: ערב הסעודית, איראן, לוחמת סייבר, לוחמה אסימטרית, ישראל, ארצות הברית

מבוא

מזה זמן שערב הסעודית ואיראן מקיימות ביניהן יריבות עזה. על אף ניסיונות שנעשו לאורך השנים להגיע להפשרה ביחסים, או לפחות להבנות אסטרטגיות מסוימות שיפחיתו את המתחים בין השתיים, ערב הסעודית ואיראן לא חדלו לראות האחת באחרת איום מרכזי. למרות זאת, ועל אף הסמיכות הטריטוריאלית בין שתי המדינות, מעולם לא פרץ ביניהן עימות צבאי ישיר בעל משמעות, ולכל היותר היו התנגשויות נקודתיות ובאמצעות כוחות של צד שלישי. סיבה מרכזית למצב זה עשויה להיות אופי הכוחות החמושים של השתיים ותפיסת ההפעלה שלהן.

סיבות היסטוריות, חברתיות וגיאופוליטיות הביאו לכך שהן ערב הסעודית והן איראן אינן מחזיקות ברשותן כוחות יבשה המסוגלים לבצע תמרונים נרחבים

רון דויטש הוא מתמחה במכון למחקרי ביטחון לאומי. ד"ר יואל גוז'נסקי הוא חוקר בכיר במכון למחקרי ביטחון לאומי.

מעבר לגבולותיהן, ובכלל זה לא האחת נגד השנייה. זאת ועוד, כוחות הצבא הסעודיים לוקים בחוסר יעילות משווע על אף תקציבי עתק, בעוד שהאיראנים משמרים תפיסת הפעלה של כוחותיהם הנובעת מרציונל של התנגדות ולוחמה אסימטרית, דבר המתבטא במעמדם ובתפקידם המרכזי של משמרות המהפכה, ובמיוחד של זרוע הטילים.[1]

תפיסת ההפעלה של הכוח הצבאי על ידי ערב הסעודית ואיראן מיתרגמת בתורה לראייה אסטרטגית־מדינית רחבה יותר, השמה דגש על לוחמה תודעתית ועל הפעלת טרור ו"שליחים" מאחורי הקלעים במטרה לערער את יריבותיהן. ייתכן וניתן לראות בתפיסת הפעלה זאת דמיון למושג חדש יחסית שהתגבש (בין אם בצדק ובין אם לאו) בשנים האחרונות – "דוקטרינת גראסימוב", ההולכת ותופסת מקום כגישה פוטנציאלית ללחימה ולמדיניות חוץ בכלל.[2] דוקטרינה זאת מיוחסת לגנרל הרוסי ואלרי גראסימוב ומבוססת על דברים שכתב בשנת 2013, ובהם תיאר מעין "זן חדש" של מלחמות. אלו כוללות, לדבריו, לצד מאמצים צבאיים קונבנציונליים, אפיקי פעולה נוספים, דוגמת שימוש בתקשורת, חתרנות פנימית, סייבר וכל אמצעי אחר המסוגל לזרוע כאוס בשורות האויב.[3]

גישה זו עשויה לקבל זווית מעניינת במיוחד כאשר היא נבחנת לאור התפתחות הלוחמה בסייבר. השילוב של הערפול המובנה עם פוטנציאל הנזק הממשי הגלום במבצעי סייבר נרחבים הופך מרחב זה לאידיאלי עבור תפיסת הפעלת הכוח של ערב הסעודית ואיראן.

מאמר זה מבקש לבחון באיזו מידה, אם בכלל, עשוי מרחב הסייבר להפוך לזירת ההתנגשות מרכזית בין ערב הסעודית ובין איראן. לצורך כך, המאמר משווה בין יכולות הסייבר של כל אחת משתי המדינות, הן ברמה ההגנתית והן ברמה ההתקפית, ומנסה להגיע למסקנה האם מרחב הסייבר עשוי להקנות לאחת מהן את היכולת להשיג את מה שנבצר ממנה לעשות באמצעים צבאיים קונבנציונליים.

הסייבר בערב הסעודית

תחום הסייבר לא זכה לתשומת לב ולא קיבל חשיבות רבה בערב הסעודית עד לשנים האחרונות. עם זאת, פגיעותה של הממלכה לאיומי סייבר העלולים להסב לה נזקים רבים הולכת וגוברת. מדובר בנזקים העשויים לבוא לידי ביטוי באמצעות שני ערוצים מרכזיים: הראשון, הערוץ ה"ישיר", כולל מתקפות אפשריות

1 עוזי רובין, **טילים כנושאי הדגל של חזון המשטר האיראני**, מכון ירושלים למחקרים אסטרטגים, 23 בנובמבר 2018.

2 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine'", *Foreign Policy*, March 5, 2018.

3 Molly K. McKew, "The Gerasimov Doctrine", *Politico Magazine*, September/October 2017.

על תשתיות ומתקנים סעודיים, צבאיים ואזרחים כאחד, מה שעשוי לגרום לנזק כלכלי רב ואף למספר גבוה של אבדות בנפש. דוגמה בולטת לפוטנציאל ההרסני של התקפה מסוג זה ניתן היה לראות ב־2017, בהתקפת סייבר שכוונה לאחד המפעלים הפטרוכימיים בממלכה.[4] מטרת ההתקפה לא הייתה גניבת מידע או פגיעה בבסיסי נתונים סעודיים, אלא גרימת נזק פיזי של ממש ופיצוץ שישבש את מערכות המפעל. המבצע כשל בשל טעות בקוד התקיפה, ששיבש את פעולתו. חוקרים סבורים כי מי שעמדה מאחורי התקיפה הייתה איראן, שתיקנה מאז את הטעות שהכשילה אותה, וכי מדובר עתה רק בשאלה של זמן עד שהיא תפעל שוב נגד ערב הסעודית, הפעם בעוצמה ובתחכום רבים יותר.[5]

מעֵבר להתמקדות באיום על תשתיות קריטיות ועל מערכות בקרה במטרה לשבש את שרשרת האספקה ואף לפגוע בה פיזית, ניתן לזהות כיום איום הולך וגובר גם על מערכות מידע ארגוניות סעודיות, שמטרתו היא לשבש אותן ולרגל אחריהן. בשלהי 2016 הותקפו מספר יעדים ממשלתיים בערב הסעודית, בהם גם מערכות המחשב של הבנק המרכזי הסעודי, על ידי התוכנה הזדונית "שאמון". בווירוס זה נעשה שימוש כבר ב־2012, במתקפת הסייבר הרחבה נגד חברת הנפט הלאומית הסעודית, אראמק"ו. דוגמאות אלו הן חלק בלבד ממסכת תקיפות רחבה בהרבה, עליה רמז בכיר במגזר הסייבר הסעודי, שהעריך כי ב־2015 לבדה ספגה הממלכה כשישים מיליון תקיפות סייבר, בקצב של כ־164,000 תקיפות ליום.[6]

לצד ערוץ התקיפה הישיר בסייבר, קיים גם ערוץ "עקיף", שעשוי לבוא לידי ביטוי בשימוש בפלטפורמות אינטרנט פופולריות, כגון "פייסבוק" או "טוויטר", כתמיכה בגורמים המתנגדים למשטר בערב הסעודית וכדי לגרום לתסיסה פנימית בממלכה. היתרון שבאופן פעולה זה גלום בכך שהוא עשוי להיות בעל חתימה נמוכה עוד יותר מאשר מתקפות הסייבר הישירות, בשל יכולתה של המדינה התוקפת להסוות את פעילותה כמחאה פנימית אותנטית, בין היתר באמצעות שימוש בחשבונות פיקטיביים. אין גם להוציא מכלל אפשרות תסריט של פעולה משולבת: פעילות סייבר בחתימה נמוכה, שתגרום לאסון אזרחי רחב היקף שיזעזע את החברה הסעודית, ובמקביל, פעילות מוגברת של חתרנות קיברנטית, שתנצל את המצב הפנימי הרגיש כדי לעודד התקוממות אקטיבית נגד בית המלוכה.

בית המלוכה הסעודי מתחיל להבין את הפוטנציאל ההרסני של הממד הקיברנטי ומנסה לפעול כדי להתמודד איתו. יחד עם זאת, קיימים מספר גורמים פנימיים

4 Nicole Perlroth and Clifford Krauss, "A Cyber-attack in Saudi Arabia Failed to Cause Carnage, but the Next Attempt could be Deadly", *The Independent*, March 21, 2018.

5 Ibid.

6 Ibrahim al-Hussein, "60 Million Cyber-attacks Targeted Saudi Arabia in One Year", *Al Arabia*, May 2, 2018.

המהווים מכשלה בפני השגת מטרה זאת. בראש ובראשונה ניתן למנות את הפיצול המובנה בממשל הסעודי, שבמסגרתו מחולקות הסמכויות לטיפול באסטרטגיה הקיברנטית בין מוקדי כוח רבים המשתייכים למשרדים ולגופים שונים. מצב זה מקשה על גיבושה ויישומה של דוקטרינת סייבר אחידה, באופן שייתן מענה לצורכי הביטחון המגוונים של הממלכה.[7]

מכשול מרכזי נוסף ביכולתה של ערב הסעודית להתמודד עם איומי סייבר קשור לפיגור הטכנולוגי היחסי של החברה הסעודית. בעיה זאת אינה חדשה ואינה ייחודית לסוגיית הסייבר, אלא נוגעת בנקודות חולי עמוקות בהרבה מהן סובלת הממלכה. עושר הנפט של ערב הסעודית יִתר במשך עשורים רבים את הצורך בפיתוח מגזרים כלכליים נוספים. כמו כן, קניית "שקט תעשייתי" אצל התושבים באמצעות סובסידיות נדיבות וריבוי מיותר של משרות ממשלתיות, מנעה, במידה רבה, מהאוכלוסייה את התמריצים לעבודה קשה ולרכישת השכלה מתקדמת. כתוצאה מכך, ערב הסעודית חסֵרה את התשתית האנושית והטכנולוגית כדי להגיע ליכולות הדרושות לה בתחום הסייבר, בכלל זה לצרכים אזרחיים, ונאלצת להסתמך בעיקר על סיוע חיצוני (תעשיית טכנולוגיות המידע תופסות נפח של כ־0.4 אחוזים בלבד מהתמ"ג הסעודי).[8]

במטרה להתגבר על קשיים אלה נקטה ערב הסעודית בשנים האחרונות מספר צעדים, שבעקבותיהם הוטב מעט מצבה. כיום ניתן למנות שלוש זרועות מרכזיות בממלכה הקשורות לתחום הסייבר ופועלות במקביל האחת לרעותה: הזרוע הראשונה היא "הרשות הלאומית להגנת הסייבר" (NCA). גוף זה, אשר הוקם ב־2017 בצו מלכותי וכפוף למלך וליורש העצר, אמון על ריכוז המדיניות, ההנחיות וההכשרה בתחום הגנת הסייבר עבור כלל הגופים הממשלתיים, כמו גם הפרטיים.[9] זהו למעשה הגוף המרכזי האחראי על הטכנולוגיה ההגנתית בממלכה; הגוף השני הוא "הפדרציה הסעודית להגנה קיברנטית ולתכנות" (SAFCAP). גוף זה כפוף לוועד האולימפי הסעודי ואחראי בעיקר על הכשרת כוח האדם והתשתית הטכנולוגית עבור מגזר הסייבר והתכנות בערב הסעודית. חלק מפעולתה השוטפת של הפדרציה הוא לארגן כנסים ותחרויות, שמטרתם היא להגביר את המודעות לסוגיות ביטחון הסייבר ולעודד את הנוער הסעודי להתמחות בתחום זה ולהוות

7 Melissa Hathaway, Francesca Spidalieri and Fahad Alsowailm, *Kingdom of Saudi Arabia Cyber Readiness at a Glance* (Potomac Institute for Policy Studies, 2017), pp. 23-24.

8 Ibid., p. 3.

9 "Follow Basic Cyber Security Standards, Govt Agencies Told", *Saudi Gazette*, October 7, 2018.

עתודה טכנולוגית פוטנציאלית.[10] לשני גופים גלויים אלה ניתן להוסיף זרוע שלישית, התקפית וחשאית יותר באופייה, שנוהלה על פי הדיווחים, לפחות עד לאחרונה, בידי מוחמד אל־קטאני, שהיה יד ימינו של יורש העצר מחמד בן סלמן. זרוע זאת, "המרכז ללימודים ולתקשורת" (CSMA) בריאד מעסיק מאות סעודים המתַפקדים כ"צבא טרולים" בערוצי המדיה החברתית, ותפקידם הוא לנטר מתנגדי משטר, למחוק תגובות ביקורתיות בנושאים רגישים ולשתול תגובות אוהדות למדיניות בית המלוכה.[11] על אף שרבות מפעילויות הסיכול של המרכז נותרו מחוץ לאור הזרקורים במערב, רצח העיתונאי ג'מאל חשוקג'י העלה לקדמת הבמה את אל קטאני ומלחמת המידע המתבצעת תחת ניהולו, מלחמה אשר במסגרתה היה חשוקג'י איום משמעותי.[12]

למרות ההתפתחויות האחרונות בערב הסעודית בתחום הסייבר, יש לקחת בחשבון שיידרש עוד זמן רב עד שניתן יהיה לגשר באופן מלא על הפערים המשמעותיים הקיימים בתחום זה בממלכה. בטווח הזמן הקצר־בינוני, עד שהתהליכים הנזכרים לעיל יצברו תאוצה, ערב הסעודית עשויה לפצות על הפערים בתחום הידע והתשתית הטכנולוגית ברכש של ידע ממדינות זרות. בכל האמור לרכש צבאי, ערב הסעודית היא הלקוחה הגדולה ביותר של ארצות הברית, ומתקיים שיתוף פעולה פורה בין שתי המדינות גם בתחום הסייבר. במסגרת ההסכמים שחתם נשיא ארצות הברית, דונלד טראמפ, בביקורו בממלכה במאי 2017 היו גם הסכמים בתחום ההגנה בסייבר, שנועדו לכסות על הפערים הקיימים אצל הסעודים בתחום זה. כן דווח כי חברות קבלן מטעם הממשל האמריקאי עוסקות במתן ייעוץ והדרכה לערב הסעודית בתחום ההגנה בסייבר וגם פועלות ישירות במשרדי הממשלה הסעודיים כדי להגן עליהם מפני התקפות סייבר. אחת מחברות אלו, Booz Allen Hamilton, אף מצאה לנכון להדגיש כי המעורבות שלה בתחום הסייבר בערב הסעודית אינה כוללת בניית יכולות התקפיות.[13]

הפערים הסעודיים בתחום הסייבר עשויים לשמש גורם משפיע גם על יחסיה של הממלכה עם ישראל, שכמעצמת סייבר, יש לה הרבה מה להציע לערב הסעודית בתחום זה. על פי דיווחים שונים, ייתכן שקשרים כאלה כבר מתקיימים, או לפחות התקיימו בעבר. במסגרת זו דווח כי גורמי ממשל הקשורים לערב הסעודית השתמשו

10 האתר הרשמי של "הפדרציה הסעודית להגנה קיברנטית ותכנות", https://safcsp.org.sa/en

11 Adam Goldman and Karam Shoumali, "Saudis' Image Makers: A Troll Army and a Twitter Insider", *The New York Times*, October 20, 2018.

12 Ignatius, david "how a Chilling Saudi Cyberwar Ensnared Jamal Khashoggi" *The Washington Post* 07.12.2018

13 Michael Forsythe, Mark Mazzetti, Ben Hubbard and Walt Bogdanich, "Consultants Stick with the Saudis", *The New York Times*, November 8, 2018.

בתוכנת ריגול ("פגאסוס") של חברת NSO הישראלית בניסיון לצותת למתנגדי המשטר.[14]

אפיק אפשרי נוסף עבור ערב הסעודית הוא יצירת תשתית הגנה משותפת בסייבר למדינות המפרץ המאוגדות ב"מועצה לשיתוף פעולה במפרץ" (GCC), או לחלקן, המתמודדות עם איומים דומים. קריאות לשיתופי פעולה כאלה כבר נשמעות, אלא שהדרך עודנה ארוכה עד שהן יעברו לפסים מעשיים אפקטיביים, לאור המתחים המשמעותיים הקיימים בין חלק מאותן המדינות.[15]

יכולות הסייבר של איראן

בניגוד לערב הסעודית, איראן מחזיקה בתשתית מבוססת יחסית של יכולות סייבר, הן הגנתיות והן התקפיות. בין יעדי ההתקפה העיקריים של איראן בשנים האחרונות נמצאות ערב הסעודית, ישראל וארצות הברית.[16] פעילות הסייבר האיראנית מפוקחת על ידי הדרגים הגבוהים ביותר במשטר, ובהם הנשיא ומפקד משמרות המהפכה, ואת יכולות הסייבר שלה מתַחזקת איראן באמצעות מספר דרכים: ראשית, המשטר האיראני משקיע כספים במחקר ובהכשרה של כוח אדם בתחום הסייבר, מתוך תפיסה אסטרטגית של חשיבותו הרבה;[17] שנית, החתימה על הסכם הגרעין עם המעצמות בשנת 2015 פתחה בפני איראן הזדמנויות לשיתופי פעולה רבים עם אוניברסיטאות ומוסדות מדעיים מסביב לעולם. אפשרות זו נוצלה על ידיה כדי לקדם גם את תחום הסייבר שלה, וזאת באמצעות שיתוף פעולה מדעי עם אוניברסיטאות שברשותן ידע בנושא זה;[18] שלישית, הניצול האיראני של ידע זר בתחום הסייבר אינו מוגבל רק לשיתופי פעולה רשמיים. בשנת 2013 נוסד מוסד ה"מבנא" (Mabna) האיראני, שמטרתו היא השגת גישה למשאבים מדעיים מחוץ לאיראן.[19] אמנם, מטרה זו אינה ממוקדת בהכרח בתחום הסייבר, אולם מדובר באפיק אפשרי נוסף בעל פוטנציאל לתרום לגיבוש יכולות הסייבר האיראניות.

14 "Israeli Hacking Firm NSO Group Offered Saudis Cellphone Spy Tools – Report", *Times of Israel*, November 25, 2018.

15 Ramola Talwar Badam, "GCC Urged to Coordinate Cyber Security following Wannacry Attack", *The National*, May 21, 2017.

16 Collin Anderson, Karim Sadjadpour, *Iran's Cyber Threat, Espionage, Sabotage and Revenge* (Carnegie Endowment for International Peace, 2018), https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

17 גבי סיבוני וסמי קרוננפלד, "התפתחויות בלוחמת הסייבר של איראן 2013־2014", **צבא ואסטרטגיה**, כרך 6, גיליון 2, אוגוסט 2014, עמ' 84.

18 Levi Gundert, Sanil Chohan and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations", *Recorded Future*, May 9, 2018.

19 על פי נתוני ה־FBI, בין קורבנות פעילות ה"מבנא" ניתן למצוא 3,768 פרופסורים ב־144 אוניברסיטאות בארצות הברית לבדה, ו־4,230 פרופסורים הפזורים על פני 176 אוניברסיטאות

אירן חשה היטב בעבר את הסכנות הטמונות במרחב הקיברנטי. הדוגמה המובהקת ביותר לכך היא הנוזקה "סטקסנט", אשר פגעה בתשתיות גרעין אירניות ב־2012. אולם עוד קודם לכן התנסתה אירן בסכנה קיברנטית מסוג אחר: המחאה הנרחבת ברחובות טהראן ב־2009 המחישה את הפוטנציאל ההרסני הטמון בקבוצות אופוזיציה פנימיות ובזליגה של רעיונות חתרניים מבחוץ. בתקופה זאת פתח המשטר האירני בפרויקט של בידול רשתות, שמטרתו הייתה העברת כלל התקשורת האירנית לרשת פנים מדינתית המנותקת מהזירה הבין־לאומית, כך שבידי המשטר תהיה השליטה המלאה על התכנים הנכנסים למדינה, כמו גם הגנה טובה יותר מפני מתקפות סייבר.[20] יעד זה מגובה על ידי פעילות אכיפה אגרסיבית של אנשי "משטרת הסייבר" האירנית כלפי גורמים חתרניים הפעילים ברשת.[21]

מלבד זאת, אירן משקיע מאמצים רבים בפיתוח ובהטמעה של יכולות הגנה קיברנטיות, כמו גם בתרגול של תפיסות הפעלה. דוגמאות לכך ניתן לראות בתרגילים שנערכו בשנים 2012 ו־2013 ובדקו את מערכי ההגנה הקיברנטית האירניים בזרועות הים והיבשה (בהתאמה) של משמרות המהפכה.[22] לאחרונה דווח באירן על חשיפה של גרסה מתקדמת יותר של תולעת "סטקסנט", אולם נטען כי היא טרם הספיקה לגרום לנזק כלשהו. בהמשך לכך העריך ראש מערך הסייבר האירני, גנרל ג'ולאם רזא ג'לאלי, שאירן אינה נמצאת עוד תחת איום סייבר משמעותי, ועל כן היא מורידה את הנושא אל תחתית סדר העדיפויות. דיווח זה עשוי להוות אינדיקציה לשיפור ניכר ביכולות הסייבר האירניות בשנים האחרונות, אם כי אין לשלול את האפשרות שמדובר במהלך הונאה תודעתי ותו לא.[23]

לצד פיתוח יכולות הגנתיות מתקדמות, עברה אירן כברת דרך מרשימה בפיתוח יכולות התקפיות בסייבר. אין ספק שאירן נמצאת במקום מתקדם יותר מאשר ערב הסעודית בכל הנוגע ליכולות כאלו, אם כי נראה שהיא עדיין מפגרת מאחורי מעצמות הסייבר הגדולות דוגמת סין, רוסיה, ארצות הברית וישראל. מערך הסייבר ההתקפי האירני מצוי בעיקר תחת אחריות משמרות המהפכה ומשתייך לתת־גוף המכונה "צבא הסייבר האירני" (ICA). מערך זה סובל מחולשה מובנית בשל אופיו הקבלני למחצה: רובם של מבצעי הסייבר ההתקפיים של אירן אינם

---

21 מ־21 מדינות שונות, ובהן ישראל, גרמניה, סין, דרום קוריאה, בריטניה וטורקיה: Lior Tabansky, "Iran's Cybered Warfare Meets Western Cyber-Insecurity" in: *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, ed. Fabio Rugge (Italia: ISPI, 2018), p. 130.

20 סיבוני וקרוננפלד, "התפתחויות ביכולות הסייבר של אירן", עמ' 85.

21 שם, עמ' 88.

22 שם, עמ' 87.

23 **אירן מאשימה חברה ישראלית במתקפת סייבר**, המרכז הירושלמי לענייני ציבור ומדינה, 5 בנובמבר 2018.

מבוצעים על ידי אנשי משמרות המהפכה עצמם, אלא על ידי יחידים וקבוצות האקרים עצמאיות למחצה, המקבלות שכר בהתאם למידת הצלחתם. היעדר מחויבות אידיאולוגית והחיפוש אחר רווחים כספיים הופכים חלק גדול מההאקרים האיראנים למועמדים בעייתיים מבחינת משמרות המהפכה. על כן, המשטר נוקט גישה רב־רובדית: בדרג הביניים מוצבים קצינים בעלי מחויבות אידיאולוגית למשטר, והם קובעים את היעדים הדרושים ומטילים משימות שונות על קבלני משנה אד־הוק, קרי קבוצות של האקרים אזרחיים המקבלים שכר לפי משימה.[24] יש להוסיף לכך כוחות של "שליחים" קיברנטיים, הפועלים בהקשר אידיאולוגי יותר. דוגמה מובהקת ל"שליח" כזה היא ארגון חיזבאללה הלבנוני, שקשריו עם הרפובליקה האסלאמית של איראן מקנים לו יכולות סייבר מתקדמות יחסית בהשוואה לארגוני טרור אחרים.[25] יכולות אלו מופעלות בשעת הצורך ומהוות זרוע קיברנטית התקפית נוספת עבור המשטר האיראני.

בנוסף לכך, מפעיל המשטר האיראני יכולות התקפיות "רכות", קרי לוחמה פסיכולוגית המתנהלת באמצעות מניפולציות מידע ברשתות החברתיות ובאתרי החדשות, בדומה לנעשה על ידי ערב הסעודית. דוגמה מובהקת ליכולת איראנית כזו, שנחשפה לאחרונה, היא מה שזכה לביטוי "אייתוללה BBC" – מבצע נרחב שבוצע מטעם המשטר האיראני ובו זויפו אתרי חדשות מכל רחבי העולם, ובראשם אתר ה־BBC בשפה הפרסית. האתרים המזויפים הכילו תוכן מניפולטיבי ומכוון, בהתאם לצורכי הלוחמה הפסיכולוגית האיראניים.[26]

סיכום ומסקנות

מאמר זה ביקש לבחון את ההיתכנות להתפתחותו של מרחב הסייבר לזירת עימות עתידית רחבה בין ערב הסעודית ובין איראן. למעשה, כבר היום מתקיימות התנגשויות בין השתיים בתוך המרחב הקיברנטי, אם כי היא לא הפכה עדיין לזירת החיכוך המרכזית ביניהן. על כן, כשדנים בעימות סעודי־איראני במרחב הסייבר, יש להבחין בין הטווח הקצר והבינוני ובין הטווח הארוך. כפי שעולה מניסיונן של שתי המדינות, שתיהן סובלות מנקודות תורפה קיברנטיות, שיש בהן פוטנציאל להסב נזק אסטרטגי משמעותי ביותר. נקודות תורפה אלו עלולות להתגלות כנקודות הבקעה שימוטטו את המשטר כולו, אם אחת מהשתיים תצליח להכות

24 Gundert, Chohan, Lesnewich "Iran's Hacker Hierarchy Exposed: How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations", p. 5.

25 Ben Schefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism", *Georgetown Security Studies Review*, March 11, 2018.

26 "Ayatollah BBC – An Iranian Disinformation Operation against Western Media Outlets", *Clearsky Cyber Security*, 2018.

בהן מספיק חזק. מכיוון שכך, הסיכון והסיכוי שמציב המרחב הקיברנטי בפני ערב הסעודית ואיראן כאחת הופך אותו למפתה, במיוחד כשמדובר בהשקעת משאבים לטווח הארוך.

לפי שעה, נראה כי היכולות הקיברנטיות הן של ערב הסעודית והן של איראן הן דלות מכדי להכיל עימות בקנה מידה מלא ביניהן. יכולות אלו ממלאות תפקיד תומך חשוב, אך עדיין לא מפותח דיו כדי לתת מענה לתפיסת הביטחון של השתיים. ר׳יה לכך הם האמצעים ההתקפיים הפשוטים יחסית המשמשים את ערב הסעודית ואיראן במרחב הקיברנטי. אלה כוללים בעיקר הפצת מידע כוזב ("פייק ניוז") וחתרנות דרך הרשתות החברתיות. לא ערב הסעודית ולא איראן מחזיקות ברשותן תשתיות סייבר התקפיות רחבות היקף: לראשונה אין עדיין, ככל הידוע, יכולת טכנולוגית עצמאית לכך, בעוד שבאיראן היא אמנם קיימת, אך נראה שהיא מבוססת בעיקר על "שכירי חרב" מזדמנים למחצה.

השאלה המעניינת יותר שצריכה להישאל נוגעת למגמות ארוכות הטווח. כפי שצוין לעיל, מקבלי ההחלטות בערב הסעודית ובאיראן מודעים היטב לפוטנציאל הנזק והתועלת שמגלם בתוכו המרחב הקיברנטי ונוקטים צעדים למיצוב שתי המדינות כשחקניות בעלות יכולת בתחום זה בטווח הארוך. לכך מצטרף שיווי המשקל האסטרטגי שמקיימות השתיים ביניהן: לא לערב הסעודית ולא לאיראן יש היכולות למוטט את הצד השני באמצעות מערכה צבאית קונבנציונלית. מכיוון שכך, הפנייה לאפיק הסייבר, על האפשרויות הגלומות בו, מהווה צעד מתבקש. במובן זה, אין לשלול את האפשרות שאנו חוזים בניצניו של מרוץ טכנולוגי סעודי־איראני (כמובן, בנוסף לשלל האיומים הקיברנטיים המעסיקים כל אחת משתי המדינות בנפרד).

קשה לחזות את תוצאותיו של מרוץ כזה: מחד גיסא, על אף שניתן להתווכח על מעמדה של איראן כמעצמת סייבר מן השורה, אין ספק שהיא נמצאת כיום בעמדת יתרון ביחס לערב הסעודית בתחום זה. לאיראן יש תשתיות הגנה מפותחות יחסית וניסיון רב ערך שנקנה בשנים של התמודדות עם מתקפות ישראליות ואמריקאיות. כמו כן, בניגוד לערב הסעודית, שנעדרת יכולות התקפיות "קשות" של ממש, לאיראן יש יכולות מוכחות של תקיפת יעדים סעודיים ומערביים (ואמריקאיים בפרט) דרך הרשת, גם אם נראה שהיא אינה יכולה לבצע מתקפה שיטתית ורחבה בדומה לישראל, לרוסיה ולארצות הברית. לבסוף, ומעל הכול, בעוד שערב הסעודית נעדרת תשתית טכנולוגית ואנושית בתחום הסייבר (ולכל היותר, תשתית כזאת נמצאת בה בחיתוליה), איראן השקיעה מאמצים רבים בהכשרת כוח אדם באוניברסיטאות השונות, כמו גם בשיתופי פעולה עם מוסדות זרים, ואף בגניבת ידע. כל אלה מציבים את איראן כמה צעדים לפני ערב הסעודית ועלולים להפוך עם הזמן לפער קטלני עבור הממלכה.

מאידך גיסא, ישנם שני גורמים משמעותיים העשויים לשחק לטובתה של ערב הסעודית במרוץ הטכנולוגי לטווח הארוך ולבלום את ההתקדמות האיראנית: הראשון שבהם הוא משאביה העדיפים של הממלכה. כוחות הביטחון הסעודיים נהנים מתקציבים שנתיים מן הגבוהים בעולם. אם הם יתועלו נכונה ותוגבר ההשקעה החכמה במרחב הקיברנטי (לצד השקעות בחינוך הטכנולוגי המקדים), תוכל ערב הסעודית להאיץ את תהליכי ההתקדמות הטכנולוגיים שלה. לעומת זאת, איראן, הכורעת תחת נטל הסנקציות הבין־לאומיות, מתקשה להקצות משאבים דומים לפיתוח ולרכישת יכולות חדשות.

גורם משמעותי שני היא מטריית ההגנה ושיתופי הפעולה המתקיימים בין ערב הסעודית ובין מעצמת הסייבר הגדולה בעולם – ארצות הברית. כבעלת ברית מרכזית, ארצות הברית עשויה לספק לערב הסעודית מטריית הגנה קיברנטית ויכולות טכנולוגיות, שיאפשרו לה להדביק את הפער מול האיראנים. לכך מצטרף מה שנראה כשיתופי פעולה חשאיים אך תדירים עם ישראל, שהיא, כאמור, מעצמת סייבר בפני עצמה. משקלם היחסי של יתרונות אלה יגבר ככל שיחלוף הזמן. אם הם ינוצלו בחוכמה על ידי הממלכה, הם עשויים להתגלות כנכס של ממש, שייצור לה יתרון על פני איראן.

בחינה של יכולות הסייבר הנוכחיות בערב הסעודית ובאיראן מראה כי עימות קיברנטי רחב היקף בין השתיים לא צפוי כנראה בטווח המיידי. עם זאת, אופיו של המרחב הקיברנטי והעמימות המובנית הקיימת בו, הופכים אותו למתאים במיוחד לתפיסת הפעלת הכוח של שתי המדינות. על כן, יש לצפות, בטווח הבינוני והארוך, לשימוש גובר של שתיהן במרחב זה, כנתיב וכדרך פעולה נוספת לפגיעה ביריב, וזאת בניגוד למגבלות הכוח הקונבנציונלי שמנעו זאת מהן עד כה.