מטהרן למחשב שלכם: כך הפכה איראן את הסייבר לכלי מלחמה

written by אלי קלוטשטיין | 26.08.2026
פורסם במקור ראשון, בתאריך 26 באוגוסט, 2026.

מומחי הסייבר האיראנים שהצליחו ביולי להשבית תחנת כוח בבריטניה למשך ארבעה ימים, לפי פרסום במדינה השבוע, העלו שוב לכותרות את הממד החשאי של המאבק בין הרפובליקה האסלאמית למערב, שמתנהל בשדה קרב דיגיטלי, עמוק בתוך הרשת הווירטואלית.

באותה עת ממש, לפי החשד, פתחו פצחנים בשירות טהרן במתקפת סייבר נרחבת על מערכות מים בארה"ב, בין היתר במינסוטה ובמישיגן. בניו-יורק טיימס דווח כי לפחות שבע מדינות היו על הכוונת האיראנית בתקרית הזאת, שאומנם לא נגרם בה נזק לאספקת המים, אך ככל הנראה ניזוקו בעקבותיה מחשבים המפקחים על איכות המים ועל רמות הכימיקלים השונים שנמצאים בהם. יש לציין שאומנם לוקח זמן רב לאתר במדויק את התוקפים ולהצביע עליהם, ולעיתים גם מנסים התוקפים להזדהות כגורמים אחרים כדי לפגוע ביחסים בין מדינות יריבות, אך החשד המיידי בהחלט נפל על טהרן.

לא הייתה זו הפעם הראשונה שההאקרים ששולח משטר האייתוללות מנסים לפגוע במאגרי מי השתייה. לפני שש שנים, ב-2020, פורסם כי ישראל הצליחה לסכל מתקפת סייבר על מתקני מים בארץ, ובעיקר עצרה את הניסיון להעלות את כמות הכלור שמצוי במים לרמה מסוכנת. הגורמים המוסמכים בישראל הזהירו כי הצלחה של מתקפה כזו יכולה להוות גם סיכון לחיי אדם, ובנוסף לעכב הזרמת מים בצינורות.

מתקפות הסייבר בתקופה האחרונה הן עדות אחת מני רבות לכך שלא חלו תמורות משמעותיות בהיגיון שמדריך את טהרן ובאופן הפעולה שלה במהלך השנים. עם זאת, מאז שעבר הסכסוך בין ישראל וארה"ב לאיראן למישור הגלוי ולעימות צבאי ישיר מסתמנת מגמה של החרפה, שכלול והתרבות של השימוש בסייבר לקידום היעדים האיראניים, באופן שמדאיג עד מאוד גורמים רבים במערב.

בשבוע האחרון, לדוגמה, הזהירו כמה רשויות ממשל בארה"ב כי מתנהל ניסיון איראני לפרוץ למערכות מחשוב מתוצרת חברת "סימנס", שמשמשות לפיקוח על מתקני מים ותשתיות חיוניות אחרות. המערכות הללו רווחות במגזרי תעשייה רבים, כולל אנרגיה, מים, ביוב, מעבדות כימיות, מפעלי מזון וחקלאות ועוד. ההתרעה, שפורסמה במשותף על ידי גורמים כמו הבולשת הפדרלית, מחלקת האנרגיה, המחלקה לביטחון המולדת ועוד כמה גופים ממשלתיים בכירים, גורסת כי המתקפות עשויות לאתר נקודות חולשה במערכות של "סימנס", וכך להוביל לשיבוש של הליכים קריטיים, תקריות אבטחה ובטיחות, נזק לציוד והשבתה של מחשבים, גניבת מידע והשפעה

ארוכת טווח.

בנוסף, מחלקת המשפטים האמריקנית הגישה לאחרונה כתב אישום נגד 17 מומחי מחשבים איראנים שפעלו במשך שנים רבות בשליחות משמרות המהפכה. לפי כתב האישום, הפצחנים תקפו אוניברסיטאות בארה"ב ומחוצה לה, מערכות ממשל אמריקניות וארגונים פרטיים, פרצו לאלפי חשבונות חברתיים, דוא"ל ומחשבים, ומשכו מהם עשרות טרה-בייט של מידע, מסמכים ועוד.

בין היתר הצליחו מומחי הסייבר לגנוב מחקרים, מאמרים וקניין רוחני, השתמשו בחלקם וניצלו אותם לטובת ההתקדמות המדעית של איראן, ואחרים נמכרו למרבה במחיר באמצעות האינטרנט. בנוסף גם הציעו ההאקרים למכירה גישה לחשבונות של אנשי הסגל ולספריות האקדמיות שלהם.

הפרשה הזאת, שתחילתה בשנת 2013, מראה כי איראן ותומכיה אינם ממקדים את פעילותם רק בפגיעה פיזית או קיברנטית באויב, וכי הם מגוונים את המתקפות שלהם לטובת צרכים שונים אחרים.

אין חוקים למלחמת סייבר

על מתקפות הסייבר האיראניות הראשונות נגד מטרות אמריקניות אפשר להצביע כבר בתחילת העשור שעבר. מחלקת המשפטים הגישה כתבי אישום אז נגד חברות הקשורות לממשל בטהרן, שנחשדו כי השביתו עשרות מערכות כלכליות ובנקאות בארה"ב החל משנת 2011. המתקפות נטרלו את אתרי האינטרנט של אותם בנקים, ועלות הנזק הגיעה בסך הכול לעשרות מיליוני דולרים. באותה עת גם הצליח פצחן אחד בשירות איראן להיכנס למערכות הבקרה על סכר באזור ניו-יורק, אף שמערכות השליטה שלו היו מנותקות, והוא לא הצליח לגרום נזק.

בשנת 2014 הותקפה חברת הקזינו "לאס-וגאס סנדס" שבראשות איל ההון היהודי-אמריקני שלדון אדלסון (גילוי נאות: אדלסון היה בעלי קבוצת ישראל היום ומקור ראשון עד מותו, והיא עודנה בשליטת משפחתו), ונגרם לה נזק ניכר. דיסקים קשיחים שלמים נמחקו, הרשת הארגונית שלה נפגעה, אתרי האינטרנט של המלונות בבעלותה הושבתו, ומידע אישי על לקוחות רבים נגנב.

בשנים הבאות הרבה גורמי ממשל עמדו על הכוונת האיראנית, כולל מחלקות המדינה והאוצר, חברות ביטחוניות בארה"ב, וגם ארגונים רבים. בין היתר השתמשו האיראנים גם במתקפות כופרה וסחיטה רבות, וכך הצליחו לגרוף מיליונים רבים של דולרים לכיסם.

בסוף העשור הקודם הגיע השיא עד אותה עת במתקפות הסייבר מטהרן, כשנפרץ חשבון הדוא"ל של היועץ לביטחון לאומי לשעבר של ארה"ב, ג'ון בולטון. במקביל נעשה ניסיון להתערב בבחירות לנשיאות ארה"ב, במהלכים שונים שמטרתם הייתה להשפיע על דעת הקהל בארה"ב ולכוון אותו נגד הנשיא דונלד טראמפ, שהתמודד על כהונה נוספת.

בדומה ללוחמה פסיכולוגית, שימוש בלחץ דיפלומטי ואפילו חסימת מצרי הורמוז, האפשרויות השונות שהציעו מתקפות סייבר שימשו את איראן עוד הרבה לפני המלחמה כאמצעי נוסף שיסייע לה למנף את המערכה הא-סימטרית שהיא מנהלת נגד האמריקנים כדי להביא אותה לעמדת יתרון גם במציאות העולמית. אלא שבחודשים האחרונים, ודווקא על רקע התבוסות שספגה הרפובליקה האסלאמית בשדה הקרב, נראה כי המתקפות הללו מתעצמות, תופסות אופי מתואם ומתוכנן יותר, והופכות לכלי מרכזי שמשמש את האיראנים כדי לפצות על חסרונות אחרים.

יתרה מכך, בעולם שבו הסייבר הוא כלי מלחמתי חדש יחסית, טרם התגבשו עד הסוף תפיסות, עקרונות פעולה ונורמות הקשורות לשימוש בו ולתגובה שיש לנקוט אחרי שנגרם נזק ממנו. כך למשל, כיצד תגיב ישראל על שימוש באמצעים קיברנטיים כדי להשבית תשתיות אזרחיות בארץ, ללא נפגעים ורק נזק כלכלי? וכיצד ניתן בקלות להפנות את האצבע המאשימה כלפי איראן, ובאיזה מחיר? מה התשובה הראויה למתקפה שאכן גובה נזק ממשי בעולם האמיתי, שאפילו מביא להרוגים ונפגעים? העמימות בתחום הזה, בשלב הנוכחי, משחקת היטב לידי האיראנים.

מומחים מסבירים כי האסטרטגיה הזאת משתלבת היטב בתפיסת העולם המלחמתית של איראן בחודשים האחרונים, הכוללת ניסיון להרתיע את האויב במנותק מכוחה האמיתי של טהרן, וכן שימוש ברשתות פרוקסי וארגוני שלוחה מרוחקים. משמרות המהפכה, שחולשים על המבצעים הקיברנטיים של איראן, מתאמים ומתכננים כך מערכה רחבה שחורגת מהפרעה לרשתות, גניבת כסף והטרדה. יתרונותיה הגדולים הם במחיריה הנמוכים, השפעותיה הגדולות והיעדר הצורך לחצות גבולות גיאוגרפיים. בהתאם, גם היקף המטרות מתרחב מאוד, והיעדים מגוונים.

מאז תחילת המלחמה בסוף פברואר 2026 נצפית עלייה גדולה בפעילות הסייבר האיראני, שכוללת מטרות רבות: ריגול, גישה למערכות אויב, שיבוש, דליית מידע, פשיעה, גניבה כלכלית ועוד. בחודש מרץ, דווח בישראל, היו יותר מחמישים אירועי פריצה למערכות ארגוניות שונות בארץ, והם נעשו באופן מאורגן ומסודר.

הפצחנים האיראנים, מעירים מומחים, מונחים על פי אסטרטגיה ברורה המתיישרת היטב עם מטרות המלחמה של איראן, ואף מסייעות להן בעיקר בכל הקשור לריגול ואיסוף מידע, ניתוח כוונות של האויב ועוד. התפתחות הבינה המלאכותית עוזרת מאוד למתקפות הסייבר האיראניות, והמומחים של איראן משתמשים בה, לפי ההערכות, לכתיבת דו"ח, ניתוח הנזק לאויב, פעולות הנדסה חברתית, מניפולציה או יצירת תוכן בקלות. הטכנולוגיה הזאת גם מגדילה בכמה מונים את אפשרויות המהירות, הטווח, הפגיעה והיכולות של הסייבר האיראני.

שילוב ידיים בין הקינטי לקיברנטי

המהלומה הראשונה שהנחית מערך הסייבר האיראני במלחמה הנוכחית נגד ארה"ב, לפי מה שפורסם עד כה, אירעה ב-11 במרץ. היא כוונה נגד חברת הטכנולוגיה הרפואית "סטרייקר", היושבת במישיגן, ואשר מפעילה סניפים רבים ברחבי העולם, כולל בישראל. האיראנים ניצלו

פרצות בתלות של החברה בשירותי ענן, חדרו למערכות מבית "מיקרוסופט", ושלחו "נוזקת מחיקה" שפקדה על יותר מ-200 אלף שרתים, מחשבים וטלפונים של החברה להתאפס.

את המבצע הובילה קבוצה "הנדלה" המפורסמת, הנשלטת בידי משרד המודיעין האיראני, שלטענתה הצליחה למחוק יותר מ-50 טרה בייט של נתונים. היא טענה כי עשתה זאת כנקמה על המתקפות נגד איראן, והגדירה את החברה "ציונית". אף שבמתקפה לא נפגע ציוד רפואי, היא הזיקה מאוד ליכולתה של החברה לקבל ולשלוח הזמנות, ציוד רפואי ומכשירים שונים. יתרה מכך, ההצלחה כבר עשתה את שלה: כעת היה ברור לאזרחים האמריקנים כי איראן תנסה לפגוע גם בהם בביתם, וכי יש ביכולתה גם להצליח בכך.

אך לצד זאת, מתקפות הסייבר גם לבשו אופי אחר, ובפועל הרימו תרומה של ממש למאמץ המלחמתי של טהרן. ביולי, למשל, פורסם כי איראן הצליחה לפרוץ לפרוטוקול טכני שמנתב מידע ברשתות תקשורת, וכך גילתה וזיהתה מיקומים של חיילים אמריקנים, כוחות ובסיסים ברחבי המזרח התיכון – מה שדייק את מתקפות הטילים האיראניות והגביר את האבדות בקרב צבא ארה"ב. בנוסף, הסוכנים של הרפובליקה האסלאמית הצליחו לחדור למצלמות אבטחה במדינות האזור, מה שנתן להם יכולת לבצע הערכות נזק, לקבל תמונה של אזורי הפגיעה ולשפר את דיוק הטילים והכטב"מים.

במידת מה, אגב, זה מזכיר את הפעולות שביצעה ישראל, לפי הדיווחים, כדי לאתר את מיקומו של מנהיג איראן עלי ח'מינאי לפני שחוסל במכת הפתיחה של המלחמה. החדירה למצלמות רחוב, במובן זה, יכולה לשמש את שני הצדדים – והאיראנים הבינו זאת היטב.

מהכיוון ההפוך, איראן כיוונה חלק מהתקיפות הקינטיות שלה למטרות שקשורות לעולם הווירטואלי, ומשלימות את הנזק הקיברנטי. מיד בתחילת המלחמה, ב-1 במרץ, תקפה איראן בטילים וכטב"מים מרכזים של אמזון בבחריין ובאמירויות, וכך השביתה את שירותי הענן של החברה ושירותים נוספים שלה. חשיבותם של מרכזי מידע כאלה, לפי ההערכה, עלתה בשל השימוש הגובר בבינה מלאכותית, וייתכן שמנהיגי איראן ביקשו לשבש אמצעים שלהבנתם מסייעים לארה"ב וישראל לתקיפות נגדם.

בסוף אותו חודש פרסמה איראן אזהרה שתתקיף חברות אמריקניות מרכזיות בתחום הטכנולוגיה והמחשוב, כולל גוגל, אפל, מטה, אורקל ועוד. בתקשורת המקומית דווח על עוד מתקפות נגד מרכזים של אמזון בתחילת אפריל, ופגיעה נוספת במרכז של אורקל בדובאי ב-2 באפריל.

לצד התועלת הצבאית, המתקפות הללו נועדו גם למטרות אחרות. בין היתר, כוונתן הייתה ליצור משוואה בין מטרות שישראל וארה"ב תקפו, ובהן מרכזי תעשייה ומחשוב איראניים, ובין יעדים דומים במערב. טהרן גם ביקשה לשלוח מסר לבנות הברית של ארה"ב באזור שאף תעשייה – חשובה ככל שתהיה – לא תחמוק מהנשק האיראני. בנוסף, מדובר ביעדים יחסית קלים לאיתור ולפגיעה, כך שהרווח מתאזן היטב עם העלות הקטנה.

באותו אופן, גם מטרת מתקפות הסייבר של איראן לא הייתה רק יצירת נזק פיזי או וירטואלי. לדברי חוקרים באוניברסיטת רייכמן, המתקפות של קבוצת "הנדלה", למשל, שירתו את היעד של כל פעולת טרור אחרת – זריעת פחד, ערעור החוסן הציבורי והשפעה על התודעה. לכן נלוו למתקפות הללו קמפיינים מתוזמנים, שכללו איומים, התרעות, מניפולציה ועוד. דוגמה שאולי אפשר להתחבר אליה יותר בקלות היא המסרונים שקיבלו רבים בישראל מאיראן, ובהם איומים מפורשים. הם נועדו לשמש אותה מטרה. היעד הוא זריעת פאניקה, דה-מורליזציה, ערעור תחושת הביטחון של האזרחים ועוד.

זה גם היעד, פעמים רבות, של חלק ממתקפות ה"פישינג" והפריצה למכשיריהם של בכירים ביטחוניים. "הנדלה", כזכור, הצליחה לחדור למכשירו של ראש הבולשת הפדרלית קאש פאטל ולפרסם משם תמונות אישיות שלו. ההאקרים האיראנים ניסו להגיע לאנשי תקשורת בארץ, וזכורות היטב הטענות לפריצות למכשירי הטלפון של הרמטכ"ל לשעבר הרצי הלוי, ראש הממשלה לשעבר נפתלי בנט והרמטכ"ל ושר הביטחון לשעבר בני גנץ.

בהנחה שרוב האנשים הללו אכן מצייתים לכללי ביטחון שדה, ולא מאחסנים על המכשירים האישיים שלהם מידע סודי, מבצעים כאלה נועדו בעיקר להביך אותם, להדגים שוב את עומק החדירה של טהרן, ולנסות לדוג חומרים אישיים מביכים או פוליטיים. האיראנים עשויים לשמור חלק מהדברים הללו, אגב, למועד מאוחר יותר, ולשלוף אותם בתזמון מתאים, או לנצל אותם למטרות סחיטה.

בארה"ב החשד היה גם שהמתקפות על מערכות המים במדינות השונות לא נועדו באמת לפגוע באספקה, אלא להוות "פיצוח תודעתי" (או פיגוע תודעתי), ולהדגים לאזרחים האמריקנים – בדומה למתקפה של "הנדלה" על חברת הטכנולוגיה הרפואית בתחילת המלחמה – את ידה הארוכה של טהרן, לעורר פאניקה וחשש מפגיעה בתשתיות הכי בסיסיות שמשמשות אותם.

היתרון הגדול של טקטיקה כזו הוא שהיא קלה וזולה, ומנגד מניבה רווחים רבים. לא צריך לפרוץ את כל מערכות ההגנה של היריב, אלא רק להיכנס פנימה, לצלם תמונות, לפרסם אותן בליווי איומים – ולהניח לאויב לדמיין את הגרוע מכול. המוח שלו כבר יעשה את יתר העבודה. ברמה ההסברתית, פעולה מוצלחת כזו יכולה גם להאדיר את הדימוי של איראן כמעצמה טכנולוגית שיכולה לפגוע במטרות הרחק מגבולותיה, ובה בעת שוחק את התדמית של העליונות האמריקנית בתחום הטכנולוגיה.

גם כעת, לאור הגברת הלחץ הכלכלי של ארה"ב ותוצאות המתקפות על מרכזי טכנולוגיה איראניים בתחילת המלחמה, מתקפות סייבר נותרו עדיין אחת האפשרויות האמינות, הזולות והמועדפות על האיראנים, שלא יעלו את סף ההסלמה של הסכסוך כל עוד לא יצטברו למסה קריטית או יפגעו במטרה רגישה במיוחד. הן גם מהוות תשובה טובה לכך שאיראן אינה יכולה להגיע פיזית בהכרח למקומות כמו בריטניה, שמסייעת לאמריקנים, ולגרום לה לשלם מחיר על מעורבותה במלחמה.

כבר כעת ניכר כי יש תוצאות למאמץ האיראני. חברות טכנולוגיה גדולות מתחילות לשקול, לפי הטענה, את בניית המרכזים הבאים שלהן במקומות בטוחים יחסית, ולא למשל במדינות המפרץ. אף שקשה למצוא מקומות "בטוחים" בעולם במיוחד לאור ההסלמה במלחמת אוקראינה-רוסיה בעניין הפגיעה במגזר האזרחי סומנו עד כה מדינות כגון מרכז ומזרח אירופה כיעדים מועדפים. מגמה כזו עלולה להיות מכה משמעותית לארצות המזרח התיכון, וזו בדיוק הכוונה של ההנהגה בטהרן. לברית עם ארה"ב, הם מדגישים, יש גם מחירים ואנו נגבה אותם.

לא ניחשף להיקף הפעילות הנסתרת

ישראל וארה"ב אינן שוקדות על השמרים גם בממד הסייבר. לצד המתקפות שנועדו לשבש יכולות איראניות, שתי המדינות עסוקות מאוד בהגנה, פועלות ישירות נגד הפצחנים בשירות טהרן ומטות הסייבר של המשטר, ומפגינות בעצמן מומחיות בתחום הקיברנטי.

דוגמה אחת, למשל, לפעולת הגנה שבוצעה במלחמה היא ההשתלטות של הבולשת הפדרלית על תשתיות של "הנדלה" ימים ספורים לאחר המתקפה על חברת סטרייקר במרץ. אירוע קיצוני יותר הוא החיסול שוב, לפי דיווחים באיראן של מפקד יחידת "הנדלה" בתקיפה ישראלית ושל סגן שר המודיעין האחראי על תיק הסייבר נגד ישראל.

במקביל, תקיפות סייבר על תשתיות איראניות נועדו גם הן לפגוע בחיי היומיום של האזרחים, לנטרל חלק מהאמצעים הצבאיים של טהרן ואפילו לדחוף עוד את הכלכלה המקומית לקראת האפשרות של נפילתה. התקלה הנרחבת שהשביתה את השירותים של ארבעה בנקים גדולים במדינה, לפי הטענה, נבעה ממתקפת סייבר שהצליחה במשך שבועות לגרום להם לא לתפקד באופן משמעותי.

כמו כן, ישראל עשתה שימוש במלחמה בלוחמה פסיכולוגית שנעזרה בסייבר, כששלחה הודעות למכשירי הטלפון של אנשי צבא איראנים, פרצה לשידורי הטלוויזיה במדינה ולאתרי החדשות שלה, ואף ביצעה פעולות נוספות. סביר להניח שאת רוב הפעילות הזאת אנו לא מכירים, ואולי לעולם לא ניחשף אליה. לא אלמן ישראל.

המאבק הזה אולי נסתר מעין, אך נראה שהוא יצרי, נחוש, נרחב ומסוכן מאוד. הוא אינו נח גם כשמוכרזת הפסקת אש, וההתפתחויות הטכנולוגיות מגדילות את היכולות ההתקפיות כל העת. כאזרחים במדינה שנמצאת כל העת על הכוונת האיראנית, חשוב לנו לסגל אמצעים ושגרת פעילות שיסייעו להפחית את החשיפה שלנו לפגיעה נרחבת, לא לפרוץ את גבולות ביטחון השדה ולהקפיד על כללים פשוטים שיעזרו להגן עלינו מפני היד הווירטואלית הארוכה של איראן. מכיוון שקו ההגנה תמיד יכול להיפרץ, וזה נכון גם בממד הסייבר, חשוב לנו להתכונן לכך במרחב הפרטי שלנו. את יתר העבודה יעשו אנשי המקצוע ויש על מי לסמוך.

*הדעות המובעות בפרסומי מכון משגב הן על דעת המחברים בלבד.