חור ברשת // מדוע ביטל הרמטכ"ל את החלטתו להקים זרוע סייבר בצה"ל יוסי מלמן, עמ' 26

צילום: רויטרס

יוסי מלמן
חשאי בשישי

חור ברשת

החלטתו של הרמטכ"ל איזנקוט שלא להקים זרוע סייבר בצה"ל התקבלה ככל הנראה גם בשל לחצים מצד אמ"ן, שלא שש לוותר על נכסיו ■ לדברי ד"ר הראל מנשרי, ראש תחום הסייבר במכון הטכנולוגי בחולון, מדובר בטעות ועל ישראל להכין "תוכנית הגנה מקיפה לקראת מערכות הבחירות הבאות"

לאחר דיונים שנמשכו חודשים אחדים, הוחלט השבוע בצה"ל שלא להקים זרוע או פיקוד סייבר. ליתר דיוק, ההחלטה הסופית נדחתה עד 2020. בכך בעצם החליט הרמטכ"ל גדי איזנקוט, המסיים שנתיים בתפקיד, שלא להחליט לפי שעה. בינתיים ימשיך בעבודת המטה בנושא צוות מיוחד באגף התכנון, בראשות אלוף עמיקם נורקין. מקור צבאי בכיר העריך עם זאת כי עד לסיום הקדנציה שלו, בעוד שנתיים, איזנקוט יחתוך ויקבל החלטה.

במשך לפחות כעשור מדברים בצה"ל, כמו גם בצבאות אחרים בעולם, על "הממד הרביעי" במלחמה המודרנית. עד למאה ה־20 לצבאות היו שתי זרועות - ביבשה ובים. המאה הקודמת הביאה עמה את הזרוע השלישית - חיל האוויר, ומאז שנות ה־50 המאוחרות גם את החלל. המרחב הקיברנטי הוא זירת המלחמה הנוספת של ה"ממד הרביעי".

בעשור הקודם, בתקופת כהונתם של עמוס ידלין כראש אגף המודיעין בצה"ל ושל מאיר דגן בראשות המוסד, עשתה ישראל קפיצת מדרגה בשדרוג יכולותיה במרחב הקיברנטי. לצדם פעל אז תא"ל נדב צפריר כמפקד יחידת 8200, שהייתה ועודנה חוד החנית של מאמצי האיסוף והריגול הטכנולוגי של ישראל נגד אויביה ויריביה, בהם סוריה, איראן וחיזבאללה (וגם חמאס).

זה נעשה בין השאר באמצעות מה שמכונה "סיגינט" - האזנות, יירוט תשדורות, פענוח צפנים, ולפי פרסומים זרים גם חדירות למחשבים. גם במוסד וגם בשירות הביטחון הכללי יש יחידות העוסקות בסיגינט, אך יכולותיהן פחותות מאלה של 8200. בגופי הסיגינט של גופי המודיעין, או לצדם, הוקמו גם יחידות ללוחמת סייבר.

שלושה שימושים עיקריים יש ללוחמת סייבר. אחד הגנתי ושניים התקפיים. ההגנתי הוא בתחום אבטחת המידע - למנוע מהיריב לחדור למחשבים בישראל בכלל ובפרט של מוסדות ממלכתיים, בין שהם צבאיים־ביטחוניים ובין שאזרחיים. הגנת הסייבר מכוונת לאבטח את המחשבים ומערכות התקשורת של גופי המודיעין, של צה"ל וגם של אתרים אסטרטגיים ותשתיות קריטיות: תחנות כוח, כורים גרעיניים, שדות תעופה, בתי חולים, מאגרי מים, מאגרי נפט וגז, בתי חולים, מוסדות פיננסיים ועוד. חדירה למחשבים של מערכות תשתית יכולה להביא לאסונות גדולים ולמותם של רבים.

ההסדרה החדשה

ישראל חתרה תמיד להיות בקדמת המדע והטכנולוגיה בעולם. כבר בראשית שנות ה־50 היה ברשותה מחשב שהוקם במכון ויצמן, ועד מהרה הוכנסו מחשבים גם לשירות צה"ל והמודיעין; היא ייסדה תוכנית גרעין, שלפי פרסומים זרים כוללת כלי נשק גרעיניים; וגם בתחום אבטחת המחשבים הייתה בין החלוצות בעולם כשהחלה לפעול בנושא כבר בשנות ה־90.

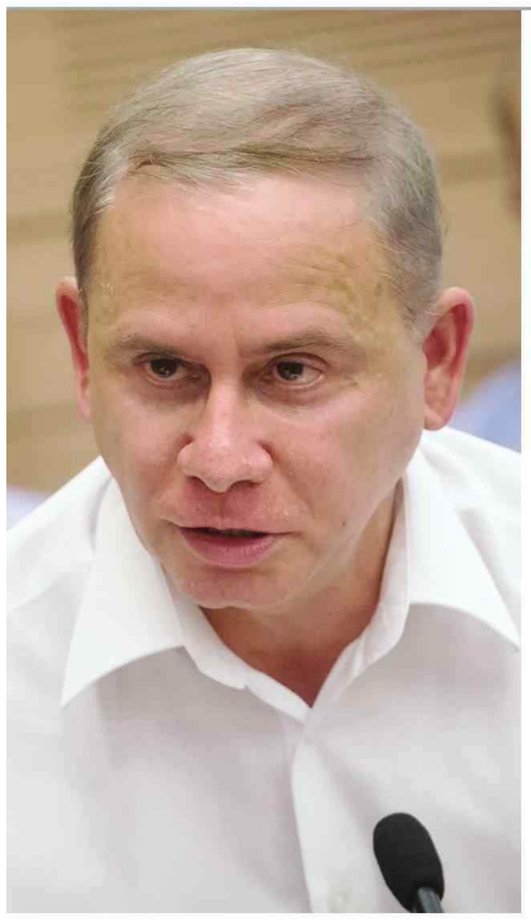
עד לפני כמה שנים האחריות הבלעדית על הגנת רשתות התקשורת והמחשבים הייתה של השב"כ. ב־2002 הוקמה "הרשות הממלכתית לאבטחת מידע" (רא"מ), שפעלה במסגרת אגף הסיגינט של השב"כ. כעבור יותר מעשור, בינואר 2012, החל לפעול במשרד ראש הממשלה "מטה הסייבר הלאומי", שבראשו עומד ד"ר אביתר מתניה. תפקידו של המטה, הכפוף לראש הממשלה, הוא להוביל את פיתוח התחום הקיברנטי, לתאם בין הגורמים השונים העוסקים בתחום, להרחיב את ההגנה על תשתיות לאומיות מפני תקיפות סייבר, ולעודד את קידום הנושא בתעשייה. במקביל הוקמה לפני כשמונה חודשים "הרשות הלאומית להגנת הסייבר", שתפעל גם היא במשרד ראש הממשלה ואותה מנהל ברוך (בוקי) כרמלי, בוגר יחידה 8200 שהיה אחראי על מערך הסייבר במשרד הביטחון וניהל בעבר חברת סייבר.

ההקמה של הרשות לוותה בחבלי לידה קשים ובמאבקי כוח מול השב"כ וגופים אחרים במערכת הביטחון, שלא ששו לאבד את הבכורה בתחום. מכיוון שהשמות של שני הגופים - "הרשות" ו"המטה" - אולי מבלבלים משהו, נקבע שהאחריות הכוללת תהיה בידי ד"ר מתניה, שהגדרת תפקידו תהיה "ראש מערך הסייבר הלאומי".

לפי ההסדרה החדשה, הרשות והמטה יהיו אחראים אך ורק לתחום האזרחי, כולל תשתיות קריטיות כמו חברת החשמל, בנקים, או מערך המחשוב של שירותי הממשלה, מה שנקרא "ממשל זמין", ועוד. תפקידם יהיה להכווין ולהנחות מקצועית את הגופים האזרחיים כיצד להגן על המערכות שלהם, להעביר להם מידע והתרעות ולסייע להם בעת מצוקה. מערכת הביטחון תמשיך להיות אחראית על עצמה ולא תהיה כפופה לרשות החדשה, אם כי התקווה והציפייה הן שהיא תשתף פעולה.

"הרשות מוקמת כגוף אזרחי והיא אינה אוספת מודיעין על יריבים", הדגיש באוזני כבר לפני כמה חודשים גורם בכיר העוסק בנושא. כלומר, תפקידה לפעול אך ורק במגזר האזרחי בתחום לוחמת סייבר הגנתית.

בתחום ההתקפי, הסייבר מזוהה לרוב עם ריגול - באמצעותו חודרים בחשאי למחשבי היריב ואוספים עליו מידע. זו פעולת ריגול, שהיום הפכה לדי שגרתית, שנעשית באמצעים טכנולוגיים. במקום לגייס סוכן בקרב היריב ולהפעיל אותו לצורך השגת מידע שנדרש על המטרה - "לצייח" בעגה המקצועית, מלשון ציון ידיעות חיוניות - עושים זאת באמצעות חדירה למחשבים. מחדירים במחשבים "סוס טרויאני" או רוגלה (מלשון ריגול) ואוספים את המידע בהפעלה מרחוק. אפשר לקרוא לפעולות אלה ריגול



כרמלי (משמאל למעלה), איזנקוט, מתניה ומנשרי. מקור צבאי בכיר מעריך כי הרמטכ"ל יקבל החלטה עד לסיום הקדנציה שלו

צילומים: הדס פרוש ומרים אלסטר, פלאש 90, יח"צ

לפי ההסדרה החדשה, הרשות והמטה יהיו אחראים אך ורק לתחום האזרחי, כולל תשתיות קריטיות כמו חברת החשמל, בנקים, או מערך המחשוב של שירותי הממשלה, ועוד. מערכת הביטחון לא תהיה כפופה לרשות החדשה, אם כי התקווה והציפייה הן שהיא תשתף פעולה

נגד תוכנה.

השימוש השני, המתוחכם וגם המסוכן יותר, שמוכר פחות לציבור, הוא לחדור למחשבים, לשתול בהם וירוס או "תולעת" שיורו להם לבצע פעולות של פגיעה בחומרה, במערכות של ציוד ומכונות שמופעלות על ידם. זה יכול להיות למטרות שיתוק של מערכות האויב, לדוגמה מערכות מכ"ם אוויריות, כדי שלא יגלו פעילות של מטוסים, כפי שמיוחס לישראל, שלכאורה פעלה נגד מערכות ההגנה האוויריות של סוריה לפני השמדת הכור הגרעיני בדיר א־זור בספטמבר 2007. וזה יכול להיות למטרות של גרימת נזק או השמדת מערכות של האויב. פעולה כזו מיוחסת למיזם משותף ישראלי־אמריקאי במחצית השנייה של העשור הקודם, נגד האתר להעשרת אורניום של איראן בנתנז.

לפי פרסומים זרים, יחידה 8200 שעליה פיקד אז נדב צפריר, שיתפה פעולה עם הסוכנות הלאומית לביטחון (NSA) של ארה"ב, שבראשה עמד גנרל קית אלכסנדר, בפיתוח שורה של וירוסים שפגעו בכאלף (כשליש) מהסרכזות (צנטריפוגות) להעשרת אורניום. במבצע היו שותפים באופן פעיל ה־CIA והמוסד, שהיה אחראי להחדרת הווירוס שכונה "סטוקסנט". המבצע כונה במודיעין האמריקאי "משחקים אולימפיים", והוא היה חלק מתוכנית רחבת ידיים במסגרת הסכם לשיתוף פעולה בין 8200 ל־NSA, שנחשף בידי אדוארד סנודן.

אגב, לארה"ב הייתה תוכנית ללוחמת סייבר התקפי רחבה עוד יותר, ששם הצופן שלה היה "ניטרו־זאוס", שנבנתה למקרה של מלחמה בין שתי המדינות ונועדה לשתק ולפגוע בכל התשתיות הלאומיות - אזרחיות וצבאיות - של איראן. התוכנית וכינויה נחשפו בשנת 2016 בסרט התיעודי "ימי אפס" של הבמאי האמריקאי אלכס גיבני (למען הגילוי הנאות, אני מרואיין בסרט).

עד היום יש ויכוח נוקב בקרב קהילות המודיעין של ישראל וארה"ב בשאלה אם המבצע המיוחס להן הצליח ועד כמה, או שמא נכשל לבלום את תוכנית הגרעין של איראן, ולמעשה הגביר את מודעותה לשיפור יכולות הסייבר שלה, הן בתחום ההגנתי והן בהתקפי.

גם היום, ניתן לשער כי יכולותיה הצבאיות והגרעיניות של איראן (למרות ההסכם שנחתם בינה לבין המעצמות הגדולות לפני כשנה וחצי לצמצום תוכנית הגרעין שלה), לצד חיזבאללה, הן בראש הצי"ח של המודיעין הישראלי.

הדגם הישראלי

על רקע זה ניתן לראות את החלטת הרמטכ"ל שלא להקים לפי שעה פיקוד סייבר כצילום מצב או שימורו. האחריות להגנת המחשבים ורשתות התקשורת של צה"ל תישאר בידי אגף התקשוב (לשעבר חיל הקשר), ואילו יכולת הסייבר ההתקפי תיוותר בידי יחידה 8200 של אמ"ן.

להחלטה קדמו כאמור דיוניים נוקבים, שבמסגרתם יצאו נציגי צה"ל לפגישות לימוד והיכרות עם גופי הסייבר הצבאיים במדינות ידידותיות כמו ארה"ב, בריטניה ועוד. במסגרת הפגישות נערכו גם משחקי מלחמה וסימולציות. בצבא ארה"ב קיים פיקוד סייבר, ואילו בבריטניה האחריות לסייבר הצבאי היא בידי יחידת המודיעין - GCHQ - המקבילה ל־8200. כששאלתי השבוע קצין בכיר במהלך תדרוך לעיתונאים מהו הדגם שעמד לנגד עיני צה"ל בקבלת ההחלטה, הוא השיב "הדגם הישראלי". לדבריו, "זה משהו שאנחנו לא רוצים לפגוע בו, כי יש לנו עליונות (בתחום הסייבר ההתקפי - י"מ) שמשרתת אותנו ומייצרת דיבידנדים למדינת ישראל".

ההחלטה שלא להקים פיקוד סייבר היא אומנם ארגונית במהותה, אך היא מעניינת, משום שהרושם שעלה בשנה וחצי האחרונות, מאז החלו הדיונים בנושא בצה"ל, הוא שהרמטכ"ל איזנקוט דווקא תומך בהקמתו. אפשר שהוא שוכנע שעדיף שלא לאחד את כל יכולות הסייבר - ההתקפיות וההגנתיות - תחת קורת גג אחת, כדי שלא לפגוע ביכולות המצוינות של הסייבר ההתקפי שפיתח אמ"ן. אך ברור גם שלהתנגדותם של ראש אמ"ן אלוף הרצי לוי ומפקד 8200, שהתקשו לוותר על הנכסים שברשותם, היה משקל בהחלטה.

זו גם הערכתו של ד"ר הראל מנשרי, ראש תחום הסייבר במכון הטכנולוגי בחולון (HIT). "ההחלטה שלא להקים פיקוד סייבר", הוא סבור, "היא טעות ונובעת להערכתי מבעיות אגו והורדת ידיים בין אמ"ן לתקשוב".

לפני שהיה לאקדמאי עסק מנשרי בנושא במשך שנים רבות במסגרת עבודתו בשב"כ. לאחרונה ערך מחקר שניתח את מלחמת הסייבר בין רוסיה לארה"ב, ששיאה היה בחודש שעבר. המשרד להגנת המולדת, ה־FBI וה־CIA הגיעו למסקנה חד־משמעית כי רוסיה הפעילה לוחמת סייבר התקפי בתקופת מערכת הבחירות בארה"ב, שכוונה בעיקר נגד מועמדותה של הילרי קלינטון והמפלגה הדמוקרטית. הנהנה העיקרי ממנה היה כמובן דונלד טראמפ, שיחסו האוהד, אם לא המעריץ לוולדימיר פוטין, מעורר פליאה והשתאות בתקשורת הבינלאומית ומאתגר את קהילות המודיעין בעולם. על רקע זה התקבלה גם החלטת הנשיא היוצא ברק אובמה לגרש 35 דיפלומטים רוסים ולסגור שני מתחמים באזור וושינגטון ששימשו את השגרירות הרוסית לפעולות ריגול בסייבר.

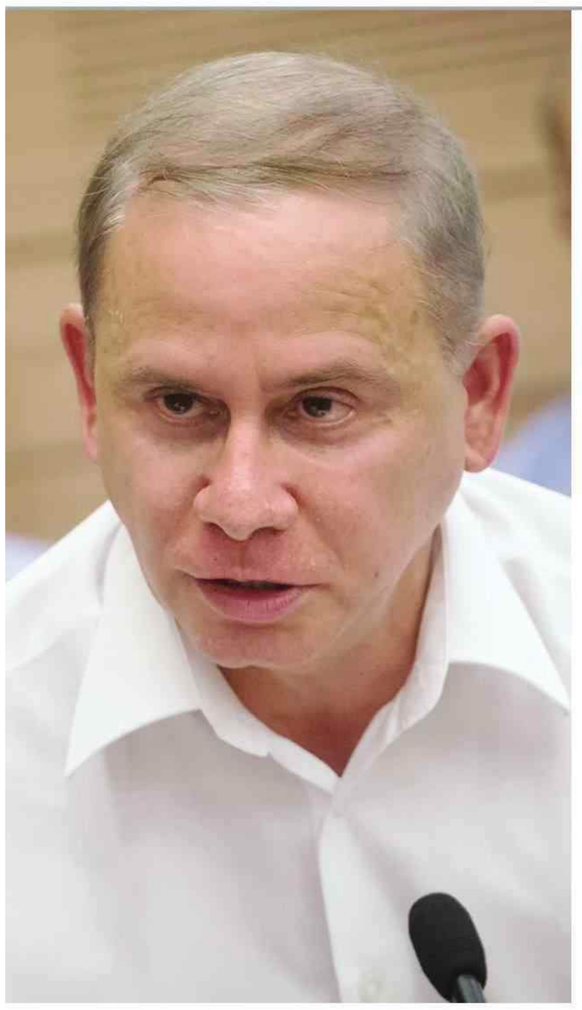
במחקרו סוקר ד"ר מנשרי את המבנה של יחידות הסייבר ברוסיה ואת השימוש שעשתה המדינה בלוחמה הקיברנטית במלחמות נגד גיאורגיה ב־2008, בעת הפלישה לאוקראינה ב־2014 ומעת לעת נגד המדינות הבלטיות שאותן היא חומדת.

המחקר מדגיש כי גם ארה"ב ככל הנראה לא טמנה את ידה בצלחת. ביולי 2016 פרסם שירות הביטחון הרוסי (FSB, הגוף הדומיננטי בקהילת המודיעין הרוסית בכלל ובנושא הסייבר בפרט) כי מערכות המחשבים של 20 ארגונים רוסיים, כולל של הממשלה ומערכת הביטחון שלה, נפרצו בידי "ממשלה זרה", ורמז כי מדובר בקהילת המודיעין האמריקאית.

לסיכום מחקרו מדגיש מנשרי: "מניסיון העבר, פעולת סייבר זוכה לתהודה ויוצרת חקיינים. בין שמטרתם של התוקפים הרוסיים הייתה לסייע לבחירתו של טראמפ או לפגוע באמינותה של קלינטון, ובין שההתקפות כוונו ישירות בידי פוטין או לא - יש להביא בחשבון כי גורמים אלה או אחרים ינסו להשפיע באמצעות פעולות במרחב הסייבר על בחירות דמוקרטיות ועל דעת הקהל במדינות אחרות ובכלל ישראל".

ומכאן ממליץ מנשרי לגורמי ההגנה וקובעי המדיניות בישראל לקדם "תוכנית מקיפה להגנה על מערכות המידע וההצבעה לקראת מערכות הבחירות הבאות". כמו כן עליהם לבחון דרכים "שיאפשרו לדמוקרטיה הישראלית להתמודד מפני הניסיונות לקעקע אותה באמצעות פעולות 'תודעה', המכונות גם 'השפעה על דעת הקהל' או 'לוחמה פסיכולוגית'". ❖

melmanyossi1950@gmail.com



כרמלי (משמאל למעלה), איזנקוט, מתניה ומנשרי. מקור צבאי בכיר מעריך כי הרמטכ"ל יקבל החלטה עד לסיום הקדנציה שלו

צילומים: הדס פרוש ומרים אלסטר, פלאש 90, יח"צ

לפי ההסדרה החדשה, הרשות והמטה יהיו אחראים אך ורק לתחום האזרחי, כולל תשתיות קריטיות כמו חברת החשמל, בנקים, או מערך המחשוב של שירותי הממשלה, ועוד. מערכת הביטחון לא תהיה כפופה לרשות החדשה, אם כי התקווה והציפייה הן שהיא תשתף פעולה

אגב, לארה"ב הייתה תוכנית ללוחמת סייבר התקפי רחבה עוד יותר, ששם הצופן שלה היה "ניטרו־זאוס", שנבנתה למקרה של מלחמה בין שתי המדינות ונועדה לשתק ולפגוע בכל התשתיות הלאומיות - אזרחיות וצבאיות - של איראן. התוכנית וכינויה נחשפו בשנת 2016 בסרט התיעודי "ימי אפס" של הבמאי האמריקאי אלכס גיבני (למען הגילוי הנאות, אני מרואיין בסרט).

עד היום יש ויכוח נוקב בקרב קהילות המודיעין של ישראל וארה"ב בשאלה אם המבצע המיוחס להן הצליח ועד כמה, או שמא נכשל לבלום את תוכנית הגרעין של איראן, ולמעשה הגביר את מודעותה לשיפור יכולות הסייבר שלה, הן בתחום ההגנתי והן בהתקפי.

גם היום, ניתן לשער כי יכולותיה הצבאיות והגרעיניות של איראן (למרות ההסכם שנחתם בינה לבין המעצמות הגדולות לפני כשנה וחצי לצמצום תוכנית הגרעין שלה), לצד חיזבאללה, הן בראש הצי"ח של המודיעין הישראלי.

הדגם הישראלי

על רקע זה ניתן לראות את החלטת הרמטכ"ל שלא להקים לפי שעה פיקוד סייבר כצילום מצב או שימורו. האחריות להגנת המחשבים ורשתות התקשורת של צה"ל תישאר בידי אגף התקשוב (לשעבר חיל הקשר), ואילו יכולת הסייבר ההתקפי תיוותר בידי יחידה 8200 של אמ"ן.

להחלטה קדמו כאמור דיוניים נוקבים, שבמסגרתם יצאו נציגי צה"ל לפגישות לימוד והיכרות עם גופי הסייבר הצבאיים במדינות ידידותיות כמו ארה"ב, בריטניה ועוד. במסגרת הפגישות נערכו גם משחקי מלחמה וסימולציות. בצבא ארה"ב קיים פיקוד סייבר, ואילו בבריטניה האחריות לסייבר הצבאי היא בידי יחידת המודיעין - GCHQ - המקבילה ל־8200. כששאלתי השבוע קצין בכיר במהלך תדרוך לעיתונאים מהו הדגם שעמד לנגד עיני צה"ל בקבלת ההחלטה, הוא השיב "הדגם הישראלי". לדבריו, "זה משהו שאנחנו לא רוצים לפגוע בו, כי יש לנו עליונות (בתחום הסייבר ההתקפי - י"מ) שמשרתת אותנו ומייצרת דיבידנדים למדינת ישראל".

ההחלטה שלא להקים פיקוד סייבר היא אומנם ארגונית במהותה, אך היא מעניינת, משום שהרושם שעלה בשנה וחצי האחרונות, מאז החלו הדיונים בנושא בצה"ל, הוא שהרמטכ"ל איזנקוט דווקא תומך בהקמתו. אפשר שהוא שוכנע שעדיף שלא לאחד את כל יכולות הסייבר - ההתקפיות וההגנתיות - תחת קורת גג אחת, כדי שלא לפגוע ביכולות המצוינות של הסייבר ההתקפי שפיתח אמ"ן. אך ברור גם שלהתנגדותם של ראש אמ"ן אלוף הרצי לוי ומפקד 8200, שהתקשו לוותר נגד תוכנה.

השימוש השני, המתוחכם וגם המסוכן יותר, שמוכר פחות לציבור, הוא לחדור למחשבים, לשתול בהם וירוס או "תולעת" שיורו להם לבצע פעולות של פגיעה בחומרה, במערכות של ציוד ומכונות שמופעלות על ידם. זה יכול להיות למטרות שיתוק של מערכות האויב, לדוגמה מערכות מכ"ם אוויריות, כדי שלא יגלו פעילות של מטוסים, כפי שמיוחס לישראל, שלכאורה פעלה נגד מערכות ההגנה האוויריות של סוריה לפני השמדת הכור הגרעיני בדיר א־זור בספטמבר 2007. וזה יכול להיות למטרות של גרימת נזק או השמדת מערכות של האויב. פעולה כזו מיוחסת למיזם משותף ישראלי־אמריקאי במחצית השנייה של העשור הקודם, נגד האתר להעשרת אורניום של איראן בנתנז.

לפי פרסומים זרים, יחידה 8200 שעליה פיקד אז נדב צפריר, שיתפה פעולה עם הסוכנות הלאומית לביטחון (NSA) של ארה"ב, שבראשה עמד גנרל קית אלכסנדר, בפיתוח שורה של וירוסים שפגעו בכאלף (כשליש) מהסרכזות (צנטריפוגות) להעשרת אורניום. במבצע היו שותפים באופן פעיל ה־CIA והמוסד, שהיה אחראי להחדרת הווירוס שכונה "סטוקסנט". המבצע כונה במודיעין האמריקאי "משחקים אולימפיים", והוא היה חלק מתוכנית רחבת ידיים במסגרת הסכם לשיתוף פעולה בין 8200 ל־NSA, שנחשף בידי אדוארד סנודן.

על הנכסים שברשותם, היה משקל בהחלטה.

זו גם הערכתו של ד"ר הראל מנשרי, ראש תחום הסייבר במכון הטכנולוגי בחולון (HIT). "ההחלטה שלא להקים פיקוד סייבר", הוא סבור, "היא טעות ונובעת להערכתי מבעיות אגו והורדת ידיים בין אמ"ן לתקשוב".

לפני שהיה לאקדמאי עסק מנשרי בנושא במשך שנים רבות במסגרת עבודתו בשב"כ. לאחרונה ערך מחקר שניתח את מלחמת הסייבר בין רוסיה לארה"ב, ששיאה היה בחודש שעבר. המשרד להגנת המולדת, ה־FBI וה־CIA הגיעו למסקנה חד־משמעית כי רוסיה הפעילה לוחמת סייבר התקפי בתקופת מערכת הבחירות בארה"ב, שכוונה בעיקר נגד מועמדותה של הילרי קלינטון והמפלגה הדמוקרטית. הנהנה העיקרי ממנה היה כמובן דונלד טראמפ, שיחסו האוהד, אם לא המעריץ לוולדימיר פוטין, מעורר פליאה והשתאות בתקשורת הבינלאומית ומאתגר את קהילות המודיעין בעולם. על רקע זה התקבלה גם החלטת הנשיא היוצא ברק אובמה לגרש 35 דיפלומטים רוסים ולסגור שני מתחמים באזור וושינגטון ששימשו את השגרירות הרוסית לפעולות ריגול בסייבר.

במחקרו סוקר ד"ר מנשרי את המבנה של יחידות הסייבר ברוסיה ואת השימוש שעשתה המדינה בלוחמה הקיברנטית במלחמות נגד גיאורגיה ב־2008, בעת הפלישה לאוקראינה ב־2014 ומעת לעת נגד המדינות הבלטיות שאותן היא חומדת.

המחקר מדגיש כי גם ארה"ב ככל הנראה לא טמנה את ידה בצלחת. ביולי 2016 פרסם שירות הביטחון הרוסי (FSB, הגוף הדומיננטי בקהילת המודיעין הרוסית בכלל ובנושא הסייבר בפרט) כי מערכות המחשבים של 20 ארגונים רוסיים, כולל של הממשלה ומערכת הביטחון שלה, נפרצו בידי "ממשלה זרה", ורמז כי מדובר בקהילת המודיעין האמריקאית.

לסיכום מחקרו מדגיש מנשרי: "מניסיון העבר, פעולת סייבר זוכה לתהודה ויוצרת חקיינים. בין שמטרתם של התוקפים הרוסיים הייתה לסייע לבחירתו של טראמפ או לפגוע באמינותה של קלינטון, ובין שההתקפות כוונו ישירות בידי פוטין או לא - יש להביא בחשבון כי גורמים אלה או אחרים ינסו להשפיע באמצעות פעולות במרחב הסייבר על בחירות דמוקרטיות ועל דעת הקהל במדינות אחרות ובכלל ישראל".

ומכאן ממליץ מנשרי לגורמי ההגנה וקובעי המדיניות בישראל לקדם "תוכנית מקיפה להגנה על מערכות המידע וההצבעה לקראת מערכות הבחירות הבאות". כמו כן עליהם לבחון דרכים "שיאפשרו לדמוקרטיה הישראלית להתמודד מפני הניסיונות לקעקע אותה באמצעות פעולות 'תודעה', המכונות גם 'השפעה על דעת הקהל' או 'לוחמה פסיכולוגית'". ❖

melmanyossi1950@gmail.com