מלחמת הדור הבא

אנשי משמרות המהפכה מנסים להרעיל את המים שלנו, ומיד לאחר מכן נמל איראני סופג מכה. ארגון טרור בשירות טהרן תוקף בית חולים כאן וגורמים עלומים מחבלים בתחנות הדלק בטהרן. אלה לא תרחישים אפוקליפטיים, אלא תיאור המערכה בזירת הסייבר, שמתנהלת כבר שנים, ורק הסלימה מאז שבעה באוקטובר. אל"מ במיל' גבי סיבוני, בעבר מפקד סיירת והיום מומחה סייבר, משרטט את מפת המלחמה הדיגיטלית, ומנסה להסביר למערכות בישראל איך אפשר, בצעדים פשוטים ובעלות אפסית, להדוף את רוב האיומים

← מאיה פולק

לא לענות לשיחות של 0022 או 1866+. הם אומרים את השם שלך ואומרים ללחוץ 1 כדי לקבל עזרה. לא לענות בכלל, יש מתקפת סייבר על ישראל" – זה נוסח ההודעה שהועברה פעמים רבות בקבוצות הוואטסאפ בשעות הבוקר והצהריים בשבעה באוקטובר. התחושה הייתה שמתקפת הפתע שנפתחה בדרום לא מסתפקת בזירה הקרקעית, אלא מתרחבת לזירה נוספת שיכולה להגיע לכל בית במדינה. ההודעות הלכו וצברו תאוצה, עד שבשעה 12:40 נשמעה צפירת הרגעה חלקית: מערך הסייבר הלאומי הודיע שהוא אומנם העלה כוננות, אך "בשלב הזה אין התקפת סייבר ספציפית הקשורה במצב הנוכחי".

ובכל זאת, נראה שהחששות לא היו מנותקים לגמרי מהמציאות. חברת קלאודפלייר, המתמחה בהגנה מפני תקיפות סייבר, פרסמה כעבור שבועות אחדים דו"ח שמראה כי ישראל אכן חוותה מתקפה כזאת בשבעה באוקטובר ובימים שלאחריו. בין השאר נרשמו כמיליון בקשות חיבור לאתרים מסוימים בתוך שנייה אחת – טקטיקה שמטרתה להפיל אותם ולהשבית את פעילותם. בעבר כבר נוטרו התקפות שקשורות לחמאס, אך הפעם ההיקף היה חריג. אחד מיעדי המתקפה היה אתר ארכיון המדינה; הוא הושבת לזמן ארוך, קבצים רבים נמחקו ממנו ועד היום הוא לא שב לפעילות מלאה, כפי שמעיד־מתנצל הטקסט בעמוד הבית שלו. גם בית החולים זיו בצפת עבר מתקפת סייבר, שיוחסה לחזבאללה ולאיראן. 300 אלף רשומות של מטופלים נגנבו באירוע הזה, שהיה ככל הידוע מתקפת הסייבר הרביעית שכוונה בשנתיים האחרונות לבית חולים ישראלי. מערך הסייבר הלאומי המשיך לטעון, הן בתגובה לפרסום ב־ynet והן בדו"ח שיצא בדצמבר, כי חזית הסייבר שנפתחה בשבעה באוקטובר הייתה לכל היותר "פעילות שהתעצמה בהדרגה" ו"מתקפה מהסוג הנמוך ביותר... המשולה לטיפות גשם באוקיינוס".

אל"מ במיל' גבי סיבוני, מומחה ביטחון, סייבר וטכנולוגיה צבאית, נשמע גם הוא מסויג כשהוא מסכם את צבר האירועים שהתרחשו במרחב הסייבר הישראלי בארבעת החודשים האחרונים. "אני לא יודע להגיד אם הייתה 'מתקפה רשמית'", הוא אומר. "בהחלט יכלה להיות, כי חמאס פיתח יכולות סייבר לא מבוטלות. אבל אני לא חושב שלתקוף את ארכיון המדינה היה עוזר איכשהו למתקפת הנוח'בה, ובדרך כלל חמאס עושה בתחום הסייבר דברים שמסייעים לו לממש את מטרותיו בשטח".

בלי לתת רעיונות לאויב, למה כוונתך?

"אם אני חמאס, במקום לחדור לרשומות של בית חולים בצפון אולי הייתי מעדיף לתקוף את משטרת אופקים גם בסייבר. כך הייתי יוצר אמצעי נוסף שיתמוך במתקפה שלי בשטח.

"אחד מתרחישי המלחמה שכתבתי יחד עם יובל (תא"ל יובל בזק, עמיתו למחקר – מ"פ) דיבר על פעולה צבאית משולבת של חזבאללה, חמאס, איראן וגם חלק מערביי ישראל וערביי יהודה ושומרון, במטרה לקעקע את מדינת ישראל. בתרחיש כזה, איראן הייתה פותחת במתקפה נרחבת בממד הסייבר. במתקפת הטרור בשבעה באוקטובר, איראן אולי הייתה מעורבת מבחינת הרוח וההכוונה, אך להבנתי היא לא הייתה מעורבת בקביעת העיתוי ובצדדים אופרטיביים־טקטיים. לפי ההערכות, גם היא וגם חזבאללה הופתעו באותו היום. בה בעת, מתחת לפני הקרקע יש לישראל מלחמת סייבר תמידית עם איראן, ולא רק איתה. רוסיה, שתומכת באיראן, עובדת פה בארץ, פועלת לאסוף ולגנוב מידע, וחשוב לומר זאת: גם לרגל. בואו לא נתבלבל, גם ידידים שלנו עושים את זה, ואני מניח שאפילו ידידינו הטובים ביותר פועלים פה במרחב הסייבר ואוספים עלינו מידע".

ונניח שהותקפנו ואתרים חשובים נפרצו, מה אפשר לעשות כדי להחזיר אותם לתפקוד במהירות המרבית?

"אחד הדברים החשובים הוא להבין את המצב, וזה דורש זמן, כי במקרים רבים תקיפת סייבר היא אירוע מזדחל. אפילו בשבעה באוקטובר, כשתקפו אותנו בשטח בגלוי, לקח שעות עד שבמטה הכללי הבינו את גודל המתקפה. בסייבר זה מסובך עוד יותר. עובר זמן עד שאתה מבין שצבר אירועי שיבוש קשורים זה לזה, וקשה לדעת מתי הצפרדע הזאת כבר בתוך המים הרותחים. צריך לפתח כלים קוגניטיביים להסתכל על אירועים, לבנות מודעות מצבית. זה גם עניין של איך אתה מתנהל במשבר.

"חשוב לבנות תפיסה שכוללת נהלים שגם יתורגלו בעוד מועד. זה רצף של כמה פעולות: לבנות את תפיסת ניהול המשבר – מהיכולת

"לוקח זמן לזהות שאתה תחת מתקפת סייבר, כי במקרים רבים זה אירוע מזדחל. אפילו בשבעה באוקטובר עברו שעות עד שבמטה הכללי הבינו את גודל המתקפה. בסייבר זה מסובך עוד יותר. עובר זמן עד שאתה מבין שצבר של אירועי שיבוש קשורים זה לזה, וקשה לדעת מתי הצפרדע כבר בתוך המים הרותחים"

"מערכת ההתרעה כשלה לא בגלל היעדר מידע, אלא בשל ניתוח שגוי ומוטה". סיבוני

צילום: אריק סולטן

"יש חברות לא ישראליות שמייצרות דברים דומים ל'פגסוס', אבל הן לא נפגעו. אני לא חסיד תיאוריות קונספירציה, אבל יש פה כנראה מהלך מחושב ששם את ישראל במוקד, כדי לפגוע ביכולת הישראלית. הסיבות מגוונות, וכולן צבועות בצדקנות"

לזהות שאתה נמצא באירוע, לבנות את כל המערכת הארגונית ולהגדיר מי אחראי על מה, כי אם כולם עושים הכול לא קורה כלום. גם ברמה הלאומית וגם ברמה הארגונית צריך לקבוע מי אחראי על תקשור המשבר הזה לבעלי העניין – לבעלי המניות אם מדובר בעסק, או לציבור הרחב. צריך לתרגל באופן שוטף תרחישים של מתקפת סייבר רחבה, ובצבא כבר יש תרגילים כאלה. כך נבנית מערכת נהלים שאתה משפר אותה כל הזמן".

סכנת השתעבדות

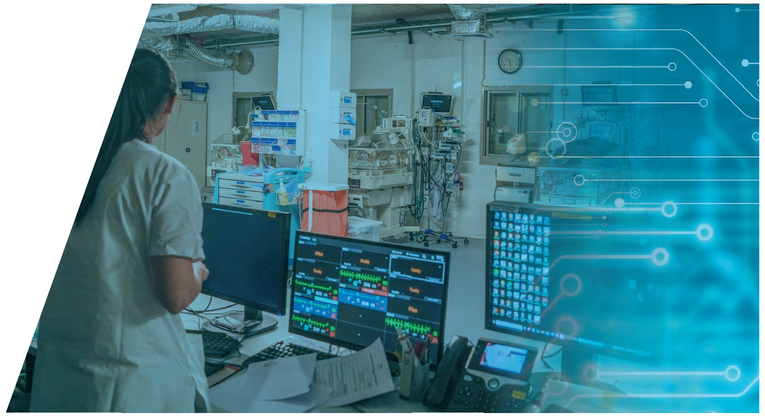
יחד עם שותף אחר שלו, פרופ' קובי מיכאל, כותב סיבוני בימים אלה מסמך חזון ותשתית רעיונית למדינת ישראל שאחרי המלחמה. השם שנבחר לייומה לקוח מעולם התוכנה: "ישראל 2.0", רמז לעדכון הגרסה שהמדינה תידרש לו. "חזון ישראל 2.0 נוגע בכל מרכיבי החיים שלנו כמדינה, ולכן גם בסייבר ובדרכי ההתמודדות של המדינה עם האיומים במרחב הזה", אומר לנו סיבוני על ההצעה שהם כותבים בתוך עמיתי מחקר בכירים במכון משגב לביטחון לאומי ולאסטרטגיה ציונית. "עלינו להיות מאורגנים לתרחיש של מתקפת סייבר רחבה שתתקיים כמהלך מלווה לפתיחה של מלחמה, או במצב חירום ביטחוני או אזרחי. ישראל צריכה לגבש אסטרטגיה הגנתית מקיפה להתמודדות עם מגוון תרחישים המורים אך ריאליים, ולגזור ממנה את תהליכי בניין הכוח בהקשרי כוח אדם, אמצעים וטכנולוגיה, התארגנות המערכת הלאומית ושיתוף פעולה בינלאומי. לבסוף עליה להטמיע את האסטרטגיה באימונים ותרגילים. כדי להמשיך להוביל בתחום הטכנולוגיה לצד שמירת הביטחון, יש לחלק נכונה את משאבי ההון האנושי שלנו בין המרחב הטכנולוגי ובין צורכי ההגנה הפיזית, כלומר הכוחות הלוחמים".

סיבוני, 66, עוסק בייעוץ לצה"ל ולשלל גופי ביטחון. לצד תפקידו במכון משגב הוא גם עמית מחקר בכיר במכון ירושלים לאסטרטגיה וביטחון (JISS) ומכהן כפרופסור חבר בתואר לניהול ביטחון סייבר באוניברסיטת פרנסיסקו דהיטוריה במדריד. ויש לו עיסוק נוסף: נגן גיטרה חשמלית בהרכב רוק, אוסף גיטרות תלוי בחדר העבודה הביתי שלו, מעל אוסף ספרי מלחמה שבולטים בו ספרים על הביטל וגבלס וכתביו של צ'רצ'יל בכריכה אדומה.

כאיש צבא הוא גדל בגולני ופיקד על שתי תוכניות במכון למחקרי ביטחון לאומי בתל־אביב (INSS): התוכנית לצבא ואסטרטגיה והתוכנית לביטחון סייבר. הוא יימד שם שני כתבי־עת אקדמיים, ובמשך השנים פרסם כמה ספרים בנושא סייבר. האחרון שבהם הוא "ישראל ואיום הסייבר – כיצד הפכה מדינת הסטארט־אפ למעצמת סייבר עולמית" (יחד עם ריצ'רד פרידליך ומתי כהן, ראה אור באנגלית).

כשחושבים על הקמת חומת הגנה דיגיטלית, אומר סיבוני, צריך לזכור את מה שנאמר על קו מאז'ינו, קו בר־לב וההומה הסינית: קו המגע לעולם ייפרץ. "אויב נחוש ידע כיצד לחדור למחשב שלך. גם מחשב שנמצא בתוך כור אטומי באיראן, אפשר לחדור אליו בעזרת כסף וטכנולוגיה מתאימה".

לאחר מתקפת שבעה באוקטובר יצא מערך הסייבר הלאומי בקמפיין נגד ה"שַׁתָּקָפת", המחלה של שיתוף מידע ברבים בלי לברוק אם הוא אמין. דמות הסבתא (בגילומו של יניב ביטון) שמזהירה כי החות'ים מגיעים על בננות לאילת העלתה חיוך, אבל סיבוני לא מחייך כשהוא מדבר על תכונה אנושית דומה שמסייעת למתקפות הסייבר להצליח – "למשל, פתיחה נמהרת של קבצים. כדי שמתקפה תכה במחשב זה או אחר, מישהו צריך להיכנס להודעת דוא"ל שקיבל או לרשת חברתית, להוריד משם קובץ, ואז לפתוח אותו. במקרים רבים, חסימת המתקפה כרוכה בסך הכול בהגברת מודעות העובדים באמצעות סרנאות והדרכות. זה לא דורש השקעה כספית גדולה, אבל זה הדבר שאני, בכל שנותיי כיועץ בתחום, הכי מתקשה להסביר. אנשים אומרים 'תגיד לי לקנות אנטי־וירוס, אני מבין', אבל את ההתנהלות הנכונה הם מתקשים להנחיל.



המרכיב האנושי במתקפת סייבר הוא מרכזי. מתקן התפלת מים ישראלי. משמאל: בית החולים זיו שהותקף בשבעה באוקטובר

"בתחילת שנת 2021 זכיתי במכרז לבחירת סוקרים למתן שירותי סקר סיכוני סייבר בשני בתי חולים, מטעם חברת 'ענבל', שעשתה עבודה עבור משרד הבריאות וחברת הביטוח הממשלתית. אחד מבתי החולים היה רמב"ם", מספר סיבוני. השבוע הצטרף גם רמב"ם לרשימת המוסדות הרפואיים שייתכן כי נפלו קורבן למתקפת סייבר: לפי הודעה מטעם משרד הבריאות ומערך הסייבר הלאומי, האירוע זוהה ונגבלם ללא שיבוש או השפעה על תפקוד המרכז הרפואי. "רציתי לפעול בבתי החולים הללו בנושא של מודעות העובדים, אבל בסופו של דבר זה לא הסתייע. האירועים שהתרחשו השבוע בבתי החולים היו חלק מהניתוח שהעברתי להם, ואני בהחלט סבור שטוב יהיה להעמיק את ההגנה על מוסדות כאלה. יש שם דברים שהם לא בשליטתנו, אך המרכיב המרכזי הוא זה האנושי".

מתקפת סייבר, אומר סיבוני, עשויה לגרום לרבי מסוים להיחזות כדבר אחר; זו יכולה להיות זהות השולח של דוא"ל תמים לכאורה, וזו יכולה להיות רשומה בנקאית או רפואית שמציגה מידע שלנו. אנחנו מצידנו צריכים לעשות את זה לאויבים שלנו, ועם זאת אני תמיד אומר: מדינת ישראל צריכה להפנות את מרב המאמצים להגנה, מעט למודיעין ועוד פחות מכך להתקפה. ההגנה היא הדבר המרכזי".

לאחרונה דווח על מיזוג טכנולוגי לפיתוח בינה־על מלאכותית שתוכל אפילו לקבל החלטות ביטחוניות. סבור לחניה שהתחום הזה מגיע גם למערכת הביטחון הישראלית, אבל עם כל הכבוד לפיתוחים, מה קורה אם אין לך המידע המדויק להזין במכונה?

"זאת בדיוק הסכנה שאני מדבר עליה – ההשתעבדות למכונות. צריך לזכור תמיד את המשפט הכי חשוב בתוכנה ומכונות 'חושבות': Garbage in, garbage out".

מכה של ילד בגן

גם אם טרם פרצה מלחמת סייבר כוללת, דו"ח של מערך הסייבר הלאומי מדצמבר 2023 מלמד שאופי הפגיעות בארגוני ומוסדות ישראליים בחודשים האחרונים משקף במשתו את אופייה של מתקפת הטרור בשטח: רצון להשפיל, להפעיל טרור פסיכולוגי ולשבש את החיים. לפי הדו"ח, תקיפות הסייבר מאז שבעה באוקטובר "מכוונות למטרות נזק (CNA), בניגוד למיקוד שזוהה לפני הלחימה ובתחילתה, שהתאפיין יותר במתקפות למטרות ריגול ונגבת מידע (CNE)". אחת מדרכי הפעולה היא הפעלת "כופרות" – תוכנות שמשתלטות על מאגר מידע וגורמות ל"הולגת המידע החוצה (לשם קיום משא ומתן על המידע, השפלת הקורבן, התדרבות מצד התוקף) או פשוט מחיקה לשם גרימת נזק". עוד מציין הדו"ח שימוש בטכניקות דומות לאלה שמופעלות במלחמת אוקראינה־רוסיה, כגון "לוחמה פסיכולוגית (תודעה) כאמצעי להדהוד מתקפות סייבר, ושימוש ברשתות חברתיות להעצמת ההשפעה".

המתקפות על ישראל נועדו לא רק לפגיעה ישירה במחשבים "ישראליים", מסכים סיבוני, אלא גם להפעלת טרור פסיכולוגי ודמוליזיה. את המטרה הזאת אפשר להשיג בין השאר באמצעות "דיפ פייק" – טכנולוגיות בינה מלאכותית שיודעות לזייף באופן משכנע צילומים או קטעי קול. "אנחנו מדברים בהקשר הזה על 'מבצעי השפעה' – פעילות שמטרתה להשפיע על המחשבות שלך. זה קיים לא רק בסייבר, עושים את זה כל הזמן, גם העיתונים והטלוויזיה משחקים לנו במוח. אני יכול עכשיו לדאוג שכאשר תיכנסי לאתר חדשות מסוים, רק את תקבלי יידיעות מסוימות שהכנסתי לשם, ומי שעומד לידך לא יקבל אותן. העולם הזה בעייתי מאוד, וגם נושא ההגנה מפניו מורכב ביותר. זה יכול להגיע לקיצוניות למשל בתקופות של בחירות, כי אז עלול מישהו להשפיע באמצעות סייבר על איך תיראה הנהגת המדינה. לא מדובר רק על פעולת סייבר קלאסית, כלומר פגיעה במהלך התקין של הבחירות או שיבוש התוצאות. יש עולם אחר, 'רך' יותר, שבו פועלים באופן שיטתי כדי להשפיע על מה שאנשים חושבים ועל מה שהם יצביעו לבסוף. כשזה נעשה בגבולות השיח הפוליטי המדינתי, זה פחות בעייתי בעיניי, אם כי יהיו שיחלקו עליי".

אתה באמת לא רואה בעייתיות בכך?

"אני טוען שאי אפשר למנוע את זה. השפעה על דעות פוליטיות בתוך המדינה היא לגיטימית, והיא חלק מהשיח הציבורי. לעומת זאת כשרוסיה מנסה להתערב למשל בבחירות בגרמניה, זה כבר אסור. צריך ליצור בידול בין התערבות זרה למה שקורה בפנים, בין המפלגות. זה מסובך מאוד, אבל ניתן לביצוע. אפשר לבנות מנגנון שיאסוף מידע ויזהה מה מקור הקמפיין, ואז לחשוף זאת לציבור ולבקש מהרשתות החברתיות להסיר את הפוסטים הבעייתיים".

הן לא תמיד עושות לשתף פעולה עם בקשות באלה.

"אתה יכול לבקש מהן, ואתה יכול לחוקק חוקים שמחייבים אותן לוודא שגולשים מהארץ לא יראו את החומרים האלה. אפשרות נוספת היא לתקוף בסייבר את מי שעשו לך את זה. לפעול מולם, לסכל אותם".

מאז שבעה באוקטובר אנחנו שומעים גם על האקרים פרו־ישראלים שתוקפים אתרים של איראן ושל חמאס. ישראל צריכה לעודד פעולות בזאת?

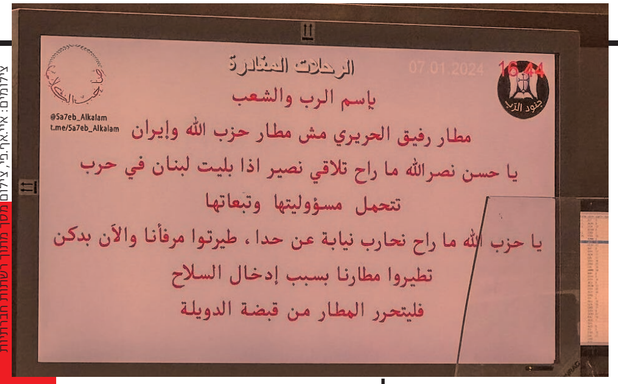
"העמדה שלי היא שהפעלת כוח צריכה להיות מתואמת, מסונכרנת ומבוצעת בידי המדינה. אם רוצים, שייקחו את האקרים האלה וישלמו להם משכורות. הפעילות הפיראטית הזאת סתמית בעיניי. זה כמו שתושבי העוטף, בעקבות ירי רקטות מעזה, היו מחליטים שהם מחזירים לחמאס בירי רקטות משלהם".

לדברי סיבוני, גם פעולות סייבר התקפי שיחסו לישראל בפרסומים זרים, לא תמיד קלעו למטרה. לדוגמה הוא מזכיר את התקלה המסתורית שפקדה בדצמבר 2023 את תחנות הדלק באיראן, ושיבשה את תפקודן: 70 אחוזים מהן הושבתו. "זה דרמטי אולי בתור הדגמת יכולת, החיים שם השתבשו מעט, אך לא יותר. האם השתנה משהו והשגנו איזו הרתעה? זה יותר כמו ילד בגן שקיבל מכה ומחזיר מכה".

הוא מציין שהאיראנים מצידם ניסו לא רק לשבש את מהלך החיים התקין, אלא אף לגרום לאסון. "ב־2020 הם ביצעו מתקפת סייבר שניסתה להשתלט על מתקני מים בישראל ולשבש את הזנת הכלור למי השתייה. בתנאים מסוימים זה יכול להיות קטלני. הם הצליחו לחדור לכשישה מתקנים, אבל לא הצליחו לפגוע בפעילותם, כי התקפים לא עובדים רק על מערכת אחת; יש מערך הגנות שלם שבנוי גם על הגנה מכנית. זמן קצר לאחר מכן נודע שגורם עלום שיבש את פעולת הנמל הראשי של איראן למשך שבוע. פעולה כזאת אני יכול להבין: הגורם הזה רצה להוראות שיש לנו יכולות ולא כדאי להתעסק איתנו. אבל גם זה לא שינה הרבה. כמו בסיפור של תחנות הדלק, כך גם כאן – יש חילופי מהלומות, אבל הן לא באמת משפיעות על התמונה הגדולה של המערכה".

דו"ח של מייקרוסופט שפורסם השבוע מאשש רבות מהערכותיו של סיבוני. מומחי החברה לא מצאו סימנים לתיאום מוקדם בין איראן לחמאס בתחום הסייבר, אך מיד לאחר פריץ מתקפת הטרור בשבעה באוקטובר החלו

"מרחב מלחמה נוסף". השקת ספינת מלחמה איראנית. משמאל: הודעת מתקפת הסייבר על מסכי שדה התעופה בביירות, בחודש שעבר



"אם למשל בנק הותקף על ידי איראן, מערך הסייבר לא היה יכול להיכנס למערכות שלו ולבדוק מי התקיף אותו, אלא אם הבנק הסכים לכך. בימים האלה, במתח בין פגיעה בפרטיות ובין הביטחון הלאומי, אני חושב שצריך לתת משקל גדול יותר לביטחון. ישראל שומרת על איזון נכון בנושא, גם לעומת מדינות אחרות בעולם"

קבוצות האקרים מאיראן לנסות לשבש אתרים ישראליים. אם בתקופה שקדמה למלחמה נרשמה התקפה כזאת אחת לחודשיים, בחודש אוקטובר לבדו זוהו 11. במקביל פתחה איראן ב"הפצצה תעמולתית" – הן ברחבי העולם והן כאן בארץ. חשבונות מזויפים ברשתות החברתיות הפיצו מסרים נגד הממשלה ובפרט נגד נתניהו, תוך שהם משתמשים גם בתמונות שנוצרו בבינה מלאכותית.

אם לא באמצעות מהלומות־נגד קטנה מה ישם, ביצד אפשר להשתמש בסייבר ההתקפי בנשק של ממש?

"הוא צריך להיות משולב במענה הכולל של מדינת ישראל. אם עכשיו אנחנו תוקפים בעזה, אנחנו צריכים להפעיל במקביל גם את הסייבר. הוא יכול להיות כלי במבצעי תודעה, בשיבוש התקשורת של האויב וגם בשיבוש אמצעי לחימה. אני מניח שמי שאמון על הנושא במערכת הביטחון עושה את הדברים".

בסכסוך הישראלי־הפאלסטיני יש גם אירועים של פעולה פיזית נגד כלים ממוחשבים. בדקות הראשונות של מתקפת שבעה באוקטובר, מזכיר סיבוני, הפאלסטינים בעזה ניתקו את המצלמות בגדר הרצועה, וכך מנע מהתצפיתניות בגבול לקבל תמונה בזמן אמת. גם זאת מתקפת סייבר, הוא אומר, אף שהיא לא מתבטאת בפריצה למחשב, אלא בחבלה בציוד. ארבע שנים קודם לכן, במבצע "גן סגור", הפציץ צה"ל מבנה בעזה ששימש את חמ"ל יחידת הסייבר של המאס. כך סוכלה מתקפת סייבר שנועדה "לפגוע במרקם החיים בישראל", כפי שנכתב אז. "יש נטייה לחשוב שאם מתקיפים אותך בסייבר, אתה צריך להגביל את עצמך למענה באמצעות הסייבר בלבד", אומר סיבוני. "בפועל זה לא כך. אם האויב שולח מטוסים להפציץ אותך, לא חייבים לענות להם במטוסים משלך; אפשר גם לתקוף את שדה התעופה ו'לדפוק' אותו בארטילריה. גם באיומי סייבר אפשר לפגוע בנשק קינטי. זו עוד פלטפורמה, זה עוד מרחב מלחמה, ואם אתה פוגע בו – לא משנה באיזו דרך עשית זאת".

הדו"ח של מערך הסייבר הלאומי מצייו היבט נוסף של פעילות המאס שעבר למרחב הווירטואלי: בשנים האחרונות החל ארגון הטרור להשתמש במטבעות דיגיטליים כדי לממן את פעילותו. "שותפים במערכת הביטחון בישראל זיהו ותפסו ארנקים דיגיטליים שהכילו עשרות מיליוני דולרים במגוון רחב של טוקנים (מטבעות קריפטוגרפיים) אשר המובילים ביניהם הם ביטקוין, איתריום וטרון", נכתב בדו"ח. "הסיפור הכלכלי הוא מרכזי, והמערכה בנושא הזה צריכה להיות ארוכת טווח", אומר סיבוני. "למוסד היה ארגון מעצמו שעסק בתחום הזה במשך שנים, ואני מניח שישראל ממשיכה לפעול לסיכול כספי טרור. תפיסת כספים היא מהכלים הכי חשובים כשרוצים למנוע טרור ולפגוע בחמאס ובחזבאללה".

מכל שמתגלה היקף המנדטים האימתניות של המאס ברצועה, גוברת ההערכה שבספי המזוזוזות מוקצר לא היו יכולים להספיק לבנים לפרויקט הזה. האם אתה סבור שישאר הכסף הניע בדרכים דיגיטליות?

"בהחלט יש להניח ששיטות כאלה שימשו את המאס. הם ניצלו כל מה שהמדע סיפק, אין לי ספק בזה".

ביטחון גובר על פרטיות

בהרצאה שנשא בספטמבר מטעם מכון ירושלים סיפר סיבוני על מכשול שעומד בפני חברות הסייבר הישראליות, גם אלה העוסקות בטכנולוגיות הגנה: לאורך שנים וגורמים פוליטיים במדינות שונות. "יש חברות לא ישראליות שמייצרות דברים דומים, אבל הן כמובן לא נפגעו. אני לא חסיר של תיאוריות קונספירציה, אבל יש פה כנראה מהלך מחושב ששם את ישראל במוקד, כדי לפגוע בסופו של דבר ביכולת הישראלית".

מי עומד מאחורי המהלך? אם מדובר בארה"ב, מה היא מנסה להשיג בכך?

"לדעתי קשה להניח שמהמהלך הזה לא נועד לפגוע בישראל ובחברות האמורות. הסיבות יכולות להיות רבות ומגוונות, וכולן צבועות בצבעי צדקנות".

לצד זאת סיבוני מדבר על חשש מהאפשרות שטכנולוגיה שפותחה במערכת הביטחון הישראלית תגיע גם לידיים אירניות. הדבר יכול לקרות למשל אם בוגרי מערך הסייבר בצה"ל יעברו בחברה בחו"ל, יביאו לשם ידע שרכשו בצבא, ואותה חברה תמכור את הטכנולוגיה לאויב. "זה נושא בעייתי ולא פשוט", הוא אומר. "אין כאן במדינה מנגנון רציני לניהול קניין רוחני שפותח במסגרת השירות הצבאי. אנחנו צריכים לחשוב כיצד לבנות מנגנון שכזה".

בכלל, סיבוני ניסה לגרום למדינת ישראל לקבוע רגולציה בנושא הדרישות של הגנת הסייבר, אך ללא הצלחה. ארגוני צבא וביטחון קובעים לעצמם את הרגולציה בנושא, הוא אומר, ותשתיות הכרחיות מקבלות הנחיה ממערך הסייבר הלאומי כיצד להגן על עצמן, אך ככל שיותר מטה מבחינת קריטיות הארגון למרקם החיים הלאומי, ההגנה הולכת ומתרופפת.

"אין במדינה מגנון לניהול קניין רוחני שפותח בשירות הצבאי". חיילים במרכז שליטה סייבר

צילום: יהושע יוסף

"אם עכשיו אנחנו תוקפים בעזה, אנחנו צריכים להפעיל במקביל גם את הסייבר. הוא יכול להיות כלי במבצעי תודעה, בשיבוש התקשורת של האויב וגם בשיבוש אמצעי לחימה. אני מניח שמי שאמון על הנושא במערכת הביטחון עושה את הדברים"

צילום מסך

מודעות להתנהלות נכונה היא אתגר. קמפיין ה"שתפת" של מערך הסייבר הלאומי

"במשרדי ממשלה הדבר נעשה ברמה נמוכה יותר, ומתחתיהם משתרע כל עולם העסקים, כלומר רוב החברות במשק; אין בהן הנחיה מספקת כיצד להתמגנן מפני מתקפות סייבר.

"ניהלתי בעבר חברה שביצעה פרויקטים בתחום הנדסת הסביבה, ושם הכרתי את הרגולציה וראיתי שאם אתה רוצה להקים עסק, אתה צריך להראות שאתה לא פוגע בסביבה. כמו בנושא הזה כך גם בסייבר, החוטבות שמוטלות על העסק צריכות להתאים לגודל שלו ולפוטנציאל הפגיעה שלו. אי אפשר לעשות גזרה שווה בין עסק קטן ובין מפעל התפלה, חברת תרופות או תחנת כוח. הצעתי לבנות מנגנון שידע לקטלג את סוגי החברות והגופים במדינה, כך שכל אחד יידרש להגנה המתאימה לו. אם הפגיעה בך עלולה להקרין ברמה הלאומית, אתה תהיה נתון לרגולציה ברמה המרבית.

"המדינה תוכל לאפשר לעצמה כלי בקרה נוספים כדי לוודא שמיזמים מסוימים יעמדו בקריטריונים, ובמקרים מסוימים אף תוכל לדרוש מבעלי עסקים פרטיים להגיש תסקיר עמידות קיברנטית ולחייבם למלא אחר הנחיות הביטחון. המדינה היא שתקבע את הנורמות, ותגדיר 'משפחות כלים' להגנה שכל עסק יוכל לבחור מתוכן. אם לא יעשה זאת, ריישינו עלול להישלל. הכלי המרכזי שאני מציע להשתמש בו הוא חוק רישיוי העסקים, שכבר קיים. לא צריך לחוקק שום דבר חדש".

או למה לא עושים זאת?

"התהליכים הבירוקרטיים לוקחים זמן, וזה טבעי. צריך גם להגיד ביושר שרגולציה היא מנגנון מדכא עסקים. צריך למצוא איזון בין עידוד רכישת הגנות ובין עניינה של מי שלא עושה זאת. לתפיסתי, מערך הסייבר צריך להוביל את זה, אבל זה לא קורה".

כלי אחר שהיה יכול לסייע בעניין הוא "חוק הגנת הסייבר ומערך הסייבר הלאומי", שעד כה לא הושלמה חקיקתו. מערך הסייבר הלאומי, שהוקם ב־2015 וכפוף למשרד ראש הממשלה, מופקד כיום על אבטחת מידע והגנת מרחב הסייבר במדינה, על בניין הכוח ועל ביסוס עוצמתה של ישראל בתחום. על אף כל ההגדרות הללו, הוא מוגבל ביכולותיו לפעול. "כרגע, אם בנק הותקף בידי איראן, מערך הסייבר לא יוכל להכנס למערכות שלו ולבדוק מי התקיף אותו, אלא אם הבנק מסכים לכך", מסביר סיבוני. "החוק המוצע מגדיר את סמכויות מערך הסייבר לסכל מתקפות, גם אם כוונו נגד גורמים אזרחיים. זה חוק חשוב, אבל החקיקה נעצרה ברגע שהתחילו סכסי הבחירות המרובים".

בנובמבר 2023, בהיערד חוק סייבר, נאלצה המדינה לפרסם תקנות לשעת חירום בנושא. לאחר מכן נוצר "חוק ההתמודדות עם תקיפות סייבר המורות במגזר השירותים הדיגיטליים ושירותי האחסון (הוראת שעה – חרבות ברזל) 2023", שתקף לשבעה חודשים. לפי החוק, אם יוזהה תקיפת סייבר המורה, או כאשר יש חשש לתקיפה שעלולה לפגוע "בביטחון המדינה, בביטחון הציבור או ביכום האספקה והשירותים החיוניים", מוטל על ספק השירותים הדיגיטליים לטפל בכך באופן מיידי. אם לא נקט את הפעולות הנחוצות, אפשר לדרוש ממנו למסור לידי המדינה עותק של החומרים שבידיו, כדי שמערך הסייבר יבדוק את היקף הנזק.

במשך השנים הובע חשש שחוק מעין זה מאפשר לפגוע בסודיות או בפרטיות. "בימים האלה, במתח שבין פגיעה בפרטיות ובין הביטחון הלאומי, אני חושב שצריך לתת משקל גדול יותר לביטחון", אומר סיבוני. "ערך החיים גובר על ערך הפרטיות. אני סבור שישראל שומרת על איזון נכון בנושא, גם לעומת מדינות אחרות בעולם".

שיבת המוחות

במאמריו מדגיש סיבוני את חשיבות עולם ההייטק והסייבר הישראלי כקטר הכלכלה המקומית. לפי דו"ח של 2023*2012 היה קצב הצמיחה הממוצע של מספר העובדים בענף ההייטק פי שלושה מהקצב הכללי במשק... שיעור ההייטק מהתמ"ג היה יותר מ־18 אחוז, כשהתוצר הכפיל את עצמו בתוך עשור ל־290 מיליארד שקלים".

גלגליו של הקטר הזה מתנהים כבר בשירות הצבא, כשמלב"ים רבים בעלי נתונים אישיים גבוהים בוחרים לשרת בתחום הסייבר. עם זאת, סיבוני מזהיר שהדבר עלול להביא לפגיעה באיכות כוח האדם שמגיע לחילות השדה ולשדרות הפיקוד. חלק ממשרתי הסייבר עוברים לאחר מכן לעבוד בחו"ל, הוא מציין, "אבל אני לא חושב שיש מגמה של בריחת מוחות. אני גם חושב שאחרי המלחמה אנו צפויים לגלי עלייה, כולל של ישראלים שיחליטו לחזור ארצה".

אתה צופה שהדהשקעות הזרות בחברות הנהך ישראליות יצטמצמו בעקבות המלחמה?

"קשה להעריך, אבל אני מניח שלא יהיה שינוי מהותי, וימשיכו להשקיע בישראל. זה קשור מאוד גם לתוצאות המלחמה. למיטב ניסיוני ומהיכרותי את הנעשה בוול סטריט, גם הביקוש ליחידות קרביות יגדל בעקבות המלחמה. נדמה לי שאחרי שבעה באוקטובר הנוער שלנו מבין טוב מכולם את הצורך והחשיבות של השירות הקרבי".

בצד מחקרי הסייבר כתב סיבוני ב־2019, יחד עם הרמטכ"ל לשעבר גדי אייזנקוט, מסמך של "קווים מנחים לתפיסת ביטחון לישראל". מאמריו דיברו על הצורך לחזור ליסודות, על הדרך לקעקע את האיום האיראני ושלחותיו הטרוריסטיות, ועל ההכרה "להתכונן למלחמה הנכונה" ולהיות התקפיים יותר. היום הוא אומר שהדברים שלו ושל שותפיו נותרו בקול קורא במדבר.

מאמר אחד, שהוא שקד עליו עם יובל בוק ערב המלחמה, נכתב במלאת מאה שנה למאמר "על קיר הברזל" לזאב ז'בוטינסקי. המנהיג הרוויזיוניסטי דיבר בשעתו על הצורך להגיב בכוח נגד הערבים, משום שהם מצידם לעולם לא ישלימו עם קיומו של רוב יהודי בארץ ישראל. עוד לפני פרסום המאמר נודע כי בנו של יובל בוק, גיא, לוחם בגדוד 51 של גולני, נהרג בקרב בקיבוץ כיסופים.

"לצערנו, המציאות הקדימה אותנו", כותבים השניים בהקדמה חדשה למאמר. "באחד הימים השחורים בתולדות עמנו, נפער סדק ב'קיר הברזל', כשלצירו פצע אישי... קו אדום נמתח בין פרעות קישינב לטבח בקיבוץ בארי, והוא נובע מיסודות רבים שהתעתרו בתפיסת 'קיר הברזל'. אולם מבעד לאפלה של אותה שבת שחורה בצבצו נקודות אור, התגלתה גבורתו של הישראלי... המבחן הצפוי לנו בחודשים הקרובים ידרוש את כל תעצומות הנפש של החברה הישראלית כדי לגרוע את היד שהונפה מעל ראשה ולסגור את הסדקים שנפערו בקיר הברזל".

"כולם חשבו שיש פטנטים, להילחם בלי להילחם", אומר סיבוני. "בדרך הקשה מתברר לנו שצריך להילחם דרך הרגליים, ללכת בבוץ. הלחימה היא גם באמצעות הסייבר כמובן, אבל 95 אחוזים של המאמץ הם בסנקים המלוכלכים, בחומרי נפץ שיכולים להתפוצץ גם כשאנחנו לא רוצים. ככה נראית מלחמה, ולא התכוננו למלחמה הזאת. לא בנינו את הצבא בצורה נכונה, לא הסתכלנו על המענה האסטרטגי הנכון מול האויבים שלנו, וכך הגענו להיכן שהגענו. עכשיו אנחנו חייבים לעשות תיקון". ■

"הפעלת כוח צריכה להיות מתואמת, מסונכרנת ומבוצעת על ידי המדינה. אם רוצים, שייקחו את ההאקרים שפעלו נגד איראן וישלמו להם משכורות. הפעילות הפיראטית הזאת סתמית בעיניי. זה כמו שתושבי העוטף, בעקבות ירי רקטות מעזה, היו מחליטים שהם מחזירים לחמאס בירי רקטות משלהם"

לתגובות: dyokan@makorrishon.