מגמות אסטרטגיות בתחום הסייבר

דודי סימן־טוב

העולם עובר לסביבה הדיגיטלית, כאשר בתקופת משבר הקורונה הואצו תהליכי דיגיטליזציה וגברה תלותם של המשק הכלכלי ושל אזרחים בשירותי מחשוב מרכזיים. כך העולם הפיזי נעשה פגיע ורגיש הרבה יותר מבעבר לתקלות או לפגיעה זדונית. ואכן, ניכרת עלייה בהיקפים ובגיוון של פעילות עוינת בסייבר. בהתאם לכך גובר אתגר ההגנה על מרחב הסייבר, המדינתי והאזרחי כאחד.

בשנה האחרונה נרשמה עלייה במנעד ובהיקף תקיפות הסייבר, הן לתכליות אסטרטגיות דוגמת ריגול ושיבוש מערכות, הן לתכלית כלכלית ותודעתית ואף לתקיפות של חברות אבטחת מידע. באחרונה התרחבה רמת החיכוך הקיברנטי בין מדינות, וכן גברה פעילותם וגם העזתם של גורמי פשע מקוון. בהתאמה, ניכרה גם תגובה אקטיבית ואגרסיבית מצד גורמי הסייבר במדינות המותקפות. על רקע זה הופך מרחב הסייבר לתווך עימות אסטרטגי. העימות בין ארצות הברית למדינות אחרות ובראשן סין, איראן ורוסיה החריף, ובחלקו הפך גלוי. מרחב הסייבר כזירת עימות כולל גם את ישראל, ובקיץ 2020 הוחלפו מהלומות קיברנטיות בינה לבין איראן. למעשה, הסייבר עתיד להפוך לרכיב מרכזי במסגרת המערכה שבין המלחמות — המב״ם.

על רקע מגפת הקורונה נרשמה עלייה דרמטית בתקיפות סייבר ודיס־אינפורמציה על מערכות הבריאות ועל גופי פיתוח החיסונים. נוסף על כך, נוכח המעבר האינטנסיבי של מגזרים רבים במשק לעבודה מהבית ולצריכה מרחוק הואץ תהליך דיגיטליזציה, אך זאת באופן לא מתוכנן ולא סדור. לפיכך עלה במידה ניכרת השימוש בתשתיות דיגיטליות ובראשן שירותי ענן, המהווים יעד מרכזי לתקיפה. מכאן נובע הצורך בארכיטקטורת סייבר מתאימה לעידן של עבודה מהבית וצריכה מקוונת, שצפויות להישאר בתוקף גם כשתיבלם המגפה.

יעד מרכזי לתקיפות סייבר, בשילוב מסעות דיס־אינפורמציה, הם תהליכי בחירות במדינות מערביות. כלקח מניסיונה של רוסיה להשפיע על הבחירות לנשיאות ארצות הברית שנערכו ב־2016, ארגוני סייבר מדינתיים ותאגידי המדיה החברתית סייעו בסיכול ניסיונות ההשפעה, ולקראת הבחירות לנשיאות ב־2020 הם אכן היו בהיקף נמוך מאשר בעבר. מגמה זו של שיבוש תהליכים דמוקרטיים צפויה להימשך ואף להתחזק, הן במערכות בחירות והן בתקופות שביניהן, תוך פעילות ענפה ברשתות החברתיות, שימוש ביכולות תקיפה טכנולוגיות וכן זיהום השיח.

אשר לזירה הכלכלית, ב־2020 נרשמה עלייה של 300 אחוזים ביחס לשנה הקודמת בתקיפות סייבר, במיוחד תקיפות כופרה, המבוצעות על ידי גורמים מדינתיים או גורמי פשיעה. תגובת המדינה המותקפת היא סירוב לקבל את דרישת התוקפים, ולצד זאת הגברת הפעולה האקטיבית נגדם. ואולם קשה לאכוף מדיניות מחייבת בהקשר זה, ורבים מהמותקפים נכנעים לדרישות. אחת התוצאות של התרחבות היקפה של תופעת התקיפות מסוג זה היא עלייה ניכרת במחירי הביטוח.

היכולות המתפתחות של בינה מלאכותית ושל ׳האינטרנט של הדברים׳ — שבאות לידי ביטוי למשל בכלי רכב, ברחפנים, בערים חכמות ובבתים חכמים — יוצרות פוטנציאל לתקיפה, שיבוש שגרה וסיכון חיים, והדבר מחייב התארגנות הגנתית בהתאם. ניתן לרתום יכולות של בינה מלאכותית גם לשם הגנה, אך אלו טרם באו לידי ביטוי ממשי.