המרכז למורשת המודיעין
המכון לחקר המתודולוגיה של המודיעין

כיצד מחשבים קוונטיים יעצבו את הבטחון הלאומי?

ד״ר שי הרשקוביץ

בחודש אוגוסט האחרון, חוקרים מחברת גוגל פרסמו 'בטעות' מחקר הטוען, כי הם השיגו ״עליונות קוונטית״ על מחשבי-על. לפני מספר ימים פרסמה גוגל הודעה רשמית, לפיה עליונות כזו אכן הושגה, חרף טענות, כי המחקר סובל מבעיות מדעיות קשות. אם הטענה נכונה, ייתכן ואנחנו עדים לפריצת דרך טכנולוגית מסוג ומסדר חדש, בעלת השלכות דרמטיות על הבטחון הלאומי. מומחים טוענים, כי מחשוב קוונטי צפוי לערער צבאות ועסקים, בעיקר מאחר והם יהפכו את מערכות ההצפנה הנוכחיות לבלתי-רלוונטיות. אך הבשורה המעניינת לבטחון לאומי ובמיוחד לארגוני ביון, דווקא יכולה להיות חיובית.

מהו מחשוב קוונטי?

מחשוב קוונטי נשען על מכניקת קוונטים - תחום מבוסס ומורכב למדי בפיזיקה, שכבר היום נעשה בו שימוש בטלפונים סלולאריים, מכשור רפואי, לייזרים ומוליכי-על (superconductors). אפילו מחשבים ״רגילים״ נשענים בצורה כזו או אחרת על הדינמיקה של אטומים וחלקיקים תת-אטומיים, העומדים בליבת מכניקת הקוונטים.

מחשבים קוונטיים לוקחים את הטכנולוגיה הקיימת צעד קדימה, ומייצרים מעין 'חוק מור' על סטרואידים. מחשבים רגילים משתמשים בחלקים אלקטרוניים זעירים, טרנסיסטורים, המותקנים על שבב (Chip) אחד. באמצעות דחיסת מספר גדול יותר של טרנסיסטורים על שבב, הפכנו את המעבדים הללו למכונות-על המסוגלות לבצע חישובים במהירות חסרת תקדים. 'חוק מור', שנטבע בשנת 1960 צפה, כי מספר הטרנסיסטורים שניתן לדחוס על שבב יוכפל אחת לשנתיים; וכפועל יוצא כוח המחשוב יוכפל אחת לשנתיים. למרות חילוקי דעות מסוימים, מוסכם כי חוק מור צפה בצורה מדויקת יחסית את התפתחות כוח המחשוב משנות ה-60 ועד היום. אך כפי שנראה מיד, מחשוב קוונטי יכול פוטנציאלית להאיץ את המגמה הרבה יותר.

נזכיר: כל טרנסיסטור, בכל רגע נתון, פועל בצורה בינארית: הוא כבוי (0) או פועל (1), אך לעולם לא כבוי ופועל בו זמנית. ל-0 וה-1 הללו אנחנו קוראים ביטים. לעומת זאת מחשבים קוונטיים עושים שימוש בסוג מיוחד של טרנסיסטורים שיכולים להיות או 0 או 1 בו-זמנית! זו תופעה המכונה במכניקת הקוונטים ״סופרפוזיציה״ - הימצאות של חלקיק בשני מצבים שונים בו זמנית.

טרנסיסטורים אלה מייצרים - לא ביטים, אלא קיוביטים (Qubits) - ויכולים להחזיק כמויות גדולות לעין שיעור של מידע מאשר ביטים.

קיוביטים אינם מושלמים ונוטים לסבול מחוסר יציבות; הם רגישים לטמפרטורה ולחות לדוגמא, ולכן חוקרים מפעילים אותם בתנאי קיפאון. וגם אז, הם פחות אמינים מאשר ביטים. לכן, מחשבים קוונטיים חייבים לכלול גם מנגנון לתיקון תקלות - אחת הסיבות לקצב ההתקדמות האיטי של התחום.

אבל אם נצליח לגרום למחשבים קוונטיים לעבוד הם יהיו רבי-עוצמה כל-כך, שמחשבי-העל של ימינו יהיו לעומתם כצעצועים. המאמר שפרסמו חוקרי גוגל מתבסס על מחקר שנערך על-ידי QAI (Quantum Artificial Intelligence Lab), גוגל וNASA, לצד שותפים נוספים. מחברי המאמר טבעו מטבע לשון חדש: 'החוק של נאבין' (Neven's Law), על-שמו של מנהל קבוצת הפיתוח. על-פי החוק, מחשבים קוונטיים יגדילו את כוח העיבוד בצורה אקספוננציאלית (מעריכית) ולא טורית. במקום להכפיל את כוח המחשוב אחת לשנתיים, הם ירבעו את כוח המחשוב בפרק זמן זה. נניח שמחשב רגיל ומחשב קוונטי מתחילים מאותה נקודה: לשניהם שני טרנסיסטורים על שבב. שני השבבים מכפילים את מספר הטרנסיסטורים בכל שנתיים, כך שבשנה החמישית לשניהם יש 32 טרנסיסטורים. אבל בגלל שקיוביטים יכולים להתמודד עם כמויות מידע הרבה יותר גדולות, בכל רגע נתון כוח המחשוב של השבב של המחשב הקוונטי יהיה עוצמתי אלפי מונים מזה של המחשוב הרגיל, בשל יכולת העיבוד חסרת התקדים של המעבד הקוונטי.

לא תרחיש בלהות

בהנחה שממצאי המחקר נכונים, QAI הצליחו ליצור מחשב קוונטי שהצליח להפגין את עליונותו ביחס למחשבי על. למחשב הקוונטי שפותח מעבד בן 53 קיוביט המוכנה 'סיקמור' (Sycamore). החוקרים גילו, כי סיקמור הצליח לפתור בעיה מתמטית מורכבת בדקות ספורות; בעוד שמחשב העל המתקדם בעולם (ששמו אגב, 'פסגה' – Summit), היה זקוק לכמה אלפי שנים בכדי לבצע את אותה המשימה. ניסוי זה היה מוגבל ומלאכותי - יצירת דגימה נכונה ממעגל קוונטום אקראי. מחשבים קוונטים לא ישנו את העולם עד שנצליח להשיג מעבד כללי, שיהיו לו מליונים קיוביטים. בנקודה הזו, כאשר תגיע, כל מה שידענו על מחשבים מתקדמים בני-ימינו, יהפוך להסטוריה עתיקה.

אבל מה יקרה כאשר נצליח לייצר מחשבים כאלה? כמו שרבים טוענים, מחשבים אלה יוכלו לפרוץ את כל מנגנוני ההצפנה הידועים היום, ויהפכו את כל המידע הקיים בעולם לנגיש לכל פורץ פוטנציאלי. תעשיות הטלקום, אבטחת המידע, פיננסים והרפואה הן רק כמה דוגמאות לתעשיות שיוגדרו מחדש עם הופעת המחשבים הקוונטיים. יש אף הטוענים, כי המהפכה תהיה כל-כך גדולה, שגם טכנולוגיה מפציעה אחרת – בלוקצ'יין, הנחשבת לחסינה מפריצות וממניפולציות, תהפוך גם היא למיושנת, כמעט באחת.

סין השיקה לאחרונה תכנית אסטרטגית שאפתנית במטרה להשיג עליונות קוונטית על המערב. המעבדה הלאומית הסינית למדעי המידע הקוונטיים, עשויה להתגלות כמרכז כובד בכל האמור

לעתיד המחקר והפיתוח בתחום. לאור זאת, מומחים לבטחון לאומי מזהירים מהשקעות העתק של הממשלה הסינית במחשוב קוונטי, הם מתייחסים לתרחיש בלהות שכזה.

מעבר לאיום זה, ארצות-הברית ובריטניה פרסמו לאחרונה דוחות הבוחנים את ההשלכות הצבאיות והבטחוניות של מחשוב קוונטי. לדוגמא, יריב יכול לעשות שימוש בסנסורי גרוויטציה מתקדמים (המכונים Quantum Gravimeters) המסוגלים, לפחות פוטנציאלית, לזהות כלי שיט תת-מימיים, בצורה שמכ"מים בני-זמננו אינם מסוגלים. סנסורים קוונטיים אחרים לדוגמא, יוכלו לאתר מטוסים חמקניים, או לסרוק מרחבי ענק בצורה מהירה, לרכוש מטרות ולהעביר את המידע לכלים בלתי מאוישים – בעצמם מונעים על-ידי מחשבים קוונטיים - שיתקפו את המטרות במהירות, ביעילות ובדיוק חסר תקדים.

כבר היום ארצות-הברית מנסה להדביק את ההתקדמות הסינית. בשנת 2017 מדענים סיניים עשו שימוש בהצפנה מבוססת קוונטיים בכדי לשלוח מידע מלווין סיני (Micius) אל תחנה על כדור הארץ, מרחק של 1200 ק"מ. מאוחר יותר הם ערכו שיחת וידאו בת 75 דקות שעשתה שימוש בסוג הצפנה דומה, והצליחו לשדר אותה למרחק של 7500 קילומטר.

אך לא רק ממשלות פועלות להשגת עליונות קוונטית. למעשה, חוד החנית של הפיתוחים הטכנולוגיים נמצא בסקטור הפרטי, כפי שקורא לעתים קרובות עם טכנולוגיות מפציעות אחרות. החדשות על פריצת הדרך של מדעני גוגל רק יעודדו את התחרות ויאיצו את המרוץ. מאמר בכתב בעת NATURE מגלה, כי משנת 2012 משקיעים פרטיים מימנו לפחות 52 חברות העוסקות בפיתוח טכנולוגיית קוונטים. חוץ מגוגל, ענקי הטכנולוגיה האחרים IBM, HP, וגם הענקיות הסיניות Baidu ו-Huawei עובדות גם הן על פריצות דרך בתחום. עם משקיעים מסחריים קופצים יותר ויותר על עגלת המחשוב הקוונטי, סביר עוד פחות שממשלה אחת, גדולה ככל שתהיה, תפתח בחשאי טכנולוגיה ותשיג עליונות מוחלטת שתאפשר לה לשלוט בעולם.

כך או אחרת, מחשוב קוונטי לא יווצר יש מאין ולא יופיע בהפתעה. למרות ההתפתחויות האחרונות, מחשבים קוונטיים לא יהיו נפוצים בעשור הקרוב וסביר שאפילו יותר מכך. מחשבים קוונטיים הם כל-כך מסובכים שסביר יותר שנראה מעבדות ברחבי העולם נאבקות להשיג פריצות דרך וסביר שקצב הפיתוח יתקדם עקב בצד אגודל.

מחשבים קוונטיים לא יהיו נחלתו של צד אחד בלבד. לכן, אלה המבשרים על מותן של שיטות ההצפנה של ימינו, אינם מביאים בחשבון את השימוש שיעשה במחשבים קוונטיים לצרכי הצפנה ולא רק לשבירתה. יש להניח לכן שנצליח להתמודד עם האיום על ההצפנה באמצעות הצפנה מבוססת מחשוב קוונטי, שתהיה חזקה לאין שיעור מהטכנולוגיות הנוכחיות; וסביר שהתקדמות זו תתקיים לצד ההתקדמות ביכולות השבירה של ההצפנה. כך שהמאזן העדין בין אלה המגנים על מידע ולבין אילו המנסים להשיגו, צפוי להישמר. אכן, תקופת המעבר עשויה להיות מבלבלת, אבל לא סביר שנתעורר בוקר אחד לעולם שבו כל המידע שלנו יהיה חשוף ופרוץ לכל. הגיוני יותר שנראה מרוץ חימוש של הצפנה ופריצה, בדומה לזה המתנהל היום ולמעשה, משחר ימי ההצפנה.

מחשוב קוונטי יכול להפוך את העולם לבטוח יותר

באמצעות שיפור אקספוניציאלי של היכולת לעבד כמויות אדירות של מידע, מחשבים קוונטיים עשויים דווקא לתרום לבטחון הלאומי. מחקר של IoT Analytics מלמד, כי כבר היום בעולם קיימים 17 מיליארד מכשירים מקוונים. שבעה מיליארד מתוכם מחוברים דרך האינטרנט של הדברים (IoT). מגמה הזו נמצאת עוד בחיתוליה ובעתיד הקרוב נראה מיליארדי מכשירים נוספים מתווספים ליקום דיגיטלי זה. נניח שארגון ביון מסוים מבקש לדעת מה מתרחש במקום מסוים שבו, על-פי החשש, פועל תא טרור העומד לבצע פיגוע. בהנחה שארגון הביון מסוגל לפרוץ למכשירים אלה (וכפי שחשיפות סנואדן הראו, הביון האמריקני מסוגל גם מסוגל), יהיה לו מעט זמן לאסוף ולעבד את המידע. עם מחשוב קוונטי, פעולות איסופיות וחישוביות כאלו יתבצעו בדקות ספורות, אם לא בשניות.

זה מימד חיובי של מחשוב קוונטי: כוח עיבוד חסר-תקדים זה יאפשר לבצע אנליזה במהירות, וזו בדיוק היכולת שארגוני ביון זקוקים לה בעידן של התפוצצות מידע - התפוצצות שאנחנו נמצאים אך בראשיתה.

ומה יקרה כאשר נחבר בין מחשוב קוונטי ובינה-מלאכותית? דמיינו מחשבים קוונטיים המסוגלים להתמודד עם כמויות בלתי-נתפשות של מידע המשתנה והזורם כל העת, מזהים מידע מחשיד ומשגרים התרעות. דמיינו מערכות כאלו המייצרות תובנות שאנליסטים בני-אנוש לעולם לא יוכלו לגלות.

האתגר האמיתי במחשוב קוונטי אינו טכנולוגי, אלא ארגוני, פוליטי וחברתי ומעל לכל - תפישתי. ארגוני ביון בעולם המערבי אינם מוכנים עדיין לעידן של היפר-מידע המיוצר והזורם במהירות חסרת תקדים. המבנים הארגוניים והתהליכיים שלהם, כולל התפישה הארכאית והלינארית של מעגל המודיעין (איסוף, עיבוד, מחקר, הפצה, היזון-חוזר וחוזר חלילה), עדיין מושלים בכיפה וכבר מזמן אינם מתאימים לעידן הדיגיטלי החדש. המהפכה הדיגיטלית מאפשרת היום להגיב בצורה מהירה הרבה יותר לתמהיל שונה ומורכב של איומים צבאיים, פוליטיים וכלכליים. אך כדי לעשות שימוש מושכל בטכנולוגיות מפתיעות אלו, ארגוני מודיעין חייבים לעבור שינוי דרמטי. בדיוק כפי שהגבולות בין מידע, אחסונו ועיבודו מתבטלים, כך ארגונים אלה חייבים להפוך למהירים, פחות ריכוזיים ופתוחים לצורות חדשות של שיתופי-פעולה עם העולם החיצוני, כמו גם לשיתופי-פעולה חדשים של בני-אדם ומכונות. ואחרון, ניתוח המשמעויות העתידיות של מחשוב קוונטי חייב להיעשות בזיקה לטכנולוגיות אחרות. בדיוק כפי שלא ניתן לדבר על נתוני-עתק (Big Data), מבלי להביא בחשבון בינה-מלאכותית, רובוטיקה או האינטרנט של הדברים (IoT) - כך גם עם מחשוב קוונטי. מדובר במגמה שהיא חלק ממהפכה דיגיטלית רחבה הרבה יותר הכוללת מכלול רחב של טכנולוגיות מפציעות, המשפיעות על ומושפעות ממגמות חברתיות רחבות.

הערת אזהרה לסיום

הבעיה האמיתית הטמונה במחשוב קוונטי אינה קשורה להצפנה ואינה קשורה להופעה של סנסורים חדשים. מחשוב קוונטי יכול להיות סיוט אורווליניי: מעבדים עוצמתיים המאפשרים לממשלות ולארגוני ענק לנטר כל היבט של חיינו ולדווח על כל סטייה מנורמה. כפי שראינו בסרטים וסדרות כמו Minority Report, Person of Interest או 'מראה שחורה', מחשבים מתקדמים מהסוג שמחשבים קוונטיים יכולים לייצר, יכולים בקלות לפגוע בחופש האנושי הבסיסי בטענה שפגיעה כזו נחוצה בשם שמירה על בטחון אישי וקולקטיבי.

זו בדיוק הסיבה שארגוני מודיעין חייבים כבר היום להתכונן למציאות של העתיד, במקום להמתין שמהפכה טכנולוגית זו תתרחש. ארגוני הבטחון הלאומי חייבים להשיג עליונות טכנולוגית במרוץ חימוש דיגיטלי זה, מבלי להקריב את הערכים הבסיסיים של דמוקרטיות מערביות במעלה הדרך. והממסד הפוליטי צריך לעבוד איתם יד-ביד על-מנת להגדיר חקיקה שתגן על בטחוננו, כמו גם על חירויות האזרח הבסיסיות שלנו.