INSS
המכון למחקרי ביטחון לאומי
THE INSTITUTE FOR NATIONAL SECURITY STUDIES
אוניברסיטת תל אביב
TEL AVIV UNIVERSITY

יישומי המחשב הקוונטי

יהושע קליסקי, רות פופלבסקי[1] | 16 בנובמבר, 2026

תקציר

המחשוב הקוונטי נחשב לאחת המהפכות הטכנולוגיות החשובות ביותר במאה ה-21, המבטיחה פריצת דרך דרמטית במקומות שבהם המחשוב הדיגיטלי המוכר לנו כמעט הגיע למגבלותיו הפיזיקליות. בעוד שמחשבים רגילים פועלים באמצעות "ביטים" (מתגים חשמליים שיכולים להיות אך ורק באחד משני מצבים: 0 או 1), המחשב הקוונטי משתמש ביחידות מידע המכונות קיוביטים (Qubits), שקיימות בשני המצבים בו-זמנית. יכולת זו, לצד תכונה המכונה "שזירה קוונטית", המאפשרת לחלקיקים להשפיע זה על זה באופן מיידי בכל מרחק ביקום כולו, מעניקה למחשב כוח חישוב אדיר עם יכולות ביצוע של מיליוני פעולות במקביל. עבור עולם הביטחון הלאומי וטכנולוגיות הנשק מדובר בשינוי כללי המשחק: יכולת פענוח הצפנות, פיצוח הקוד המקובל כיום, הצפנה בשיטת RSA תוך שניות, מציאת קוד מספרי שחבוי בתוך מיליוני קודים בתוך זמן קצר, סימולציות ואופטימיזציית תהליכים. בשל כך הפך המרוץ להשגת עליונות קוונטית (Quantum Supremacy) ליעד אסטרטגי ראשון במעלה עבור המעצמות הגדולות ועבור מדינת ישראל.

לחצו לקריאת החלק הראשון של מאמר זה

הגדרת המושג

במחשוב הקלאסי המוכר לנו יחידת המידע הבסיסית היא ביט, הפועל כמתג חשמלי שנמצא בכל רגע נתון באחד משני מצבים בלבד: 0 או 1. לעומת זאת, במחשב הקוונטי יחידת המידע הבסיסית היא קיוביט (Qubit) – יחידת מידע המבוססת על רכיבים אטומיים או תת-אטומיים (כגון אלקטרונים) המנצלים את עקרון הסופרפוזיציה. תכונה זו מאפשרת לקיוביט להתקיים בו-זמנית במספר רב של מצבים. אם מדובר במערכת בינארית, אזי חלקיק קוונטי יכול להתקיים בשני המצבים (0 ו-1) בו-זמנית בהסתברויות סטטיסטיות שונות, בדומה לאלקטרון שמקובל לדמות אותו לסביבון המסתובב לשני הכיוונים בעת ובעונה אחת. יכולת זו שוברת את הליניאריות של המחשוב הדיגיטלי ומאפשרת למערכת לבצע מספר עצום של פעולות חישוב במקביל, במקום לבצען באופן סדרתי.

תכונה נוספת המעניקה למחשב הקוונטי את כוחו הייחודי הוא השזירה הקוונטית (Quantum Entanglement). מדובר במצב שבו חלקיקים נעשים "קשורים" זה לזה באופן ששינוי במצבו של חלקיק אחד משפיע מייד על מצבו של האחר, ללא תלות במרחק ביניהם. השילוב בין הסופרפוזיציה לשזירה מאפשר ליצור "שערים לוגיים" ומעגלי חישוב מורכבים, המבצעים פעולות על מספר רב של קיוביטים שזורים בו-זמנית ביעילות רבה, מה שמוביל לכוח

---

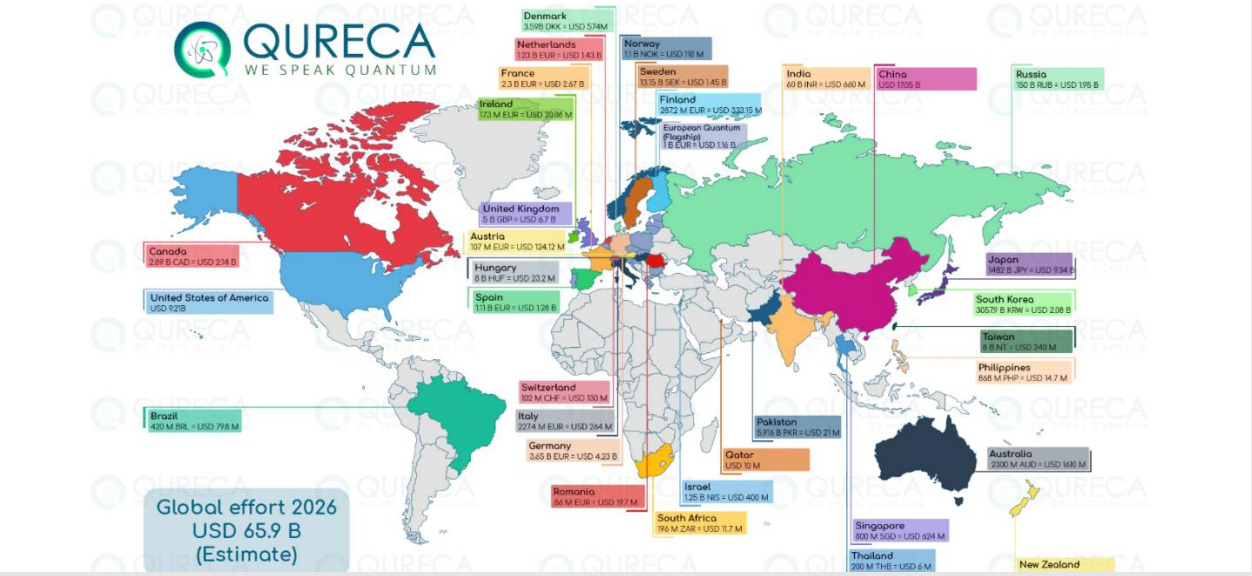
[1] מתמחה בנושאי טכנולוגיה וביטחון.

חישוב הגדל בצורה אקספוננציאלית עם כל הוספת קיוביט למערכת. כתוצאה מכך ובאמצעות אלגוריתמיקה ייחודית, מחשב קוונטי מסוגל לפצח בעיות מתמטיות מורכבות בתוך שניות ספורות – משימות שביצוען במחשב רגיל מצריך אלפי שנים.

הצורך האסטרטגי במעבר למחשוב קוונטי נובע מכך שהמחשוב הדיגיטלי הקלאסי הגיע כמעט למגבלותיו הפיזיקליות והטכנולוגיות; עוצמת החישוב של מחשב דיגיטלי תלויה במספר השבבים ליחידת שטח, אך המאמצים להמשך המזעור נתקלים במחסומים פיזיקליים שהופכים את שיפור הביצועים לקשה ויקר במיוחד. בקנה מידה זעיר זה חוקי הפיזיקה הקלאסית מפסיקים לפעול והמערכות נעשות כפופות לחוקי המכניקה הקוונטית, מה שיוצר פער הולך וגדל בין צורכי החישוב המורכבים לבין היכולות של המחשוב הקיים. המחשוב הקוונטי אינו טכנולוגיה משבשת אלא מהווה מהפכה טכנולוגית המשנה את חוקי המשחק בכך שהוא מאפשר לבצע מספר עצום של פעולות חישוב במקביל, מה שמקצר זמני חישוב של אלפי שנים לשניות ספורות ויוצר שינוי פרדיגמה בתחומים רבים, הן בתחום האזרחי והן בתחומי הביטחון הלאומי והאסטרטגיה הצבאית. יכולת זו של המחשב הקוונטי הופכת את הטכנולוגיה ליעד אסטרטגי עליון, שכן היא מעניקה יתרון מכריע ביכולת לפצח הצפנות, לנהל לוגיסטיקה מורכבת ולבצע סימולציות של שדה הקרב העתידי – משימות שהמחשוב הנוכחי כבר אינו מסוגל להתמודד עימן ביעילות.

המרוץ בעולם

התרשים להלן ממחיש את ההשקעות העולמיות בנושא הקוונטי, במיליארדי דולרים



מקור: Quantum Initiatives Wordwide, June 2026

דוח עדכני של Qureca מעריך את היקף ההשקעות הגלובלי בטכנולוגיות קוונטיות בשנת 2026 בכ- 65.9 מיליארד דולר.

המרוץ להשגת עליונות קוונטית הפך יעד אסטרטגי עבור המעצמות הגדולות, המזהות בטכנולוגיה זו מפתח לעליונות צבאית וביטחונית בשדה הקרב העתידי. גודל שוק המחשוב הקוונטי הוערך בשנת 2024 בכ-1.3

מיליארד דולר, והצפי להיקפו ב-2029 הוא כ-5.3 מיליארד דולר. דוח אחר קובע כי קצב הגידול הממוצע בשנים 2026-2032 הוא 18.3 אחוזים, כאשר נתח השוק הצומח ביותר בשנת 2025 היה צפון אמריקה (38.5 אחוזים), ומתוכו 21.4 אחוזים בארצות הברית, ונתח השוק המוביל הוא פיתוח חמרה (45.7%). דווח עדכני יותר קובע כי בשנת 2035, נפח השוק של מחשבים קוונטים צפוי להיות 40.45 מיליארד דולר, בקצב גידול שנתי של 36% לתקופה 2026-2035. דוח מפורט של חברת Bain & Company קובע כי הגידול בנפח שוק המיחשוב הקוונטי ישפיע על גידול משמעותי בנפח השוק של ענפים אחרים המשתמשים בין היתר (אך לא רק) בשיטות מחשוב קוונטי, כגון סימולציות לתכנון חמרים ותרופות, אופטימיזציית תהליכים, לימוד מכונה והצפנה. עם הבשלת הטכנולוגיה של החישוב בהיבטים של יציבות קיוביטים ותיקון שגיאות, שוק המחשוב הקוונטי יחד ענפים המשתמשים בחישוב קוונטי צפוי לנוע סביב 100-250 מיליארד דולר עד שנת 2035.

אחת ההנפקות הגדולות בשנת 2026, בסך 1.68 מיליארד דולר היא של חברת קוואנטינום שהיא חברה שנוצרה ממיזוג בין Honeywell Quantum Solutions לבין הסטארט אפ הבריטיCambridge Quantum ואשר מפתחת מחשבים קוונטיים בטכנולוגיית יונים לכודים.

סין משקיעה סכומי עתק הנאמדים בכ-15 מיליארד דולר בתוכניותיה הלאומיות. היא השיגה יתרון בתחומי ההצפנה הקוונטית והתקשורת הלוויינית, כולל הקמת רשת תקשורת חסינת ציתות באורך 1,250 מייל בין בייג'ינג לשנגחאי. מדענים סינים אף חשפו מחשב קוונטי פוטוני המבצע חישובים במהירות העולה מיליארדי מונים על היכולות של המחשוב הקלאסי.

ארצות הברית מגדירה את התחרות עם סין כעדיפות לאומית עליונה ומזרימה מיליארדי דולרים למחקר, פיתוח וחינוך כוח אדם ייעודי. יתרונה המרכזי טמון בשיתוף פעולה הדוק בין הפנטגון וסוכנויות כמו DARPA לבין ענקיות טכנולוגיה כגון גוגל ויבמ. הממשל האמריקאי פועל נמרצות לחידוש יוזמות קוונטיות כדי להבטיח את כושר התחרותיות האסטרטגי שלו מול סין ורוסיה. לאחרונה נמסר כי חברת IBM מתכוונת להשקיע בפיתוח מחשב קוונטי עמיד לשגיאות סך של 10 מיליארד דולר עד שנת 2029, ובנוסף החברה תשקיע עם משרד המסחר סך של 2 מיליארד דולר כל אחד לשם הקמת מפעל קוונטי עצמאי, Anderon. IBM מחזקת את יכולות החומרה במטרה לבנות סביב פעילות הקוונטום מערכות חומרה, תוכנה וכלי פיתוח, בדומה לאופן שאנבידיה בנתה מערכת שלמה סביב המעבדים שלה. חברת Google דווחה לאחרונה (אוקטובר 2026) על אודות פריצת דרך משמעותית בהכנת מצבים קוונטים ושערים לוגיים במעבד Willow, עם זיהוי מוקדם והפחתת שגיאות - פי 40 פחות מאשר ללא יישום השיטה שפותחה. בסיכומו של דבר, הממשל האמריקאי פועל נמרצות לחידוש יוזמות קוונטיות כדי להבטיח את כושר התחרותיות האסטרטגי שלו מול סין ורוסיה.

רוסיה משקיעה אף היא משאבים ניכרים הנאמדים בכ-1.45 מיליארד דולר, במטרה לפתח יכולות מחשוב קוונטי עצמאיות שישרתו את צרכיה הצבאיים. המאמץ הרוסי מרוכז בהבטחת חסינות למערכות ההצפנה הלאומיות שלה ומניעת היווצרות פער טכנולוגי מכריע מצד יריבותיה. טכנולוגיה זו נתפסת במוסקבה כחלק בלתי נפרד מלוחמה מודרנית וכלי חיוני לניהול אסטרטגיה ומודיעין בזמן אמת.

התקדמות כללית במזרח התיכון

אזור המזרח התיכון נמצא בשלביו הראשונים של גיבוש אקוסיסטם קוונטי, כאשר המאמצים המרכזיים מתמקדים בבניית תשתיות מחקר והכשרת הון אנושי מיומן. מדינות כמו איחוד האמירויות וקטר פועלות למצב את עצמן כשחקניות מפתח במרחב האזורי, על ידי יצירת שיתופי פעולה בינלאומיים וחיבור בין האקדמיה

לתעשייה. יוזמות אלו נועדו להקים חממות טכנולוגיות שיעודדו פיתוח פתרונות חדשניים, במקביל לקידום תהליכי התיעוש של הטכנולוגיה באזור.

באיחוד האמירויות נרשמה פריצת דרך עם השקת מעבדה קוונטית חדשה באוניברסיטת אבו דאבי, פרויקט שבוצע בשיתוף פעולה עם קבוצת Vernewell. המעבדה תוכננה לשמש כמרכז לשיתוף פעולה (hub) עבור סטודנטים, חוקרים ומומחים בתחום, תוך שהיא מתפקדת כחממה טכנולוגית שנועדה לעודד יצירת פתרונות חדשניים. מטרה מרכזית של המעבדה היא לקדם את המחקר התאורטי, לצד פיתוח תהליכים תעשייתיים ליישום טכנולוגיות קוונטיות במדינה.

בקטר מתמקד המאמץ האסטרטגי בבניית תשתית ידע רחבה ובהכשרת כוח אדם שיהיה מוכן לעידן הקוונטי (Quantum-ready Workforce). המתמחה לשם כך חתמה אוניברסיטת חמד בן חליפה (HBKU) על הסכם שיתוף פעולה עם חברת Xanadu הקנדית, בטכנולוגיה פוטונית. זהו שיתוף הפעולה הבינלאומי הראשון של המרכז הקטרי למחשוב קוונטי (QC2) מאז הקמתו ב-2022, והוא מעיד על מחויבותה של המדינה להפוך לשחקנית בלתי נמנעת בתחום דרך השקעה בהשכלה ובאימון מקצועי. שדרוג המאמץ האסטרטגי של קטר בנושא טכנולוגיות קוונטיות נקבע בהסכם שנחתם בחודש מאי 2025 בין חברת קוונטינוום (Quantinuum) לבין חברת ההשקעות הקטרית, Invest Qatar, במטרה לפתח יכולות קוונטיות מתקדמות ושיתופי פעולה טכנולוגיים בין שני הצדדים, על מנת לחזק את האקוסיסטם הקוונטי של קטר.

איראן ביססה את מעמדה כשחקנית מובילה במזרח התיכון ובקרב המדינות האסלאמיות בתחום המדע והטכנולוגיה הקוונטית, והיא מדורגת כיום במקום הראשון בכל תחומי הטכנולוגיה הקוונטית. המדינה פועלת על פי 'המסמך הלאומי למדע וטכנולוגיה קוונטית , שהוכנס לתוקף ביולי 2025 על ידי הנשיא מסעוד פזשכיאן. מסמך זה מגדיר יעדים אסטרטגיים, מדדי הערכה ומפת דרכים למחקר ומסחור של טכנולוגיות מחשוב, תקשורת וחישה קוונטיים. הישגים בולטים של איראן כוללים את הקמת רשת חלוקת המפתח הקוונטי (QKD) הראשונה בטהראן בשנת 2025 על ידי חוקרים מאוניברסיטת שריף לטכנולוגיה, המאפשרת תקשורת מאובטחת עבור המגזר הממשלתי והבנקאי. זאת ועוד, כבר בשנת 2019 פתח הארגון לאנרגיה אטומית של איראן (AEOI) מעבדה ייעודית למחקר פיזיקה קוונטית, כחלק ממאמץ נרחב הכולל גם בחינת שימושים צבאיים בתחומי המכ"ם והלוחמה הקוונטית. איראן מדורגת במקום ה-16 בעולם בפרסומים מדעיים בתחום, ורושמת הישגים מרשימים במיוחד בטכנולוגיית חישה קוונטית מרחוק (מקום 8 בעולם), שעונים קוונטיים (מקום 12) ומכ"ם קוונטי (מקום 15). עם זאת, ביוני 2023 נאלצה איראן לחזור בה מהכרזה על פיתוח מעבד קוונטי, לאחר שהמוצר שהוצג זוהה כמוצר פיתוח סטנדרטי (ARM-based development board) הזמין לרכישה ברשת.

ישראל, לצד המעצמות, המדורגת במקום גבוה בנושא שיעור ההשקעה בתוצר, רואה בטכנולוגיה קוונטית מנוע צמיחה ומרכיב קריטי בחוסנה הלאומי ובהגנה על תשתיותיה החיוניות. כפי שנראה בהמשך, ישראל ניצבת במקום השני בעולם (אחרי סין) בשיעור המושקע בתחום הקוונטים מתוך התוצר הלאומי הגולמי (GDP), העומד על כ-0.082 אחוז. המרוץ כולו מוביל לשינוי פרדיגמה שיוליד את הלוחמה הקוונטית, שבה העליונות הטכנולוגית תכריע את תוצאות המערכה.

שימוש בטכנולוגיית קוונטים כיום

יישומים בתחומי ביטחון וטכנולוגיות

- **כללי**

כפי שמפורט בהמשך, המחשוב הקוונטי מחולל מהפכה בממד המודיעיני בהיבטים של חישה וגילוי, ובפיתוח אמצעי לחימה מתקדמים. המחשב הקוונטי יוכל לפצח הצפנות RSA (שיטת ההצפנה הנפוצה ביותר כיום) בתוך שניות ספורות, מה שיהפוך את ממד הלוחמה הדיגיטלי הנוכחי לפרוץ ופגיע. יכולת החישוב האדירה מאפשרת גם סימולציות מורכבות של תהליכים כימיים וביולוגיים לפיתוח חומרים חדשים או אמצעי הגנה מפני לוחמה ביולוגית, וכן אופטימיזציה של תרחישי שדה קרב רב-ממדיים בזמן אמת, כגון הפעלה יעילה של נחילי כטב"מים באמצעות ערוצי תקשורת חסיני ציתות.

- **חישה וגילוי (Quantum Sensing)**

אחד השימושים המרכזיים והדרמטיים ביותר בטכנולוגיה קוונטית כיום הוא בתחום הגילוי והחישה, או שעונים אטומיים למדידת זמן מדויקת ביותר, דבר המעניק יתרון אסטרטגי אל מול מערכות נשק חמקניות. החישה הקוונטית מתבססת על יכולות של מערכות קוונטיות לגלות עצמים שונים באמצעות מדידת שינויים מזעריים בפרמטרים פיזיקליים שונים, כמפורט בהמשך. מכ"ם קוונטי (Quantum Radar) מסוגל לחשוף מטוסים וטילים חמקנים שנועדו לבלוע או להסיט גלי רדיו של מכ"מים רגילים, וזאת על ידי שימוש בזוגות פוטונים שזורים המאפשרים להבחין בין האובייקט לבין רעשי רקע ושיבושים אלקטרוניים. נוסף על כך, חיישנים קוונטיים רגישים במיוחד משמשים לזיהוי צוללות ומוקשים תת-ימיים באמצעות מדידת שינויים מזעריים בשדות מגנטיים וחשמליים, יכולת המשנה את פני הלחימה הימית והופכת את המרחב התת-ימי לשקוף הרבה יותר עבור המגן.

מכ"ם קוונטי, כאמור לעיל, נועד לחשוף מטוסים וטילים חמקנים על ידי שימוש בפוטונים שזורים. המערכת פועלת על ידי שליחת פוטון אחד לעבר המטרה ושמירת הפוטון השני בתחנת השיגור; כאשר האות חוזר המערכת בודקת את ה"חתימה" של השזירה הקוונטית, מה שמאפשר לה להפריד בין האובייקט לבין רעשי רקע כבדים או שיבושים אלקטרוניים שנועדו להטעות מכ"מים רגילים. בזכות יכולת זו המכ"ם מסוגל לזהות עצמים שתוכננו לבלוע או להסיט גלי רדיו מבלי שהם יהיו מודעים לכך שנתפסו. טכנולוגיה זו נמצאת בשלבי פיתוח. חוקרים באוניברסיטת ווטרלו (קנדה) פועלים לפיתוח המערכת כדי להתגבר על רעשי רקע ותנאי מזג אוויר קשים, אך היא טרם הוגדרה במקורות כמערכת מבצעית קיימת בשטח.

גילוי תת-ימי. חיישנים קוונטיים מנצלים את עקרונות המכניקה הקוונטית כדי לזהות שינויים מזעריים ביותר בפרמטרים פיזיקליים, כגון שדות מגנטיים ושדות חשמליים. יכולת זו הופכת אותם לכלי אידיאלי לאיתור צוללות אויב וזיהוי מוקשים תת-ימיים, שכן הם מסוגלים לקלוט את החתימה המגנטית הייחודית של כלים אלו גם במרחב ימי רועש. השימוש בחיישנים אלו משנה את פני הלחימה התת-ימית והופך את המרחב ל"שקוף" עבור הכוח המגן. טכנולוגיה זו קיימת וכבר נמצאת בשימוש. חיישנים אלו משמשים כיום יותר ויותר לחישוב נתונים צבאיים ולגילוי צוללות אויב. מדובר באחד התחומים שבהם הטכנולוגיה הקוונטית כבר משפיעה במידה רבה על המבצעיות הצבאית.

לוחמת מידע והצפנה

פיצוח הצפנות – המחשב הקוונטי מסוגל לבצע פירוק לגורמים של מספרים ראשוניים גדולים בני מאות ספרות (פקטוריזציה) במהירות אדירה באמצעות אלגוריתם שור (Shor's algorithm). מחשב רגיל יזדקק לאלפי שנים כדי לפצח את שיטת ההצפנה RSA הנפוצה כיום, ואשר מתבססת על מספר פעולות מתמטיות המבוססות על מכפלת שני מספרים ראשוניים גדולים, ואילו מחשב קוונטי יוכל לבצע זאת בתוך שניות ספורות. יכולת זו הופכת את מערכות התקשורת, הפיקוד והשליטה הנוכחיות לפגיעות לחלוטין ומשנה את אופי הלוחמה בממד הדיגיטלי. טכנולוגיה זו נמצאת בשלבי פיתוח, עם פוטנציאל עתידי רב. אף על פי שהאלגוריתם קיים, המחשבים הקוונטיים הנוכחיים עדיין נמצאים בשלבים ניסיוניים עם מספר מוגבל של קיוביטים, ואינם מסוגלים בשלב זה לפצח הצפנות RSA מורכבות.

תקשורת חסינת ציתות (QKD) מבוססת על פרוטוקול בנט בראסאר BB8: השיטה מבוססת על חלוקת מפתח קוונטי (Quantum Key Distribution) ומשתמשת בעקרונות המכניקה הקוונטית כדי להחליף מפתחות הצפנה בין שני צדדים באופן מאובטח לחלוטין. מדובר בתקשורת דרך סיבים אופטיים או תקשורת בערוצים במרחב – מה שמוגדר מקצועית כתקשורת במרחב החופשי (Free-space Communication). בשל התכונה הקוונטית שכל מדידה של חלקיק גורמת לקריסת המצב שלו, כל ניסיון של מאזין חיצוני ליירט את המידע או להעתיקו יגרום לשיבושים מיידיים שיחשפו את ניסיון ההאזנה ללא יכולת הסתרה. טכנולוגיה זו מאפשרת יצירת ערוצי תקשורת חסינים לחלוטין לציתות או לפענוח על ידי צד שלישי. היא קיימת וזמינה בצורה מסחרית. QKD נחשב ליישום הבשל ביותר של התקשורת הקוונטית, וסין כבר השלימה רשת קוונטית תת-קרקעית שאורכה כ-1,250 מייל בין בייג'ינג לשנחאי.

סימולציות ופיתוח חמרים ואמצעי לחימה

סימולציה קוונטית נחשבת ליישום המעשי המבטיח ביותר בטווח הקצר, בייחוד עבור תהליכים פיזיקליים מרובי חלקיקים – יתרון מובנה בסימולציה של מבנים מולקולריים מורכבים ותהליכים כימיים. כידוע, חתן פרס נובל ריצ'רד פיינמן כבר קבע כי "הטבע אינו קלאסי" ורק מערכת קוונטית יכולה לדמות תהליכים קוונטיים המתרחשים בטבע, למשל סינתזה כימית. מנגד, תהליכים הנעשים ברמה הקוונטית תובעים משאבי זיכרון אדירים ממחשבים קלאסיים כדי שיוכלו לחקות בהצלחה את התהליך הקוונטי. יכולת החישוב של מחשב קוונטי מאפשרת פיתוח יעיל ומהיר של חומרים כימיים חדשים כגון חומרי נפץ חדשים, חומרים עמידים לקורוזיה או אמצעי הגנה מתקדמים מפני לוחמה כימית וביולוגית, באמצעות הדמיה של מנגנונים ביולוגיים מולקולריים. סימולציות אלו חוסכות זמן עבודה עצום במעבדות, בפרט כאשר סינתזה של חומרים כימיים היא במקרים רבים ברמה של ניסוי וטעייה, ומאפשרות פיתוח אמצעי לחימה באופן סמוי ויעיל. יישום זה קיים ונמצא בשימוש מחקרי מתקדם. חברות כמו רולס רויס כבר משתפות פעולה עם מרכזים קוונטיים לפיתוח כלי חישוב לסימולציה של חומרים מורכבים, בעלי מספר רב של מולקולות, או סימולציות של מבנים ביולוגיים מורכבים. כך למשל, דווח לאחרונה כי מחשב קוונטי של חברת IBM ביצע סימולציה של מבנה חלבון בן 12 אלף אטומים. בנוסף, חיישנים קוונטיים יוכלו לסייע בזיהוי המיקום של שיגורי טילים או בזיהוי חתימה של נשק להשמדה המונית.

אופטימיזציה של שדה הקרב

- **נחילי כטב"מים**

מחשוב קוונטי מציע יכולת חסרת תקדים לפתרון בעיות אופטימיזציה מרובות משתנים, המהוות אתגר עצום למחשבים קלאסיים בשל הדינמיות של שדה הקרב המודרני. הטכנולוגיה מאפשרת לחשב בו-זמנית מספר עצום של נתיבים ומצבי מערכת מצומדים, תוך איתור הפתרון המיטבי שבו המערכת נמצאת ברמת האנרגיה הנמוכה ביותר. יכולת זו חיונית לשליטה בנחילי כטב"מים, שכן היא מאפשרת סנכרון מדויק של כלים אוטונומיים רבים הפועלים כיחידה אחת בתוך תרחישים מורכבים וקיצוניים.

נוסף על חישוב הנתיבים, השילוב בין מחשוב קוונטי לבינה מלאכותית (Quantum Machine Learning) יוצר מערכות המגיבות לשינויים בזמן אמת ומספקות מענה רב-ממדי למתקפות נחילי כטב"מים. שימוש בערוצי תקשורת קוונטיים חסיני ציתות מאפשר להפעיל את נחילי התקיפה הללו ללא חשש משיבוש השליטה או האזנה לפקודות המבצעיות על ידי האויב. יכולות אלו צפויות להעניק לצד המחזיק בטכנולוגיה יתרון טקטי מכריע בניהול קרבות המבוססים על מהירות ודיוק.

- **לוגיסטיקה ותכנון אסטרטגי**

תחום הלוגיסטיקה והאספקה נחשב לאחד היישומים המבטיחים ביותר עבור אופטימיזציה קוונטית בטווח הקצר, בייחוד בפתרון בעיות מורכבות של ניתוב ושינוע משאבים. מחשבים קוונטיים מסוגלים לנתח משתנים גיאופוליטיים, כלכליים וחברתיים במקביל, כדי לחזות אזורי עימות ולתכנן את פריסת הכוחות בהתאם. יכולת זו מאפשרת שיפור דרמטי בתכנון נתיבי אספקה, תוך הבטחה להצבת הציוד והמשאבים במיקום המדויק ביותר ובזמנים קריטיים, גם תחת איומים משתנים.

מעבר לתכנון השוטף, הטכנולוגיה מאפשרת לבצע סימולציות של תרחישי מלחמה רבים במקביל, מה שמסייע בבחינת אסטרטגיות חדשות וניבוי תנועות אויב. יכולת העיבוד המהירה הופכת את התכנון האסטרטגי לדינמי ומאפשרת למפקדים לקבל החלטות מבוססות נתונים בזמן אמת על בסיס ניתוח דפוסי פעולה מבצעיים. אופטימיזציה זו של שרשראות האספקה והתכנון האסטרטגי לא רק חוסכת במשאבים אלא גם מחזקת את החוסן הלאומי ומבטיחה עליונות צבאית במערכות ממושכות.

השקעות לאומיות: המאמץ הישראלי

ישראל רואה בטכנולוגיה הקוונטית מרכיב קריטי בחוסנה הלאומי ובביטחונה, ולכן השיקה בשנת 2020 את התוכנית הלאומית למדע וטכנולוגיה קוונטית. תוכנית זו מתוקצבת בסכום של 1.5 מיליארד ש"ח בהובלת שיתוף פעולה בין רשות החדשנות, המִנהל למחקר ופיתוח אמצעי לחימה ותשתית טכנולוגית (מפא"ת) במשרד הביטחון, הוועדה לתכנון ותקצוב (ות"ת) ומשרדי ממשלה נוספים. מאמץ זה נועד להבטיח שישראל תישאר בחזית הטכנולוגית ותוכל לפתח יכולות עצמאיות בתחומי החומרה והתוכנה הקוונטית.

ההשקעות הישראליות מתמקדות בבניית תשתית רחבה הכוללת בניית מחשב קוונטי כחול-לבן. בשנת 2022 הקצו רשות החדשנות ומפא"ת 200 מיליון ש"ח לבניית מחשב קוונטי, בהשתתפות חברות ישראליות ובינלאומיות והאקדמיה. אושר גם תקציב של 115 מיליון ש"ח למַאגָד (קונסורציום) העוסק בפיתוח טכנולוגיות מחשוב קוונטי.

בסך הכול, בין השנים 2018 ל-2023 השקיעה ישראל כ-480 מיליון דולר בתחום זה, נוסף על השקעות בסך 650 מיליון דולר מטעם קרנות הון סיכון, נכון ליוני 2025. סך ההשקעות נכון למחצית 2026 בחברות הקוונטום בישראל מוערך בכ-800 מיליון דולר עם פוטנציאל גידול נוסף בשיעור בהשקעות בשיעור של 200-300 מליון דולר עד לסוף שנת 2026.

חשיבותו של התחום עבור ישראל משתקפת בדירוגה העולמי: בישראל פועלות כ-20 חברות בנושאי קוונטום מתוך כ-270 חברות בעולם, ישראל מדורגת כיום במקום החמישי בעולם במונחי השקעה כספית בחברות קוונטים, ובמקום השביעי במדד החדשנות והאקו־סיסטם. בנוסף, ישראל ניצבת במקום השני בעולם (אחרי סין) בשיעור המושקע בתחום הקוונטים מתוך התוצר הלאומי הגולמי (GDP), העומד על כ-0.082 אחוז. השקעה מסיבית זו, לצד הון אנושי איכותי ותשתית אקדמית מפותחת, נועדה להבטיח את "העליונות הקוונטית" של ישראל אל מול המעצמות והשחקנים האזוריים. הטבלה הבאה מפרטת בקצרה מס' חברות ישראליות הפעילות בתחום התכנה, הבקרה והחומרה של המחשוב הקוונטי:

חברה	טכנולוגיה	הערות
Quantum Art	מפתחת קיוביטים מבוססים על יונים (אטומים טעונים במטען חשמלי)	שמירת מידע לזמן רב יותר מהאחרים, דיוק בפעולות חישוב
Quantum Source	קיוביטים מבוססים על פוטונים	עבודה בטמפרטורת החדר עם פוטונים בודדים
Quantum Transistors	מבוסס על יהלום עם פגם במבנה בו נלכד אלקטרון המשמש כקיוביט	עבודה בטמפרטורת החדר, זמן קוהרנטיות ארוך
Q-Factor	מפתחת קיוביטים מבוססים על אטומים נייטרליים לכודים בקרני לייזר	פועל בטמפרטורת החדר אך איטי יחסית לאחרים בפעילות בין השערים הלוגיים של הקיוביטים
Quantum Machines	מפתחת מערכות בקרה להפעלת הקיוביטים	מספקת חומרה ותוכנה
Israel Quantum Computing Center (IQCC)	מרכז פיתוח לאומי למחשבים קוונטים על בסיס קיוביטים בשיטות שונות	מפעילה כיום מחשב קוונטי שפועל עם קיוביטים על בסיס על-מוליכים ומערכות בקרה תוצרת Quantum Machines
QuamCore	פיתוח ארכיטקטורה ייחודית לחיווט קיוביטים מבוססי על-מוליכים לקריאוסטט (מקרר) אחד	חיווט אופטימלי מקטין רעשי רקע ושגיאות
QTREX Quantum	פיתוח תשתית חיבור מתוחכמת לתיקשורת נתונים במחשב קוונטי	תשתיות החיבור פועלות בסביבה קריאוגנית
Quedma	הפחתה ותיקון שגיאות במחשב קוונטי	מאפשר למחשב הקוונטי לקבל תוצאות מדויקות עבור חישובים מורכבים
Classiq[2]	פיתוח תכנה ייחודית למחשבים קוונטים	מפתחת אלגוריתמים ממוקדי מטרה עם תרגום אוטומטי של הקוד לשפת מכונה

סיכונים והזדמנויות :היתרון האיכותי והאיום

כפי שכתבנו בעבר, המעבר לעידן הקוונטי טומן בחובו סכנה ממשית לשחיקת היתרון האיכותי של ישראל. בעוד שכיום מחשבי-על הם נחלתן של מעצמות בלבד, הטכנולוגיה הקוונטית צפויה להיות נגישה וגמישה יותר להפעלה. הגישה הקלה יותר ליכולות חישוב אדירות עלולה לאפשר למדינות קטנות, ובטווח הרחוק אף לארגונים סמי-צבאיים (ארגוני טרור), להחזיק ביכולות שבעבר היו שמורות למעצמות, ובכך לאיים על עליונותה הטכנולוגית של ישראל מול אויביה.

הסיכון המרכזי בממד הצבאי הוא קריסת מערכות ההצפנה הנוכחיות. יכולתו של המחשב הקוונטי לפצח הצפנות RSAבתוך שניות עלולה להפוך את הממד הדיגיטלי בשדה הקרב לפרוץ לחלוטין. המשמעות היא שכלל מערכות

התקשורת, הפיקוד והשליטה והתשתיות החיוניות של ישראל עלולות להפוך לפגיעות וחדירות, מה שיחייב שינוי דרמטי בתפיסת הגנת הסייבר ובדוקטרינת הלחימה הדיגיטלית.

לצד הסיכונים, הטכנולוגיה מציעה הזדמנויות אסטרטגיות חסרות תקדים. השגת עליונות קוונטית תאפשר לישראל לפתח תקשורת חסינת ציתות, לשפר במידה משמעותית יכולות בינה מלאכותית ולבצע סימולציות מורכבות לפיתוח חומרי נפץ חדשים ואמצעי הגנה מפני לוחמה כימית וביולוגית. עבור ישראל, הובלה בתחום הקוונטים היא יעד טכנולוגי וגם מנוע צמיחה ומרכיב הכרחי בהרתעה הלאומית וביכולת לתת מענה מיטבי לתרחישים קיצוניים בשדה הקרב העתידי.

למרות הפוטנציאל המבטיח שלו, שוק טכנולוגיות המחשוב הקוונטי עומד בפני מספר אתגרים. מגבלות טכניות כגון חוסר יציבות, שיעורי שגיאות ואובדן המידע האצור בקיוביטים משום שחדלו להיות קוהרנטיים (Qubit Decoherence), נותרו מכשולים כבדי משקל לפיתוח מחשבים קוונטיים אמינים וניתנים להרחבה. המורכבות והעלות הקשורות לבנייה ולתחזוקה של חומרת קוונטים הם משמעותיות ומגבילות את הגישה לתאגידים גדולים ולפרויקטים במימון ממשלתי. קיים מחסור באנשי מקצוע המיומנים בתכנות ואלגוריתמים קוונטיים, מה שמפריע לפיתוח ומסחור יישומים מהירים.

זאת ועוד, היעדר סטנדרטים ופרוטוקולים מקובלים באופן אוניברסלי יוצר בעיות של יכולות הדדית בין פלטפורמות וטכנולוגיות קוונטיות שונות. אי-ודאות בשוק עקב האופי המתפתח של הטכנולוגיה גורמת להשקעה זהירה ולאופקי תשואה רחוקים יותר. חששות אבטחת סייבר סביב הפוטנציאל של מחשוב קוונטי לשבירת שיטות הצפנה קיימות מחייבים פתרונות מקדימים ומוסיפים אתגרי רגולציה ותאימות. יתר על כן, המערכת הקוונטית זקוקה לכלי פיתוח, לתוכנה וליישומים חזקים יותר כדי לממש את פריסת היקף הרחב שלה. שילוב עם תשתיות ITקיימות הוא גם מורכב, ומחייב שינוי נרחב וגישות חדשות. למחשוב קוונטי בארגון יש פוטנציאל לפתרון צרכים ארגוניים בנושאים של פיננסים, בריאות, לוגיסטיקה ואופטימיזציה של תהליכים, וכן מינוף יכולות המחשוב הקוונטי להאצת פיתוח עסקים. נפח השוק בשנת 2033 צפוי להגיע לערך של 3.25 מיליארד דולר, עם קצב גידול ממוצע של 32.5 אחוזים בשנים 2026-2033.

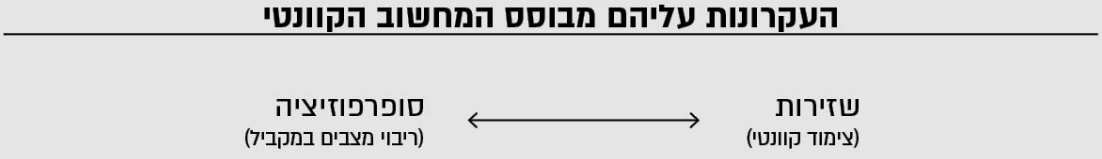
סיכום, מסקנות והמלצות לקראת "מהפכה קוונטית"

המחשוב הקוונטי מייצג שיפור הדרגתי בכוח העיבוד ואף מהווה שינוי פרדיגמה עמוק במדע ובטכנולוגיה, הפורץ את המגבלות הפיזיקליות של המחשוב הדיגיטלי הקלאסי. בעוד שהמחשוב המסורתי מתקרב למיצוי יכולת המזעור של השבבים, המחשב הקוונטי מציע חלופה מהפכנית המאפשרת ביצוע מיליוני פעולות במקביל, מה שמעניק יתרון אסטרטגי חסר תקדים בתחום הביטחון הלאומי.

המהפכה הזו תשנה מן היסוד את הממד הדיגיטלי בשדה הקרב: היכולת לפצח הצפנות RSA בתוך שניות תהפוך את מערכות הפיקוד, השליטה והאינטרנט הנוכחיות לפגיעות, ובכך למעשה תסיים או תצמצם במידה ניכרת את עידן הלוחמה הדיגיטלית כפי שהכרנו אותו, ותפתח את עידן הלוחמה הקוונטית. הטבלה הבאה מסכמת בקצרה את היתרונות הגלומים במהפכה הקוונטית:

נושא	יתרון	הערות
מחשוב קוונטי	ביצוע פעולות סבוכות במהירות רבה או בעיות שלא ניתנות לפתרון במחשב דיגיטלי קלאסי	במצב זה מדובר על עליונות קוונטית (Quantum Supremacy)
סימולציה קוונטית	סימולציה של תהליכים ומערכות קוונטיות (אטומיות או מולקולריות)	סימולציה של תהליכים כימיים או פיזיקליים שאינם ניתנים לביצוע, או תובעים משאבי זיכרון אדירים ממחשבים קלאסיים
תקשורת קוונטית	העברת מידע רגיש חסין להאזנה בכל סוגי ערוצי התקשורת באמצעות פוטונים, על ידי יישום תכונות פיזיקליות שלהם	ניסיון האזנה הוא למעשה פעולת מדידה הגורמת לקריסת המצבים הקוונטיים של הפוטון, שיבוש התקשורת וגילוי ניסיון ההאזנה
פיצוח צפנים	למחשב הקוונטי יכולת לפצח צפנים המבוססים על פעולות במספרים ראשוניים	מיועד למטרה זו. הוא מבוסס על Shor אלגוריתם פעולות מתמטיות סבוכות שמבוצעות בו-זמנית במחשב קוונטי
רשתות קוונטיות (Quantum Network)	חיבור בין רשת מחשבים קוונטיים וחיישנים להעברת מידע בטכנולוגיה שמיישמת עקרונות קוונטיים	השיטה משמשת להעברת מידע קוונטי בערוצים שונים, כולל לוויינים, ונקראת גם אינטרנט קוונטי (Quantum Internet)
הדמיה קוונטית	גילוי ומיפוי עצמים ברזולוציה גבוהה ובהגברה משמעותית לעומת החיישנים הקיימים	גילוי עצמים או מיפוי תלת-ממדי על ידי מדידת שינויים פיזיקליים זעירים כאמצעות יישום תכונות קוונטיות של פוטונים או אלקטרונים
אופטימיזציה קוונטית	מציאת דרכים מיטביות לביצוע פעולות שונות	ניתוח מצבים, תרחישים ואפשרויות בתחומים שונים במהירות וביעילות

הופעת הלוחמה הקוונטית (Quantum Warfare) במסגרת המהפכה הקוונטית מחייבת גיבוש של אסטרטגיות, דוקטרינות ואתיקה צבאית חדשות שיתאימו ליכולות החדשות שנוצרו, בדגש על יישום טכנולוגיות קוונטיות בתקשורת לוויינים, חישה מרחוק, שעונים אטומיים והדמאה. הטכנולוגיה הקוונטית לא רק משפרת את הדיוק של מערכות נשק קיימות אלא גם משנה את אופן ניהול הקרב עצמו, החל מחיזוי מדויק יותר של תנועות אויב ועד אופטימיזציה של תגובה לנחילי תקיפה בזמן אמת. שינוי זה דורש מהמעצמות ומהמדינות השואפות לעליונות טכנולוגית לחשוב מחדש על מושגי יסוד בביטחון לאומי, שכן הנגישות העתידית לטכנולוגיה זו עלולה לשחוק את היתרון האיכותי של מדינות מול ארגונים סמי-צבאיים. האיור הבא מדגים בצורה סכמתית שדה קרב עתידי מנוהל על ידי מערכות קוונטיות:





אינפוגרפיקה על סמך נתונים מתוך Quantum computing in the military

ההמלצה המרכזית למקבלי ההחלטות היא חתירה למוכנות קוונטית מקיפה, הכוללת הצטיידות בחומרה ובתוכנה וכן פיתוח פרוטוקולים חדשים להצפנה לתקשורת, למניעת האזנה. מרכיב קריטי במוכנות זו הוא הכשרת כוח אדם ייעודי המורכב ממהנדסי טכנולוגיה קוונטית בעלי יכולת ניתוח והערכה של נתונים המופקים מחיישנים וממחשבים קוונטיים.

מכיוון שגיוס מומחים אלו לצבא מהווה אתגר, מומלץ לשלב את עקרונות המדע והטכנולוגיה הקוונטית בתוכניות הלימוד של האוניברסיטאות והמכללות הצבאיות, כדי להבטיח שהדרג הפיקודי והטכנולוגי יהיה ערוך להטמעה ולתפעול של המערכות בשדה הקרב העתידי. לבסוף, מפקדים צבאיים חייבים להיות מודעים לטכנולוגיות מתפתחות ומשבשות כדי לשמור על כוחות רלוונטיים, ואחת מהטכנולוגיות הללו היא מחשוב קוונטי.

למרות שמחשוב קוונטי נמצא עדיין בשלבים מוקדמים, ועדיין יש בעיות בייצור קיוביטים אמינים, עסקים וממשלות משקיעים רבות במחקר ופיתוח וממשלות ברחבי העולם כבר מגלות עניין רב בנושא. ייתכן שיש לכך השלכות של ממש הן בהיבט האזרחי והן בהיבטים הצבאיים.

תודות לגב' הדס לורבר ולד"ר נדב כהן על ההערות המועילות.