فصلنامه علمی امنیت ملی
سال دوازدهم، شماره چهل‌وسوم، بهار ۱۴۰۱
مقاله پنجم از صفحات ۱۶۸-۱۲۱

مقاله پژوهشی: # تأثیر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده

سید نصیب‌الله دوستی مطلق[۱]

تاریخ دریافت: ۱۳۹۹/۰۸/۱۸ **تاریخ پذیرش: ۱۴۰۰/۰۴/۱۹**

چکیده

فضای سایبر در عصر ظهور فناوری‌های کوانتومی از نظر زیرساخت، محتوا، کاربرد و حتی امنیت و حکمرانی یقیناً متحول خواهد شد. به دست آوردن الگوی مفهومی فضای سایبر کوانتومی پیش‌زمینه طراحیِ نظام امنیت و دفاع سایبری در عصر ظهور فناوری‌های سایبر کوانتومی خواهد بود. فضای سایبریِ آینده در عصری که فناوری‌های کوانتومی به‌طور مؤثری در آن مورد استفاده و بهره‌برداری قرار می‌گیرند تمام مفاهیم مرتبط با ساختار فضای سایبر با در نظر گرفتن فناوری‌های سخت‌افزاری و نرم‌افزاری کلاسیکی در کنار سخت‌افزارها و نرم‌افزارهای کوانتومی و سیستم‌های حسگری کوانتومی ساختار کامل و جامعی از فضای سایبر آینده را به وجود می‌آورد.

این پژوهش ابتدا با این پرسش بنیادین روبه‌رو می‌شود که «چارچوب مفهومی فضای سایبری، ابعاد، مؤلفه‌ها و شاخصه‌های اساسی آن در عصر کوانتومی چیست»؟ و سپس با به‌کارگیری فن خوشه‌بندی در تحلیل محتوا و تکنیک دلفی درصدد طراحی فضای سایبری آینده برمی‌آید. به این منظور، ابعاد زیرساخت، محتوا، کاربرد و شناختی (اجتماع-مردم) را که در ساختار مفهومی فضای سایبری کلاسیکی مطرح است، در نظر گرفته و مؤلفه و شاخصه‌های کلی فضای سایبری کلاسیکی را استخراج می‌کند. سپس با بررسی و تحلیل محتوا، فناوری‌های کوانتومی اثرگذار بر هرکدام از ابعاد، مؤلفه‌ها و شاخصه‌های فضای سایبر کلاسیکی، جهت تعیین ساختار فضای سایبر آینده که متأثر از علوم و فناوری‌های کوانتومی است، ارائه خواهد شد.

کلیدواژه‌ها: **فضای سایبر، فناوری‌های کوانتومی، محاسبات کوانتومی، ارتباطات کوانتومی، حسگری کوانتومی.**

۱. استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، پژوهشکده آماد و فناوری دفاعی، تهران، ایران
doustimotlagh@chmail.ir

مقدمه و بیان مسئله

رایانه‌های کوانتومی نسل جدیدی از ماشین‌های محاسباتی هستند که برخلاف رایانه‌های کلاسیکی، اطلاعات را بر پایه بیت‌های کوانتومی (کیوبیت‌ها) ذخیره می‌نمایند و از اصول مکانیک کوانتومی نظیر درهم‌تنیدگی، برهم‌نهی حالت‌ها، اصل توازیِ کوانتومی و به‌خصوص مفهوم ناموضعیتِ کوانتومی جهت ذخیره‌سازی، فشرده‌سازی، اصلاح خطا، پردازش و بازخوانی اطلاعات کوانتومی استفاده می‌کنند. ایده رایانش کوانتومی اولین بار در سال ۱۹۸۲ میلادی توسط ریچارد فایمن مطرح شد. اهمیت رایانه‌های کوانتومی در توانایی بالقوه آن‌ها در شبیه‌سازهای کوانتومی، انجام محاسبه هم‌زمان با تعداد نمایی از متغیرها (مسائل در کلاس پیچیدگی چندجمله‌ای نامتعین)[1] در الگوریتم‌های کوانتومی، حل بهتر و سریع‌تر مسائل بهینه‌سازی، شکست الگوریتم‌های رمزنگاری، ایجاد سیستم‌های ناوبری و زمان و مکان‌سنجی دقیق نظامی، تأییدکننده‌های کوانتومی[2]، تولید اعداد رندوم کاملاً تصادفی کوانتومی، ارتقای امنیت سایبری، تحول در بررسی سیستم‌های پیچیده اقتصادی، هوش مصنوعی و یادگیری ماشین‌های کوانتومی و حتی ایجاد تغییرات بنیادین در علوم انسانی همچون ایجاد نگرش‌های نوین در رهبری و مدیریت کوانتومی است. در سال‌های اخیر تلاش‌های تجربی و نظری بسیار زیادی در زمینه ساخت رایانه‌های کوانتومی صورت گرفته؛ به‌گونه‌ای که نوبل فیزیک در سال ۲۰۱۲ میلادی به تلاش‌های انجام‌شده در این مجموعه اهدا شده است. اهمیت این موضوعات به قدری است که حتی در تازه‌ترین سند راهبردی امنیت سایبری ایالت متحده نیز بر لزوم سرمایه‌گذاری در حوزه اطلاعات کوانتومی تأکید ویژه‌ای شده است.

در سال ۲۰۱۰ میلادی اولین رایانه‌های ۱۲۸ کیوبیتی با نام تجاری دی‌وِیِ‌ووان[3] ساخته شد. پیش از پایان سال ۲۰۱۲ میلادی تلاش برای ساخت رایانه‌های کوانتومی ۵۱۲ کیوبیتی آغاز شد و در سال ۲۰۱۳ میلادی این رایانه ساخته شد. توسعه گیت منطقی سیلیکونی دو

1. Nondeterministic polynomial (NP).
2. Quantum verifier.
3. D-wave one.

کیوبیتی در سال ۲۰۱۵ میلادی و ساخت رایانه کوانتومی ۱۷ کیوبیتی در سال ۲۰۱۷ میلادی توسط شرکت آی‌بی‌ام از دیگر دستاوردهای اخیر این حوزه است. در نوامبر ۲۰۱۷ میلادی، آی‌بی‌ام از پردازنده ۵۰ کیوبیتی خود رونمایی کرد و شرکت اینتِل[1] نیز در سال ۲۰۱۸ میلادی پردازنده ٤۹ کیوبیتی خود را به نمایش عموم درآورد. در مارس ۲۰۱۸ میلادی، گردهمایی جامعه فیزیک آمریکا شاهد رونمایی از آخرین دستاورد فیزیکدانان گوگل بود؛ تراشه‌ای به نام بریستلکون[2] که می‌تواند محاسبات کوانتومی را با پردازش ۷۲ کیوبیت انجام دهد. با این حال برای دستیابی به برتری کوانتومی[3]، کامپیوترهای کوانتومی باید بتوانند حداقل ۱۰۰ کیوبیت منطقی (کیوبیت بدون خطا) را پردازش کنند. از این منظر پردازنده‌های کوانتومی امروزی را می‌توان ذیل عنوان پردازنده‌های کوانتومیِ اندازه-متوسط دارای نوفه[4] دسته‌بندی کرد، چراکه نخست تعداد کیوبیت‌های آن‌ها زیاد نیست و دوم به دلیل حضور اختلالات محیطیِ گرمایی یا کوانتومی دارای نوفه هستند (کیوبیت‌ها در این قطعات دارای خطا بوده و کیوبیت منطقی نیستند). در حال حاضر گوگل توانسته است پردازنده کوانتومی با نام تجاری سیکامور[5]، حاوی ۵۳ کیوبیت را در عمل تولید کرده و مورد بهره‌برداری‌های گسترده علمی قرار دهد.

بسیاری از کشورها در سرتاسر جهان برنامه‌های ملی فناوری کوانتومی را از میلیون‌ها تا میلیارد دلار آغاز کرده‌اند که شامل کشورهای استرالیا، کانادا، چین، اتحادیه اروپا، ژاپن، هلند، روسیه، سنگاپور، انگلستان و ایالات متحده می‌باشند. در عین حال، بازیگران عمده صنعتی مانند گوگل[6]، آی بی ام[7]، مایکروسافت[8]، اینتل، آتوس[9]، علی‌بابا، تسنت[10] به همراه

1.Intel.
2. Bristlecone.
3. Quantum supremacy.
4. Noisy Intermediate-Scale Quantum (NISQ) processor.
5. Sycamore quantum processor.
6. Google.
7. IBM.
8. Microsoft.
9. Atos.
10. Tencent.

تعداد زیادی از جدیدترین استارت آپ‌های کوچک و بزرگ کوانتومی، آزمایشگاه‌هایی را ایجاد کرده‌اند که سخت‌افزار و نرم‌افزارهای کوانتومی را توسعه داده و تولید می‌کنند. مجموعه این دستاوردهای که اکنون از آن با نام انقلاب دوم کوانتومی یاد می‌شود، زمینه‌ساز ظهور عصری است که در آن انواع جدیدی از فناوری‌ها جایگزین فناوری‌های موجود در زمینه ارتباطات و خدمات مخابراتی و اینترنتیِ الکترونیکی و امنیت تبادل اطلاعات شده است.

بیان مسئله

استفاده از رایانه، پردازنده‌ها و حسگرهای الکترونیکی که در سیستم‌های کنترلی استفاده می‌شود، روزبه‌روز در حال افزایش است. این امر سبب شده که امنیت سایبر و به‌طور کلی امنیت رایانه‌ها و وسایل ارتباطی مرتبط با رایانه به یک مسئله حیاتی تبدیل شود. در سال‌های اخیر فناوری محاسبات پیشرفت‌های سریعی یافته و به‌ویژه روش‌های محاسباتیِ قدرتمند کوانتومی جایگزین همتایان کلاسیکی خود شده‌اند. با این حال، هکرهای سطح دولتی و غیردولتی امنیت شبکه‌های ارتباطی و فضای سایبر را در محاسبات رایج کلاسیکی تهدید می‌کنند. علاوه بر این، در سازمان‌های مخفی کشورهای متخاصم می‌توان هکرهای غیردولتی را برای حمله به فضای سایبر کشورهای دیگر استخدام و ساماندهی کرد. اکثر سیستم‌های فعلی سایبری از فناوری‌های سایبر کلاسیکی و دستگاه‌های محاسباتی کلاسیک استفاده می‌کنند. با این حال تعدادی از مؤسسات تحقیقاتی در حال انجام آزمایشات و بهره‌برداری از سیستم‌ها و ادوات کوانتومی در فضای سایبر هستند. نفوذ و حملات سایبری و تکنیک‌های هوشمند مخابرات کوانتومی بسیار پیشرفته‌تر از برنامه‌های ارتباطی کلاسیکی امروزی است و بنابراین بسیاری از کشورها، حتی کشورهای پیشرفته صنعتی نگران امنیت سایبری کشورشان در عصر توسعه فناوری‌های کوانتومی در فضای سایبر می‌باشند.

بنابراین سؤال اصلی که در اینجا با آن مواجه هستیم این است که ابعاد، مؤلفه‌ها و شاخصه‌های فضای سایبر در عصر ظهور فناوری‌های کوانتومی به چه صورت خواهند بود؟

چه مدل مفهومی فضای سایبری که مشتمل بر فناوری‌های سایبری کلاسیکی و فناوری‌های کوانتومی رایانش و ارتباطات کوانتومی باشد می‌توان برای عصر ظهور فناوری‌های کوانتومی ارائه داد؟ در ادامه تلاش خواهد شد تا به این پرسش بنیادین پاسخ داده شود.

۱. مبانی نظری

پیشینه پژوهش: اصطلاح فضای سایبر[1] از ترکیب دو واژه «سایبر» و «فضا» تشکیل شده است که برای درک بهتر این اصطلاح، هر یک از واژه‌ها جداگانه بررسی می‌شود. سایبر از لغت یونانی «سایبرنتیک»[2] به معنای «سکاندار» یا «راهنما» مشتق شده است.

فضای سایبر عبارتی است که در دنیای ارتباطات، اینترنت و رسانه‌های الکترونیکی بسیار شنیده می‌شود. کارکرد اصلی این فضا آن است که محیطی برای تعامل تعداد زیادی از افراد فراهم آورده، به‌طوری که بتوانند با یکدیگر در ارتباط بوده و بر آن تأثیر گذاشته و تأثیر بپذیرند. پس محیط سایبر اساساً ماهیتی رسانه‌ای دارد. در حقیقت فضای سایبر، فضایی انتزاعی است که از اتصال رایانه‌هایی پدید آمده است که تمامیِ انسان‌ها، ماشین‌ها و منابع اطلاعاتی در جهان را به هم وصل کرده است (شکل ۱ را ببینید).

شکل ۱: الگوی شماتیک از تعریف فضای سایبر متشکل از انسان، ماشین و منابع اطلاعاتی

1 Cyberspace
2 kybernetes

مدل‌های مفهومی مختلف فضای سایبر

برای فضای سایبر مدل‌های مفهومی سه لایه، چهار لایه و پنج لایه ارائه شده است که در زیر به آن‌ها پرداخته می‌شود.

ـ مدل سه لایه فضای سایبر لیبیکی

در سال ۲۰۰۹ میلادی، مارتین لیبیکی[1] (Libicki, 2009) برای نیروی هوایی آمریکا یک چارچوب مفهومی فضای سایبری ارائه نموده است: فضای سایبری یک محیط مجازی است، به مراتب غیرمحسوس‌تر از زمین، آب، هوا، یا حتی فضا و طیف فرکانس رادیویی RF. یک راه درک فضای سایبری و به‌ویژه درک حملات سایبری در حالت کلی آن است که نگرش و دیدگاهی سه لایه‌ای از آن وجود داشته باشد که متشکل از یک لایه فیزیکی، یک لایه نحویِ قرار گرفته بر روی لایه فیزیکی و یک لایه منطقی در بالا است (جدول ۱ را ببینید). در زیر به توضیح هر یک از این لایه‌ها پرداخته می‌شود.

جدول ۱: مدل سه لایه فضای سایبر لیبیکی

فضای سایبر	لایه منطقی	اطلاعات
	لایه نحوی	برنامه‌ها و پروتکل‌های ارتباطی برای تشخیص وسیله، قالب‌بندی بسته‌ها، آدرس‌دهی، مسیریابی، قالب‌بندی مستندات، پردازش پایگاه داده و ...
	لایه فیزیکی	رایانه‌ها
		شبکه‌های ارتباطی

همه سیستم‌های اطلاعاتی در لایه فیزیکی قرار می‌گیرند که متشکل از رایانه‌ها و شبکه ارتباطی میان این رایانه‌ها است. برداشتن لایه فیزیکی منجر به ناپدید شدن سیستم می‌شود. قطعاً امکان حمله به یک سیستم اطلاعاتی از طریق ابزارهای وابسته به نیروی محرکه وجود دارد، با این حال حمله‌های فیزیکی برای چنین منظوری آن‌چنان کار ماهرانه‌ای نیست (درست همان‌طور که نمی‌توان برای فریب دادن یک رایانه قطعات آن را خراب کرد).

1. Martin C. Libicki.

لایه نحوی، شامل دستورالعمل‌هایی است که طراحان و کاربران به ماشین و پروتکل‌ها می‌دهند تا از طریق آن‌ها ماشین‌ها با یکدیگر تعامل داشته باشند. این لایه متشکل از تشخیص وسیله، قالب‌بندی بسته‌ها، آدرس‌دهی، مسیریابی، قالب‌بندی مستندات، پردازش پایگاه داده‌ها و ... است. برخی از زیرساخت‌های ارتباطی دارای لایه نحوی ضخیم‌تری هستند. این لایه، لایه‌ای است که نفوذ و هک کردن در آن به وقوع می‌پیوندد، چراکه نفوذگران بیرونی انسانی به دنبال آن هستند که توانایی خود را به طراحان و کاربران تحمیل کنند.

بالاترین لایه، لایه منطقی است که شامل اطلاعاتی می‌شود که ماشین حاوی آن است. برخی از اطلاعات، نظیر جدول‌های جستجوی آدرس (مسیریاب‌ها) یا کدهای کنترل چاپگر، به‌منظور پردازش سیستم مورد استفاده قرار می‌گیرند. این نوع اطلاعات دارای شکل معنایی بوده، اما دارای هدف نحوی هستند. سایر انواع اطلاعات (نظیر دستورالعمل‌های برش یا اطلاعات کنترل فرایند)، با هدف کنترل ماشین‌های رایانه‌ای استفاده می‌شوند. مابقی اطلاعات سیستم نیز تنها برای انسان‌ها قابل فهم است، زیرا به زبان طبیعی کدبندی شده‌اند.

ـ مدل سه لایه‌ای فضای سایبر استریت

این مدل مفهومی به‌منظور تشریح فضای سایبری معرفی شده است که به سه لایه قابل تقسیم است (جدول ۲ را ببینید) (Strate, 1999):

۱) فضای سایبری مرتبه صفر: هستان‌شناسی فضای سایبری. این لایه در حقیقت پی و شالوده فضای سایبری است.

۲) فضای سایبری مرتبه اول فضای سایبری فیزیکی، مفهوم و ادراکی است. این لایه شامل عناصر پایه و بلوک‌های پیش‌ساختهٔ فضای سایبری است.

۳) فضای سایبری مرتبه دوم: ترکیب رسانه ارتباطی سایبری و فضا است که نشان‌دهنده یک ترکیب از عناصر پایه لایه قبل است.

جدول ۲: مدل سه لایه فضای سایبر استریت

فضای سایبری مرتبه دوم: ترکیب	فضای رسانه سایبری[1]		
	فضای علمی[2]	فضای اطلاعات یا داده‌ای[3]	فضای تعاملی یا رابطه‌ای[4]
فضای سایبری مرتبه اول: بلوک‌های پیش‌ساخته	فضای فیزیکی[5]	فضای مفهومی[6]	فضای ادراکی[7]
فضای سایبری مرتبه صفر: هستان‌شناسی	پارافضا یا غیرفضا[8]		فضا-زمان[9]

ـ مدل چهار لایه فضای سایبر شاوو

طبق مدل شاوو چهار لایه کلیدی برای فضای سایبری وجود دارد که آن را کاملاً یکتا می‌سازد و برای پاسخگویی به بسیاری از پرسش‌های مرتبط با آن مهم هستند (Shaw, 2010). لایه‌های فضای سایبری عبارت‌اند از:

۱) مؤلفه زیرساخت (سیستمی)،

۲) مؤلفه کاربردی و محتوایی،

۳) مؤلفه جامعه و مردم،

٤) مؤلفه مدیریتی (حاکمیتی).

بر طبق این مدل می‌توان چهار بُعد یا چهار لایه کلیدی برای فضای سایبری متصور شد که آن را یکتا می‌سازد و برای پاسخگویی به بسیاری از پرسش‌های مرتبط با آن مهم هستند. ابعاد فضای سایبری عبارت‌اند از: بُعد سیستم‌ها، بُعد محتوا و کاربرد، بُعد مردم و اجتماع و یک‌بعدی که بر این سه بُعد نظارت می‌کند به نام بُعد حاکمیت (جدول ۳ را ببینید).

1.Cybermedia Space.
2.Aesthetic Space.
3. Information or Data Space.
4. Interaction or Relational Space.
5. Physical Space.
6. Conceptual Space.
7. Perceptual Space.
8. Paraspace or Nonspace.
9. Space-time.

جدول ۳: مدل چهار لایه فضای سایبر شاوو

لایه حاکمیت پوشش‌دهنده همه جوانب فضای سایبر		
لایه زیرساخت یا سیستمی زیرساخت و معماری فنی	لایه محتوا/کاربرد پایگاه اطلاعاتی و سازوکارهای دسترسی و پردازش اطلاعات	لایه مردم و جامعه ارتباطات و تعاملات بین انسان‌ها و اطلاعات

بُعد زیرساخت یا سیستمی[1]

این بُعد شامل جنبه‌های فنی، زیرساختی و معماری فضای سایبری است. این بُعد شامل ۱- سخت‌افزار و نرم‌افزارهای کاربردی است که کاربران به‌منظور ۲- ذخیره‌سازی، ۳- انتقال و ٤- پردازش اطلاعات در فضای سایبری به آن‌ها اتکا دارند. در سطح جهانی، یک بخش مهم اقتصاد امروزی مرتبط با ساخت ریزپردازنده‌ها، کامپیوترهای شخصی، مسیریاب‌ها، سرویس‌دهنده‌ها و سیستم‌های عامل برای این بُعد است. همچنین، یک بخش قابل ملاحظه از اقتصاد اختصاص به عملیاتی کردن و نگهداری زیرساخت‌های ارتباطی متصل‌به‌هم در سطح بین‌المللی، شرکت‌های مخابراتی (فراهم‌کنندگان سرویس اینترنت[2]، شرکت‌های تلفن همراه و سایر شبکه‌های همگانی) برای ارتباطات غیرنظامی و نظامی دارد.

بُعد محتوا و کاربرد[3]

این بُعد به محتوا و اطلاعات که در فضای سایبری وجود داشته و همچنین ابزارهایی که برای دستیابی و پردازش این اطلاعات مورد استفاده قرار می‌گیرد، ارجاع دارد. بُعد محتوا و کاربرد به بُعد سیستمی اتکا دارد و کاربردها را در راستای مدیریت و اشتراک اطلاعات برای کاربران فراهم می‌کند. برخی از پراستفاده‌ترین کاربردهای امروزی، شامل پست الکترونیکی، موتورهای جستجو، پیام‌رسان‌های فوری، تجارت الکترونیکی، وبلاگ‌ها،

1. Systems domain.
2. Internet service providers (ISPs).
3. Context and Application domain.

سایت‌های شبکه‌های اجتماعی، تلفن اینترنتی، اخبار، نقشه‌ها و اشتراک‌گذاری فایل نظیر به نظیر[1] است. بُعد محتوا و کاربرد فضای سایبری خیلی پویا است، چراکه هر روز کاربردهای جدیدی پدیدار می‌شوند که به کاربرانشان اجازه تعامل با یکدیگر و نیز اطلاعاتشان (به‌صورت منعطف) می‌دهند (Zimet & Skoudis, 2009).

بُعد جامعه و مردم[2]

این بُعد به ارتباطات و تعامل‌های بین انسان‌ها در فضای سایبری و همچنین به اطلاعاتی که به اشتراک می‌گذارند ارجاع دارد. دو بُعد قبلیِ فضای سایبری امکان رشد بُعد انسانی و اجتماعی را با تسهیل ایجاد انجمن‌ها در فضای سایبری برای دسترسی و اشتراک اطلاعات مابین کاربران را فراهم نمودند.

در حال حاضر، انجمن‌های بی‌شماری که متناسب با نیازهای کاربران هستند و برای مقاصد مختلفی نظیر اخبار برخط، بهداشت و همچنین مقاصد درمانی، مذهبی، سیاسی و فناوری مورد استفاده قرار می‌گیرند. این سایت‌ها به اعضا از سرتاسر جهان اجازه تعامل‌های اجتماعی و اشتراک اطلاعات را به‌صورت منظم می‌دهند. متأسفانه، انجمن‌های برخط متعددی وجود دارند که دارای رفتارهای منفی برای امنیت ملی هستند. تروریست‌ها انجمن‌هایی در فضای سایبری ایجاد نموده‌اند تا از این طریق اعضای جدید جذب نموده، عملیات خود را هماهنگ و پیغام‌هایشان را منتشر کنند. همچنین گروه‌های بزهکار، انجمن‌هایی را در فضای سایبری ایجاد کرده‌اند که جرائم مختلفی در آن مرتکب شده و معاملات مالی‌شان را در آن پیگیری می‌کنند.

بُعد حاکمیتی[3]

این بعد همه بُعدهای قبلی فضای سایبری را تحت تأثیر قرار می‌دهد. این بُعد مشخصات فناوری (بُعد سیستم‌ها)، استانداردسازی برای قالب‌بندی و تبادل داده‌ها (بُعد

1. Peer-to-peer.
2. People and Social Domain.
3. Governance domain.

محتوایی و کاربردی) و چارچوب‌های قانونی کشورها برای کاربران فضای سایبری (بُعد انسانی و اجتماعی) را تحت تأثیر قرار می‌دهد. سازوکارهای مدیریتی اینترنت به‌شدت پیچیده بوده و نیازمند هزینه نمودن منابع قابل توجه در محاکم مختلف برای نیل به اهداف هستند. اگر مدیریت بر اساس معیارهایی نظیر آزادی، دموکراسی، شفافیت، پویایی، وفق‌پذیری، مسئولیت‌پذیری، کارآمدی و مؤثر بودن ارزیابی شوند، می‌توان ادعا نمود که مدیریت اینترنت در این زمینه‌ها به‌خوبی عمل نموده است (Zimet & Skoudis, 2009).

ـ مدل پنج لایه‌ای فضای سایبر

در سال‌های اخیر در کشور فرانسه یک مدل پنج لایه‌ای در صورت‌بندی فضای سایبری ارائه گردیده که الهام گرفته‌شده از علم زمین‌شناسی است («2010» A Draft Apocryphal and Anthropocentric Cyberspace,).

در این مدل فضای سایبری، یک پشتوانه اطلاعاتی برای اتصال موجودات زنده و ماشین‌ها است و دارای سه مؤلفه (ویژگی اطلاعاتی) از سیستم‌های اطلاعاتی یا فنون بیولوژیکی است که عبارت‌اند از (جدول ٤ را ببینید):

ـ معنایی (معنی اطلاعاتی)[1]

ـ نحوی (جریان اطلاعات)[2]

ـ لغوی (ذخیره اطلاعات)[3]

طبق این مدل، فضای سایبری دارای یک ساختار پنج لایه‌ای، مشابه لایه‌های زمین‌شناسی است که در ادامه به تفکیک معرفی می‌شوند.

1. Semantics.
2. Syntactic.
3. Lexical.

جدول ٤: مدل پنج لایه فضای سایبر

لایه پنجم: سایبر چهارم (همگرایی انسان و ماشین)	فضای سایبر
لایه چهارم: (ارتباطات سراسری انسان‌ها)	
لایه سوم: سایبر دوم (پیدایش نوشتار و ریاضیات)	
لایه دوم: سایبر نخست (پیدایش زبان و معنای انسانی)	
لایه اول: سایبر پایه	

لایه اول: سایبر پایه[1]

مبدأ فضای سایبری به‌طور دقیق معلوم نیست. احتمالاً منشأ فضای سایبری، شروع حیات و نخستین تبادل اطلاعات مابین موجودات زنده از طریق ژن‌ها، محرک فرمون، شکار و ... بوده است. برای مثال ژن، بخشی از سه ویژگی فضای سایبری است. این پوشش حداقل چهار میلیون سال است که ساخته شده و مبنای فضای سایبری امروزی است. همه لایه‌های بعدی مبتنی بر این لایه حیات (که مدام در حال تغییر است)، ساخته خواهند شد.

لایه دوم: سایبر نخست[2] (پیدایش زبان و معنای انسانی)

این لایه زبان مبدأ فضای سایبری است که به‌وسیله انسان‌ها ساخته شده و به صدها هزار سال قبل مربوط می‌شود. هیچ‌کس نمی‌داند که زبان چه زمانی به وجود آمده است. زبان جهت ارتباط انسان‌ها و توسعه گروه‌های اجتماعی، اقتصادی، فرهنگی، سیاسی و جنگی استفاده می‌شود. زبان اجازه پیدایش الگوهای رفتاری را می‌دهد. اطلاعات به‌وسیله انسان‌هایی که قدم‌به‌قدم در فضا و زمان حرکت می‌کنند، ذخیره می‌شود که البته با تغییرات قابل توجه اطلاعات نیز همراه است. سنت‌های زبانی (شفاهی) در حقیقت به توسعه تمدن‌های پیشرفته در هر قاره منجر شده است. تحولاتی مشابه آن‌ها را می‌توان در فضای سایبر نیز جستجو کرد.

1. Cybersocle.
2.Cyberprimaire.

لایه سوم: سایبر دوم[1] (پیدایش نوشتار و ریاضیات)

سایبر دوم، از حدود سه هزار سال قبل از میلاد شروع می‌شود. نوشتار، جزء سه ویژگی فضای سایبری است. امروزه اطلاعات در صفحات (مغناطیسی، نوری و ...) ذخیره می‌شوند، با این حال کماکان در قفسه‌ها و لوحه‌های باستانی نیز وجود دارد. خواندن/نوشتن جریان اطلاعات را میسر می‌کند. همچنین، با پیدایش ریاضیات، فهم بهتر جهان هستی میسر شده و به‌تدریج، امکان ذخیره‌سازی و نسخه‌برداری مطمئن اطلاعات ممکن شد. در نتیجه، تفکرات ثبت‌شده در مستندات ممکن است که برای قرن‌ها به فراموشی سپرده شده، اما دوباره ظاهر شوند. به‌طور مشابه، امکان حمل مستندات به جاهای دیگر زمین حمل شوند.

لایه چهارم: سایبر سوم[2] (ارتباطات سراسری انسان‌ها)

سایبر سوم با جهانی‌سازی اکتشافات بزرگ شروع شد. دوره‌ای که استعمار و جنگ‌های جهانی در آن اتفاق افتادند. این لایه مبتنی بر دو پدیده است:

ـ توسعه چاپ پس از اختراع فنون چاپ. این پیشرفت با ضبط بر روی دیسک و نوار در انتهای این دوره تکمیل شد.

ـ لغو تدریجی فاصله در سطح جهان با توسعه تلگراف، تلفن، تلویزیون، رادیو و ... .

سایبر سوم فاصله‌ها را کاهش داد و امکان ارتباط سریع نواحی مختلف جهان را فراهم نمود. اطلاعات می‌توانستند در یک قاره ذخیره شده و به‌سرعت به قاره‌های دیگر منتقل شوند. اتصال انسان‌ها کامل شده و امکان اعمال حاکمیت در کشورهایی متشکل از سرزمین‌های پیوسته بزرگ (نظیر روسیه) یا پراکنده شده در گوشه‌های مختلف جهان (نظیر امپراتوری بریتانیا) فراهم شد.

1. Cybertertiaire.

لایه پنجم: سایبر چهارم[1] (همگرایی انسان و ماشین)

این مرحله، مرحله فعلی است. توسعه الکترونیک، کامپیوترها و اینترنت نشانه این تغییر مهم در جامعه بشری است. این لایه، در پیوند با لایه‌های دیگر فضای سایبری، توسعه‌دهنده اتصال انسان‌ها و زندگی آن‌ها است که به اندازه کافی در ادبیات علمی به آن پرداخته شده است. نانوفناوری، حیات مبتنی بر فناوری، بیولوژی مصنوعی و رباتیک به‌تدریج در راستای هموار کردن تفاوت‌های انسان، ماشین و مصنوعات جاندار همگرا می‌شوند. این فرایند در حال پیشرفت است و ممکن است ده‌ها بلکه صدها سال به طول بیانجامد و منجر به شکل‌هایی از برخوردهای سیاسی شود. بسیاری از کشورها یا مفسرین، تنها به لایه فعلی و احتمالاً سایبر سوم علاقه‌مند هستند.

در مجموع با توجه به مدل‌های مفهومی سه لایه، چهار لایه و پنج لایه‌ای که بیان شد و ارتباطی که فناوری‌های سخت‌افزاری و نرم‌افزاری با هم دارند، مناسب‌ترین مدلی که در عین جامعیت، شفافیت بالاتری از لحاظ تقسیم‌بندی اجزا و ساختار فضای سایبر داراست مدل چهار لایه شاوو (Shaw, 2010) است. همان‌طور که گفته شد، در این مدل مفهومیِ فضای سایبرِ کلاسیکی، ابعاد فضای سایبری عبارت‌اند از: بُعد سیستم‌ها، بُعد محتوا و کاربرد، بُعد مردم و اجتماع و یک‌بعدی که بر این سه بُعد نظارت می‌کند به نام بُعد حاکمیت. با توجه به اینکه بُعد چهارم که حاکمیتی است و در آن استانداردسازی و چارچوب‌های قانونی کشورها برای کاربران فضای سایبری تعیین می‌شود، در بررسی تأثیرات علوم و فناوری‌های کوانتومی بر لایه‌های مختلف مدل مفهومی فضای سایبر، می‌توان لایه حاکمیتی را کنار گذاشت و تأثیرات علوم و فناوری‌های کوانتومی را بر سه لایه اصلی زیرساخت، محتوا و کاربرد و لایه جامعه و مردم در فضای سایبر مورد تحقیق و بررسی قرار داد. در جدول ۵ ابعاد، مؤلفه‌ها و شاخصه‌های فضای سایبرِ کلاسیک براساس مدل مفهومی فضای سایبر شاوو ارائه شده است.

جدول ۵: ابعاد، مؤلفه‌ها و شاخصه‌های فضای سایبر کلاسیک براساس مدل مفهومی چهار لایه فضای سایبر شاوو.

ابعاد	مؤلفه‌ها	شاخصه‌ها
زیرساخت (سیستمی)	رایانش الکترونیکی	رایانه‌های و پردازنده‌های منطقی الکترونیکی (رایانه، موبایل، تبلت)
	ارتباطات و مخابرات الکترونیکی	منابع سیگنال‌های الکترونیکی مایکروویو (تراشه‌ها و بوردهای الکترونیکی تولید سیگنال)
		خطوط ارتباطی (فیبر نوری، بیسیم)
		تقویت‌کننده‌های سیگنال (تقویت‌کننده فیبر نوری، تقویت‌کننده سیگنال میکروویو و رادیویی)
		مسیریاب‌های الکترونیکی
		سوییچ‌های الکترونیکی
		آشکارسازها (در فرکانس‌های رادیویی و میکروویو الکترونیکی)
		حافظه‌های الکترونیکی
	حسگرهای الکترونیکی و مخابراتی و سیستم‌های کنترل نظارتی و دریافت داده[1]	دوربین‌ها، سیستم‌های الکترونیکی نظارت و کنترل، موقعیت‌یاب ماهواره‌ای، حسگر موقعیت و شتاب، ...
		رادارهای الکترونیکی
		PLC ها و حسگرهای الکترونیکی (حسگر فشار، دما، ولتاژ، بار، ...)
محتوا (اطلاعات) و کاربرد	زبان‌های برنامه‌نویسی	زبان‌های برنامه‌نویسی (متن‌گرا، شی‌گرا)
	نرم‌افزارهای کاربردی	نرم‌افزارهای ارتباطی (ایمیل، تلگرام، واتس‌آپ، ...)، نرم‌افزارهای موتورهای جستجو (گوگل، یاهو، مایکروسافت، ...) نرم‌افزارهای خدمات بانکی، نرم‌افزارهای محاسباتی، نرم‌افزارهای مدیریت داده، وبلاگ‌ها، دایره‌المعارف‌های آنلاین (ویکی‌پدیا)
جامعه و مردم در فضای سایبر	خبرگزاری‌های آنلاین	خبرگزاری‌های رادیویی و تلویزیونی آنلاین
	ارتباطات آنلاین علمی	برگزاری جلسات علمی آنلاین، شرکت در کنفرانس‌های علمی به‌طور آنلاین، ...
	ارتباطات آنلاین مذهبی	برگزاری مجالس مذهبی آنلاین، پخش زنده دعاها و نمازهای جماعت به‌طور آنلاین، ...
	ارتباطات آنلاین سلامت‌محور	ارتباطات و وبلاگ‌های سلامت‌محور تحت وب
	ارتباطات تجاری و سیاسی	خدمات بانکی، بورسی آنلاین، برگزاری جلسات مدیران و اجلاس‌های سیاسی به‌طور آنلاین

1. SCADA.

مفهوم‌شناسی متغیرها

فضای سایبر: فضای سایبر، مجموعه‌ای است از سیستم‌های الکترونیکی و شبکه‌های رایانه‌ای، زیرساخت‌های ارتباطی، تجهیزات سخت‌افزاری، سیستم‌های ارتباطی و کنترلی و حسگری به‌منظور تولید، ذخیره‌سازی، پردازش، تبادل، بازیابی و بهره‌برداری از داده‌ها(Shaw, 2010). برخی فضای سایبر را با اینترنت یکی می‌گیرند که اشتباه است؛ چراکه فضای سایبر ارتباطات صورت گرفته مبتنی بر سیستم‌های مخابراتی، الکترونیکی و حسگری را نیز شامل می‌شود. برخی نیز فضای سایبر را فضای مجازی[1] معنا می‌کنند که این نیز اشتباه است، فضای سایبر اگرچه مجازی است (به این معنا که در عالم واقعیت وجود ندارد)، اما دقیقاً معادل «مجازی» نیست. برای این منظور لازم است اشاره کنیم واژه مجازی دو حوزه را پوشش می‌دهد و هم برای بیان آنچه در جهان واقعیت وجود ندارد به کار می‌رود و هم در علوم رایانه برای توصیف آنچه توسط سیستم الکترونیکی رقم می‌خورد.

مدل مفهومی: مدل‌سازی مفهومی، طرح توصیف‌گری از برخی جنبه‌های موضوع پژوهش برای تحقق مفاهیم درونی آن و ارتباط بین آن مفاهیم است. محصول اصلی این فعالیت استخراج مفاهیم و رابطه بین آن‌ها است (رضا تقی‌پور ۱۳۹۷ زمستان).

علوم و فناوری‌های کوانتومی: فناوری‌های کوانتومی مبتنی بر قوانین و اصول فیزیک کوانتومی هستند که این قوانین بر دنیای فوتون و ذرات زیراتمی حاکم می‌باشند که از سال ۱۹۰۰ میلادی به بعد توسط فیزیکدانان ارائه شدند و نگرش ما نسبت به ساختار ماده را تغییر دادند. برخی از این اصول و قوانین در تضاد کامل با بینش کلاسیک ما از جهان بزرگ‌مقیاس هستند. ازجمله این اصول و قوانین، اصل عدم قطعیت است که اندازه‌گیری دقیق و هم‌زمان کمیت‌هایی مانند مکان یک ذره و سرعت آن را غیرممکن می‌داند. همین باعث می‌شود که پیش‌بینی ما از تحولات دنیای زیراتمی نه بر مبنای قطعیت، بلکه بر مبنای احتمال باشد. محاسبه احتمال با استفاده از شکل ریاضی تابع موجی است که ذره را همراهی می‌کند (Chang, Lin, Chiu, & Huang, 2020). بنابر توصیف موجی از ذرات، یک

1. Virtual Space.

ذره تا زمانی که مورد اندازه‌گیری و مشاهده قرار نگرفته است، در هر حالتی می‌تواند باشد که به آن برهم‌نهی کوانتومی[1] گفته می‌شود. خصلت موجی ذرات سبب می‌شود که ذره از مکان‌هایی عبور کند که به لحاظ قوانین جهان بزرگ‌مقیاس ممنوع هستند که این پدیده تونل‌زنی[2] نام دارد. همچنین دو ذره می‌توانند دارای ارتباطی عجیب و شگفت‌انگیز شوند؛ به‌طوری که تغییر در وضعیت یک ذره توسط ذره دیگر به‌صورت آنی حس می‌شود که به آن درهم‌تنیدگی[3] می‌گویند. خصوصیت‌های گفته‌شده از اصلی‌ترین پارامترهای شکل گرفتن فناوری‌های کوانتومی در بسیاری از حوزه‌های مختلف مانند الکترونیک، پزشکی، مخابرات و ... از نیمه دوم قرن بیستم به بعد شده است (Bennett & Brassard, 2020). حوزه‌های فناوری‌های کوانتومی را می‌توان به حوزه‌های ارتباطات، محاسبات، شبیه‌سازی و حسگرها تقسیم کرد. در دو دهه اخیر که معلوم شده است که می‌توان از ویژگی‌های برهم‌نهی و درهم‌تنیدگی در فناوری‌های مرتبط با محاسبات و پردازش اطلاعات و ساخت رایانه‌های کوانتومی و همین‌طور ایجاد ارتباطات امن و رمزگذاری‌شده استفاده کرد (دوستی‌مطلق، ۱۳۹۶).

رایانه‌های کوانتومی قدرت محاسباتی بسیار بالایی دارند و قادرند محاسباتی را انجام دهند که با رایانه‌های کلاسیک میلیون‌ها میلیون سال طول می‌کشد. همچنین رایانه‌های کوانتومی محدودیت‌های رایانه‌های کلاسیک را ندارند. یکی از مهم‌ترین زیرمجموعه‌های این فناوری‌ها حوزه ارتباطات است. عصری که در آن به سر می‌بریم عصر اطلاعات و ارتباطات است و انسان امروزی به سرعت و دقت در تولید، ذخیره‌سازی، انتقال و بازیابی اطلاعات در شبکه‌های ارتباطی نیاز روزافزونی دارد که ازجمله آن‌ها می‌توان به شبکه رایانه‌ها، اینترنت و مخابرات اشاره کرد که در آن‌ها ارسال داده‌ها با سرعت و امنیت بالا دارای اهمیت فراوانی است. ارسال اطلاعات محرمانه و مخابره پیام به‌صورت امن و غیرقابل دسترس برای هکرها، از دیرباز فکر آدمی را به خود مشغول کرده است.

1.Quantum Superposition.
2.Tunneling.
3.Entanglement.

تأثیر علوم و فناوری‌های کوانتومی بر فضای سایبر

در عصر ظهور علوم و فناوری‌های کوانتومی ابعاد، مؤلفه‌ها و شاخصه‌های مختلف فضای سایبر تحت تأثیر قرار می‌گیرند؛ بنابراین ساختار فضای سایبر به‌صورت یک ساختار متشکل از سیستم‌های کلاسیکی و کوانتومی درمی‌آیند؛ بنابراین شناخت دقیق و کامل علوم و فناوری‌های کوانتومی و نقش و تأثیر آن‌ها بر هرکدام از لایه‌های فضای سایبر امری ضروری و انکارناپذیر به شمار می‌آید.

با بررسی اسناد و مدارک و تحقیقات صورت گرفته در زمینه علوم و فناوری‌های کوانتومی به‌خصوص در یک دهه اخیر می‌توان بر اساس مدل مفهومی فضای سایبر کلاسیک شاوو، لایه زیرساخت فضای سایبری را که متأثر از علوم و فناوری‌های کوانتومی است به سه زیر لایه یا سه مؤلفه تقسیم کرد: مؤلفه محاسبات کوانتومی، مؤلفه ارتباطات کوانتومی و مؤلفه حسگری کوانتومی. درواقع علوم و فناوری‌های کوانتومی در هرکدام از این سه مؤلفه فضای سایبر فناوری‌های نوظهوری را به وجود آورده است که هم محاسبات و رایانش را متحول ساخته است و هم ارتباطات و مخابرات و هم سیستم‌های حسگری را به‌طور کامل تحت تأثیر قرار داده است. در ادامه هرکدام از این سه مؤلفه و شاخصه‌های آن‌ها تبیین می‌شوند.

مؤلفه محاسبات کوانتومی

حوزه محاسبات کوانتومی یکی از حوزه‌های فناوری جدید است که به آن فناوری‌های کوانتومی گفته می‌شود. فناوری‌های کوانتومی مبتنی بر قوانین و اصول فیزیک کوانتومی هستند که بر دنیای زیراتمی حاکم می‌باشند و از سال ۱۹۰۰ میلادی به بعد توسط دانشمندان ارائه شده، نگرش ما را نسبت به ساختار ماده تغییر داد. برخی از این اصول و قوانین در تضاد کامل با بینش کلاسیک ما از جهان بزرگ‌مقیاس دارند. ازجمله این اصول و قوانین، اصل عدم قطعیت است که اندازه‌گیری دقیق و هم‌زمان کمیت‌هایی مانند مکان یک ذره و سرعت آن را غیرممکن می‌داند. همین باعث می‌شود که پیش‌بینی ما از تحولات

دنیای زیراتمی نه بر مبنای قطعیت بلکه بر مبنای احتمال باشد. محاسبه احتمال با استفاده از شکل ریاضی تابع موجی است که توصیف‌کننده یک ذره در دنیای کوانتومی است. بنا بر توصیف موجی از ذرات، یک ذره تا زمانی که مورد اندازه‌گیری و مشاهده قرار نگرفته است، در هر حالتی می‌تواند باشد که به آن برهم‌نهی کوانتومی گفته می‌شود. خصلت موجی ذرات سبب می‌شود که ذره از مکان‌هایی عبور کند که از منظر قوانین جهان بزرگ‌مقیاس ممنوع باشند؛ پدیده‌ای که از آن با نام تونل‌زنی کوانتومی یاد می‌شود. همچنین دو ذره می‌توانند دارای ارتباطی عجیب و شگفت‌انگیز شوند؛ به‌طوری که تغییر در وضعیت یک ذره توسط ذره دیگر به‌صورت آنی حس می‌شود که به آن درهم‌تنیدگی می‌گویند (Hidary, 2019; Resch & Karpuzcu, 2019).

رایانه‌های کوانتومی قدرت محاسباتی بسیار بالایی دارند و قادرند محاسباتی را انجام دهند که با رایانه‌های کلاسیک هزاران سال طول می‌کشد. همچنین رایانه‌های کوانتومی محدودیت‌های رایانه‌های کلاسیک را ندارند. بررسی مختصر نشان می‌دهد که بسیاری از کشورها در بخش‌های مختلف (علمی، اقتصادی، امنیتی-دفاعی) توجه ویژه‌ای به حوزه رایانه‌های کوانتومی داشته‌اند. این موضوع را می‌توان در حجم عظیم سرمایه‌گذاری‌های بخش‌های مختلف این کشورها به‌وضوح مشاهده کرد.

یکی از اصول بسیار مهم در مکانیک کوانتومی تحول سیستم‌ها بر اساس تبدیل‌های یکانی[1] است. مبنای ریاضی عملیات مبتنی بر جبر خطی در فضای ریاضی مورد استفاده در مکانیک کوانتومی موسوم به فضای هیلبرت تعریف می‌شود که در کلی‌ترین حالت می‌تواند به‌وسیله ماتریس‌های یکانی با درایه‌های مختلط نمایش داده شود. به بیان ساده‌تر گیت‌های کوانتومی، ماتریس‌هایی یکانی هستند که اثرشان روی یک حالت کوانتومیِ توصیف‌کننده سیستم، حالت جدیدی را به دست می‌دهند. شرح دقیق ریاضیات گفته‌شده در بسیاری از منابع آمده است. پل بنیوف[2] در سال ۱۹۸۰ میلادی در کار خود نشان داد که تبدیلات

1. Unitary transformation.
2. Paul Benioff.

یکانی معادل با همان گیت‌های منطقی مورد استفاده در محاسبات است و بنابراین می‌توان محاسبات را با استفاده از این تبدیل‌ها انجام داد. سال ۱۹۸۵ میلادی، دیوید دویچ[1] نشان داد که چگونه می‌توان از توازی کوانتومی[2] و تبدیلات یکانی برای رسیدن به محاسبات سریع‌تر استفاده کرد. دویچ روش معروف خود را برای تعیین اینکه یک تابع ثابت است یا متوازن، به کار برد و نشان داد که محاسبات کوانتومی بسیار کارآمدتر از محاسبات کلاسیک است. در روش دویچ، تعیین توابع ثابت و متوازن تنها با یک بار مقداردهی انجام می‌شود، در حالی که در محاسبات کلاسیک راهی جز مقداردهی به ازای تمام حالت‌های ورودی ممکن وجود ندارد. کار دویچ برتری محاسبات کوانتومی نسبت به محاسبات کلاسیک را به اثبات رساند. پس از آن، دویچ به همراه جوزا[3] این روش را توسعه دادند و توانستند با همین سرعت این خصوصیت را برای توابع با ورودی بیشتر هم به کار ببرند. تا مدتی این ایده فقط از لحاظ نظری جالب توجه بود تا اینکه پیتر شور[4] در سال ۱۹۹٤ میلادی الگوریتمی کوانتومی، برای تجزیه اعداد به عوامل اول معرفی نمود. روش شور قادر است در زمانی بسیار کم اعداد را به عوامل اول تجزیه کند. پس از او، لو گروور[5] الگوریتمی را ایجاد کرد که از رایانه‌های کوانتومی برای جستجو در پایگاه داده‌های نامرتب استفاده می‌کند؛ بنابراین الگوریتم‌های مورد استفاده در رایانه‌های کوانتومی، کاملاً متفاوت از همتایان کلاسیک خود هستند. الگوریتم‌های دیگری نیز ایجاد شده‌اند و تا به امروز تلاش برای ارائه الگوریتم‌های کارآمد کوانتومی ادامه دارد. جدول زیر مقایسه‌ای کلی از رایانه‌های کلاسیک و کوانتومی را نشان می‌دهد.

1. David Deutsch.
2. Parallelism.
3. Jozsa.
4. Peter Shor.
5. Lov Grover.

جدول ٦: مقایسه رایانه‌های کلاسیک و کوانتومی

رایانه کلاسیک	رایانه کوانتومی
اطلاعات بر روی بیت‌ها ذخیره می‌شوند.	اطلاعات بر روی کیوبیت‌ها ذخیره می‌شوند.
بیت‌ها بر مبنای بار یا ولتاژ الکتریکی طراحی می‌شوند.	کیوبیت‌ها بر مبنای پدیده‌هایی مانند اسپین ذرات یا قطبش فوتون‌ها طراحی می‌شوند.
پردازش اطلاعات توسط گیت‌های کلاسیک انجام می‌شود.	پردازش اطلاعات توسط گیت‌های کوانتومی انجام می‌شود.
عملیات منطقی مبتنی بر جبر بول است.	عملیات مبتنی بر جبر خطی در فضای هیلبرت تعریف می‌شود که در کلی‌ترین حالت می‌تواند به‌وسیله ماتریس‌های یکانی با درایه‌های مختلط نمایش داده شود.
هیچ محدودیتی برای تکثیر و اندازه‌گیری سیگنال‌ها وجود ندارد.	برای تکثیر و اندازه‌گیری سیگنال‌ها محدودیت وجود دارد.
مدارها به‌راحتی توسط فناوری‌های میکروسکوپیک سریع و مقیاس‌پذیر (مانند CMOS) پیاده‌سازی می‌شوند.	در رایانه‌های کوانتومی مدارها با استفاده از فناوری‌های میکروسکوپیک مانند تراشه‌های مبتنی بر مدارهای ابر رسانایی پیوند جوزفسون پیاده‌سازی می‌شوند.

توسعه رایانه‌های کوانتومی که توان محاسباتی بالایی دارند، می‌تواند عواقب وخیمی برای امنیت سایبر داشته باشد. به‌عنوان مثال، اعتقاد بر این است که اگر یک رایانه کوانتومی به اندازه کافی بزرگ ساخته شود، حل مسائل ریاضیاتی مهم مانند فاکتورگیری و لگاریتم‌های گسسته و همچنین حل مسائلی که با دشواری همراه است را قطعی می‌سازد و امنیت بسیاری از پروتکل‌های به‌کاررفته (مانند RSA، DSA، ECDSA) را می‌تواند به‌طور مؤثر به خطر اندازد و سیستم‌های رمزنگاری امروزی را به‌راحتی بشکند. در حالی که این نظریه از دهه ۱۹۹۰ میلادی شناخته شد، اما چشم‌انداز واقعی ساخت چنین دستگاهی اخیراً به‌صورت واقعی تحقق یافته است.

شرکت گوگل در سال ۲۰۱۸ میلادی یک پردازنده ۷۲ کوبیتی را ارائه کرد که بیشتر از رکورد آی‌بی‌ام در سال ۲۰۱۷ میلادی است که پردازنده کوانتومی ۵۰ کوبیتی را ارائه داده بود. در سال ۲۰۱۸ میلادی شرکت گوگل اعلام کرده بود که تراشه جدید آن‌ها ممکن است ظرف یک سال به برتری کوانتومی (رایانه کوانتومی) دست یابد. اصطلاح «برتری

کوانتومی»[1] به توانایی یک کامپیوتر کوانتومی در انجام محاسبات فراتر از توانمندترین ابررایانه‌های کلاسیکی امروزی اشاره دارد؛ اما فقط تعداد کیوبیت‌ها مهم نیستند، بلکه ترکیبی از عواملی ازجمله عمق یک مدار کوانتومی[2] یا اینکه چه تعداد عملیات منطقی را می‌تواند قبل از تکثیر خطاها انجام دهد نیز مهم هستند و بر قدرت محاسباتی واقعی که محققان آی‌بی‌ام آن را «حجم کوانتومی»[3] نامیده‌اند، تأثیر می‌گذارد.

در ژانویه سال ۲۰۱۹ میلادی، شرکت آی‌بی‌ام یک رایانه کوانتومی را که در یک محفظه ضد آب و یک یخچال در ۲۷۳- درجه سانتی‌گراد در محیطی عاری از تابش الکترومغناطیسی یا لرزش قرار گرفته بود را ارائه کرد. رایانه کوانتومی این شرکت از ۲۰ کیوبیت بهره می‌برد.

در اواخر سال ۲۰۱۹ میلادی و چند ماه پس از اعلام آی‌بی‌ام، گوگل اعلام کرد که با استفاده از یک رایانه مشابه قادر به حل یک مسئله پیچیده تنها در ۳.۲۰ دقیقه شده است، مسئله‌ای که یک دستگاه کلاسیک می‌توانست آن را در ده هزار سال حل کند؛ بنابراین گوگل به «برتری کوانتومی» رسیده است (Arute et al., 2019).

مؤلفه ارتباطات کوانتومی

به‌طور کلی بُعد فیزیکی یا زیرساخت سیستمی ارتباطات کوانتومی از مجموعه‌ای از فناوری‌های کوانتومی تشکیل شده است که افزاره‌های کوانتومی مورد نیاز را برای انجام فرایند ارتباطات کوانتومی فراهم آورده است. این فناوری‌ها عبارت‌اند از چشمه نور کوانتومی، خطوط ارتباطی کوانتومی، مدار پردازشی، تکرارکننده کوانتومی، سوییچ کوانتومی، حافظه کوانتومی و مسیریاب کوانتومی و آشکارسازهای کوانتومی. در ادامه شاخصه‌های مؤلفه ارتباطات کوانتومی بیان می‌شود.

1. Quantum supremacy.
2. Depth of a quantum circuit.
3. Quantum volume.

چشمه‌های نور فوتونی (تک فوتون و درهم‌تنیده)

چشمه‌های فوتونی منابع تولید فوتون‌ها بوده که برای فناوری‌های کوانتومی همچون محاسبات و ارتباطات کوانتومی بسیار پرکاربرد و پراهمیت هستند. فوتون‌ها به‌عنوان حامل‌های اطلاعات کوانتومی در سیستم‌های کوانتومی مورد استفاده قرار می‌گیرند. این منابع قابلیت تولید فوتون‌ها را داشته و به‌ویژه در سیستم‌های رمزنگاری کوانتومی امن حیاتی هستند. یک چشمه فوتونی ایده‌آل باید بتواند به‌صورت دقیق و تک‌به‌تک در بازه زمانی مورد نظر و با بازده کافی (به‌صورت کنترل‌شده و به‌سادگی در شرایط محیطیِ عادی) فوتون تولید کند؛ اما در واقعیت و تاکنون هیچ چشمه فوتونی ایده‌آلی ساخته نشده است. به همین منظور چندین نوع از چشمه‌های فوتونی تولید شده که هرکدام دارای معایب و مزایای خاص خود هستند که ممکن است آن‌ها را برای هر کاربرد خاصی مناسب سازد. از چشمه‌های فوتونی برای تولید فوتون‌های درهم‌تنیده یا تک فوتون‌ها استفاده می‌شود که البته منابع هرکدام گونه‌های خاص خود را دارند. فوتون‌های درهم‌تنیده تولیدشده از این منابع باید به‌صورت جفتی و قابل تمایز و کنترل تولید داشته باشد. چشمه‌های تک فوتون نیز به دو گروه منابع فوتونی دقیق که معمولاً بازده و کنترل‌پذیری کمی دارند و احتمالی که در ازای ارائه بازده مناسب و کنترل‌پذیری بهتر به‌صورت احتمالی تعدادی فوتون تولید می‌کنند، تقسیم کرد. در منابع احتمالی چشمه‌های تک فوتونی همواره احتمال تولید حالاتی با بیش از یک فوتون وجود دارد که البته می‌توان با ایجاد شرایط مناسب این احتمال را به حداقل رساند (Gupta, P. Pandey, P. & Pathak A.2006; Eisaman, M. D. et al. 2011).

خطوط ارتباطی

خطوط ارتباطی که در شبکه‌های کوانتومی و ارتباطات کوانتومی برای تبادل کیوبیت‌ها استفاده می‌شود خطوط فیبر نوری و شبکه‌های بی‌سیم هستند که در ارتباطات کلاسیک نیز مورد استفاده قرار می‌گیرند.

مدارهای پردازشی کوانتومی

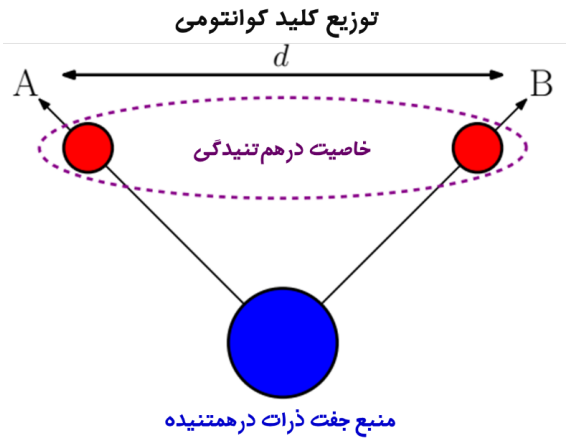
مدارهای پردازشی کوانتومی که در ارتباطات کوانتومی استفاده می‌شوند شامل مدارهای منطقی کوانتومی هستند که فرایندهای منطقی را بر روی کیوبیت‌ها (سیستم‌های فیزیکی دوترازه) انجام می‌دهند. این مدارهای منطقی شامل گیت‌های منطقی هادامارد، CNOT کنترلی، گیت‌های منطقی پائولی و ... هستند. در حقیقت هر مدار کوانتومی می‌تواند به‌منظور پیاده‌سازی یک الگوریتم کوانتومی به کار گرفته شود.

تکرارکننده‌های کوانتومی

در یک سیستم مخابرات کوانتومی، اطلاعات کوانتومی را از یک نقطه به نقطه‌ای دیگر ارسال می‌کردند. به دلیل استفاده از زیرساختی به نام درهم‌تنیدگی کوانتومی، سیستم‌های مخابرات کوانتومی بسیار امن و غیرقابل نفوذ هستند. توزیع و کنترل درهم‌تنیدگی در مقیاس جهانی از ملزومات مخابرات کوانتومی راه دور است. هم‌اکنون تنها سیستم کوانتومی مناسب برای مخابرات کوانتومی راه دور فوتون‌ها هستند. یکی از مشکلات طرح‌های مبتنی بر فوتون، تلفات فوتون و پدیده ناهمدوسی در کانال‌های کوانتومی (فیبر نوری و فضای آزاد) است. این موضوع فاصله قابل عبور برای تک فوتون را به حدود کمتر از ۵۰۰ کیلومتر محدود می‌کند. این مشکل را می‌توان با تقسیم فواصل طولانی به فواصل کوتاه‌تر برطرف کرد، به‌طوری که بتوان درهم‌تنیدگی را در این فواصل کوتاه‌تر حفظ کرد. سیستمی که این وظیفه را به عهده دارد، تکرارکننده کوانتومی نامیده می‌شود.

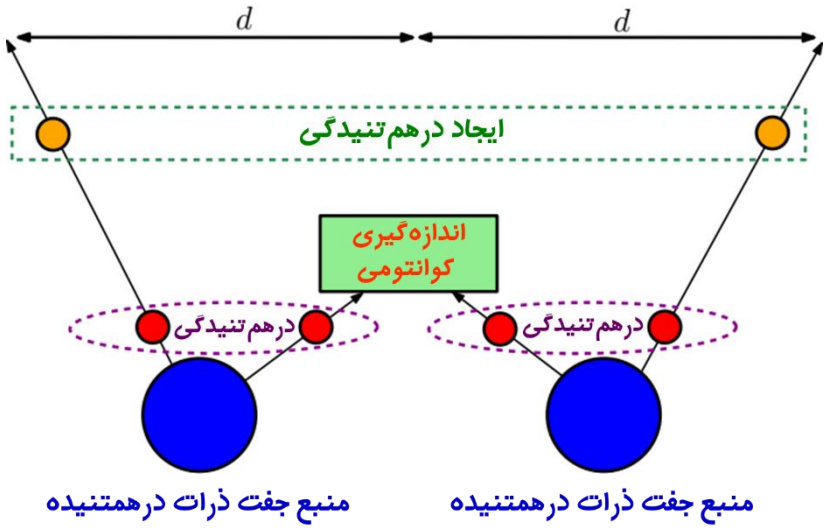
در ارتباطات کلاسیکی (مخابرات کلاسیکی یا مخابراتی که هم‌اکنون از آن استفاده می‌شود)، برای انتقال اطلاعات در مسافت‌های طولانی از دکل‌های مخابراتی به‌عنوان تکرارکننده‌ها استفاده می‌کنند؛ بنابراین مشابه حالت کلاسیکی، برای توزیع حالت‌های کوانتومی در مسافت‌های طولانی نیز از تکرارکننده‌های کوانتومی استفاده می‌شود. از سوی دیگر، آزمایش‌ها نشان می‌دهد که به هر میزان توزیع کلید کوانتومی پیشرفت کند، به‌عنوان یک قاعده کلی انتقال حالت‌های کوانتومی در مسافت‌های بیشتر از ۵۰۰ کیلومتر امکان‌پذیر

نیست. از این رو نیاز به تکرارکننده‌های کوانتومی برای دست‌یابی بـه مسـافت‌هـای بیشـتر بسیار ضروری است. یکی از روش‌های پیاده‌سازی توزیع کلید کوانتومی درواقع اسـتفاده از خاصیت درهم‌تنیدگی یک جفت ذره است. پیاده‌سازی توزیع کلید کوانتومی بـا اسـتفاده از خاصیت درهم‌تنیدگی با ارسال یک ذره از یک جفت درهـم‌تنیـده بـه طـرف دیگـر کانـال کوانتومی امکان‌پذیر است. از این رو توزیع کلید کوانتومی را می‌توان به‌عنوان توزیع جفـت ذرات درهم‌تنیده خلاصه نمود (شکل ۲را ببینید).



شکل ۲: توزیع کلید کوانتومی با استفاده از خاصیت درهم‌تنیدگی [Li, Z.D et al. 2019].

شکل (۳) یک تکرارکننده کوانتومی را نشان مـی‌دهـد کـه از دو منبـع ذرات درهـم‌تنیـده تشکیل شده است. چهار ذره در چهار فیبر نوری مختلف (یا چهار کانال کوانتـومی مختلـف) قرار می‌گیرد؛ به‌گونه‌ای که یک ذره از هر منبع به یک دستگاه اندازه‌گیـری کوانتـومی مـی‌رود در حالی که دو ذره باقی‌مانده در جهات مخالف قرار دارند. در دستگاه اندازه‌گیـری کوانتـومی می‌توان برهمکنش‌هایی را ایجاد نمود که باعث درهم‌تنیـدگی بـین ایـن دو ذره گـردد و ایـن درهم‌تنیدگی نیز متعاقباً باعث ایجاد درهم‌تنیدگی بـین دو ذره‌ای خواهـد شـد کـه در جهـت مختلف از هم قرار داشتند. از این رو دو ذره دوردست با یکدیگر درهم‌تنیده می‌شوند. در این حالت می‌توان توزیع کلید کوانتومی را برای مسافتی بیش از حالت قبل (دو برابر حالتی که بـا یک منبع درهم‌تنیدگی کار می‌کردیم، یعنی 2d) ارسال نمود (شکل ۳ را ببینید).



شکل۳: طرح‌واره‌ای از یک تکرارکننده کوانتومی [Li, Z.-D et al., ۲۰۱۹]

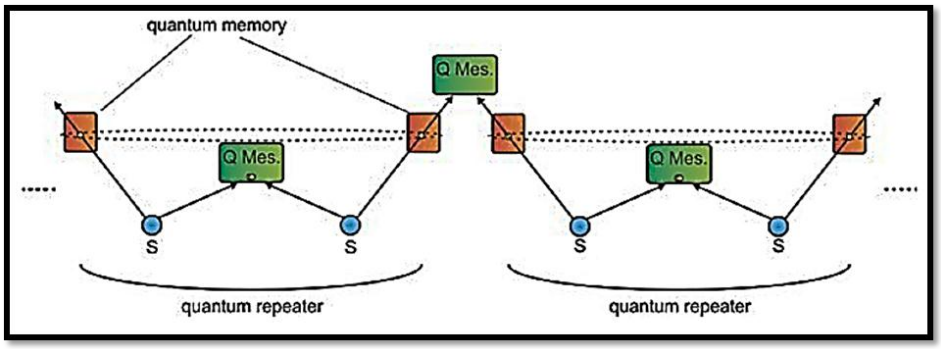
به‌منظور افزایش مسافت‌های بسیار زیاد، می‌توان از زنجیره تکرارکننده‌های کوانتومی یکی پس از دیگری قرار دارند، استفاده نمود(شکل٤). آزمایش‌ها نشان می‌دهد که اضافه کردن یک حافظه‌ی کوانتومی به هر طرف تکرارکننده کوانتومی، عملکرد آن را به‌طور بالقوه‌ای افزایش خواهد داد؛ بنابراین وجود تکرارکننده‌های کوانتومی به‌منظور افزایش مسافت انتقال حالت کوانتومی بسیار ضروری است و این باعث ایجاد شبکه ارتباطی و در نتیجه اینترنت کوانتومی در آینده نزدیک خواهد شد. در یک تکرارکننده‌ی کوانتومی سه فناوری اساسی و مهم وجود دارد که عبارت‌اند از [Li, Z.-D et al., 2019] :

ـ تعویض درهم‌تنیدگی[1]،

ـ تصفیه‌ی درهم‌تنیدگی[2]،

ـ حافظه‌ی کوانتومی.

1. Entanglement swapping.
2. Entanglement purification.



شکل ٤: زنجیره‌ای از تکرارکننده‌های کوانتومی به همراه حافظه کوانتومی [Li, Z.-D et al., ۲۰۱۹].

مسیریاب کوانتومی

فوتون‌ها با استفاده از کابل‌های فیبر نوری از یک منطقه به منطقه دیگر ارسال می‌شوند. درواقع هدایت فوتون از یک کانال فیبر نوری به کانال دیگر، نیازمند مسیریاب کوانتومی است. برای این منظور از سیگنالی به نام سیگنال کنترل استفاده می‌شود تا با توجه به خاصیت درهم‌تنیدگی بین سیگنال کنترل و سیگنال داده (سیگنالی که اطلاعات را حمل می‌کند)، بعد از اندازه‌گیری روی سیگنال کنترل، بتوان مسیر مناسب را برای سیگنال داده مشخص کرد. مسیریاب‌های کوانتومی به دو نوع مسیریاب اپتیکی و مسیریاب مبتنی بر، برهم‌کنش اتم با فوتون تقسیم می‌شوند.

حافظه کوانتومی

حافظه‌های کوانتومی کاربردهای متنوعی دارند. حافظه‌های کوانتومی نه‌تنها در فناوری‌های کوانتومی، بلکه در مطالعات نظری و بنیادین فیزیک نقش بسزایی دارند. یکی از کاربردهای مهم حافظه‌های کوانتومی استفاده از آن‌ها به‌عنوان منابع تک فوتون است. منابع تک فوتون نقش کلیدی در بیشتر الگوریتم‌ها و پروتکل‌های مبتنی بر فناوری‌های کوانتومی دارند. یکی از روش‌های مرسوم و در عین حال غیرتعینی برای تولید تک فوتون‌ها استفاده از روش (Parametric down-conversion) است. به‌سادگی و به کمک یک

حافظه‌ی کوانتومی می‌توان از همین روش، منبع تک فوتون تعینی ساخت. از روش‌های تبدیل پایین پارامتری و تلفیق چهارموج می‌توان برای تولید زوج‌های درهم‌تنیده استفاده کرد. ولی این زوج‌ها به‌صورت غیرتعینی تولید می‌شوند. با قرار دادن یک آشکارساز در یکی از خروجی‌ها و یک حافظه‌ی کوانتومی در خروجی دیگر می‌توان یک منبع تک فوتون ساخت. روش کار به این صورت است که وقتی آشکارساز کلیک کرد به این معنا است که زوج درهم‌تنیده تولید شده است. در این صورت فوتون دیگر در حافظه‌ی کوانتومی ذخیره شده و به اصطلاح «شارژ» شده است. در این صورت چون در حافظه‌ی کوانتومی یک فوتون قرار دارد می‌توان از آن به‌عنوان یک منبع تک فوتون استفاده کرد. منابع تک فوتون نقش بسزایی در محاسبات کوانتومی نوری دارند.

حافظه کوانتومی در توسعه و پیشرفت بسیاری از دستگاه‌های پردازش اطلاعات کوانتومی ضروری است، ازجمله یک ابزار هماهنگ‌سازی که منطبق سازی فرایندهای مختلف در یک کامپیوتر کوانتومی را بر عهده دارد، مفهوم یک دروازه کوانتومی که اجازه عبور حالات بدون تغییر را می‌دهد و در نهایت سازوکار تبدیل فوتون‌های قاصد به فوتون‌های درخواستی مثال‌هایی هستند که حافظه‌های کوانتومی در آن‌ها نقش مؤثری ایفا خواهند کرد. علاوه بر کامپیوترهای کوانتومی، از حافظه‌های کوانتومی نیز برای پیاده‌سازی ارتباطات کوانتومی در فواصل بالا –که در تکرارکننده‌های کوانتومی کاربرد دارد– استفاده می‌شود.

رمزنگاری کوانتومی مبتنی بر توزیع کلید کوانتومی

در فضای سایبر کوانتومی ارتباطات امن و تبادل داده امن به‌طور کلی به دو صورت ترابرد کوانتومی و رمزنگاری مبتنی بر توزیع کلید کوانتومی[1] صورت می‌گیرد.

در سال‌های اخیر پیشرفت‌های سریع و قابل توجهی در زمینه امنیت فضای سایبر کوانتومی در کشورهای توسعه‌یافته و سازمان‌ها یا شرکت‌ها و مؤسسات تحقیقاتی مهم

1. QKD.

جهان در بهره‌برداری از فناوری‌های کوانتومی در ارتباطات یا رمزنگاری کوانتومی جهت افزایش امنیت تبادل اطلاعات صورت پذیرفته است (Zhang et al., 2019). بالاترین سیستم نرخ بیت در حال حاضر مبادلات کلید ایمن را در یک مگابیت در ثانیه (بر روی فیبر نوری با طول بیش از بیست کیلومتر) و ده کیلوبیت بر ثانیه (بر روی فیبر نوری با طول بیش از ۱۰۰ کیلومتر) نشان داده است، که در سال ۲۰۰۸ میلادی با همکاری دانشگاه کمبریج و توشیبا با استفاده از پروتکل رمزنگاری BB84 حاصل شده است (Dixon, Yuan, Dynes, Sharpe, & Shields, 2008). در سال ۲۰۰۷ میلادی، آزمایشگاه ملی لس‌آلاموس/NIST توزیع کلید کوانتومی در طول ۱۴۸.۷ کیلومتر فیبر نوری با استفاده از پروتکل BB84 را به دست آورد (Hiskett et al., 2006). نکته قابل توجه این است که این مسافت تقریباً برای تمام مسافت‌هایی که در شبکه‌های فیبر نوری امروزی ایجاد شده است مناسب است و کاملاً هم‌خوانی دارد. اروپایی‌ها به‌طور مشترک QKD فضای آزاد را برای بیش از ۱۴۴ کیلومتر بین دو جزیره از جزایر قناری با استفاده از فوتون‌های درهم‌تنیده و با استفاده از پروتکل ایکرت در سال ۲۰۰۶ میلادی به دست آوردند (Ursin et al., 2006) و همین گروه در اتحادیه اروپا در سال ۲۰۰۷ میلادی با استفاده از پروتکل BB84 و با بهره‌گیری از حالت‌های Decoy موفق به دستیابی به همان نتایج شدند (Schmitt-Manderbach et al., 2007).

از آگوست سال ۲۰۱۵ میلادی، طولانی‌ترین فاصله با استفاده از کانال ارتباطی فیبر نوری (۳۰۷ کیلومتر) توسط دانشگاه ژنو و شرکت کورنینگ به دست آمد (Korzh et al., 2015). در همان آزمایش، نرخ کلید راز ۱۲.۷ کیلوبیت بر ثانیه تولید شد که آن را به بالاترین سیستم نرخ بیت در مسافت ۱۰۰ کیلومتری تبدیل کرد. در سال ۲۰۱۶ میلادی تیمی از کورنینگ و مؤسسات مختلف در چین مسافت ۴۰۴ کیلومتر را انجام دادند، اما با نرخ بیت کمتری که این آزمایش را برای این مسافت نمی‌توان کاربردی دانست (Yin et al., 2017).

در سال ۲۰۱۶ میلادی استارت آپی به نام کوانتوم اکسچنج[1]، گزارش کرده است که می‌تواند از طریق کانال فیبر نوری به طول ۸۰۵ کیلومتر که در امتداد ساحل شرقی آمریکا

1. Quantum Xchange.

قرار دارد، اطلاعات را انتقال داده و طولانی‌ترین شبکه توزیع کلید کوانتومی آمریکا را به وجود آورد. به‌علاوه دانشگاه شیکاگو، آزمایشگاه ملی آرگون و آزمایشگاه شتاب‌دهنده ملی فرمی[1]، به‌تازگی اعلام کردند در یک سرمایه‌گذاری مشترک قصد دارند بستری آزمایشی را با هدف امن‌سازی ارتباط داده به کمک ترابرد کوانتومی ایجاد کنند. کانال فیبر نوری یادشده، فاصله دو شهر نیویورک سیتی و ایالت نیوجرسی را به یکدیگر متصل کرده، به بانک‌ها و شرکت‌ها امکان می‌دهد تا اطلاعاتشان را در بستری امن انتقال دهند.

با وجود این انتقال کلیدهای کوانتومی در فواصل طولانی به گره قابل اعتماد نیاز دارند تا عملکردی مشابه را با تکرارکننده و تقویت‌کننده‌های استاندارد موجود در کابل‌ها از خود به نمایش بگذارند. پژوهشگران در این رابطه اعلام کرده‌اند که سیزده عدد از این گره‌ها را تاکنون تولید کرده‌اند. در این بخش‌ها، کلیدهای کوانتومی در قالب بیت‌های دیجیتالی رمزگشایی شده، سپس مجدداً به‌صورت کیوبیت تبدیل می‌شوند. البته از نظر نظریه در هنگام اجرای این کار، اگر آسیبی به کیوبیت‌ها برسد هکرها امکان دسترسی به اطلاعات را کسب می‌کنند. با وجود همه موارد یادشده، پژوهشگران توضیح می‌دهند که ارسال فوتون در طول کابل فیبر نوری مسئله بزرگی نیست؛ اما حفظ حالت درهم‌تنیدگی آن‌ها چالش اصلی را ایجاد می‌کند به‌خصوص اگر این کار در فواصل طولانی صورت گیرد. به همین منظور، دانشگاه‌ها و آزمایشگاه‌های ملی آمریکا با همکاری یکدیگر محیطی را به‌منظور طراحی و آزمایش روشی‌های مختلف ارسال کیوبیت به وجود آورده‌اند.

یک سال بعد، در ژوئن سال ۲۰۱۷ میلادی، به‌عنوان بخشی از پروژه «آزمایش‌های کوانتومی در مقیاس فضایی[2]»، فیزیکدانان چینی به سرپرستی پن ژیان‌وی[3] در دانشگاه علوم و فناوری چین فوتون‌های درهم‌تنیده را در مسافت ۱۲۰۳ کیلومتری بین دو ایستگاه زمینی اندازه‌گیری کردند و زمینه را برای آزمایش‌های QKD بین قاره‌ای در آینده فراهم کردند(Popkin, 2017). در آزمایش دیگری فوتون‌ها از یک ایستگاه زمینی به ماهواره‌ای به

1. Fermi National Accelerator Laboratory.
2. Quantum Experiments at Space Scale.
3. Pan Jianwei.

نام Micius ارسال شد و سپس در ایستگاه زمینی دیگری دریافت شد که در آنجا «بقای درهم‌آمیختگی دو فوتونی و نقض نامساوی بل تا ۰.۰۹± ۲.۳۷ مشاهده کردند». مسافت کلی این انتقال داده از ۱۶۰۰ تا ۲۴۰۰ کیلومتر متغیر است (Yin et al., 2017). سپس در همان سال پروتکل BB84 با موفقیت در خطوط ماهواره‌ای از ماهواره Micius به ایستگاه‌های زمینی در چین و اتریش آزمایش شد. در این آزمایش کلیدها ترکیب شدند و برای انتقال تصاویر و فیلم‌ها بین پکن در چین و وین در اتریش استفاده شدند (Liao et al., 2018). دو سال بعد، در ماه مه سال ۲۰۱۹ میلادی، گروهی به سرپرستی هنگ گوا[1] در دانشگاه پست و مخابرات پکن[2] آزمایش‌های میدانی یک سیستم QKD با متغیر پیوسته را از طریق شبکه‌های فیبر نوری زمینی متداول در دو شهر شیان و گوانگژو در مسافت‌های ۳۰.۰۲ کیلومتر (پهنای باند ۱۲.۴۸ dB) و ۴۹.۸۵ (پهنای باند ۱۱.۶۲ dB) گزارش دادند (Zhang et al., 2019).

همچنین در زمینه رایانش و محاسبات کوانتومی در سال‌های اخیر پیشرفت‌های چشم‌گیری صورت پذیرفته است که ازجمله مهم‌ترین آن‌ها می‌توان به پیشرفت‌های نظری و تجربی در حوزه رایانش کوانتومی توپولوژیک[3] اشاره کرد که نخست آنکه عاری از خطا بوده و در برابر اختلالات محیطی به‌طور ذاتی مقاوم است و دوم تنها کاندیدای رایانش کوانتومی جهان‌شمول[4] است.

مؤلفه حسگری کوانتومی

بالا بردن دقت در اندازه‌گیری هم از جهت علمی و هم از جهت فناوری و مهندسی همیشه دارای اهمیت بوده است. بسیاری از پیشرفت‌هایی که امروزه در حوزه‌های مختلف علوم رخ می‌دهد، به مدد ابزارهای دقیق است. ساخت ابزارهای دقیق توانایی پژوهشگران

1. Hong Guo.
2. Beijing University of Posts and Telecommunications.
3. Topological quantum computing.
4. Universal quantum computing.

را تا حد دست‌کاری اتم‌ها بالا برده و آن‌ها را قادر ساخته که با تک اتم‌ها کار کنند. کسب چنین توانایی‌ای منجر به جایزه‌ی نوبل فیزیک در سال ۲۰۱۲ میلادی گردید. در ادامه شاخصه‌های مؤلفه حسگری کوانتومی بیان می‌شود.

شتاب و گرانش‌سنج کوانتومی

مونیتورینگ شتاب برای بسیاری از فناوری‌ها، از ناوبری و هدایت گرفته تا سامانه‌های الکترونیک مرسوم ضروری است. شتاب‌سنج‌های معمول بر اساس اندازه‌گیری دقیق جابجایی جسم که می‌تواند با استفاده از خازن‌ها، پیزوالکتریک‌ها، تونل جریان یا روش‌های اپتیکی انجام شود، کار می‌کنند. اگرچه روش‌های اپتیکی می‌توانند جابجایی‌های بسیار کوچک را اندازه بگیرند، اما چون بر اساس تداخل الکترومغناطیسی کار می‌کنند، شتاب‌سنج‌های اپتیکی فعلی نمی‌توانند در مقیاس تراشه مجتمع‌سازی شوند یا در سنجش‌هایی که به توده جرم آزمایشی بزرگ نیاز دارند، استفاده شوند.

حسگرهای مبتنی بر سامانه‌های اپتومکانیک، بر مبنای ویژگی‌های اساسی نظریه کوانتوم و گرانش عمل می‌کنند. در این حسگرها فشار برهمکنش بین نور (فوتون) و ماده با استفاده از یک تشدیدکننده نوری (کاواک) اندازه‌گیری می‌شود. در بسیاری از حالات با اندازه‌گیری جابجایی فرکانس رزونانس کاواک می‌توان با دقت بسیار بالایی شتاب را اندازه گرفت. سامانه‌های اپتومکانیک با استفاده از یک نانوحفره کریستال–فوتونیِ یکپارچه می‌توانند به بررسی دقیق میزان جابه‌جایی جرم بپردازند. با استفاده از نانوحفره در بلورهای فوتونیکی مسطح (همچون سدیم–نیترید) می‌توان به معماری تراشه‌ای و ایجاد تفکیک‌پذیری‌های بالا در سنجش شتاب رسید. اندازه بسیار کوچک (در حدود سانتی‌متر مربع) و حساسیت بسیار بالای $10^{-12} m/\sqrt{Hz}$) این نوع حسگرها، استفاده آن‌ها در صنعت و تحقیقات آزمایشگاهی را بسیار گسترده کرده است.

رادار کوانتومی

یک فناوری شناسایی نوین کوانتومی است که در چارچوب الکترودینامیک کوانتومی مورد بررسی قرار می‌گیرد. سامانه‌های رادار کوانتومی یک دگرگونی بنیادین در توسعه‌ی رادار ایجاد خواهند کرد. تجزیه‌وتحلیل نظری نشان می‌دهد که اندازه‌گیری‌های کوانتومی می‌تواند بر محدودیت‌های کوانتومی استاندارد غلبه کند و به سطح حساسیت فوق‌العاده برسد. سامانه‌های رادار کوانتومی می‌توانند از عهده‌ی آشکارسازی اهداف متعارف برآید و نیز در شناسایی سامانه‌های راکتی و جنگ‌افزارهای رادارگریز ناحیه‌ی میکروموج توانمند است.

برای اولین بار لاکهید مارتین[1] شرکت هوافضا، تجهیزات نظامی و امنیت اطلاعات آمریکا اختراعی را در زمینه‌ی رادار کوانتومی به ثبت رسانده است، هرچند از سال ۲۰۰۸ میلادی هیچ اطلاعات جدیدی در مورد این برنامه ارائه نشده است. این ممکن است یا منعکس‌کننده سطح بالایی از محرمانه بودن پروژه یا برعکس، می‌توان ناشی از فقدان پیشرفت معنی‌دار آن باشد. چین ادعا می‌کند که این رادار را توسعه داده است و می‌تواند در صورت عملی بودن این فناوری ویژه بر توانایی‌های رادارگریز ایالات متحده غلبه کند و ارتش آزادی‌بخش خلق چین[2] را در کاهش چیرگی قدرت نظامی ایالات متحده توانمند می‌سازد.

رادار کوانتومی می‌تواند رادار کلاسیک را بهبود بخشد و از کاربردهای آن می‌توان به موارد زیر اشاره کرد:

۱. **نظامی**: نظارت، رهگیری اهداف متحرک شامل هواپیماها و موشک‌ها، هدایت و ناوبری و دید از پشت موانع.

۲. **کاربردهای غیرنظامی معمول**: استفاده در سامانه‌های تصویربرداری ماهواره‌ای، هدایت کشتی و هواپیما و کاربردهای هواشناسی.

1.Lockheed Martin.

2. The Chinese People's Liberation Army.

۳. کاوش‌های فضایی: مقدار قابل توجهی از آوارهای طبیعی و ساخته‌شده توسط انسان (از سنگ‌های کوچک گرفته تا ماهواره‌های قدیمی) در اطراف زمین وجود دارد. این اجسام کاوش‌های فضایی با سرنشین و بدون سرنشین را به خطر می‌اندازند.

٤. دفاع از سیاره زمین: چند سال گذشته شاهد علاقه‌مندی به راهبردهای مقابله با تهدیدات سیاره‌ای بوده‌ایم (ردیابی سیارک‌ها، ستاره‌های دنباله‌دار و دیگر اجسام نجومی که می‌تواند به زمین برخورد کنند). در این راستا، رویداد Shoemaker-levy9 که در آن یک ستاره دنباله‌دار به سطح مشتری برخورد کرد، امکان وقوع رویدادهایی در سطح انقراض بیشتری در سیاره ما را آشکار کرد.

تأثیر علوم و فناوری‌های کوانتومی بر لایه محتوا و کاربرد

رایانش و محاسبات کوانتومی یک زمینه نسبتاً نوین است که زمینه‌های جدیدی را به همراه خود به وجود آورده است. فناوری‌های کاملاً متفاوتی برای اجرای الگوریتم‌های کوانتومی وجود دارند و زبان‌های برنامه‌نویسی کوانتومی باید بتوانند نیازهای تمام کاربران را برآورده سازند. با توجه به رشد سریع محاسبات کوانتومی، تعداد زبان‌های برنامه‌نویسی کوانتومی در حال افزایش است. در حال حاضر بیش از ۱۹ زبان برنامه‌نویسی کوانتومی در سطح جهان وجود دارد.

برنامه‌نویسی کوانتومی فرایند پیاده‌سازی دستورالعمل‌هایی به نام برنامه‌های کوانتومی است که بر روی یک رایانه کوانتومی قابل اجرا باشد. زبان برنامه‌نویسی مکانیزمی ساختمند را جهت تعریف داده‌ها، عملیات یا تبدیل‌هایی که امکان دارد به‌طور خودکار روی آن داده انجام شود فراهم می‌آورد. معمولاً یک زبان برنامه‌نویسی شامل یک محیط نرم‌افزاری جهت وارد کردن متن برنامه، اجرا و رفع اشکال آن است. امروزه در زمینه رایانه‌های کوانتومی پیشرفت‌هایی صورت گرفته است و پیش‌بینی می‌شود که با توجه به قابلیت‌های بسیار بالای آن‌ها، این رایانه‌ها به‌زودی جایگزین کامپیوترهای کلاسیک یا در کنار آن‌ها به‌کارگیری شوند.

زبان‌های برنامه‌نویسی و نرم‌افزارهای کوانتومی

در سال ۱۹۹۶ میلادی اولین قدم در ایجاد زبان‌های برنامه‌نویسی کوانتومی توسط نیل[1] برداشته شد (Knill, 1996). نیل یک کد برای بیان الگوریتم‌های کوانتومی روی یک ماشین کوانتومی با حافظه‌ای با دسترسی تصادفی[2] یا به‌اختصار QRAM را معرفی نمود. بعد از آن در سال ۱۹۹۸ میلادی اولین زبان برنامه‌نویسی کوانتومی QCL[3] توسط برنهارد اومر[4] ارائه شد. سپس زبان‌های برنامه‌نویسی کوانتومی qGCL[5] (سال ۲۰۰۱)، Q[6] (سال ۲۰۰۳)، QPL[7] (سال ۲۰۰۴)، QML[8] (سال ۲۰۰۵) و Scaffold (سال ۲۰۱۲) معرفی شدند. از سال ۲۰۱۳ میلادی با معرفی زبان برنامه‌نویسی کوانتومی Quipper که اولین زبان برنامه‌نویسی کوانتومی سطح بالا است (Green, Lumsdaine, Ross, Selinger, & Valiron, 2013)، رقابت مابین کشورهای مختلف جهان به‌منظور ایجاد زبان‌های برنامه‌نویسی کوانتومی جدید به اوج خود رسید. سپس زبان برنامه‌نویسی کوانتومی مانند LIQUi| ⟩ در سال ۲۰۱۴ میلادی و QWIRE و IQu در سال ۲۰۱۷ میلادی معرفی شدند (Paolini, Roversi, & Zorzi, 2017). سرانجام شرکت مایکروسافت نیز در سال ۲۰۱۸ میلادی زبان برنامه‌نویسی کوانتومی سطح بالا خود به نام #Q را معرفی نمود و دور تازه‌ای از رقابت را میان کشورها و شرکت‌های مختلف به وجود آورد (Svore et al., 2018).

شرکت آی‌بی‌ام یک کیت نرم‌افزار اطلاعات کوانتومی به نام QISKit را توسعه داده است که یک کتابخانه کامل برای نوشتن، شبیه‌سازی و اجرای برنامه‌های کوانتومی است. این شرکت اخیراً کیت نرم‌افزار اطلاعات کوانتومی خود را به چهار بخش تقسیم کرده‌اند. بخش اول Terra نام دارد که اجازه برنامه‌نویسی در سطح ورودی‌ها و پالس‌های کوانتومی را

1. Knill.
2. Quantum Random Access Machine.
3. Quantum Computation Language.
4. Bernhard Ömer.
5. Quantum Guarded Command Language.
6. Quantum.
7. Quantum programming language.
8. Qt Modeling Language.

فراهم می‌نماید. بخش دوم Aqua نام دارد که یک زبان سطح بالا برای اجرای الگوریتم‌های مورد استفاده در شیمی کوانتومی و مسائل بهینه‌سازی است. بخش سوم Ignis نام دارد و جهت مشخص نمودن خطاها و بهبود اجرای ورودی‌ها مورد استفاده قرار می‌گیرد. بخش آخر Aer نام دارد. این بخش برای مطالعه محدودیت محاسبات کوانتومی با استفاده از شبیه‌سازی در دستگاه‌های کلاسیک مورد استفاده قرار می‌گیرد. QISKit برنامه‌های کوانتومی را به زبان‌های سطح پایین‌تر به نام OpenQASM ترجمه می‌کند. OpenQASM یک زبان اسمبلی کوانتومی است (Cross, Bishop, Smolin, & Gambetta, 2017). شرکت‌های دیگر نیز نرم‌افزارهای کوانتومی متعددی ارائه داده‌اند و در حال حاضر ده‌ها نرم‌افزار کوانتومی توسط شرکت‌های پیشرو در این زمینه ارائه شده است. جدول ۷ نمونه‌هایی از نرم‌افزارهای منبع باز را از سال ۲۰۰۰ تا سال ۲۰۱۶ میلادی نشان می‌دهد.

جدول ۷: لیستی از شبیه‌سازهای رایانه‌های کوانتومی منبع باز به همراه زبان مورد استفاده و مراکز ارائه‌دهنده این منابع

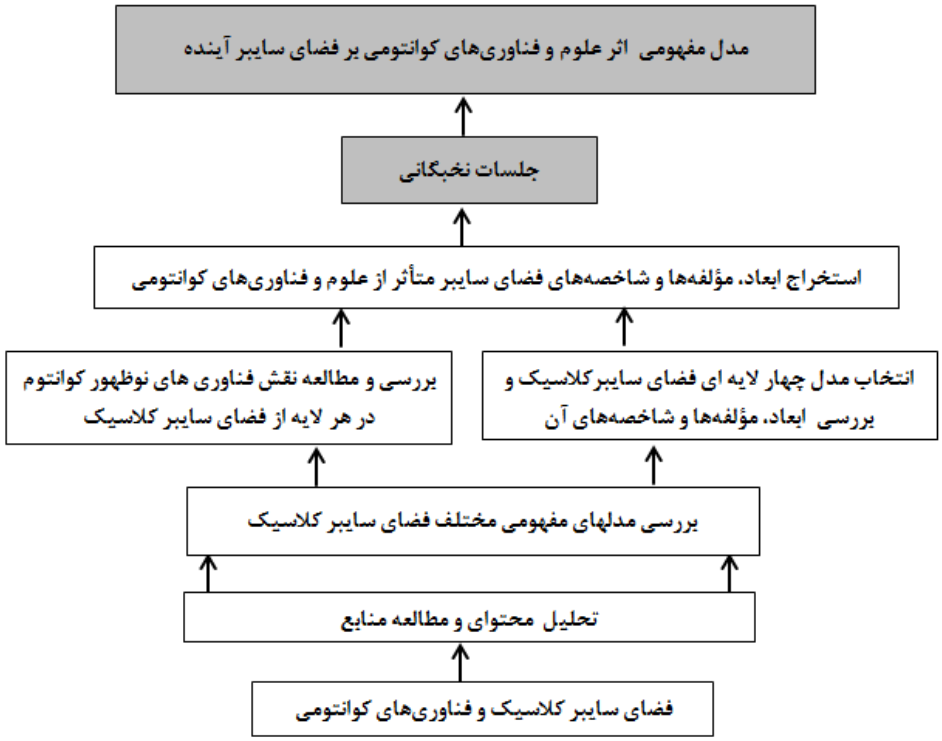
سال	نام	زبان	دانشگاه، شخص یا شرکت ارائه‌کننده
2000	QuCalc	Mathematica	Universite de Montreal, Canada
2000	Quantum-Superpositions	Perl	Damian Conway
2001	QMatrix	Mathematica	University of Potsdam, Germany
2002	Quantum-Entanglement	Perl	Alex Gough
2002	qoToolbox	Matlab	University of Auckland
2004	QGame++	C++	Hampshire College, USA
2004	CHP	C	Berkeley, USA
2005	Qsims	C++	Travis Beals
2005	Quack!	Matlab	Peter Rohde
2005	QIP	Mathematica	Carnegie-Mellon University, USA
2006	Qubiter	C++	Artiste-qb, Canada
2007	Zeno	Java	Federal University of Campina Grande, Brazil
2007	QCF	Matlab	Oxford University
2007	QDD	C++	David Greve
2007	LanQ	C-like	Hynek Mlna řík
2009	Cove	MS NET	Colorado Technical University, USA
2009	PyQu	Python	Google, USA
2009	Quantum-Octave	GNU Octave and Matlab	Polish Academy of Sciences, Poland
2010	QuBit	C++	Steven Goodwin

سال	نام	زبان	دانشگاه، شخص یا شرکت ارائه‌کننده
2010	jQuantum	Java	Fachhochschule Südwestfalen
2011	QuCoSi	C++	Frank S. Thomas
2011	Quantum	Mathematica	Tecnológico de Monterrey, Mexico
2012	Squankum	Java	Johns Hopkins Center
2012	TRQS	Mathematica	Polish Academy of Sciences, Poland
2012	QI	Mathematica	Polish Academy of Sciences, Poland
2012	Eqcs	C++	Peter Belkner
2013	Libquantum	C	Hannover, Germany
2013	Q++	C++	Cybernet Systems Corp
2013	Quantum Construct	C++	Shekhar Suresh Chandra.
2013	Qitensor	Python	Dan Stahlke
2013	qMIPS101	Java	University of Seville, Spain
2013	sqct	C++	University of Waterloo, Canada
2014	QuanSuite	Java	Artiste-qb, Canada
2014	QCL	C-like	AIT Austrian Institute of Technology
2014	Quantum Computing Playground	qScript	Google, USA
2014	QWalk	C	University of Illinois, USA
2014	jsqis	Javascript	University of California, USA
2014	Quipper	Haskell	Dalhousie University, Canada
2015	QuTip	Python	RIKEN, Japan; University of Michigan, USA
2015	SpinDec	C++	University College London, UK
2015	Quantum++	C++	University of Waterloo, Canada
2015	QDENSITY	Mathematica	University of Pittsburgh, USA
2015	QUIBIT4MATLAB	Matlab	WIGNER RCP, Hungary
2016	QETLAB	Matlab	University of Waterloo, Canada
2016	Liqui|>	F#	Microsoft Research, USA
2016	Quantum Fog	Python	Artiste-qb, Canada
2016	Qubiter	Python	Artiste-qb, Canada

۲. روش‌شناسی تحقیق

یکی از روش‌های کسب دانش گروهی، روش دلفی است که دارای ساختار پیش‌بینی و کمک به تصمیم‌گیری در طی مراحل مطالعه و بررسی محتوا (پیمایش)، جمع‌آوری اطلاعات و در نهایت، اجماع گروهی است. امروزه تکنیک دلفی در تحقیقات آینده‌پژوهی به‌شدت مورد توجه و استفاده قرار می‌گیرد. از این رو، در این پژوهش بنابر روش دلفی برای ارائه مدل مفهومی فضای سایبر کوانتومی با استفاده از تحلیل محتوا و مراجعه به اسناد

و مدارک بهره گرفته می‌شود و نتایج آن به اجماع نظر نخبگان و خبرگان می‌رسد و در نهایت ابعاد، مؤلفه‌ها و شاخصه‌های مدل مفهومی اثر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده حاصل می‌شود. چهار مرحله برای ارائه مدل مفهومی تأثیر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده مطابق فلوچارت زیر انجام شده است.



شکل ۵: فلوچارت تحقیق ارائه مدل مفهومی اثر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده

در مرحله اول، پس از تحلیل محتوا و بررسی اسناد و مدارک، مدل‌های مختلف فضای سایبر کلاسیک استخراج شده است. مدل‌های مفهومی فضای سایبر سه لایه، چهار لایه و پنج لایه هرکدام بنابر یک دیدگاه ساختاری برای فضای سایبر ارائه می‌دهند که جنبه‌های مختلف آن را با توجه به دیدگاه کلی در نظر می‌گیرند. در مرحله دوم با توجه به اینکه مدل چهار لایه‌ای دیدگاه کامل‌تری برای فضای سایبر دارا است و هم جنبه‌های فنی و سیستمی

فضای سایبر را در نظر می‌گیرد و هم جنبه‌های اطلاعاتی و محتوایی و هم جنبه جامعه و مردم مناسب‌ترین مدل مفهومی فضای سایبر است که می‌توان پیشرفت‌های فناوری و علوم کوانتومی را در آن لحاظ کرد، این مدل چهار لایه‌ای انتخاب شد و تأثیر فناوری‌های کوانتومی در هرکدام از لایه‌های آن مورد بررسی و تحقیق قرار گرفت.

در مرحله سوم، ابعاد مؤلفه‌ها و شاخصه‌های فضای سایبر متأثر از علوم و فناوری‌های کوانتومی استخراج شد و به‌صورت یک ساختار لایه‌لایه (جدول ۷) ارائه گردید. در مرحله چهارم این ساختار در جلسات نخبگانی مورد بررسی و نظرسنجی خبرگان و نخبگان قرار گرفت و پس از اجماع نظر آن‌ها ابعاد، مؤلفه‌ها و شاخصه‌های مدل مفهومی اثر فناوری‌های کوانتومی بر فضای سایبر آینده ارائه شد.

۳. تجزیه‌وتحلیل یافته‌ها

در جدول ۸ ابعاد مؤلفه‌ها و شاخصه‌های فضای سایبر کوانتومی آورده شده است (دو بعد محتوا و کاربرد در کنار هم قرار می‌گیرند). در این مدل مفهومی لایه‌های سیستمی یا زیرساخت کوانتومی، محتوا (اطلاعات) و کاربرد کوانتومی و لایه جامعه و مردم در فضای سایبر کوانتومی ارائه شده است. لایه چهارم لایه حاکمیتی است که در این لایه استانداردسازی و چارچوب‌های قانونی کشورها برای کاربران فضای سایبری تعیین می‌شود. در حال حاضر لایه حاکمیتی کوانتومی و لایه حاکمیتی کلاسیک یکسان است و تغییراتی برای آن ارائه نشده است.

جدول ۸: جدول ابعاد، مؤلفه‌ها و شاخصه‌های مدل مفهومی تأثیر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده

ابعاد	مؤلفه‌ها	شاخصه‌ها
زیرساخت کوانتومی	محاسبات کوانتومی	رایانه‌های و پردازنده‌های منطقی کوانتومی بر اساس مدارهای ابررسانایی
	ارتباطات کوانتومی	چشمه‌های نور فوتونی
		خطوط ارتباطی
		مدارهای پردازشی کوانتومی
		تکرارکننده کوانتومی
		مسیریاب‌های کوانتومی
		سوییچ‌های کوانتومی
		آشکارسازهای تک فوتونی
		حافظه‌های کوانتومی
	حسگری کوانتومی	شتاب‌سنج کوانتومی
		رادارهای کوانتومی
		ساعت‌های کوانتومی
محتوا (اطلاعات) و کاربرد کوانتومی	زبان‌های برنامه‌نویسی کوانتومی	زبان‌های برنامه‌نویسی دستوری، تابعی و چند پارادایمی
	نرم‌افزارهای کاربردی کوانتومی	QISKit، Forest، Qbsolv
جامعه و مردم در فضای سایبر کوانتومی	شرکت‌های طراح نرم‌افزارهای کوانتومی	ایسارا، ام دی آر، ...
	شرکت‌های طراح الگوریتم‌های کوانتومی	کیندم، لیبر کوانتوم، ...
	شرکت‌های سخت‌افزاری کوانتومی	گوگل، دی-ویو، رگیتی، ...
	شرکت‌های فعال در یادگیری ماشین کوانتومی	نترا مارک، فاتم کامپیوتینگ،...
	شرکت‌های فعال در سنجش کوانتومی	کیونامی
	شرکت‌های فعال در ارتباطات کوانتومی	ای‌دی کوانتک، مجیک کیو، اینفیت کوانت، ...

با مقایسه دو جدول مدل مفهومی فضای سایبر کلاسیک (جدول ۵) و مدل مفهومی تأثیر علوم و فناوری‌های کوانتومی بر فضای سایبر آینده (جدول ۸) در سه لایه زیرساخت (سیستمی)، محتوا و کاربرد و لایه جامعه و مردم در فضای سایبر مشاهده می‌شود که هم در رایانش و هم در ارتباطات و سیستم‌های حسگری علوم و فناوری کوانتومی فضای سایبر را تحت تأثیر قرار می‌دهند. همچنین در لایه محتوا (اطلاعات) و کاربرد روش‌های الگوریتم‌نویسی مبتنی بر الگوریتم‌های کوانتومی و زبان‌های برنامه‌نویسی کوانتومی ساختار فضای سایبر را کاملاً تحت تأثیر قرار می‌دهند.

در لایه جامعه و مردم در عصر کوانتوم شرکت‌های فنی بسیاری تأسیس شده است و به‌طور عمده در این بخش از فضای سایبر متخصصین علوم و فناوری‌های کوانتومی فعال هستند و لذا در حال حاضر فعالیت‌های جامعه و مردم در زمینه کوانتوم در فضای سایبر عمداً به متخصصین و محققین عرصه کوانتوم محدود می‌شود که در شرکت‌های توسعه‌دهنده سخت‌افزارها و نرم‌افزارها و الگوریتم‌های کوانتومی فعالیت می‌کنند. همچنین در لایه محتوا و کاربرد در عصر ظهور علوم و فناوری‌های کوانتومی، رایانش و محاسبات کوانتومی زمینه‌های نوینی را به همراه خود به وجود آورده است؛ بنابراین فناوری‌های کاملاً متفاوتی برای اجرای الگوریتم‌های کوانتومی وجود دارند و زبان‌های برنامه‌نویسی کوانتومی باید بتوانند نیازهای تمام کاربران را برآورده سازند. با توجه به رشد سریع محاسبات کوانتومی، تعداد زبان‌های برنامه‌نویسی کوانتومی در حال افزایش است و ده‌ها شرکت در زمینه توسعه زبان‌های برنامه‌نویسی کوانتومی و نرم‌افزارهای کوانتومی فعال هستند.

در حال حاضر پژوهشگران بسیاری در تلاش هستند رایانه‌های کوانتومی با کاربردهای عملی به‌روز ایجاد کنند؛ اما مسائل سخت‌افزاری تنها چالش‌های پیش روی این فناوری نیستند، بلکه چنین بستر جدیدی به شیوه‌های برنامه‌نویسی و الگوریتم‌های جدیدی نیاز دارد. پروفسور آلن اسپورو گوزیک[1] استاد دانشگاه تورنتو (استاد دانشگاه هاروارد تا سال ۲۰۱۰) که

1. Alán Aspuru-Guzik.

به علت توسعه انواع الگوریتم‌ها شهرت بسیاری در جوامع علمی به دست آورده است، قصد دارد بازار فعالیت‌های خود را گسترده‌تر نماید. پروفسور آلن گوزیک مدتی قبل استارت‌آپ کوانتومی رایانش زاپاتا[1] را با بودجه‌ای ۵.٤ میلیون دلاری تأسیس نمود. هدف نهایی این استارت‌آپ ایجاد نوعی فروشگاه الگوریتم‌های کوانتومی است. در قالب این بستر به شرکت‌هایی که قصد دارند از قدرت پردازشی بیشتری بهره‌مند شوند، نرم‌افزارهای تجاری ارائه خواهد نمود. از آنجایی که حوزه رایانش کوانتومی کاملاً جدید است، متخصصان بسیار کمی قابلیت توسعه نرم‌افزارهای پیشرفته را برای سخت‌افزارهای آن دارند. همچنین هدف این استارت‌آپ این است که شرکت‌ها بدون نیاز به دانش فنی لازم قابلیت استفاده از چنین محصولاتی را به دست آورند. با افزایش تعداد کیوبیت‌ها، قدرت پردازشی رایانه‌های کوانتومی نیز افزایش پیدا می‌کند. از طرفی پژوهشگران معتقدند به‌زودی نمونه‌ای واقعی از این تجهیزات ایجاد خواهد شد که نسبت به سریع‌ترین ابررایانه‌های سنتی از قدرت بیشتری برخوردار است؛ اما دستیابی به آن با چالش‌های بسیاری همراه است. مدت‌زمان نگهداری اطلاعات توسط سامانه‌های کوانتومی در بازه ثانیه است. از طرفی کوچک‌ترین تغییر دما یا ایجاد ارتعاشی باعث از دست رفتن داده‌ها خواهد شد.

الگوریتم‌های کوانتومی علاوه بر اینکه محاسباتی خاص را با سرعتی بسیار زیاد انجام می‌دهند، قابلیت رفع مشکلات بالا را نیز دارند. شرکت زاپاتا کامپیوتینگ[2] نسبت به الگوریتم‌های کوانتومی توسعه داده شده توسط پروفسور گوزیک با دانشگاه هاروارد مذاکره انجام داده است. این استارت‌آپ قصد دارد الگوریتم‌هایی قابل اجرا در طیف وسیعی از رایانه‌ها را به وجود آورد. به همین دلیل با شرکت‌هایی مانند گوگل، آی‌بی‌ام، Rigetti Computing و IonQ و فعالان حوزه سخت‌افزارهای کوانتومی همکاری می‌نماید. البته این مراکز نیز در حال ایجاد الگوهای خاص خود هستند و در عمل توسعه الگوریتم برای

1. Zapata Computing.
2. Zapata Computing.

حوزه‌های مختلفی مانند یادگیری ماشین، علم شیمی و مواد از روندهای کاملاً متفاوتی برخوردار هستند.

شرکت‌های دیگری نیز در زمینه رمزنگاری کوانتومی فعالیت دارند مانند شرکت محاسبات کوانتومی کمبریج[1] که دستگاه رمزنگاری کوانتومی خود به نام آیرن‌بریج[2] را معرفی نموده است. آیرن‌بریج با استفاده از یک پردازنده کوانتوم- فوتونیکی چهار کیوبیتی، کلیدهای رمزنگاری تصادفی را ایجاد می‌نماید. آیرن‌بریج می‌تواند کلیدهایی تولید کند که غیرقابل هک هستند؛ بنابراین این دستگاه رمزنگاری در محیط‌های آسیب‌پذیر امروز، امنیت مطلق و همچنین امنیت پسا کوانتومی را فراهم می‌آورد. آیرن‌بریج به چالش‌های امنیتی و آسیب‌پذیری‌های مهم در زیرساخت‌های امروز می‌پردازد و در مقیاس جهانی پیامدهای ساختاری مهم برای امنیت سایبری و رمزنگاری کوانتومی دارد. در آینده نزدیک شاهد ایجاد شرکت‌های کوانتومی بسیاری در سطح دنیا خواهیم بود. این شرکت‌های کوانتومی جدید نقش مهمی در حوضه محاسبات، مخابرات، شبکه‌های امن ارتباطات کوانتومی ایفا خواهند نمود.

٤. نتیجه‌گیری

فضای سایبر یک سرمایه‌های ملی برای کشورها به شمار می‌آید؛ بنابراین بایستی از فضای سایبر در برابر تهدیدات و حملات سایبری دشمن حفاظت نمود. امروزه بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشورها، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشورها، یا خود، بخشی از فضای سایبری را تشکیل می‌دهند یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشورها نیز به این فضا منتقل یا به‌طور کلی

1. Cambridge Quantum Computing.
2. Ironbridge.

در این فضا، شکل گرفته است. عمده فعالیت‌های رسانه‌ای نیز بـه ایـن فضـا منتقـل شـده، بیشتر مبادلات مالی، پولی و بانکی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمـد حاصـل از کسب‌وکارهای فضای سایبر در تولیـد ناخـالص ملـی افـزایش چشـم‌گیـر یافتـه و از میـان شاخص‌های تعیین‌شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سـایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخـش قابـل تـوجهی از سـرمایه‌هـای مـادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسـابات معنوی شهروندان نیز از این حوزه کسب شده یا تأثیر عمده مـی‌پـذیرد. بـه عبـارت دیگـر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجـوه مختلـف زنـدگی شـهروندان را بـه مخـاطره خواهد انداخت.

ضـرورت و اهمیـت صـیانت از فضـای سـایبری کشـور، در مقابـل انـواع تهدیـدات و تهاجمات سایبری و به‌ویژه جنگ سایبری، موجب گردید کشورها با هدف تمرکز بـر دفـاع از زیرساخت‌های حیاتی، حساس و مهم در مقابـل انـواع تهدیـدات و تهاجمـات سـایبری زیرساخت‌هایی را ایجاد کنند یا سرمایه‌گذاری‌های کلانی برای دسـت‌یـابی بـه راهکارهـای حفظ امنیت اطلاعات در بستر فضای سایبر انجام دهند. از طرف دیگر، توسـعه رایانـه‌هـای کوانتومی در سال‌های اخیر که توان محاسباتی بالایی دارند، می‌تواند عواقب وخیمـی بـرای امنیت سایبر داشته باشد. به‌عنوان مثال، اعتقاد بر این است اگر یک رایانه کوانتومی با تعـداد کیوبیت‌های بالا که حل مسائل مهم مانند فاکتورینگ و لگاریتم‌های گسسته و همچنین حل مسائل پیچیده را قطعی می‌سازد، ساخته شود آنگاه امنیت بسیاری از پروتکل‌های به‌کاررفتـه (مانند RSA، DSA، ECDSA) را می‌توانـد بـه‌طـور مـؤثر بـه خطـر انـدازد و سیسـتم‌هـای رمزنگاری امروزی را به‌راحتی بشکند. در حالی که این نظریه از دهه ۱۹۹۰ میلادی شناخته شده است، اما چنین دستگاهی اخیراً به‌صورت واقعی تحقق یافته اسـت. بـا ایـن حـال، بـا توجه به خطر بزرگی که مهاجمان سایبر مجهز به فناوری‌هـای کوانتـومی مـی‌تواننـد ایجـاد

کنند، مسئله و مشکل در زمینه امنیت سایبری این است کـه فنـاوری‌هـای کوانتـومی در آن نقش مهمی ایفا می‌کنند.

فناوری‌های کوانتومی همچنین می‌توانند مزایایی ویژه‌ای برای امنیت سایبر داشته باشـند. برای مشاهده این وجه مثبت فناوری‌های کوانتومی، بایستی امکان‌پذیری مراحـل کوانتـومی در پروتکل‌ها برای کاربران را مدنظر قرار دهیم تا مشـخص شـود چـه بهبـودی نسـبت بـه سازوکار کاملاً کلاسیکی به دست آید. این حقیقتی است که بهبودها در اساس امکـان‌پـذیر هستند و نمونه قابل ذکر توزیع کلید کوانتومی[1] اسـت. در QKD بـا اسـتفاده از کانـال‌هـای کوانتومی[2] و کانال‌های تأییدشده کلاسیکی می‌توان یک کلید رمـز تسـهیم شـده را بـین دو قسمت مجزا از هم از طریق امنیت اطلاعات نظری[3] ارسال کرد. بسط کلیـد امـن اطلاعـات نظری، اساساً فقط با استفاده از ارتباطات کلاسیکی میسر نمی‌شود، بلکه داشتن یک پروتکل با امنیت اطلاعات نظری به این معنا است که امنیت مبتنی بر فرضـیات ارتباطـات نیسـت و در نتیجه حتی در صورت وجود یک مهاجمی که رایانـه کوانتـومی در اختیـار دارد، امنیـت می‌تواند حفظ و پایدار باقی بماند؛ بنابراین در عصر ظهور علوم و فنـاوری‌هـای کوانتـومی بایستی یک مدل مفهومی کامـل از سـاختار فضـای سـایبر کوانتـومی و ابعـاد، مؤلفـه‌هـا و شاخصه‌های آن داشت تا بتوان برنامه‌های راهبردی مناسبی برای تحقق زیرساخت‌های لازم برای داشتن فضای سایبر امن اتخاذ کرد.

1. QKD.
2. Quantum channels.
3. Information theoretic security.

فهرست منابع ومآخذ

الف. منابع فارسی

- دوستی‌مطلق، ن. ا. (۱۳۹٦)، رایانه‌های کوانتومی؛ مفاهیم، کاربردها و مطالعات بازار، مرکز راهبردی فناوری‌های همگرا، تهران.
- رضا تقی‌پور، ع. ا. (۱۳۹۷ زمستان)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره سی‌ام.

ب. منابع انگلیسی

- Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., . . . Buell, D. A. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505-510 .
- Bennett, C. H. & Brassard, G. (2020). Quantum cryptography :Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557* .
- Chang, C.-R., Lin, Y.-C., Chiu, K.-L., & Huang, T.-W. (2020). The Second Quantum Revolution with Quantum Computers. *AAPPS Bulletin, 30*(1 .(
- Cross, A. W., Bishop, L. S., Smolin, J .A., & Gambetta, J. M. (2017). Open quantum assembly language. *arXiv preprint arXiv:1707.03429* .
- Dixon, A., Yuan, Z., Dynes, J., Sharpe, A., & Shields, A. (2008). Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Optics express, 16* ,(۲۳) .۱۸۷۹۷-۱۸۷۹۰
- A Draft Apocryphal and Anthropocentric Cyberspace. (2010 .(
- Green, A. S., Lumsdaine, P. L., Ross, N. J., Selinger, P., & Valiron, B. (2013). *An introduction to quantum programming in quipper*. Paper presented at the International Conference on Reversible Computation.
- Hidary, J. D. (2019). *Quantum Computing: An Applied Approach*: Springer.
- Hiskett, P. A., Rosenberg, D., Peterson, C. G., Hughes, R. J., Nam, S., Lita, A., . . . Nordholt, J. (2006). Long-distance quantum key distribution in optical fibre. *New Journal of Physics, 8*(9), 193 .
- Knill, E. (1996). *Conventions for quantum pseudocode*. Retrieved from
- Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., . . . Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics, 9*(3), 163 .
- Liao, S.-K., Cai, W.-Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., . . . Liu, W.-Y. (2018). Satellite-relayed intercontinental quantum network. *Physical review letters, 1* .۰۳۰۵۰۱ ,(۳)۲۰
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*: RAND corporation.
- Paolini, L., Roversi, L., & Zorzi, M. (2017). Quantum programming made easy. *arXiv preprint arXiv:1711.00774* .
- Popkin, G. (2017). China's quantum satellite achieves 'spooky action'at record distance. *Sci Mag, 15* .

- Resch, S., & Karpuzcu, U. R. (2019). Quantum computing: an overview across the system stack. *arXiv preprint arXiv:1905.07240* .
- Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl ,T., . . . Rarity, J. G. (2007). Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical review letters, 98*(1), 010504 .
- Shaw, D. S. (2010). *Cyberspace: What senior military leaders need to know*. Retrieved from
- Strate, L. (1999). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication (includes Communication Reports), 63*(3), 382-412 .
- Svore, K., Geller, A., Troyer, M., Azariah, J., Granade, C., Heim, B., . . . Roetteler, M. (2018). *Q# Enabling scalable quantum computing and development with a high-level DSL*. Paper presented at the Proceedings of the Real World Domain Specific Languages Workshop 2018.
- Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H ,.Scheidl, T., Lindenthal, M., . . . Trojek, P. (2006). Free-space distribution of entanglement and single photons over 144 km. *arXiv preprint quant-ph/0607182* .
- Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., . . . Dai, H. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science, 356*(6343), 1140-1144 .
- Zhang, Y., Li, Z., Chen, Z., Weedbrook, C., Zhao, Y., Wang, X., . . . Wang, Z. (2019). Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology, 4*(3), 035006 .
- Zimet, E., & Skoudis, E. (2009). A graphical introduction to the structural elements of cyberspace. *Cyberpower and national security*, 91-112.