



خداحافظی با دنیای صفر و یک

ماه گذشته وزارت دفاع آمریکا در گزارش سالانه به کنگره این کشور مدعی شد اطلاعات فوق‌سری پنتاگون توسط هک‌های چینی ربوده شده و دولت چین به آخرین پیشرفت‌های دفاعی ایالات متحده دسترسی یافته است.

ماه گذشته وزارت دفاع آمریکا در گزارش سالانه به کنگره این کشور مدعی شد اطلاعات فوق‌سری پنتاگون توسط هک‌های چینی ربوده شده و دولت چین به آخرین پیشرفت‌های دفاعی ایالات متحده دسترسی یافته است.

چند روز بیشتر از انتشار این خبر نمی‌گذشت که ادوارد اسنودن، کارمند سازمان سیا در اظهاراتی جنجالی از برنامه سری آمریکا و انگلیس برای دسترسی به اطلاعات شخصی کاربران اینترنت در آمریکا و کشورهای دیگر پرده برداشت.

اتفاقاتی از این دست نگرانی‌های بین‌المللی را در مورد ایمنی فضای مجازی به شکل قابل توجهی افزایش داده است.

تاسیسات هسته‌ای کشورمان نیز در سال 90 مورد حمله ویروس استاکس نت قرار گرفت و چند سانتریفیوژ نیروگاه نطنز به‌طور موقت از کار افتاد.

استاکس نت بنا به گفته مسئولان کشورمان از طریق حافظه جانبی آلوده وارد کشور شده بود ولی از اینترنت برای ارسال اطلاعات جمع‌آوری شده به کشورهای دیگر استفاده می‌کرد.

پس از آمریکا دولت استرالیا هم ادعاهای مشابهی را در مورد جاسوسی سایبری چین مطرح کرد و گفته می‌شود روسیه هم از عواقب این حملات در امان نمانده است.

فضای اینترنت دیگر به هیچ وجه امن نیست و همه کشورهای دارای فناوری‌های پیشرو از این ناامنی احساس خطر می‌کنند.

این جدال‌های سیاسی فارغ از صحت و سقم آنها بار دیگر همه توجهات را به لزوم یافتن راه حلی مطمئن برای افزایش ایمنی فضای مجازی جلب کرد اما شرکت‌های عظیم طراحی و تولید سخت‌افزار و نرم‌افزار قادر نیستند راه حلی برای این معضل ارائه دهند و همه نگاه‌ها به آزمایشگاه‌های فیزیک ذرات و تحقیقات گسترده فیزیکدانان کوانتومی دوخته شده است.

نبرد جدیدی میان دانشمندان و هکرها آغاز شده و آن‌طور که از شواهد برمی‌آید دیر یا زود، دانشمندان مثل همیشه فاتحان عرصه نبوغ و نوآوری خواهند بود.

البته هدف آنها بیرون راندن هکرها از دنیای صفر و یک نیست. در واقع آنها دنیای صفر و یک را برای همیشه به هکرها واگذار خواهند کرد و برای انجام محاسبات و ذخیره و کدگذاری اطلاعات به دنیای جدید کوانتوم قدم می‌گذارند.

آغاز عصر رایانه‌های کوانتومی را باید پایانی بر چند دهه حکمرانی هکرها - این راهزنان دنیای مجازی - دانست.

کشور استرالیا عکس‌العمل جدی‌تری به شایعات مطرح شده در مورد سرقت اینترنتی اطلاعات نظامی‌اش نشان داد.

دانشمندان این کشور ماموریت دارند یک شبکه اطلاعاتی غیرقابل نفوذ برای نگهداری اطلاعات نظامی طراحی کنند. در ادامه به بررسی بخشی از نتایج قابل توجه این تحقیقات می‌پردازیم.

کابوس هکرها

فرآیند رمزنگاری مثلثی است که در یک راس آن رمزنگار یا فرستنده رمز، در راس دیگر گیرنده رمز و در راس سوم هکر قرار می‌گیرد.

هکر می‌تواند بدون این که فرستنده و گیرنده رمز متوجه حضور او باشند به شبکه وارد شود و به اطلاعات مورد نیاز خود دسترسی

پیدا کند.

روش رایج برای مقابله با هکرها استفاده از کدهای پیچیده است تا شکستن آنها در حد امکان دشوار باشد ولی این تلاش ها راه به جایی نبرده است.

در رایانه های کوانتومی در صورت ورود هکرها، رایانه به صورت هوشمند از حضور آنها مطلع می شود و اطلاعات مورد نظر آنها را در شبکه جابه جا یا نابود می کند.

تصور کنید بجای این که رمز دشواری برای گاوصندوق خود انتخاب کنید و نگران شکسته شدن آن به وسیله سارقان باشید، سازوکاری را طراحی کنید که وقتی سارق به گاوصندوق شما در اتاق خواب نزدیک می شود، گاوصندوق به طور خودکار به اتاق پذیرایی انتقال می یابد.

رایانه کوانتومی چیست؟

هر جزء یا بیت اطلاعات در رایانه های معمولی بر روی انبوهی از اتم ها در ریزتراشه های سیلیکونی ذخیره می شود ولی در رایانه های کوانتومی، نقش بیت های اطلاعاتی را بخشی از یک اتم مانند الکترون ها یا هسته آن بازی می کنند.

وظیفه بررسی خواص ماده در مقیاس اتم و کوچک تر از آن بر عهده فیزیک کوانتوم است بنابراین به هر کدام از این بیت های جدید یک بیت کوانتومی یا به اختصار کیوبیت می گوئیم.

تفاوت کیوبیت ها با بیت ها در این است که یک بیت در یک لحظه فقط می تواند صفر یا یک باشد ولی یک کیوبیت به طور همزمان می تواند مقدار صفر، یک، یا هر عددی بین صفر و یک داشته باشد.

با این روش می توان با در اختیار داشتن فقط 300 اتم فسفر، کیوبیت هایی به تعداد همه ذرات بنیادین عالم در اختیار داشت.

نکته: چشم انداز آینده مسیری که دانشمندان بیش از یک دهه پیش گام در آن گذاشتند رایانه های کوانتومی و شبکه اینترنتی کوانتومی فوق سریع است. از گذشته تا امروز که هسته اتم را برای ثبت اطلاعات انتخاب کرده ایم راه دور و درازی را پیموده ایم

اتم ها به قدری کوچک هستند که نقطه پایان این جمله از حدود صد میلیارد اتم کربن تشکیل می شود.

اگر بخواهید با چشم غیرمسلح، هسته یکی از این اتم ها را ببینید باید این نقطه را با همین تعداد اتم به اندازه قطر کره زمین از قطب شمال تا جنوب گسترش دهید و اگر بخواهید یک الکترون را ببینید باید قطر همان نقطه را تا صد برابر قطر خورشید افزایش دهید ولی دانشمندان چگونه می توانند اطلاعات را بر روی هسته اتم یا الکترون های آن ثبت کنند؟

برای انجام این کار آنها باید یکی از ویژگی های ذرات بنیادین به نام اسپین که می تواند رو به بالا یا پایین باشد دستکاری و کنترل کرد. جهت اسپین ها کلید اصلی ساخت رایانه کوانتومی است.

روش کار به این صورت است که یک اتم فسفر درون یک نانو ساختار سیلیکونی قرار می گیرد و تا دمای صفر مطلق سرد می شود سپس با تاباندن لیزر، اسپین یک الکترون را تغییر می دهد.

برای ساخت رایانه کوانتومی باید اسپین الکترون را کنترل کرد و آن را به سمت بالا یا پایین قرار داد.

تحقیقات بسیاری در مورد چگونگی کنترل اسپین انجام شده که هیچ یک به تنهایی انتظارات دانشمندان را برآورده نکرده است.

محققان استرالیایی امیدوارند بتوانند با ترکیب یافته های قبلی به روش مطلوب دسترسی پیدا کنند.

پس از آن نوبت یافتن روشی برای بازخوانی اطلاعات می رسد. محققان استرالیایی توانستند با ترکیب دو روش موجود برای خواندن اسپین یعنی روش الکتریکی و روش اپتیکی، شگفتی دانشمندان را برانگیزند؛ چراکه این دو روش به هیچ وجه با یکدیگر همخوانی ندارد.

آنها اتم ها را به صورت اپتیکی یونیده و سپس از روش الکتریکی برای بازخوانی اطلاعات استفاده می کنند.

در رایانه های کوانتومی جدید فقط از بیت های جامد شبیه ریزتراشه های امروزی استفاده نمی شود بلکه این رایانه ها ترکیبی از کیوبیت های حالت جامد و کیوبیت های اپتیکی را همزمان به کار می گیرند.

استفاده از کیوبیت های اپتیکی هم مانند فیبرهای نوری سرعت انجام محاسبات و انتقال اطلاعات را افزایش می دهد.

چشم انداز آینده مسیری که دانشمندان بیش از یک دهه پیش قدم در آن گذاشتند رایانه های کوانتومی و شبکه اینترنتی کوانتومی فوق سریع است.

به نظر می رسد از زمانی که ارسطو اعتقاد به وجود اتم را غیر قابل قبول می دانست تا امروز که هسته اتم را برای ثبت اطلاعات انتخاب کرده ایم راه دور و درازی را پیموده ایم.

هنوز هم دشواری های فراوانی در راه ساخت رایانه های کوانتومی وجود دارد و دانشمندان احتمال تحقق کامل این هدف را تا 10 سال آینده بسیار اندک می دانند ولی مهم این است که امروز پیشرفت های به دست آمده صورت سوال را از «آیا می توان چنین رایانه هایی ساخت یا خیر؟« به «چگونه می توان بر موانع باقیمانده غلبه کرد؟« تغییر داده است.

مسعود توکلی - جام جم