UNCOMMON STANDARDS

Competing approaches to cybersecurity threaten stability

H3 ACT PLAN TRACK PARK OPP THR NEU

The technologies and standards that underpin communication around the world are, for the most part, global and interoperable. Common standards mean that designs can be checked once by all interested parties; interoperability means that errors and vulnerabilities are likely to be caught early. From a cybersecurity perspective, this is positive, enabling nations to secure systems at a scale that was previously impossible. This stability and interoperability is, however, under threat as nations states edge closer to balkanisation of technology and standards.

States have been weaponising information for some time now, breaking into other countries' networks to steal data, seed misinformation or disrupt infrastructure. And now - because they don't like the increase in strategic dependence on other states - they are developing their own standards and technologies that diverge from global commons and which embody their values. This signals a fundamental shift in how technology is developed, owned, accessed and leveraged by nation states and companies. New alliances will form around the creation of indigenous and sovereign versions of the technology we use to communicate and manage modern life. We will see standards bodies fragment and supply chains and infrastructure redesigned to align with these new realities. States will start to take more drastic action to ensure that their supply chains are protected, and that their sovereign "silicon-to-service" technology stacks are insulated from the actions of others and enforce their national values.

The global debate around 5G security has led to a position where we will likely see two independent camps moving forward, ostensibly led by the US and China. Other nations will have to decide which camp better serves their national interest, since the companies that produce this technology are bound to those countries. This will establish a pattern which will be repeated across other critical technologies. In this world, the multi-stakeholder approach to standards that ensures no one party has too much power will be critical to ensure we can continue to do cybersecurity at scale.

If we fail, the world will become less connected, less resilient and less secure.

QUANTUM COMPUTING

Transformative tech or empty promise?

H3 ACT PLAN TRACK PARK OPP THR NEU

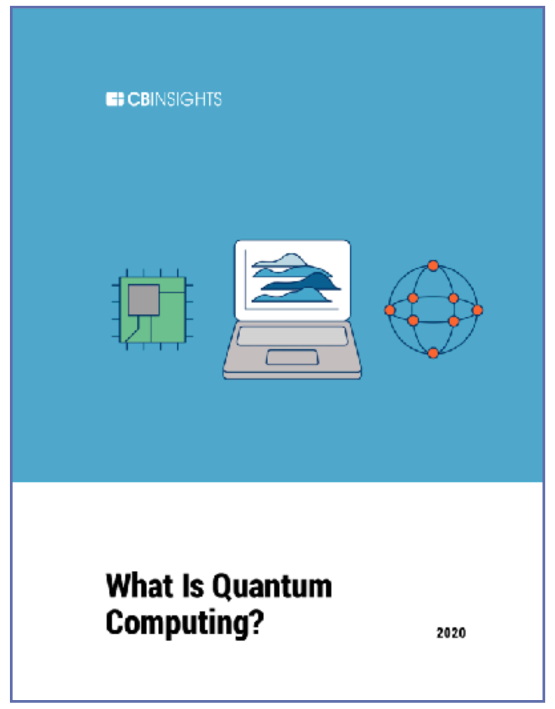
Big, stable quantum computers would be useful devices. They could perform some calculations faster than any non-quantum machine - searching a database, precisely simulating complex chemical reactions to aid development of drugs, speeding up the analysis of optimisation problems for (eg) the transport industry (by finding efficient routes) and finance (by maximising profits given a set of constraints). Boston Consulting Group foresees quantum computers improving the operating income of their users by between $450bn and $850bn a year by 2050.

Unfortunately, big, stable quantum computers do not yet exist. But small unstable ones do. John Preskill, a quantum-computing researcher at the California Institute of Technology, dubs such machines nisqs—Noisy, Intermediate-Scale Quantum computers. A growing number of companies and investors are hopeful that nisqs themselves will be able to do useful work in the meantime. These firms are hunting for "quantum advantage" - a way in which even today's limited machines might have an impact on their bottom lines.

The big question is what all this is leading up to. There is plenty of promise, but, as yet, no certainty. Finding algorithms that are both commercially useful and simple enough to work within a nisq machine's limitations is not easy. A report published last year by America's National Academy of Sciences reminded readers that no commercial applications are currently known to exist.

Optimists think that, with a bit of luck and progress, the first commercially relevant applications of quantum computers will appear within the next two or three years. In particular, he reckons it is worth keeping an eye on the finance industry, where quantum computers could boost trading algorithms and portfolio management. "To develop a new battery or a new drug you have to test the product," he points out. This can take years. A slick new financial algorithm could be deployed in days. And given the scale of the markets, even a tiny advantage could be worth a great deal of cash.

FURTHER READING



CBINSIGHTS

What Is Quantum Computing?

2020

TECHNOLOGY HOME PAGE