

Scenario 1 – Quantum Leap

The year is 2025, and the first countries to achieve practical quantum computing capabilities have spent the past several years trying to construct a non-proliferation regime that would preserve the economic, strategic and military advantages the technology has begun to generate. But other countries – and even large cities – that are behind in the race have resisted the offer to access watered-down quantum services from the few elite providers in return for restraint in development. Instead, many attempt to pursue “quantum autonomy”. Technology development accelerates almost to the exclusion of ethical, economic and other sociopolitical concerns as quantum leaks into the “deviant globalization” sphere of drug cartels and other worldwide criminal networks. Ultimately, the carrots of a restrictive non-proliferation bargain aimed at governments have not been enticing enough (and the sticks not fearsome enough) to hold a regime together, and the model that more or less worked to contain the spread of nuclear weapons in a previous era fails with quantum. In 2025, the Americans and the Chinese in particular are starting to wonder if their next best move is to reverse course and speed up the dissemination of quantum computing to their respective friends and allies, while the deviant sector is racing ahead.

In 2018, a series of secret executive actions drew US quantum computing research entirely under the purview of the Department of Defense. Obsession with the military applications of the technology – particularly the ability to break traditional encryption – dominated other potential applications and became the singular focus of the US government’s research efforts. Congress cooperated, and authorized a massive research budget coupled with extremely tight export controls. This naturally incited a vocal resistance movement among commercial and academic research communities – until they saw what access to a huge government research budget and the massive resources of the Department of Defense could do to multiply their research capabilities. For some, it was a devil’s bargain, but, with enough dollars for those who played along and legal consequences for resisting, it was a bargain nearly impossible to resist.

In 2020, the US Department of Defense announced that it had achieved a practical quantum-capable computer. The initial device was retained by the US government, with limited access provided to academia for research on defence-related applications. Additional quantum computers were announced by the private sector, but most of their computational activity was classified, raising suspicions that the US intelligence and defence communities were using most of the capabilities available to crack encrypted communications. The US government placed strict controls

on products and services the private sector could offer with quantum computing, burying the initial launch of private quantum-as-a-service offerings in a mire of bureaucratic processes. Limited exceptions were made for governments of the Five Eyes intelligence partners, which reinforced suspicions about the primary applications that were run on the machines.

The surveillance capabilities certainly paid off. The United States and its allies announced a series of significant breakthroughs abroad and at home in countering extremist threats, breaking up terrorist cells and penetrating foreign intelligence operations. Encryption-breaking appeared to give the quantum players a major leg up. Quantum-enabled artificial intelligence (AI) also facilitated major improvements in cybersecurity capabilities, providing a flexible defence against attacks on government and private networks that could both react in near-real time to attackers and trace them almost instantly through their traditional methods of obfuscation – turning the long-standing challenge of cyber-attack attribution into something approximating an exact science.

Due process for the use of quantum computing to break encryption and conduct surveillance was weak. US policy institutions, still mired in debates about the Foreign Intelligence Surveillance Act (FISA) and government hacking, were simply unprepared to tackle the depth of legal and ethical questions posed by this fundamental shift in the technology landscape. Foreign governments perceived the new, quantum-enabled American intelligence complex as omniscient, and began to revert to older, less efficient forms of communication, but they were often surprised at just how far into the secret world quantum capabilities could reach with analytic and predictive models. The largest global drug and smuggling cartels were even more surprised, and suffered a massive downturn in their profits as a result.

Tight control over the commercial use of quantum computing sparked regular outcries in the marketplace, but the defence and intelligence communities stood their ground. Still, the lack of broader market participation highlighted a disadvantage for first movers in quantum: the need for further research limited the applications the US could write for quantum computers. Tight controls over access led to a much slower expansion of programming languages and hardware architectures than expected. While the commercial and research sectors talked about the opportunity costs of restricted access, the defence community saw this smaller base of knowledge as something to be defended. Much as the development of nuclear power technology became tainted by the legacy of the atomic bomb, the public became increasingly suspicious of quantum computing.

Meanwhile, European investment in quantum computing doubled over the next few years as the access-for-restraint bargain corroded. A Franco-German consortium soon announced quantum capability and (ironically) offered very limited services to fellow EU member governments in return for their restraint. In 2022, news broke that China had also developed a working quantum computer, and was leasing (heavily monitored) access to state-supported companies. Private companies in the US and Europe immediately demanded access to next-level computational power, fearing the competitive advantage of their Chinese counterparts, but commercial interests were again put second to the defence and intelligence communities' conceptions of what was needed for national security.

In a reprise of the Non-Aligned Movement of the 1970s, a number of other countries (led, as in the 1970s, by India) organized to argue in international fora that quantum technology was a common human heritage and could not on normative grounds be kept secret, owned by individual nations or used for military purposes. What was surprising was how many large, self-consciously global cities joined this movement, which took on a very modern feel when a Toronto-Seoul-Johannesburg (TSJ) consortium pledged to pursue quantum capabilities with the promise of open access for humanitarian and health applications across the globe.

The quantum powers responded by joining together to counter this movement. In 2023, China, the US, the UK, France and Germany set down a formal, joint non-proliferation agreement that would allow the sale of quantum-enabled computing services internationally, but limited the usage of the services to applications with no intelligence or military value. Export of the underlying technology was forbidden, and the quantum-enabled countries agreed to use their shared capabilities in a partnership to detect unauthorized quantum activity on international networks.

This QNPT (Quantum Non-Proliferation Treaty) proposition was offered to other countries as a global public good, and the quantum powers seemed ready in some instances to extend the deal to city-consortia such as TSJ. What they were not prepared to do, or even discuss in detail, was extend the deal to deviant and criminal networks. Rumours emerged that a parallel consortium of the Tijuana, Sinaloa and Juárez cartels (ironically, also TSJ) had joined together to pursue quantum technology by stealing information, hijacking networks and even, in a few peculiarly unreported incidents, kidnapping scientists who were travelling outside the major QNPT states.

The promise of quantum computing for commercial and humanitarian purposes had been undermined by defence and intelligence objectives. Financial services firms were willing to pay to gain access to quantum computers' efficiencies for specific applications, but sectors like healthcare were less interested in exposing research data to the technology for fear of what governments would learn.

Berkeley, California, declared itself a "Quantum-Free Zone". Groups of academic researchers continued to speak out episodically against government grants supporting defence research, but these efforts fizzled out just as the previous efforts had.

By 2023, the schism between nations that possess quantum computing capacity and those that do not had become the most prominent feature of mainstream international alignments. Ultimately, the "carrots" of limited access to quantum computing offered as part of the QNPT were not enticing enough: the applications and services were too limited, and few states wanted to risk foreign governments (even allies) having access to their computational activity. Meanwhile, the deviant underground market for quantum processing flourished under the radar. It may be that some countries aligned themselves with the drug cartels in this endeavour – no one knows for sure – though there is clear evidence of shell organizations, proxies and cut-outs that blur the lines.

It's as if the quantum countries simply missed the fact that this technology could and would proliferate more quickly and widely than had nuclear weapons technology – and that criminals and cartels would be particularly unrelenting in their pursuit of it. As a result, the non-proliferation regime isn't working. Sanctions are plausible sticks when it comes to countries, but no one is ready to fight a war to stop the spread of quantum technology – even if it were clear who you would fight such a war against.

As 2024 drew to a close, Russia announced it had built a quantum computer. Was it based on engineering details stolen from the drug cartel consortium? The technology looked remarkably similar. And then, despite a threat of severe sanctions by the US and EU, Russia signed a public deal to distribute details of the technology to Iran and India, which stoked new tensions with Saudi Arabia and Pakistan, both of which appealed to Washington to re-establish a balance of quantum power by "arming" them with the technology as well. Rumours arose that a similar appeal was made to China, in case the US did not see the light. At the same time, Russia signed an equivalent technology-sharing deal with Israel and Japan, two countries that had appealed to the US for access but were left by Washington to fend for themselves.

The last straw for the QNPT came in 2025, when the Toronto-Seoul-Johannesburg consortium announced it has also crossed the quantum threshold and built a machine far more advanced than any country had demonstrated. Non-proliferation has failed, and the opposite argument – more is better – is gaining broad credence. A consensus is emerging that the real way to "control" this technology is to give everyone open access and refocus attention on commercial and common human heritage applications, while letting the defence and intelligence sectors settle into a large-scale mutual deterrence equilibrium.

Cryptography remains broken for most individuals, but the increasing availability of quantum-resistant cryptography has started to generate more demand from businesses. The US has moved to radically privatize and deregulate some of the largest quantum providers in an attempt to recapture competitive advantage over the growing – and now global – quantum economy. But some of the most advanced applications for quantum are now appearing in the deviant underground sectors of the global economy, a kind of quantum dark web where legitimate businesses and many governments have limited visibility and access. There, quantum capabilities are being used to optimize the supply chain for things such as human beings and body parts, for illegal drugs and illegal VR experiences that exceed anything a drug could elicit, as well as for “mundane” illegal trade in rare animals and stolen art.

It’s possible that the broader promise of quantum computing will materialize by 2030 and beyond, but that part of the story has been significantly delayed by the ill-fated non-proliferation programme. And quantum has yet to wash off the public stain of its early monopolization by the defence community. It has become another source of contention between the major powers and everyone else. And perhaps most interestingly, it is quantum computing that is being seen in 2025 as the technological breakthrough that propelled the notion of networked cities from abstract theory to reality. It has also become a major engine of growth for illicit globalizers whose profits feed an entirely unregulated and ruthlessly competitive set of business activities, which may be outracing legitimate uses.