The Quantum Computing Threat to National Security

By Arthur Herman

Google announced last month that it had achieved "quantum supremacy," demonstrating the potential of a new kind of computer that can perform certain tasks many orders of magnitude faster than the most advanced supercomputers. It's a crucial moment for America's national security, which depends on winning the race to do what quantum computers will do best: decrypt the vast majority of existing public-key encryption systems.

Google claims supremacy, but the risk remains that U.S. complacency lets China crack all its codes.

Google reports that its quantum computer, dubbed Sycamore, solved a mathematical calculation in 200 seconds that would take a supercomputer 10,000 years. IBM, a quantum competitor, asserted that Google's claim of supremacy is overblown, and that the world's most powerful classical computer, the Summit OLCF-4 at Oak Ridge National Laboratory, could have done the same calculation in 2.5 days—roughly a thousandfold difference rather than 1.5 trillionfold. Still, quantum computers are no longer science fiction.

To process information, digital computers use bits, essentially switches that can be either off or on, corresponding with the binary digits, 0 and 1. Quantum computers employ "qubits," which use the probabilistic nature of quantum physics to represent any combination of 0 and 1 simultaneously, enabling them to encode more complicated data.

Their computing power grows exponentially as the number of qubits expands. Sycamore's 54-qubit chip allowed it to outcompute the best supercomputer. A 2,000- to 4,000-qubit quantum computer would render most public-key encryption architectures—used for applications from banking and credit cards to the power grid—obsolete. They rely on numbers too big for conventional computers to factorize, but which a quantum computer could.

Building quantum computers is a very heavy lift. They require hugely expensive infrastructure to stabilize the qubits at temperatures near absolute zero. They also generate high error rates, or "quantum noise," for which researchers have to compensate. Developers are probably years away from the large-scale code-breaking quantum computer everyone worries about—although once scientists and engineers start using quantum computers to build the next generation of quantum computers (since modeling complex systems like themselves is one of their strengths) the timeline could quickly shorten.

Beijing is America's chief quantum-computing rival. It spends at least $2.5 billion a year on research—more than 10 times what Washington spends—and has a massive quantum center in Hefei province. China aspires to develop the code-breaking "killer app," which means protecting U.S. data and networks from quantum intrusion is a vital security interest.

Congress enacted the National Quantum Initiative Act late last year, which commits an additional $1.25 billion over five years—still a fraction of China's effort. In addition to more money, the U.S. needs a three-phase national-security strategy to protect and defend American data, networks and infrastructure from future quantum attack.

First, dramatically increase efforts to develop encryption methods based on algorithms large and complex enough to foil quantum intrusion. The National Institute of Standards and Technology is working to set a comprehensive standard for these quantum-resistant algorithms so they can be deployed by 2024, but companies in the U.S., Canada and elsewhere are already building algorithms and other protective tools.

Second, use quantum technology itself to create the "unhackable" networks of the future. The same particles that make quantum computing possible can provide randomized and unhackable keys for encrypted transmissions, in the form of quantum random number generators and quantum key distribution, a method of securing information shared between two parties. Dismissed as a fantasy a few years ago, quantum cryptography has spawned companies in the U.S., Switzerland, South Korea and Australia, which are deploying the first components of a new quantum-based information-technology infrastructure. Eventually this will include satellites using quantum keys to transmit encrypted data.

Here again China has moved quickly. It launched the world's first quantum satellite in 2016 and shocked the world by creating a quantum-encrypted intercontinental video link from space to a China-Austria study group in Vienna. China has also created a 1,263-mile ground link between Beijing and Shanghai using quantum-encrypted keys between relay stations, which offers an ultrasecure network for transmitting sensitive data, including for China's military and intelligence services.

Third, require that all U.S. data and networks, including future 5G technology, be made secure from quantum attack while devoting resources to build the hack-proof quantum communication networks of the future. That will require working with America's closest allies, several of which are making key breakthroughs in the same quantum and postquantum technologies.

Promoting such cooperation has been a core mission at the Quantum Alliance Initiative, which convened a consortium of companies and universities from the U.S. and allied countries to develop global standards for quantum random number generators and quantum key distribution late last year. But no one can do all this alone, not even Google plus IBM plus Microsoft and the other big companies working in quantum computing. Leadership from the federal government is more imperative than ever. Google's breakthrough proves that the threats, as well as the opportunities, of quantum technology are real—and that quantum is poised to become the national-security issue of the 21st century.

Mr. Herman is director of the Hudson Institute's Quantum Alliance Initiative and author of "1917: Lenin, Wilson, and the Birth of the New World Disorder."

Make Pluto Great Again

By Taylor Dinerman

In astronomy as in politics, no issue is truly settled until it has become irrelevant. The question of Pluto—planet, dwarf planet or Kuiper belt object?—is still up for debate. "I believe Pluto is a planet," NASA Administrator Jim Bridenstine announced. He may not be an astrophysicist but his agency controls a very large chunk of the Earth's budget for space science, so he's not a man the American astronomy establishment can easily ignore.

For NASA the important question is not the nomenclature of Pluto, but whether or not to send a follow-up probe there. The New Horizons mission has been wildly and surprisingly successful. Launched in 2006 over the objections of a small but very noisy antinuclear group that felt threatened by the spacecraft's plutonium-powered radioisotope thermoelectric generator, at the time it was the fastest spacecraft in history.

NASA and planetary scientist Alan Stern, the driving force behind New Horizons, have started thinking about another mission to Pluto, one that probably wouldn't be launched until at least 2027 and thus won't reach its destination until the mid-2030s. By then a new crop of planetary scientists will have come of age and will be ready to study whatever the new vehicle sends back to Earth.

As the debate over its planetary status heats up again, NASA contemplates sending another probe.

The yet-unnamed mission is planned to go into orbit around Pluto and will be designed to stay there for a couple of years before using the gravity of the moon Charon to swing itself out on a further

THE WALL STREET JOURNAL.
PUBLISHED SINCE 1889 BY DOW JONES & COMPANY
Rupert Murdoch, Executive Chairman, News Corp
Robert Thomson, Chief Executive Officer, News Corp
Matt Murray
William Lewis