WILL HURD SECURITY 12.07.2017 08:00 AM

Quantum Computing Is the Next Big Security Risk

Opinion: Quantum computers will rock current security protocols that protect government and financial systems.

HOTLITTLEPOTATO

The 20th century gave birth to the Nuclear Age as the power of the atom was harnessed and unleashed. Today, we are on the cusp of an equally momentous and irrevocable breakthrough: the advent of computers that draw their computational capability from quantum mechanics.

WIRED OPINION

ABOUT

US representative Will Hurd (R-Texas) (@HurdOnTheHill) chairs the Information Technology Subcommittee of the Committee on Oversight and Government Reform and serves on the Committee on Homeland Security and the Permanent Select Committee on Intelligence.

The potential benefits of mastering quantum computing, from advances in cancer research to unlocking the mysteries of the universe, are limitless.

But that same computing power can be used to unlock different kinds of secrets—from your personal financial or health records, to corporate research projects and classified government intelligence.

computers are able to factor large numbers more efficiently than classical computers. Large number factoring is the foundation of today's encryption standards.

The impact of quantum on our national defense will be tremendous. The question is whether the United States and its allies will be ready.

The consequences of mastering quantum computing, while not as visual or visceral as a mushroom cloud, are no less significant than those faced by the scientists who lit up the New Mexico sky with the detonation at the Trinity test site 72 years ago. In the same way that atomic weaponry symbolized power throughout the Cold War, quantum capability is likely to define hegemony in today's increasingly digital, interconnected global economy.

Unlike traditional computers, which process information in binary bits, quantum computers exploit the ability of quantum bits (qubits) to exist in multiple states simultaneously. This allows them to perform incredibly complex calculations at speeds unimaginable today and solve certain classes of problems that are beyond the grasp of today's most advanced super computers.

Today, quantum computers are beginning to move out of research labs in search of broader investment and applications. In October, Google announced that by the end of this year it expects to achieve quantum supremacy—the point at which a quantum computer can outperform a classical computer.

Because nations around the world, including China, are investing heavily in research and development, the world is likely less than a decade away from the day when a nation-state could use quantum computers to render many of today's most sophisticated encryption systems useless.

From academics to the National Security Agency, there is widespread agreement that quantum computers will rock current security protocols that protect global financial markets and the inner workings of government.

Already, intelligence agencies around the world are archiving intercepted communications transmitted with encryption that's currently all but unbreakable, in the hopes that in the future computing advances will turn what's gibberish now into potentially valuable intelligence. Rogue states may also be able to leverage the power of quantum to attack the banking and financial systems at the heart of western capitalism.

MORE ON QUANTUM COMPUTING

CYBERSECURITY
Quantum Computers Versus Hackers, Round One. Fight!
BY LILY HAY NEWMAN

CLOUD COMPUTING
The Race to Sell True Quantum Computers Begins Before They Really Exist
BY CADE METZ

Q&A
David Ignatius on the Future of High-Tech Espionage

intercepting the encrypted financial data that flows across the globe and being able to read it as easily as you are reading this. Quantum computers are so big and expensive that—outside of global technology companies and well-funded research universities—most will be owned and maintained by nation-states. That means the first quantum attacks are likely to be organized by countries hostile to the US and our allies. Rogue states could read military communiques the way the United States and its allies did after cracking the Nazi Enigma codes.

In short, quantum computing presents both an unprecedented opportunity and a serious threat. The United States must lead this transition, in collaboration with its allies around the world. Whether lawmakers want to think of it as a new Manhattan Project or a race to the moon, the US cannot abdicate leadership in scientific discovery or international security.

The window is closing, fast. It took more than five years and nearly half a trillion dollars for companies and governments to prepare for Y2K, which resulted in a non-event for most people. But, the US is not ready for what experts call Y2Q (Years to Quantum), and the time to prepare is now. Even in a pre-quantum era, the need for quantum-safe encryption is real. Banks, government agencies, insurers, hospitals, utilities, and airlines all need to be thinking now about how to implement security and encryption that will withstand a quantum attack.

On complex, large-scale networks, it can take years to roll out even a relatively straightforward update. Quantum-safe encryption relies on mathematical approaches that even quantum computers have difficulty solving. The challenge is ensuring that every point through which data flows, and even the data itself, is wrapped in quantum-safe security.

Private sector research and development are happening in pockets across North America and among the US's allies. Google and IBM both have well-publicized programs to build viable quantum computers. At the same time, though, the US and its allies must take practical steps to prepare for the quantum threat. The National Institute of Standards and Technology is working to evaluate quantum-safe cryptographic candidate algorithms. Other organizations like the European Telecommunications Standards Institute and the United Nations' International Telecommunications Union are working to ensure our standards for connecting systems continue to evolve to be quantum safe. Companies like ISARA are among a small cadre of cryptographers and programmers building quantum-safe security solutions to help high-risk industries and organizations begin protecting themselves.

It's these kinds of efforts that the US and its allies must collaborate on to align the goals of scientific discovery, technological advancement, and national security. As companies build powerful quantum machines, leaders must simultaneously understand the risks those machines pose and the counter-measures required. Executives in every industry need to understand the implications that quantum computing will have on their legacy systems, and take steps to be ready. At a minimum, that means retrofitting their networks, computers, and applications with encryption that can withstand a quantum attack.

Nowhere is it more vital to begin preparations than with the vast network of governmental systems that do everything

challenges of the past century with resolve and determination. The US must do the same with quantum computing.

WIRED Opinion *publishes pieces written by outside contributors and represents a wide range of viewpoints. Read more opinions here.*

FEATURED VIDEO

What the What Is Quantum Computing? We've Got You Covered

TOPICS QUANTUM COMPUTING SECURITY GOVERNMENT CONGRESS

MORE FROM WIRED

Got What It Takes to Compete in Speed Climbing?

BY RHETT ALLAIN

One Very Specific Reason Rami Malek Deserved His Oscar

BY ANGELA WATERCUTTER

Why We Need Guidelines for Brain Scan Data

BY EVAN D. MORRIS

The First Hurricane Relief Drone Almost Flew in The Bahamas

BY MICHELE COHEN MARILL

The Shift to Electric Vehicles Propels a Strike Against GM

BY ALEX DAVIES

Marketers Wanted a New Generation to Target, Hence Alphas

BY EMMA GREY ELLIS

James Cameron and the Saga of the Deepest* Solo Dive Ever

BY MATT SIMON

Today's Cartoon: Clean Energy

BY WIRED CARTOONS

WIRED is where tomorrow is realized. It is the essential source of information and ideas that make sense of a world in constant transformation. The WIRED conversation illuminates how technology is changing every aspect of our lives—from culture to business, science to design. The breakthroughs and innovations that we uncover lead to new ways of thinking, new connections, and new industries.

MORE FROM WIRED

CONTACT

RSS

Site Map

Accessibility Help

Condé Nast Store