Hudson Institute

Quantum Computing: How to Address the National Security Risk

Dr. Arthur Herman
Idalia Friedson

August 2018

Hudson Institute

Quantum Computing: How to Address the National Security Risk

Dr. Arthur Herman
Idalia Friedson

For more information about obtaining additional copies of this or other Hudson Institute publications, please visit Hudson's website, www.hudson.org.

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org** for more information.

Hudson Institute
1201 Pennsylvania Avenue,
N.W. Suite 400
Washington, D.C.
20004

P: 202.974.2400
info@hudson.org
www.hudson.org

Table of Contents

Introduction

Imagine a computer solving the mathematical problems that today's fastest supercomputers can't begin to unlock, in less than a blink of an eye. Imagine a technology that can enable an observer to see through walls, or see into the darkest depths of the world's oceans. Imagine a technology that can build essentially unhackable global networks, while rendering an antagonist's most secret data instantly transparent.

All these are characteristics of quantum computers and quantum technology, which will define the future of global information technology for decades, possibly centuries, to come. It represents a revolution as profound as any in modern history, and it's one on which we stand at the brink, with all its promise—and its perils.

Arthur Herman, "Winning the Race in Quantum Computing," *American Affairs*, Summer 2018

In the 21st century, global supremacy will belong to the nation that controls the future of information technology (IT)—at the heart of which will be quantum technology.

Quantum computers will use the principles of quantum mechanics to operate on data exponentially faster than traditional computers—in ways that will far surpass the capabilities of even today's fastest supercomputers.

For example, a quantum computer with 300 quantum bits ("qubits") could conduct more calculations than there are atoms in the universe. The benefits of this accelerated calculating power will include earlier cancer detection, improvements in machine learning, better pharmaceutical drugs, and more.[1]

Unfortunately, such a computer could also render today's public encryption systems obsolete in less than the blink of any eye.

Such a system would pose a threat to national security because it could open the encrypted secrets of countries, companies, and individuals and cripple critical infrastructure and financial systems. A foreign competitor with the edge in quantum computing could also threaten America's economic security while reaping the many economic benefits of the quantum era.

Therefore, America is involved in another contest that is just as vital to national security, the economy-- and even the future of liberal democracy--as the race to build the atomic bomb in World War II: the race to build the first fully operational quantum computer, which experts believe will play out in the next 10-20 years.

[1] Sergei Kouzmine, "4 Ways That Quantum Technology Could Transform Health Care," *Fast Company*, September 4, 2013, https://www.fastcompany.com/3016530/4-ways-that-quantum-technology-could-transform-health-care.

In October 2017, Hudson Institute hosted a conference bringing together, perhaps for the first time, members of the two halves of the international quantum community: quantum computing experts and experts in quantum-safe cybersecurity. The two groups discussed in a public forum how to frame the future dialogue between policymakers and lawmakers, on the one hand, and the makers of quantum technology, on the other, about what America must do to prepare for the quantum revolution.

That dialogue is now underway, as lawmakers are becoming aware that the quantum computing revolution will have not only a profound scientific and economic impact, but national security consequences as well. At the October conference, Hudson senior fellow Arthur Herman compared the need for a National Quantum Initiative with the Manhattan Project, which ensured that the U.S. would possess the first atomic bomb. Five months later, Morgen Wright, senior fellow at the Center for Digital Government, drew the same comparison. As with the Manhattan Project, Wright wrote in *The Hill*, for the quantum project, "All hands have to be on deck. Money has to be spent. Research has to be done. And access to our research and scientific facilities has to be denied to the Chinese, Russians, and other adversarial countries."[2]

This concerted effort must begin now because America's leading competitors, including Russia and the Republic of China, are also working urgently to develop such a quantum computer and are positioning themselves to dominate the quantum era.

The purpose of this report is two-fold.

First, this report explains the significance of quantum technology and analyzes why it poses a national opportunity as well as a potential threat.

Second, this report sets out the principles around which a national quantum strategy can be built. As will be explained, more resources are needed to win the quantum computing race than just increased federal funding or federal oversight. For example, America's private sector has the most essential role to play in preserving and promoting American IT leadership in the quantum era. Meanwhile, government should help to set priorities, standards, and goals for emerging cybersecurity measures while leaving the private sector to do what it does best: innovate and make an emerging technology as efficient and cost-effective as possible in the shortest amount of time.

In any case, it would be a mistake to assume that America's decades-long dominance of IT will automatically translates into dominance in the quantum era. But with the right strategy and the proper commitment of resources, including funding, the United States can retain its global edge in IT and lead the world's other democracies forward into the quantum era.

---

[2] Morgan Wright, "America's Enigma Problem with China: The Threat of Quantum Computing," *The Hill*, March 5, 2018, http://thehill.com/opinion/national-security/376676-americas-enigma-problem-with-china-the-threat-of-quantum-computing.

1. Quantum Computing: A Serious National Security Threat

The development of quantum technology is not merely a scientific and economic consideration but also a strategic national security concern because a quantum computer will be able to hack into and disrupt nearly all current information technology. Both the national security risks and the economic benefits necessitate that the U.S. win the race to the world's first fully operational quantum computer.

How will quantum computers be able to hack into today's seemingly secure encryption?

All current computers, even supercomputers, use electrical signals to process data in a linear sequence of "bits," where each bit is either a one or a zero. This classical system of ones and zeros is referred to as the binary system.[3]

Quantum computers, however, operate using a quantum bit, or qubit, and each qubit is a physical photon, rather than an electrical signal. In the bizarre world of quantum mechanics, these photons can be in two states at once, essentially functioning as a zero and a one at the same time. This allows a quantum computer to do two—or more—computations at once. Add more qubits, and the computing speed grows exponentially. These quantum physical properties will allow quantum computers to solve problems thousands of times faster than today's fastest supercomputers.[4]

The key advantage over classical computers, however, isn't in the quantum computer's speed of operations but its ability to dramatically reduce the number of operations needed to get to a result. This increased computing power poses a problem for asymmetric encryption, the encryption schema used to protect nearly all of today's electronic data. Asymmetric encryption is secure because it is based on math problems that would take a classical computer centuries to solve.

For example, asymmetric encryption—often called public-key encryption—relies on two keys. One is the private key, which consists of two large prime numbers known only to the party securing the data (for example, a bank). The public key sits in cyberspace and is the product of multiplying together the two private primes to create a semiprime. The only way a hacker could access such encrypted credit card information would be by factorizing or breaking down the large public key—often 600 digits or longer—back to the correct two numbers of the private key. This task simply takes too long for current computers because they must sequentially explore the potential solutions to a mathematical problem.[5]

---

[3] F. Arnold Romberg, "Computers and the Binary System," in *Mathematics, 2nd ed.*, ed. Mary Rose Bonk, vol. 1 (Farmington Hills, MI: Macmillan Reference USA, 2016), 159–65.
[4] Arthur Herman, "The Computer That Could Rule the World," *Wall Street Journal*, October 27, 2017, https://www.wsj.com/articles/the-computer-that-could-rule-the-world-1509143922.
[5] Ibid.

Meanwhile, a quantum system is able to look at every potential solution simultaneously and generate answers—not just the single "best answer," but nearly ten thousand close alternatives as well—in less than a second. This is roughly the equivalent of being able to read every book in the Library of Congress simultaneously in order to find the one that answers a specific question.[6]

Why is a quantum computer so dangerous?

The danger lies in the sheer enormity of critical information that is now protected by such asymmetric encryption, including bank and credit card information, email communications, military networks and weapons systems, self-driving cars, the power grid, artificial intelligence (AI), and more. While asymmetric encryption is effective at thwarting today's hackers armed with classical computers, quantum computers will be able to hack into these systems and disrupt their operation and/or steal protected data.

Experts like to refer to the day that a universal quantum computer will be able to hack into asymmetric encryption as "Q-Day" or "Y2Q"—reminiscent of the Y2K computer meltdown that was thankfully avoided due to the hard work of technologists.

In addition, a quantum computer attack could be virtually impossible to detect because the combination of the available public key with the quantum-deciphered private key would allow a hacker to impersonate someone in the targeted system. Therefore, someone within the hacked network would have to notice unusual internal activity in order to detect a hack—and even then, it would be difficult to determine if the disruptive activity is the result of a quantum computer attack or another type of cyberattack.

By any measure, then, a quantum computer, which will be able to hack into asymmetric encryption, poses an obvious national security threat. At its worst, Q-Day could be the equivalent of a quantum Pearl Harbor—especially because a large proportion of American infrastructure systems are operated electronically, including the grid, water purification and transportation systems, and traffic light and railroad systems. Even more alarmingly, it would be a stealth Pearl Harbor that no one would detect until it was too late.

Because there is not a succinct term to refer to a future large-scale quantum computer that can hack into asymmetric encryption, at Hudson Institute's Quantum Alliance Initiative (QAI) policy center, we refer to such a computer as a quantum prime computer.[7] As discussed later in this section, estimates vary regarding when a quantum prime computer will be built.

---

[6] Ibid.

[7] To be precise, a quantum prime computer is one that can reverse-factor large semi-prime numbers used in asymmetric encryption back to their original prime numbers, or keys. These keys unlock the protected data.

Because subatomic particles are inherently unstable, keeping sufficient numbers of qubits entangled long enough to do calculations is exceedingly difficult. Physicists call this inherent instability decoherence. When a given qubit decoheres, it loses its superposition and can no longer act as both zero and one at the same time, but only one or the other. The ability to compute in the way a quantum calculation requires therefore disappears. Unfortunately for quantum scientists, the slightest disturbance can cause a qubit to decohere; this means engineers must constantly work on ways to mitigate the effects of minute disruptions from the slightest movement, sound, or even light. This is also why many quantum computers are built inside vacuums and deep subzero temperatures.[8]

All this means that major breakthroughs in quantum computing technology come very slowly and take considerable investment in time, money, and human resources. Achieving the ultimate breakthrough to a quantum prime computer will be the slowest of all, and some experts say that it may not happen before 2030.[9]

All the same, though a quantum prime computer may still be years off, a significant breakthrough in quantum computing is likely less than a year or two out on the horizon: quantum supremacy.

Understanding Quantum Supremacy

The term quantum supremacy is sometimes used to characterize the ability of future quantum computers to hack into asymmetric encryption, but it is actually a term with a very specific and narrower meaning. Quantum supremacy will be achieved when a quantum computer is able to successfully solve a problem no classical computer can solve, even a relatively artificial problem.[10]

Many experts believe that quantum supremacy will be achieved by a continuous entanglement of approximately 50 qubits. In March 2018, Google entangled 72 qubits, although it has not yet been able to keep its qubits entangled to demonstrate quantum supremacy.[11]

Though real-world applications of quantum supremacy are debatable and likely to be limited in the near term,[12] there are broader implications. Quantum computers will have taken the first step in demonstrating that they can indeed solve problems that

---

[8] Arthur Herman, "The Computer That Could Rule the World," *Wall Street Journal*, October 27, 2017, https://www.wsj.com/articles/the-computer-that-could-rule-the-world-1509143922.
[9] "Modern Cybersecurity Totally Futile in Quantum Computing Era," ABI Research, October 24, 2017 https://www.abiresearch.com/press/modern-cybersecurity-totally-futile-quantum-comput/
[10] Ariel Bleicher, "Quantum Algorithms Struggle against Old Foe: Clever Computers," *Quanta Magazine*, February 1, 2018, https://www.quantamagazine.org/quantum-computers-struggle-against-classical-algorithms-20180201/.
[11] Tom Simonite, "Google, Alibaba Spar over Timeline for Quantum Supremacy," *Wired*, May 20, 2018, https://www.wired.com/story/google-alibaba-spar-over-timeline-for-quantum-supremacy/.
[12] Alexandra Ossola, "Quantum Computing Is Going to Change the World. Here's What This Means for You," *Futurism*, January 8, 2018, https://futurism.com/quantum-computing-qa/.

today's classical computers cannot, not only in theory but in fact. Even so, it is important to note that even with achieving supremacy, quantum computers will not be able to replace classical computers outright—and will not for the foreseeable future.[13] They will, however, begin to take an increasingly leading role in the world of computing.

Ultimately, achieving quantum supremacy will be an important milestone in demonstrating the viability of quantum computers and in moving closer to a true quantum prime computer.

Three Types of Quantum Computing Machines

Today there are three types of quantum machines in use. One is the quantum annealer, of which the D-Wave system is the leading example.[14] Quantum annealers do not attempt to manipulate the qubits as they compute. That means they can do calculations using one thousand qubits or more and rely on qubits getting entangled more or less at random. In this way, a quantum annealer can be used to solve complex sampling and optimization problems.[15]

The second type of quantum computer—or rather computer model—is the quantum emulator, or simulator, which is actually an analog system. The quantum emulator allows the study of quantum systems that are difficult to study in the laboratory and impossible to model even with a supercomputer. They are special-purpose devices designed to provide insights about specific physics problems, such as by simulating certain aspects of the earth's climate in a controlled experiment or simulating the best way for electricity to be transmitted without loss. Recently two independent teams of scientists, including one from the Joint Quantum Institute, have used more than 50 interacting atomic qubits to mimic magnetic quantum matter.[16]

The third type of quantum computer, and the one most commentators refer to when discussing quantum computing, is the universal quantum computer. The universal quantum computer will be able to run almost any type of algorithm and discover patterns in data that existing digital computers, including the fastest supercomputers, cannot. The computing power needed for a universal quantum computer, however, requires entangling the qubits during the entire time of computing—a challenging feat.

---

[13] Andrea Morello, "Double or Nothing: Could Quantum Computing Replace Moore's Law?," *The Conversation*, June 12, 2018, https://theconversation.com/double-or-nothing-could-quantum-computing-replace-moores-law-362.
[14] There is debate about whether a quantum annealer can be referred to as a quantum computer.
[15] Arthur Herman, "Winning the Race in Quantum Computing," *American Affairs*, May 30, 2018, https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/.
[16] Emily Edwards, "Quantum Simulators Wield Control over More than 50 Qubits," Joint Quantum Institute, December 1, 2017, http://jqi.umd.edu/news/quantum-simulators-wield-control-over-more-50-qubits.

The Difficulty in Predicting Q-Day

Hypothetically, if the first useful universal quantum computer can be looked at as quantum computer 1.0, each subsequent version will boast a higher number of entangled qubits, providing an increasing amount of computing power. A quantum prime computer, then, will be the approximate equivalent of quantum computer version 5.0, with a massive jump in the number of entangled qubits compared to the number that computer makers have successfully entangled today. Compared to Google's 72 qubits, for example, experts predict that a quantum prime computer will require 4,000 entangled qubits (often referred to as logical qubits) to break RSA 2096, and 2,500 qubits to break elliptical curve cryptography—two widely used asymmetric cryptosystems.

There is considerable debate as to whether such a computer is 5, 10, or 15 years off. IBM, for example, predicts that large-scale quantum computers, or what we are calling a quantum prime computer, may be only five years away.[17]

Why is it so difficult to predict the evolution from today's quantum computer 1.0 to a quantum prime computer?

First, it is difficult to make such a prediction because there are different architecture models for making qubits (e.g., superconducting, topological, and ion trap).[18] Leading companies are employing these different approaches, but many theoretical and engineering hurdles remain.

Second, quantum computer 1.0 will be used to design the next generation of quantum computers. [19] Scientists have long been warning about the end of Moore's Law, which is used to predict the acceleration of technology. With the invention—and potential ubiquity—of quantum computing, there truly is no way to know if Moore's Law will be applicable for predicting how quickly we will reach a quantum prime computer. [20]

Last, emerging technology will also have a role to play in designing future quantum computers. For example, artificial intelligence is closer on the horizon than quantum computers and will be useful in writing algorithms and software for quantum

---

[17] John Breeden, "Tomorrow's Quantum Computers Are Already Threatening Today's Data," *Defense One*, July 10, 2018, https://www.defenseone.com/threats/2018/07/future-quantum-computers-already-threatening-todays-data/149557/.
[18] Sam Sattel, "The Future of Computing—Quantum & Qubits" *EAGLE* (blog), Autodesk 2D and 3D Design and Engineering Software, May 24, 2017, https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/.
[19] Will Knight, "Serious Quantum Computers Are Finally Here. What Are We Going To Do with Them?," *MIT Technology Review*, February 21, 2018, https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/.
[20] "Technology Quarterly: After Moore's Law," *Economist*, February 25, 2016, https://www.economist.com/technology-quarterly/2016-03-12/after-moores-law.

computers in the near and long term. [21] Again, it is difficult to anticipate how much AI will help accelerate the time frame from quantum computer 1.0 to a quantum prime computer, but the impending intersection of quantum and AI is clear.

When reading differing analyses, it is important to note that quantum computing companies have a vested interest in predicting a longer timeline for realization of a quantum prime computer (often citing 20 years or more), while quantum cybersecurity experts have an interest in predicting an earlier date (some say as soon as 2026).[22]

The point is that there are too many variables to predict with precision when a quantum computer will pose such a significant threat to national security.

The Threat to Stored Data

However, in a profound way the existential threat that a quantum computer poses to encryption today is not years away, but already upon us. Nation-states whom we consider competitors or adversaries are currently collecting and storing sensitive data knowing that they will be able to decrypt this information when a quantum prime computer is realized.[23] This means that data not protected prior to Q-Day will be just as vulnerable as data not protected afterwards.[24]

Collection of such data might not be problematic for fields where information that is 10-20 years old is no longer relevant; however, the intelligence community frequently marks information as classified for at least 50 years in order to protect the nation's most important information and personnel assets.[25] There is debate on how soon a quantum prime computer will be realized, but experts all agree that it will be within 50 years—certainly within a time frame in which information that has been harvested and stored will have negative effects on the U.S. economy and national security.

Thankfully, there is a solution to the threat posed by a quantum computer attack, namely quantum cybersecurity—and developing and implementing it must be a priority.

---

[21] Cade Metz, "Building A.I. That Can Build A.I.," *New York Times*, November 5, 2017, https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html.
[22] Scott Totzke, "IoT and the Quantum Threat. What To Do?," *ITSP Magazine*, June 28, 2017 https://www.itspmagazine.com/from-the-newsroom/iot-and-the-quantum-threat-what-to-do
[23] John Breeden. "Tomorrow's Quantum Computers Are Already Threatening Today's Data," *Defense One*, July 10, 2018, https://www.defenseone.com/threats/2018/07/future-quantum-computers-already-threatening-todays-data/149557/.
[24] Meredith Rutland Bauer, "Quantum Computing Is Coming for Your Data," *Wired*, July 19, 2017, https://www.wired.com/story/quantum-computing-is-coming-for-your-data/.
[25] Exec. Order No. 13526, 3 C.F.R. 13526 (2009), https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf.

2. Quantum Cybersecurity: How to Implement Layered Security

As we have seen, it is extremely difficult to predict when a quantum computer able to hack into asymmetric encryption—and therefore stealthily hack into the majority of U.S. electronic data—will be realized. At the same time, hackers are harvesting sensitive data now with the understanding that they will be able to decrypt such information in only 10–20 years.

But while quantum computing poses a grave national security threat, quantum cybersecurity harnesses the same principles of quantum physics to provide the solution.

The term "quantum cybersecurity" is often used to encompass both quantum security's software aspects (post-quantum cryptography) and hardware aspects (quantum cryptography).

Today there are three important technologies underlying quantum cybersecurity solutions, and they can be implemented in a layered approach with a coherent timeline—one that mirrors the evolution of quantum computers.

Quantum Random-Number Generators

Existing encryption algorithms can be strengthened by adding in truly random numbers. Also known as quantum keys, these are the strongest encryption keys currently available, and they make use of cosmic background energy to harness perfectly occurring randomness. Scientists measure the crackle of energy in the fabric of the universe as it spontaneously creates and self-destructs. It is impossible to predict the frequency and timing of the cosmically sourced radioactive particles as they strike the electronic sensors, allowing quantum physicists to harness this quantum noise and convert it into true random numbers.

Banks, governments, and private cloud carriers are already implementing quantum random-number technology. There is a range of additional uses for the technology, including blockchain software and other forms of encrypted data, that would benefit from protection against both a classical computer and a quantum computer.[26]

A quantum random-number generator (QRNG) by itself will not be able to thwart a quantum computer forever, but as Dr. Raymond Newell of Los Alamos National Lab notes, "A quantum number generator isn't just used for quantum cryptography; it can

[26] Idalia Friedson, "How Quantum Computing Threatens Blockchain," *National Review*, February 28, 2018, https://www.nationalreview.com/2018/02/quantum-computing-blockchain-technology-threat/.

be used for any cryptography and makes all cryptography better. It can make your computer safer today."[27]

Post-quantum Cryptography

The next step is to develop post-quantum cryptography, often referred to as quantum-resistant algorithms (QRAs). Just as asymmetric encryption uses difficult math problems to stump classical computers, post-quantum cryptography will use difficult math problems to stump a quantum computer. The challenge lies in creating useful math problems for this purpose.[28]

One of the challenges with post-quantum cryptography is that the projected timeline for implementation is too far past the projected development of a quantum prime computer. The National Institute of Standards and Technology (NIST), housed within the Department of Commerce, is working to develop and certify standards for such algorithms. NIST's tentative timeline for this project goes only so far as to put together draft standards for 2022–24, while noting that this timeline is subject to change.

However, as Dr. Lily Chen noted at the 2018 summit of AFCEA (Armed Forces Communications and Electronics Association) in Washington, D.C.,[29] after such standards are created, it will take another 10 years before they are implemented, potentially pushing the NIST timeline out to 2034+.[30] Even accepting the most conservative predictions about the probable date for achieving a quantum prime computer (approximately 20 years away), this puts the timeline for protecting valuable data from the quantum threat uncomfortably behind the emergence of the threat itself.

Quantum Communication Networks

While QRNGs and post-quantum cryptography are software solutions, the third, longer-term method is a hardware technology called quantum communication networks. These networks use quantum key distribution technology to transmit data between two points by encoding data on individual particles. Any attempted hack automatically severs the connection, thus alerting the parties that an intrusion was attempted. Because quantum communication networks use quantum physics, the

---

[27] Raymond Newell, Hudson Quantum Conference, Panel on Quantum Cybersecurity, Question & Answer, October 17, 2017, https://www.hudson.org/events/1465-the-coming-quantum-revolution-security-and-policy-implications102017.
[28] Idalia Friedson, "How Quantum Computing Threatens Blockchain," *National Review*, February 28, 2018, https://www.nationalreview.com/2018/02/quantum-computing-blockchain-technology-threat/.
[29] Lily Chen, AFCEA 2018 Cybersecurity Technology Summit, Panel on Quantum Computing, February 27, 2018.
[30] "Post-Quantum Cryptography Workshops and Timeline," Computer Security Research Center, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline.

information is unhackable as it is travelling between the two points.[31] China used this type of technology in its Micius satellite and in the 2,000 kilometer network it built between Beijing and Shanghai.[32]

Yet there are limits to how far these networks can transmit information, and a quantum repeater—essentially an amplifier—will need to be created for them to become viable over long distances.[33]

An important step in developing and commercializing these promising quantum networks is to draft and implement compliance and compatibility standards. Unlike many instances where government pushes for standards and requirements in implementing a new technology, it is actually private industry that is driving the push for quantum network standards. This is because standardization is necessary to accelerate and expand the commercialization of quantum information technology by stimulating a global supply chain and driving costs sharply down (by one expert's estimate, as much as one hundredfold).

A crucial component of this standardization is defining interoperability standards so that one quantum network can connect to a different quantum network. Either way, a clearly defined set of standards will make it possible for companies and other entities to connect their products into larger and larger networks, which in turn will enable quantum technology to advance more rapidly and ultimately create a global quantum internet.[34]

Additionally, standards will inform government policy and in turn, such policies will set future requirements for those working in quantum technology across the globe, which is one reason the U.S. should aim to be the front-runner in developing standards.

Establishing Leadership in Quantum Cybersecurity

In quantum cybersecurity—unlike quantum computing—the United States is not currently a global leader. Only a handful of American start-ups dot the landscape. By contrast, the closest U.S. allies, such as Australia, Canada, and the UK, boast the

---

[31] Idalia Friedson, "The Information Age Needs Quantum Cybersecurity," *RealClearFuture*, May 22, 2017, http://www.realclearfuture.com/articles/2017/05/22/the_information_age_needs_quantum_cybersecurity_111955.html.

[32] Emerging Technology from the arXiv, "Chinese Satellite Uses Quantum Cryptography for Secure Video Conference between Continents," *MIT Technology Review*, January 30, 2018, https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/.

[33] Keith W. Crane et al., "Assessment of the Future Economic Impact of Quantum Information Science," IDA Science & Technology Policy Institute, August 2017, https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2017/P-8567.pdf.

[34] Will Hurd, "Quantum Computing Is the Next Big Security Risk," *Wired*, December 12, 2017, https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/.

leading private sector quantum cybersecurity firms. QuintessenceLabs in Australia, for example, develops the entire suite of quantum cybersecurity solutions mentioned here, while ISARA Corporation is located in Canada's quantum valley ecosystem and focuses on post-quantum cryptography. Meanwhile, the recognized world leader in quantum cryptography and quantum key distribution—ID Quantique—was recently purchased by SK Telecom in South Korea, another significant U.S. ally.

With Australia, Canada, and the UK, the United States has an added advantage in terms of technology and information-sharing: all four countries are members of the Five Eyes intelligence community, which originated in U.S.-UK intelligence cooperation in World War II.

Therefore, the United States should look to its closest allies to develop and commercialize quantum cybersecurity measures. Such solutions must be implemented before the development of a quantum prime computer. Otherwise, the results could be catastrophic.

Particularly for critical infrastructure, a combination of software and hardware solutions will be beneficial. For example, until it becomes commercially and scientifically viable to secure the entire U.S. power grid with quantum networks, such hardware will be used only in high-density areas, alongside quantum-resistant algorithms.

In conclusion, America should adopt an "all of the above" approach (similar to its approach to missile defense) to research, commercialize, and integrate layered quantum cybersecurity solutions, first by implementing quantum random-number generators, and then by rolling out post-quantum cryptography and quantum cryptography.

Doing so, however, will require some important thinking about a national quantum cybersecurity strategy, in addition to a national quantum computing strategy. Today, the country that has taken the lead in combining the two is not the United States, but China.

3. The United States versus China: Contrasting Strategies

The U.S. is widely regarded as the leader in quantum computing, thanks largely to the innovation and resources of the private sector. Nonetheless, China is closing the gap.

The race to the world's first quantum computer is characterized by an international competition for the best way to make and entangle qubits—the fundamental building blocks of quantum computers.

Intel, for example, is working to develop "spin qubits," which harness the spin states of single electrons. It hopes to then scale down these qubits and manufacture them out of silicon—no surprise given the computing giant's existing semiconductor and silicon technologies.[35]

In January 2018 Intel unveiled its 49-qubit quantum-processor chip, dubbed "Tangle Lake," which uses superconducting circuits and operates at extremely cold temperatures.[36] Superconducting circuits are arguably the most popular approach to building qubits and the one taken by Google, IBM, Rigetti Computing, and Quantum Circuits.[37] The benefits of superconducting circuits are that they utilize existing technologies widely used in the semiconductor industry and compute quicker than qubits. Their drawback is the same as silicon qubits, namely that they require extremely cold temperatures in order to operate.

In March, Google announced the development of its Bristlecone quantum processor, a 72-qubit chip it hopes will allow it to achieve quantum supremacy in 2018—a feat it incorrectly predicted it would achieve in 2017. Nonetheless, many experts see Google and Chinese company Alibaba in lockstep to reach quantum supremacy first, though Alibaba claims that Bristlecone's technical imprecision will prevent Google from achieving quantum supremacy.[38]

Another industry titan, IBM, has successfully built and measured an operational prototype 50-qubit processor. This builds upon the 20-qubit quantum computing

---

[35] Jeremy Hsu, "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy," *IEEE Spectrum*, January 9, 2018, https://spectrum.ieee.org/tech-talk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy.

[36] "2018 CES: Intel Advances Quantum and Neuromorphic Computing Research," *Intel Newsroom*, January 8, 2018, https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/.

[37] In short, superconducting circuits work when a resistance-free current oscillates around a circuit loop while a microwave signal places the current in a superposition state. Sam Sattel, "The Future of Computing—Quantum & Qubits," *EAGLE* (blog), Autodesk 2D and 3D Design and Engineering Software, May 24, 2017, https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/.

[38] Tom Simonite, "Google, Alibaba Spar Over Timeline for Quantum Supremacy," *Wired*, May 20, 2018, https://www.wired.com/story/google-alibaba-spar-over-timeline-for-quantum-supremacy/.

system accessible to third-party users through IBM's cloud computing platform and will be made available in the next-generation IBM Q systems.[39]

Additionally, American startup Rigetti Computing—founded by a former IBM employee—is making a name for itself. It is the only company besides IBM and Alibaba to make available to customers a programmable "quantum logic gate" model computer, i.e. a basic quantum circuit using a small number of qubits, in Rigetti's case a 19-qubit processor.[40]

Another model for creating qubits is ion trap computing, led in the U.S. by IonQ Inc., a start-up that was spun off from a University of Maryland lab.[41] In ion trap computing, lasers are used to cool and trap ions, or electrically charged atoms, placing them in a superposition state. Remarkable progress has been achieved to date, and today's ion traps can hold dozens of ions for hours and have coherence times longer than thousands of seconds. Furthermore, ion trap computing does not require extremely cool temperatures. One of the drawbacks, however, is that it is the slowest of all the qubit types in development and requires a multitude of compact lasers to remain stable.[42]

Microsoft and Nokia Bell Labs are working on topological qubits, perhaps the most intriguing model because it relies on a particle whose existence is still theoretical and widely disputed.[43] These majorana fermions, or "quasiparticles" as they are often known, reside at the boundary between two particles. In March 2018, Microsoft pointed to research in the journal *Nature* to highlight clear evidence of the existence of majorana fermions.[44] The company also recently released a free preview version of its Quantum Development Kit, which includes its proprietary and domain-specific Q# programming language.

In order to give the American effort in developing quantum computing technology a further boost, in June 2018, legislation was introduced in the U.S. House of Representatives (H.R. 6227), followed by companion legislation in the Senate (S. 3143). The bill, nicknamed the National Quantum Initiative Act, calls for the

---

[39] Will Knight, "IBM Raises the Bar with a 50-Qubit Quantum Computer," *MIT Technology Review*, November 13, 2017, https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/.
[40] "Rigetti Rolls Out Latest Forest Quantum Developer Environment," *HPCwire*, February 27, 2018, https://www.hpcwire.com/2018/02/27/rigetti-rolls-latest-forest-quantum-developer-environment/
[41] Kathy-Anne Soderberg and John Harrington, "Changing Computing and Networking Forever, One Qubit at a Time," Wright-Patterson Air Force Base, July 18, 2017, http://www.wpafb.af.mil/News/Article-Display/Article/1250638/changing-computing-and-networking-forever-one-qubit-at-a-time/.
[42] Sam Sattel, "The Future of Computing—Quantum & Qubits," *EAGLE* (blog), Autodesk 2D and 3D Design and Engineering Software, May 24, 2017, https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/.
[43] Natalie Wolchover, "The Future of Quantum Computing Could Depend on This Tricky Qubit," *Wired*, May 20, 2014, https://www.wired.com/2014/05/quantum-computing-topological-qubit/.
[44] Jeremy Kahn, "Microsoft Edges Closer to Quantum Computer Based on Elusive Particle," Bloomberg, March 28, 2018, https://www.bloomberg.com/news/articles/2018-03-28/microsoft-edges-closer-to-quantum-computer-based-on-elusive-particle.

acceleration of basic research, establishes interagency collaboration, promotes standards development, and establishes research and education centers. It also calls for the allocation from FY 2019–23 of $625 million to the Department of Energy, $250 million to the National Science Foundation, and $400 million to the Department of Commerce, which houses NIST.[45] This spending would be in addition to the $200 million or so that the United States currently spends on quantum research and technology, spread over several federal agencies.

Even this expanded federal effort, however, pales by comparison to China's commitment to winning the quantum computing race. Its government announced in September 2017 its intention to build the world's largest quantum research facility in Hefei province.[46] The $10 billion, four-million-square-foot national laboratory is slated to be completed around March 2020, and is dedicated to making major advances in quantum technology, including computers, sensors, and cryptography. The *South China Morning Post* wrote that the government's "mission is to develop a quantum computer that can be used by the military to crack the most secure encrypted codes in seconds and enable submarines to operate on stealth mode underwater for more than three months."[47]

Within six months of the Chinese government's announcement, Chinese giants Alibaba Group Holding, Tencent Holdings, and Baidu announced their own quantum computing research departments. In partnership with the government-owned Chinese Academy of Sciences (CAS), Chinese industry leader Alibaba Cloud, announced the release of its 11-bit quantum processor via its cloud services in March 2018. Alibaba had partnered with CAS in 2015 to create the CAS-Alibaba Quantum Computing Laboratory, which it claims participated in the development of the world's first photon quantum computer that same year.[48]

Baidu was the last of the three IT giants to join the race, but the head of its Institute for Quantum Computing, former University of Technology Sydney Professor Duan Runyao, is widely recognized as a world leader in his field.[49] Indeed, Professor Runyao is an illustrative example of how China is seeking to close the quantum computing gap with the United States by recruiting foreign talent and expertise to collaborate and travel to different Chinese institutions in the name of global scientific advancement. Universities, companies, and governments in the West, including in the United States, are only just beginning to assess the national security risks of such information sharing and the quantum "brain drain" to China.

---

[45] National Quantum Initiative Act, H.R. 6227, 115th Cong. (2018), https://www.congress.gov/bill/115th-congress/house-bill/6227/text.
[46] Stephen Chen, "China Building World's Biggest Quantum Research Facility," *South China Morning Post*, September 11, 2017, https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility.
[47] Ibid.
[48] "Alibaba Cloud and CAS Launch One of the World's Most Powerful Public Quantum Computing Services," Alibaba Cloud Documentation Center, March 1, 2018, https://www.alibabacloud.com/press-room/alibaba-cloud-and-cas-launch-one-of-the-worlds-most.
[49] Masha Borak, "After Alibaba, Baidu Leaps Into Quantum Computing," *TechNode*, March 8, 2018, https://technode.com/2018/03/08/baidu-quantum-computing/.

While China recognizes that the U.S. is the world leader in quantum computing, its leadership is determined to establish an insurmountable lead in the crucial field of quantum cybersecurity. The Chinese government understands that a quantum technology strategy must not be limited to quantum computing, and thus China leads the way in unhackable quantum communications. Its first milestone was the 2016 launch of its Micius quantum satellite, a crucial step in establishing a secure ground-to-space quantum communications network. China has also made key advances in developing a similarly unhackable 2,000-kilometer quantum communications network from Shanghai to Beijing.[50]

This intensive Chinese government and industry focus on quantum computing and technology highlights China's efforts to "transform itself from the factory of the world into an advanced economy build on hi-tech industries," as noted in the *South China Morning Post*.[51] China, whose government has the advantage of long-term strategic thinking, as well as control of IT companies and access to enormous amounts of "private" data, also plans to be the leader in artificial intelligence by 2030.

Though quantum and AI are distinct technologies, they will not be developed in isolation from one another. In fact, quantum computers will be able to speed up the machine learning underpinning AI, while artificial intelligence will be able to write algorithms and programs for quantum computers.[52] Quantum technology is integral not only to China's broader strategic thinking about its hi-tech future, but also to the way that technologists and policymakers worldwide imagine the relationship between quantum and AI. This is because of the ways in which each of these technologies will help develop the other—as well as the fact that AI will be vulnerable to hacking and commandeering by an intruder if not protected by quantum cybersecurity.

Furthermore, China understands that emerging technologies will eventually intersect, including quantum, which is another reason it is investing heavily in its fiber-optic infrastructure. One goal of the "Broadband China" strategy is to increase the percentage of households with broadband access from 40 percent in 2015 to 70 percent by 2020.[53] By contrast, a 2017 Deloitte study reported that fewer than 20 percent of U.S. households have fiber optics, with the rest relying on slower copper technologies or no broadband services at all.[54]

---

[50] Arthur Herman, "Winning the Race in Quantum Computing," *American Affairs*, May 30, 2018, https://americanaffairsjournal.org/2018/05/winning-the-race-in-quantum-computing/.
[51] Zen Soo, "China's Race for the Mother of All Supercomputers Just Got More Crowded," *South China Morning Post*, March 12, 2018, https://www.scmp.com/tech/science-research/article/2136669/chinas-race-mother-all-supercomputers-just-got-more-crowded.
[52] Cade Metz, "Building A.I. That Can Build A.I.," *New York Times*, November 5, 2017, https://www.nytimes.com/2017/11/05/technology/machine-learning-artificial-intelligence-ai.html
[53] "When Computers Became Classic: Understanding the Race Towards Quantum," Wilson Center, September 14, 2017, https://www.wilsoncenter.org/publication/when-computers-became-classic-understanding-the-race-towards-quantum.
[54] "Communications Infrastructure Upgrades: The Need for Deep Fiber," Deloitte, July 13, 2017, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5GReady-the-need-for-deep-fiber-pov.pdf.

An advanced fiber-optic infrastructure—particularly one compatible with quantum cybersecurity technology—will be paramount for underpinning a hi-tech society because it is the highway on which emerging technologies such as quantum computing and AI will run.

4. The Need for a U.S. National Quantum Strategy

The Chinese example demonstrates that quantum computing and quantum cybersecurity must be viewed holistically and through a strategic security lens. Whereas the private sector has much of the economic incentive to develop a quantum computer, market forces have not catalyzed industry to develop quantum cybersecurity in the necessary time frame. Because the advent of a quantum computer powerful enough to hack into asymmetric encryption threatens the power grid, food and water supply, and defense networks, the U.S. government must take a central role in actively developing, commercializing, and implementing effective quantum cybersecurity measures before that happens.

Numerous factors make it difficult to predict Q-Day, when a quantum computer will be able to tear through the encryption protecting most of America's data. Yet if history is any indication, this emerging technology will be here sooner rather than later.

In addition to the bipartisan National Quantum Initiative bill discussed previously, a draft bill was released by Senator Kamala Harris's office calling for the Department of Defense to fund quantum computing research. Importantly, the bill's first principle notes that "focused and continued investment in the development of viable quantum information science technology is vital to national security." It also states that quantum communication is a critical area of development. The bill draft calls for ensuring that the best technology is made available for U.S. defense; and emphasizes that work should be maintained at the lowest classification level so that information-sharing and technology-shared can continue as efficiently as possible. [55]

This bill hopefully signals the beginning of an important paradigm shift, to the idea that the national discussion on quantum technology should largely be viewed as a conversation about national security, in which quantum computing and quantum cybersecurity must be looked at as two halves of the whole strategy. Therefore, the principles identified at the outset of the Harris bill should be considered and emulated in the five-year strategic plan that would be mandated after passage of the National Quantum Initiative Act.

The plan should do the following:

- Prioritize which assets to secure (grid, food supply, water supply, military networks, etc.).
- Prioritize which technologies to invest in.
- Determine a timeline for such prioritized goals.
- Discuss the importance of developing standards and a timeline for doing so.
- Highlight the role of public-private-academic partnerships.

[55] Quantum Computing Research Act of 2018, S. 2998, 115th Cong. (2018), https://www.congress.gov/bill/115th-congress/senate-bill/2998/text.

- Address the issue of a trained workforce and the role of STEM education.
- Discuss the intersection of classification levels and innovation.
- Highlight the role of cooperation with allies.

A crucial element of the U.S. government's strategy to develop quantum cybersecurity should entail working with the closest U.S. allies, many of which are global leaders in quantum cybersecurity, like Canada, Australia, and the UK.

Such cooperation will allow the United States and its allies to fulfill the goal of realizing the world's first universal quantum computer in a free, democratic society, while effectively securing critical information in advance of the grave security threats posed by a quantum computer.

In the race to hi-technology, authoritarian regimes have distinct advantages, including their access to "private" data, ability to pour money into specific innovation goals, and ability to mobilize and influence the private sector. However, as the United States has demonstrated time and time again, the power of innovation, collaboration, and free markets can best authoritarian regimes and ultimately lead the way to a freer and more prosperous future.

Conclusion

To protect and extend American global leadership in the 21st century, the U.S. must combine two separate but convergent missions: pursuing a quantum computer, while simultaneously securing its information networks using quantum cybersecurity. It is imperative that the United States make its most sensitive information quantum-secure well in advance of the predicted timeline for a quantum computer attack, whether that information resides in the private or the public sector.

U.S. competitors, particularly China and Russia, are making noticeable strides in quantum technology, including computers, sensors, and cybersecurity. The United States must maintain its lead in computing and take significant steps to overtake China in quantum cybersecurity, particularly quantum cryptography, by promoting and adopting an integrated layered approach to quantum-safe cybersecurity.

In addition, the United States must work on these technologies in conjunction with its closest allies, especially the Five Eyes, as they are currently leading the way in quantum cybersecurity. At the same time, in the current global security environment, America needs to systematically curtail quantum-technology cooperation with competitors.

Finally, to remain secure and globally competitive in the long term, the U.S. must educate its workforce about the implications of quantum technology and prepare employers and employees in academia and the private and public sectors to develop and utilize quantum technology. Equally importantly, Americans need to find ways to build "thinking quantum" into STEM curricula and workforce training in preparation for the quantum revolution.

Just as Sputnik in 1958 compelled the United States and its government to think seriously about the importance of scientific and technological leadership (and ultimately enabled it to win the Cold War and travel to the moon), so, too, does America need to get serious about the quantum revolution's risks and opportunities, before a competitor seizes the lead in a similarly spectacular way.

Because by then it will be too late.

It is time for America's leaders, and the public, to understand the stakes of quantum computing. What is unfolding every day at corporate, university, and government laboratories around the world is more than a scientific advance of enormous proportions and consequences; it will also determine the geopolitics of the future.

In the end, the Manhattan Project did not just win a world war; it secured the future for American leadership and the security of the free world in the atomic age. In the quantum age, the stakes will be at least as vital—and the consequences of losing the quantum race, nearly as catastrophic.

Glossary of Terms

Asymmetric encryption, also known as public-key cryptography, uses non-identical (asymmetric) public and private keys to encrypt and decrypt data.

Entanglement is a condition in which two particles are inherently linked even though they may be separated. If one particle is measured, the result for the other particle is implied.

Moore's Law states that the number of transistors on an affordable CPU (central processing unit)—which determines processor speeds and overall processing power—doubles every two years. Moore's Law predicts that this trend will continue into the foreseeable future.

Post-quantum cryptography, often referred to as quantum-resistant algorithms, refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer.

Quantum computing uses quantum mechanical phenomena such as superposition and entanglement to perform operations on data.

Quantum cryptography, often referred to as quantum communication networks, uses principles of quantum physics, as opposed to mathematical algorithms, to generate and distribute encryption keys used to safeguard the transmission of data over unprotected networks. Quantum cryptography often uses quantum key distribution.

Quantum information science (QIS) is an area of study that builds on uniquely quantum principles such as superposition, entanglement, and squeezing to obtain and process information in ways that cannot be achieved based on classical principles.

Quantum key distribution (QKD) uses quantum properties to send an encryption key between two parties. Because of the way quantum mechanics works, QKD ensures that encryption keys cannot be intercepted by a third party without the sending and receiving parties knowing.

Quantum random-number generators (QRNGs) use quantum phenomena to create entropy to generate random numbers. QRNGs are unlike pseudo-random number generators (PRNGs), which are deterministic, and other "true" random number generators (TRNGs), which use other physical processes to generate entropy, because QRNGs are provably random.

Quantum simulation refers to the use of quantum hardware to simulate quantum processes.

Qubits are the quantum version of the bits used in classical computing. However, unlike bits, which have a value of 0 or 1, qubits may assume a superposition of these two states.

Superposition is a condition in which a quantum system can be in multiple states simultaneously. The actual state of superposition cannot be known until the system is measured.

About the Authors

Arthur Herman, Ph.D., is a Senior Fellow at Hudson Institute and Pulitzer Prize finalist author of 10 books, including *1917: Lenin, Wilson, and the Birth of the New World Disorder* (HarperCollins, 2017). He is also the author of the Hudson Institute report *Pacific Partners: Forging the U.S.-Japan Special Relationship* (2017).

His *New York Times* bestseller *How the Scots Invented the Modern World* has sold more than half a million copies worldwide, and his *Freedom's Forge: How American Business Produced Victory in World War Two*, was named by the *Economist* as one of the most notable books of 2012.

He has written extensively on the intersection of technology, policy, and national security for more than half a decade. In addition, he has published several articles on quantum computing, including "Winning the Quantum Race" (*American Affairs* Summer 2018 edition), "The Computer That Could Change the World" (*Wall Street Journal*, October 2017), and "Quantum Cryptography: A Boon for Security" (*National Review*, March 2017). On October 17, 2017, he convened "The Coming Quantum Revolution: Security and Policy Implications," Washington, D.C.'s first public conference bringing together the quantum computer and quantum cybersecurity communities, including from Canada and Australia.

Idalia Friedson is a former Research Associate and Project Manager at Hudson Institute, where she helped co-found the Quantum Alliance Initiative and is currently a member of the Advisory Board. Her published articles include "How Quantum Computing Threatens Blockchain" (*National Review*) and "Behind Enemy Transmission Lines" (*National Review*), which emphasizes the role that quantum cybersecurity can play in securing the electric grid. She assisted in convening "The Coming Quantum Revolution: Security and Policy Implications," where she chaired a panel on quantum cybersecurity. She graduated from Amherst College with a B.A. in law, jurisprudence, and social thought.

About the Quantum Alliance Initiative

The Quantum Alliance Initiative (QAI) was established following Hudson's October 2017 inaugural international conference on the coming quantum revolution. QAI serves as the flagship policy center for Hudson's efforts to shape U.S. policy on quantum technology, including quantum computers, sensors, and networks.

QAI's mission is to develop and champion policies that enable the United States to win the race to a universal quantum computer, while ensuring that it is resistant to a quantum computer cyberattack, thus allowing Americans to enjoy the maximum benefits of quantum technology with minimum disruption. QAI consists of Hudson Institute experts in cybersecurity, national security, defense, and emerging technology.

Additionally, the Initiative maintains an advisory board that includes leaders in technology, policy, law, and defense.

QAI's focus includes leveraging existing alliances to: 1) secure present and future vital infrastructures from quantum attack; 2) create a Quantum Alliance network among U.S. allies such as Canada, Australia, and Great Britain, to which other nations can be added over time; and 3) develop and secure present and future supply chains for quantum technology.

Acknowledgments

The authors would like to thank the members of the QAI advisory board for contributing invaluable insight and expertise on quantum technology—especially regarding technical concepts—since the Initiative began. In particular, they would like to thank Dr. Chris Monroe, professor of physics at the University of Maryland and co-founder and chief scientist at IonQ, Inc., for his review of technical elements in this report. Furthermore, they would like to thank Thomas Keelan for his help in editing the report and intern Brent Cronce for his invaluable assistance with research and citations.

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit **www.hudson.org for** more information.

Hudson Institute
1201 Pennsylvania Avenue,
N.W. Suite 400
Washington,
D.C. 20004

P: 202.974.2400
info@hudson.org
www.hudson.org