global POLICY

Quantum Computing and Global Security

By Nayef Al-Rodhan- 20th February 2015

Nayef Al-Rodhan outlines the implications of quantum computing for progress and security.

The fast-evolving processing power of computers is a fact that hardly surprises anyone today. This was predicted five decades ago by the co-founder of Intel, **Gordon Moore**, in what is now widely known as the Moore Law. He postulated that processor speed (and overall processing power) for computers would double every 18 months and that the number of transistors on an integrated chip would double at the same pace. The law gained so much popularity that it became some sort of self-fulfilling prophecy and **chip fabricators** raced to make processors faster, smaller and simultaneously cheaper.

In the past decade, this trend appears to have reached a plateau as the **difference in processing speed** between 2000 and 2009 has barely doubled in a 10-year span. This has prompted conclusions that the end of Moore's Law, anticipated for a while now, is nearing. To keep up with the demand to increase processing power, big companies will have to invest much more in research, thus potentially spiking up the prices of processors.

While the accuracy of Moore's Law is now losing ground, this does not mean that the search for supercomputing has faded too. Moving away from conventional computing, with its already impressive power, quantum computing is part of a new revolutionary generation of computer research which aims to surpass not only limitations in speed but also in the **technical limits of the chip-making material**. Whatever speed can be imagined with computers, it is nowhere near what quantum computing is expected to achieve.

In the 1980s, the **notion that quantum psychics** could be used to perform computations simultaneously, on massive amounts of information, emerged for the first time. The quantum computer is considered a "**seventies child**" as its conceptual foundations were first laid during the late '70s and early '80s. The interest in developing such a machine, with unprecedented speed and agility, was revived in the mid 1990s, when computer theorists began to explore the possibilities of developing quantum computers. Highly ambitious researches placed overly optimistic bets that quantum computers could be in use by 2010. To date, scientists have yet to create an operational quantum computer but this task is surely not hampering its research and development. "**The Holy Grail of supercomputing**" is now drawing increasing interest and investment: NASA, IBM and Google's D-

Wave Systems are among the most important actors in the field and more recently, the National Security Agency joined the ranks by pledging $ 80 million on basic research in quantum computing.

What is so special about quantum computing?

Unlike a classic computer, quantum computers do not work in an orderly and linear manner. **Conventional computers** function according to binary logic, using 1s and 0s ("either/or" distinctions) and stringing together combinations of these. By contrast, quantum computing uses quantum bits or qubits, which are basically quantum particles such as electrons or atom nuclei. This gives quantum computers unique functionalities as qubits communicate with each other through entanglement and calculate every existing possibility at the same time. Qubits are placed in a state of "**superposition**" where they do not have values of 1 or 0 but both. In this regard, quantum computing is a step further from what is possible in the real world as **qubits** can be in more than one state at a time.

This means that quantum computers would be capable of huge calculations and enormous processing power. They could **surpass conventional computers** in speed and could help solve or race through problems that would normally take other systems eons to solve.

The ongoing research is also charting new grounds in material science and our understanding of materials properties. For example, a leading start-up in quantum computing, **D-Wave Systems**, claims that certain types of metals, such as niobium (a soft metal that becomes superconducting at low temperatures), are key to the development of the quantum processor. Moreover, other recent breakthroughs in **silicon-wrapped quantum technology** prove again that more thorough investigation of materials and properties of chemical elements can unlock the unknowns that have delayed progress.

Quantum computers, once fully functional, will mark the ultimate frontier in computing, being able to make calculations billions of times faster. It is their extraordinary features which also prompt immediate considerations about their social and security implications. In a future not too distant, when the quantum leap will have reached an operational stage, we can expect a series of groundbreaking uses. For a start, **quantum computers** could help scientists find cures for cancer, advance research of Alzheimer's disease, or find distant planets; they could be used to simulate or test certain political and military scenarios and inform policymakers about possible outcomes. But by far, the greatest scope for interest (and investment) so far has been the promise of quantum computing in the area of cryptography.

Quantum computers could potentially be capable of **breaking public key encryption**, which is responsible for protecting almost all private communication online. Not surprisingly, the US spy agency, **the NSA**, has been at the forefront for the development of the supercomputer which could crack most keys used for encrypted communication. Its sponsored research project, called "**Penetrating Hard Targets**", aims to build a computer that could break almost all forms of encryption that protects medical, business, e-commerce, banking or government records in the world. Clearly, if successful, this would be the ultimate 'Big Brother moment' for the agency. Today, long encryption keys (particularly for sensitive information) are very difficult to break, taking up to several years but quantum computer could accelerate the process, making it millions of times faster. Similarly, since qubits cannot be cloned, hacking a code encrypted with a quantum computer is virtually impossible and hacking would mostly be a concern if a hacker were to have access to a quantum computer.

Racing for the supercomputer

The development of quantum computing remains highly disputed and advancing slow due to a combination of scientific unknowns, mixed reactions in the academic community and industries. A persistent obstacle has been

the challenge of instability and vulnerability. Quantum computers combine computing with quantum mechanics, an extremely complex and still mysterious branch of physics. On top of this, as **calculations take place at the quantum level**, no outside interference (such as light or noise) is permissible since the qubits would collapse and it would disrupt the calculations. This makes quantum computing extremely expensive to build and maintain.

However, as elusive as the search for the super computer might be, it has sparked a competition in which both states and private shareholders have stakes.

The US Defence agencies have been investing in quantum computing research for over a decade and other countries have gradually entered the race as well. Now China, Russia and other European states are investing in quantum research and Canada's Institute of Quantum Computing at University of Waterloo is over a decade old. In late 2013, the **UK government announced** it would spend £270 million to build a network of quantum computing centres.

Security Implications

The construction of a functional quantum computer means much more than simply winning the innovation race and it has clear national security relevance. In the context of the current of development, the race is now fought at an academic level, where researchers work in interdisciplinary labs to shrink transistors to the quantum scale.

However, as pointed out by many, science is now inevitably done in global collaborative frameworks and it is quite difficult to estimate if there are guaranteed paybacks for individual nations. Ultimately, the Herculean efforts and funding that defence agencies pledge often pass through private industry and will benefit the commercial sector too, not only the government.

Quantum computing will have very disruptive effects, both at national levels and internationally. They will have implications for **information security**, impacting both symmetric-key algorithms and public-key algorithms. If spying and mass surveillance are already impressively effective with the more limited means we now have in place, quantum computing will simply enable unprecedented breaches of privacy and access to confidential data in businesses, hospitals, banks or governments worldwide. The NSA **no longer hides** its support and sponsorship for the development of quantum computing which could be used to crack any encryption system in the world. Hand-in-hand with the race for the supercomputer is the race to 'own' the internet and gain virtually unlimited access to information. Quantum communication will redefine how we communicate, making data transfer faster and more able since quantum computers can process enormous amounts of information with high encoding and decoding speeds.

The amount of distrust already existing over questions of privacy both domestically and between governments is only expected to surge, creating further domestic and diplomatic frictions and accelerating competition between states. A likely scenario is that with functional quantum computers, some governments will speed up the investment for the creation of other, **cryptography-capable computers**. At the same time, this competitive situation will leave behind less resourceful countries, widening a digital gap that is already stark.

The unique potential of quantum computers could also give unmerited temporary advantage to some individuals, retailers or groups over others. Quantum computers could dramatically improve stock market predictions thus benefiting **wealthy financial institutions**. This is not an imminent risk since the fees for access to quantum computing will be staggering, yet the possibility of quantum computing entering the Wall Street is not to be dismissed.

Coexistent with its numerous security risks, quantum computing offers a set of unique opportunities for humanity and states. From better logistic optimizations to DNA sequencing, better predictions in global warming and weather forecasting, quantum computing means new potential to tackle global challenges, improve healthcare and

find cures for diseases, solve optimization, labour or economic problems (including in agriculture or water management). The application of quantum computers to solve optimization problems could be especially useful in the defence sector or space, where it can significantly impact the speed and accuracy of operations. A quantum computer could calculate ideal paths for travel either on land or air and it could improve code verification dramatically. Indeed, software verification is a key element in the defence industry's push for quantum computers, especially as complex software systems are increasingly at the heart of defence applications. The **F-35 joint strike fighter**, for instance, has more than 10 million lines of code on the aircraft and quantum computers could be employed to do the code validation and verification.

Google also hopes that quantum computers could be used to make better and faster robots and more sophisticated artificial intelligence. Their use could also be extended to **aviation** in instances such as snowstorms where quantum computers could help find optimal alternative routes instantly. The Space agency NASA has also shown interest in quantum computing and its **Quantum Artificial Intelligence Laboratory** is working on exploring the likely applications of quantum computing in space. In addition to optimization solutions during space missions, such as better planning and scheduling, the lab is also working on improving the operations of NASA's Kepler mission, which searches for habitable and Earth-sized planets. Current computational limitations, which use heuristic algorithms to identify transit signals from smaller planets, only help find approximate solutions whereas a quantum computer could perform data-intensive searches among the over 150,000 stars in the field of view of the spacecraft.

Emerging technologies for renewable energy are also taking into account the power of quantum computing and **California's renewable energy program** aims to use "smart grids" or "quantum grids", which is a network of quantum computers, to allow higher efficiency of input and output of energy. **Qubits** can also be deployed in solar panels to replace current photovoltaic cells technology or in quantum batteries and quantum dots can be embedded as semiconducting material, revolutionizing the energy sector.

Quantum computing is possibly a final threshold of scientific marvel, which will bring unparalleled precision and accuracy in computing. Given the extremely sensitive functions it can perform, it is critical that research and dissemination is done responsibly, with a view to harness its positive contributions. It is indeed critical that the development of quantum computing progresses in a way that will impede its becoming merely a tool for enhanced surveillance and endless control.

Nayef Al-Rodhan *is a Neuroscientist, Philosopher and Geostrategist. He is an Honorary Fellow at St Antony `s College, University of Oxford, and Senior Fellow and Head of the Geopolitics and Global Futures Programme at the Geneva Centre for Security Policy. Author of The Politics of Emerging Technologies. Implications for Geopolitics, Human Enhancement and Human Destiny (Basingstoke: Palgrave, 2011)*