CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Quantum Diplomacy for a New Technological Age

by Randolph Mank

December 2017

POLICY UPDATE

QUANTUM DIPLOMACY FOR A NEW TECHNOLOGICAL AGE

by Randolph Mank

CGAI Fellow
December 2017

Canadian Global Affairs Institute
Institut canadien des affaires mondiales

Prepared for the Canadian Global Affairs Institute
1800, 421 – 7th Avenue S.W., Calgary, AB T2P 4K9
www.cgai.ca

ISBN: 978-1-988493-73-2

Executive Summary

Quantum mechanics is a body of science that Albert Einstein, Max Planck, Niels Bohr and others developed in the early decades of the 20th Century. Along with its indisputable technological benefits, it also led to the development of nuclear weapons a few decades later, which has had a profound effect on global security and diplomacy. This threat remains with us today. Another of the offshoots of the 'Quantum Age' - information technology - spawned the internet and, with it, now familiar cyber vulnerabilities. Given this repeated 'promise and peril' pattern - scientific discovery, leading to technological advancement, leading to new threats - it is surprising how little serious discussion has occurred around the diplomatic and security consequences of the latest wave of new technologies. This phase features the emergence and merger of artificial intelligence, nano-technology, robotics and, soon, quantum computing. Already finding their way into modern weapons' systems, controlling the proliferation of these technologies and their misuse is a sleeper issue that will soon demand an entirely new set of diplomatic initiatives, as did the monitoring and control of nuclear weapons. This paper suggests parameters for developing quantum diplomacy to meet the challenges of this new era. Among other things, it suggests the eventual need for an international treaty to control both weaponization and proliferation of these technologies.

What do alleged Russian meddling in the U.S. presidential election, the recent spate of global cyber-attacks, increased use of cruise missiles and drones, advances in nano-technology, the commercialization of quantum computers, and rapid developments in robotics and artificial intelligence (A.I.) all have in common? They point to a rapidly changing technological landscape with broad and disruptive policy implications, not least in the spheres of security and diplomacy.

The scientific discoveries around the strange realities of quantum mechanics date back a full century.[1] Those discoveries, about the counter-intuitive behaviour of atoms and their sub-particles, have already yielded enormous technological advances, leading to today's computers, smartphones, the internet, medical imaging, and an array of other remarkable and welcome inventions.

Yet the same scientific discoveries have had profound consequences for war and peace, as well. The early promise of an atomic solution to the age-old search for clean energy, yielded quickly to the horrifying realities of nuclear weaponry during the Second World War. This in turn led to a postwar flurry of international diplomacy to control its proliferation, with the Comprehensive Nuclear Test Ban Treaty, the Nuclear Non-Proliferation Treaty, the International Atomic Energy Agency and a host of other Cold War agreements and mechanisms. Today, in the ongoing threat from North Korea, it is clear that the need to control the proliferation of this technology remains as current as ever.

If that was the first phase of the Quantum Age, and if the by now familiar Information Technology revolution -- including computers and the internet -- were its second act, we are now undoubtedly on the threshold of a new and equally portentous phase. With the pace of change exponential, not linear, the demands to control its more lethal aspects will be upon us sooner than we think.[2]

Though much has been made of the disruptive social and economic consequences of this new phase, relatively little discussion has been devoted to the challenges for global security and diplomacy.

Standing at this tipping point, it is timely to ask: what will be required of a new quantum diplomacy[3], and what should we be looking at now in preparation?

The Unfolding Quantum Age

With technological changes underway in almost every sector, it is clear that today's world will look substantially different a decade from now and beyond. As they should, governments mostly support this change and actively encourage it, eager for the economic benefits that will accrue from innovation.

The mapping of the human genome, at first expected to take decades, unfolded much faster than initially predicted and now points the way to significant future improvements in medicine. Similarly, refinements and cost efficiencies in solar and other renewables are also advancing more rapidly than expected and offer hope for a very different energy future with important environmental benefits.

Lest we forget how fast technology can change the world, it was less than twenty years ago that Canadian company, Research in Motion, now BlackBerry, played a pioneering role in smartphone development. In the short period of time since then, the impacts of mobile computing have been as profound as the commercial changes in the industry itself.

Technological change is about to speed up even more dramatically. Quantum science is on the verge of delivering qubit-powered computing, exponentially faster than anything we have ever seen. It is claimed that an already existing quantum computer is 100 million times faster than a conventional one. [4]

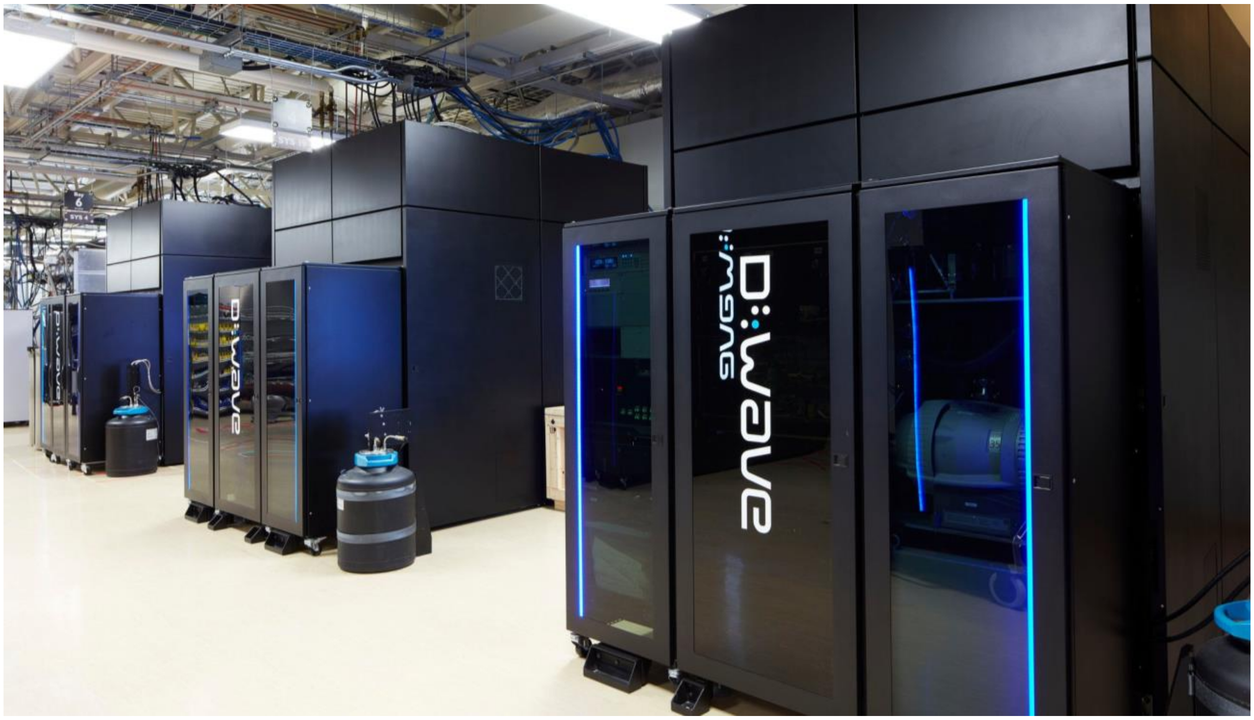

Figure 1: D-Wave Systems is a Canadian manufacturer of computers that apply the principles of quantum physics. (Martin Tessler/New York Times)

Far from being science fiction, the first quantum computers have already been developed and sold by the Canadian company D-Wave. It promotes its latest model as a 2000 qubit model, (though there remains technical debate over whether it is truly quantum).[5] NASA, Google and defense giant Lockheed Martin have been among the early customers.

If predictions of author and inventor Ray Kurzweil are correct – and he has been remarkably prescient so far – in the next 10-25 years, we will be approaching what he calls a technological 'singularity', no less than the merging of human and machine-based intelligence.[6]

Though hotly debated, we are already headed down this path, with A.I. finding its way into more and more everyday products. While warning against the existential dangers of fusing artificial intelligence and biology – as Stephen Hawking has also done – Elon Musk has founded Neuralink, a new startup aimed at achieving just this. The firm will strive to develop a 'neural lace' connecting the human brain and A.I.[7] Musk's reasoning is that humans need to find a way to keep up with and control A.I.-capable machines.

In Canada, the University of Toronto recently announced its new Vector Institute to advance research and development in A.I.[8] Already well established are the Perimeter Institute and the Institute for Quantum Computing at the University of Waterloo. The list of others around the world involved in the race to develop this technology is growing fast. Large corporations like Amazon, Google, Microsoft and IBM are already rapidly amassing most of recorded human knowledge in massive cloud data storage centers and moving ahead on A.I. as well.

These repositories of what's known as Big Data, using the vehicle of the internet, will become the neural centres of the interconnected national and global systems, whose secure functioning will become vital to our future. They could also become our Achilles' heel.

The Risks

On the one hand, we should avoid Cassandra-like fears and welcome these new technologies. After all, technological solutions to environmental degradation, climate change, poverty, and health care will be crucial to our future.

Yet, we should also admit to the risks. Those actors who both understand and know how to capitalize on new technologies are relatively few. More than governments, a comparatively small number of entrepreneurs are shaping our future, and doing so without any prescribed direction or accountability for the socio-economic and political ramifications. The move to develop autonomous vehicles, for example, has been instigated by the private not the public sector, despite profound socio-economic consequences.

The future of employment is already a subject of widespread concern, as increased automation is affecting traditional occupations. In the past decade alone, we have witnessed disruptions in whole industries, with both winners and losers in such areas as communications, finance, travel, transportation, and entertainment, to name a few. While debate continues about whether or not sufficient new replacement jobs will be created, guaranteed basic income is a policy response already under discussion and even trial.[9]

Cyber security threats are also already causing regular disruptions and eliciting policy responses. Beyond current technological capabilities, however, quantum computers combined with A.I. will be much more potent. Together with advanced algorithms, massive quantum computing power will be able to crack even the most advanced security codes in use today.

The so-called ‘Internet of Things’ – where sensors embedded in everyday items will all be connected and controlled through the internet – is being built in earnest. It is already connecting infrastructure, banking, security systems, and much else to the internet. Relying on even the best security encryption available today, it is dangerously exposed to risk. Those risks could be potentially catastrophic in the future.[10]

So, too, the internet itself, and its vast network of servers around the world, could be vulnerable. Having emerged from the oversight of the U.S. Department of Commerce just this year, the internet is now governed under an opaque and amorphous international multi-stakeholder conclave, convened several times a year by the International Corporation for Assigned Names and Numbers (ICANN) based in Los Angeles. It fiercely defends the freedom and openness of the internet, while lacking both direct accountability to any higher entity, or any national or international protector. [11]

Meanwhile, the development of advanced robotics and miniaturization through nano-technology, which has already revolutionized everything from assembly lines to heavy industries, is proceeding toward its own rapid merger with advanced A.I. Japan, with its declining birthrates and shrinking workforce, has been working on humanoid robots for decades, and consumer versions are now becoming available.[12] IBM’s famous “Watson” has shown that computers equipped with A.I. and using ‘deep learning’ can rival and even defeat the most skilled humans at our own complex games, including most famously chess and Jeopardy. Google’s ‘Deep Mind’ has done the same in the game of Go.

Figure 2: "Jeopardy!" contestants Ken Jennings and Brad Rutter compete against Watson in 2011 (Getty Images)

It would be naive to hope that these benign consumer and industrial applications of robotics, combined with still early A.I., will not find their way into more sophisticated and lethal military applications. Autonomous drones are already a frequently used weapon of aerial surveillance and warfare. Through its Defense Advanced Research Projects Agency, DARPA, the U.S. Defense Department also has other weapons systems under development that draw on advanced technologies. One company, Boston Dynamics, has recently unveiled surprisingly agile robots capable of backflips and other highly athletic movements.[13] It's reasonable to assume that America's strategic competitors are on the same path.

And this is where we reach a tipping point that merits well-considered policy responses to questions we should be posing and debating today. The marriage of these technologies will be an exponential force multiplier that will lead to a whole new level of risk in relatively short order.

The Foreign Policy Vacuum

While technological progress has been breathtaking, the intellectual energy devoted to debating its policy implications, outside of science labs and technology gatherings, has been anything but.

In the international relations field, noble attempts to generate discussion on quantum diplomacy have been few and far between.[14] Discourse among a few dozen academics is a start, but the issues need to be mainstreamed in national policy debates. Government officials, caught up in the controversies and crises of the day, are normally reluctant to look too far ahead. In the United Nations, the G7/G20, NATO, and elsewhere, well established but largely undervalued cyber-security working groups continue to play policy catch up to technological change.

Fortunately, history shows at least one case in which scientists have so far been able to regulate themselves. In 1975, microbiologists established the so-called 'Asilomar guidelines', named after the site of a biotechnology conference that year in Monterey, California. They agreed that, for reasons of global safety, deliberate containment measures should be built into any experiments on, and development of, recombinant DNA for genetic manipulation.[15]

Ironically, it's also the computer science community itself that sounded the alarm on A.I. in 2015, writing an open letter calling for international controls.[16] The United Nations responded under the Convention on Certain Conventional Weapons (CCW) and convened a so-called experts group on Lethal Autonomous Weapons Systems (LAWS) the same year.[17]

More recently, G7 finance ministers flagged the importance of cyber security in their May 2017 statement issued in Italy. G7 leaders also included references to the problem in their communiqué a few weeks later. Such declarations are important, but they are narrow in focus and ring hollow without follow up actions.

As for international law, the Budapest Convention on Cybercrime came into force in 2004 and is the main, though quite limited, vehicle for global co-operation in this field. The focus among the

52 parties to the agreement is on preventing crimes such as the dissemination of hate material and copyright infringement, as well as on co-ordinating laws and their enforcement. [18]

Given the Budapest Convention's limited aims, the international community clearly needs a more ambitious legal regime aimed at preventing the hostile use of advanced cyber, robotic, and A.I. technologies. Reviving the so far unsuccessful attempts to generate a new cyber security treaty would be a natural place to start.[19] Though necessary, it will be far from sufficient. Cyber security is indeed a real threat but other threats will flow from the proliferation of the full array of new technologies. Given that the technological trend line is irreversible and that, unchecked, its use in future warfare is as utterly predictable as it would be devastating, there is merit in championing an international campaign that extends beyond the discussions thus far.[20]

Should Canada succeed in its bid to obtain a two-year rotating seat on the United Nations' Security Council in 2021, pursuing such an agreement could be a worthy though challenging initiative during its tenure.[21] After all, Canada's 2017 defence policy review acknowledged the importance of cyber and new technology threats.[22] It would take a great deal of time and effort, but Canada's prominence in quantum computing and A.I., along with lessons learned from the mixed success of the 1999 Anti-Personnel Mine Ban Convention, might further bolster the credibility of such an initiative.

Parameters of Quantum Diplomacy

How can we meaningfully define the parameters of foreign policy debate on such new and unpredictable technology? We should begin by addressing a list of very practical questions that arise already, which suggest areas for follow up. A good starting point would be to consider the following:

First, on security, looking at two, five and 10 year timelines:

What are the main foreseeable threats from new technologies?

- National threat assessments should be reviewed to consider threats from remote controlled, highly intelligent and lethal weapons, including to critical infrastructure systems.

What systems will be required to defend against these threats?

- Post-quantum cryptography assessment projects should be initiated.
- National preparedness and business resumption plans should be reviewed.

What weapons systems will be outmoded/required?

- Major, multi-year weapons procurement plans with 10-20 year time frames should be reviewed (fighter jets, naval vessels etc) and challenged for their effectiveness against new technologies.

How can we defend against quantum attacks by non-state actors?

- Assessments, plans, and controls should be developed and co-ordinated with NATO allies and globally.

How can quantum technology be turned to security advantage?

- The role of quantum technology should be assessed in both encryption and intelligence gathering.

Second, on diplomacy:

Can A.I. become a tool for modernizing the practice of diplomacy?

- New diplomacy tools should be developed for the age of Big Data, the Internet of Things, and A.I.
- New technology should be applied to the movement of people, especially travel and migration documents and tracking.

What changes to the international legal regime and institutions are needed to safeguard global security?

- An A.I., nano-technology, robotics, and quantum computing treaty should be proposed to counter both weaponization and proliferation.
- An international oversight body for monitoring and control should be considered.
- Quantum computing and A.I. export controls should be incorporated into trade agreements.

What positive opportunities do quantum technology and A.I. present?

- Explore the use of new technologies for preventive diplomacy, peacekeeping, and international development.

Such questions show how complex and entangled the challenges and opportunities will be. The point is to tackle the issues now and develop policy as the technology unfolds, rather than *ex post facto* when it may be too late.

Conclusions

Though technological advance should be embraced for its many potential benefits, the coming marriage of robotics, nano-tech, A.I. and quantum computing also presents a set of foreign policy challenges that we will need to face in the coming decades. The challenges are likely to be at least as fundamentally disruptive as those that emerged from the early decades of the Quantum Age, if not more so.

Arms races drawing on the new technologies may well affect international relations. And, as always, malevolent non-state actors will attempt – and unfortunately on occasion succeed – in using new technology to threaten national and international security. We should heed the warnings of several prominent thought leaders about the existential threats to humanity that unregulated A.I. itself poses.

Though no one can predict the future, we know enough already to begin to engage in practical assessments and debates about appropriate policy responses. Future foreign and defence policy reviews, as well as international deliberations, will need to address these coming challenges with ever increasing urgency.

While reaping the benefits of technological advancement, not to look squarely as well at its pitfalls is to put at potential risk nothing less than the security of our nations and the international system upon whose stability we depend.

[1] A good overview of the evolution of quantum science: Frank Close, **The Infinity Puzzle**, Alfred & Knopf, 2011.

[2] For a detailed explanation of exponential technological change see Ray Kurzweil, **The Singularity is Near**, Penguin, 2005.

[3] For the history of the term Quantum Diplomacy see: https://www.diplomacy.edu/blog/quantum-diplomacy-ideas-other-side-looking-glass

[4] http://www.wired.co.uk/article/quantum-computing-explained. See also: https://beta.theglobeandmail.com/report-on-business/rob-magazine/quantum-computing-technology-explained/article36397793/

[5] https://arstechnica.com/science/2017/01/explaining-the-upside-and-downside-of-d-waves-new-quantum-computer/

[6] https://www.ted.com/talks/ray_kurzweil_on_how_technology_will_transform_us

[7] http://www.theverge.com/2017/3/27/15077864/elon-musk-neuralink-brain-computer-interface-ai-cyborgs

[8] http://www.bbc.com/news/world-us-canada-39425862

[9] https://www.thestar.com/news/gta/2017/03/16/pilot-project-to-introduce-a-basic-income-in-ontario-gets-strong-public-support.html

[10] http://research.stevens.edu/post-quantum-cybersecurity

[11] http://www.theregister.co.uk/2016/09/30/internet_handover_is_go_go_go

[12] http://www.cnbc.com/2017/03/09/heres-why-japan-is-obsessed-with-robots.html

[13] https://www.bostondynamics.com/

[14] For one example see: https://projectqsydney.com/portfolio/q3-q-symposium-2016/

[15] https://profiles.nlm.nih.gov/QQ/B/C/G/D/_/qqbcgd.pdf

[16] https://futureoflife.org/open-letter-autonomous-weapons/

[17] http://www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument

[18] https://en.wikipedia.org/wiki/Convention_on_Cybercrime

[19] https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

[20] https://www.justsecurity.org/32268/cyber-security-treaty/

[21] http://www.huffingtonpost.ca/2016/09/20/justin-trudeau-un-general-assembly_n_12111644.html

[22] http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

About the Author

Randolph Mank *is a three-time Canadian ambassador and a former VP of BlackBerry. He is currently a Fellow of the Canadian Global Affairs Institute and the Balsillie School of International Affairs, as well as president of MankGlobal Inc.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.