THE KOSCIUSZKO INSTITUTE | POLICY BRIEF | FEBRUARY 2020
ISSN 1689-9873

POST-QUANTUM INTERNATIONAL SECURITY
AN INTRODUCTION

Andrea García Rodríguez, Andrea Marzeth Padilla, Robert Siudak

INTRODUCTION

Back in 1971, Thomas Kuhn wrote that the way science affected socioeconomic development was through technology (Kuhn 1971, 283), and the way societies 'felt' technology was through technological revolutions. In the field of physics, the first quantum revolution at the beginning of the 20th century changed the way we perceive the world by solving some of the inconsistencies of classical mechanics that eventually allowed the creation of the laser and transistors – the basic elements of computation systems.

The second quantum revolution that we are witnessing now aims to apply the characteristics of quantum mechanics to Information and Communication Technologies (ICTs). Quantum knowledge applied to today's technological advances promises exponential improvements in numerous fields. Through simulation, it could help to develop new drugs; with quantum sensors, it could allow for more precise defect detection in key aircrafts components; by boosting imaging and computation capabilities, it could revolutionize key industries such as manufacturing, fintech or smart mobility. Moreover, this quantum revolution will have an especially profound impact in the field of cryptography which currently serves as the basis for secure processing and exchange of digital information. Consequently, the development of quantum solutions accompanying the second quantum revolution lies in the necessity to guarantee the security of the most valuable resource in the modern world – information.

Recent developments demonstrate that quantum technologies are not merely considered a scientific or economic advancement, but also a strategic national concern (Herman and Friedson 2018). Countries are becoming increasingly aware of both the benefits and perils of investing in quantum technologies. In 2018, the U.S. government released a National Quantum Initiative Act to direct its efforts towards research on quantum computing and defence (US Congress 2018). China included quantum technologies as one of the main R&D goals in their 13th Five-Year Plan (2016-2020), spending over $150 million in 2017 under the National Key Research and Development Plan (Ministry of Science and Technology 2017). In Europe, the European Union "Quantum Flagship" programme has the objective to boost quantum research on the continent and create a common European quantum Internet (QuTech 2019, 19).

From the point of view of strategic, international affairs, quantum technologies might provide countries with new offensive tools in cyberspace, as well as novel defensive capabilities:

#QuantumOffence – is based on quantum computer capabilities, able to solve specific computational challenges more efficiently (even million times faster than traditional machines). So far, most of the cutting-edge advancements in that field have been delivered by U.S.- or Canadian-based companies, with Google, D-Wave and IBM as leaders.

#QuantumDefence – is provided thanks to quantum communication and quantum cryptography, which, bluntly speaking, are using the principles of physics to secure digital information. Leading R&D efforts in both of these fields are distributed more internationally than #quantumoffence, with a growing position of China as home to the most developed quantum communication infrastructure (a so-called "quantum internet").

Apart from #QuantumOffence and #QuantumDefence, a wide range of other quantum-related fields such as quantum sensors or materials might be categorised as dual-use technologies, with possible military applications in the ICT domain and beyond (e.g. in radars, aircrafts, soldier gear). This article serves as an introductory analysis of opportunities as much as potential threats spurring from quantum technology advancements.

#QuantumOffence

Imagine a computer that can crack today's most secure communication in the blink of an eye. Moreover, imagine a technology that can build critically unhackable global networks while instantly rendering an antagonist's most secret data (Herman, Winning the Race in Quantum Computing 2018). Quantum computing is to become one of the major, large-scale fast advancing fields worth of $283 million by 2024 (Markets and Markets 2019). This technology harnesses the principles of quantum mechanics (also known as quantum physics) to operate on data exponentially faster than traditional computers, causing a wonderful phenomenon of small scales that can surpass the capabilities of even today's fastest supercomputers (Herman and Friedson 2018, 3). Although some believe that quantum computers are not intended to replace traditional computers, they are expected to be used as a different instrument to solve certain families of complex problems that are beyond the problem-solving capabilities of traditional computing.

Data in an ordinary computer is represented as a binary-valued quantity of bits, each of which can either be 0 or 1. This represents a simple closed-ended question, such as those originated from a "yes/no" question or a "stop/go" decision. A quantum computer, on the other hand, uses quantum bits (known as qubits) which can be both 0 and 1 at the same time—this is widely known as a superposition of states. Therefore, number-crunching is done much faster on a quantum computer than on any other ordinary computer. For instance, if one has got a list of million items in their database and wants to find one specific item on that list, all an ordinary computer can do is to look through that list one item at a time until eventually it finds the item it was initially searching for. But quantum computing is different. A quantum computer can take all those items simultaneously and find the one it is looking for immediately through a process of optimization (Herman and Friedson 2018, 6). Similarly, qubits can also be paired up instantaneously, affecting each other from anywhere else in the universe. This process is defined as "entanglement", and even though in practice it is very difficult to happen, scientists have discovered that leveraging from an entangled qubit can provide very interesting results, such as hack-proof applications and an interception-proof distribution of quantum keys in data security, that cannot be obtained with an ordinary computer (Quantum Computing Report 2018).

From the hardware point of view, quantum computation needs new materials to cope with qubits requirements, such as total isolation to external disruption. It also requires internal hardware development and reimagining of components. Add to this layer new software requirements such as the need of new programming languages, algorithms, and general architecture. From the information point of view, the uncopiable nature of qubits requires a new design of information transfer systems that minimizes the margin of error and loss of information. The system must also cope with the vulnerabilities of the current most widespread cryptosystems and design new ones that are adaptable to the features of quantum bits. Moreover, a network of quantum computers that effectively sends received information is the basis of a quantum internet, which would make interactions faster and safer.

Tech giants (see Table 1) have already begun investing heavily into quantum computing. Google has introduced Bristlecone, the world's largest quantum processor to date, with a 72-qubit system, ousting IBM's 50-qubit system quantum processor (Harris 2018). Researchers expect that these recent developments will revolutionize fields that rely on complex simulations, like chemistry and solid-state physics, as well as will offer significant speed increases for search technologies (O'Connor, et al. 2018, 6). As shown by IBM's first commercial quantum computer, the machine will be able to perform any task that an ordinary computer can, offering a number of advantages over traditional computing, albeit they have never been proven nor experimentally demonstrated (E-Spin Corporation 2018). Furthermore, for a large-scale universal quantum computer to be created, applied in a real-life environment and commercialized successfully, a few things need to happen. First, error correction in computation processes needs to be improved as it is currently the Achilles' heel of complex quantum IT systems; this has to be followed by simultaneous work on energy efficiency of quantum computers and a more systemic approach to building up a workforce with specialized skills in quantum programming. The latter could be particularly tricky given that the skills needed for classical computing development are to a large extent different from those that will be needed for quantum computing programming at a large scale.

Quantum technologies are to become key instruments in the mass implementation and evolution of various emerging technologies, such as Machine Learning, Deep Learning, Probabilistic Neural Networks, and Blockchain, among others. Even though these emerging technologies could use the high computational speed of supercomputers, they are still considered slow to deliver such results. Thus, quantum computers may potentially offer the best solutions among varying weighted options more efficiently, establishing a significant

advantage compared to classical computing. For instance, using quantum systems to train and run machine learning algorithms could allow them in the future to solve complex problems quicker, potentially enhancing their performance in areas such as disease diagnosis, fraud detection, and efficient energy management (IBM n.d.). Most importantly, this and other specific applications of quantum technologies might be available even without a full-blown universal quantum computer. Thanks to the use of natural principles of physics, the so-called "quantum annealing" might already help us to solve key issues in machine learning such as a sampling problem more efficiently.

Table 1. The biggest quantum computers (universal/gate model)

Manufacturer	Name	Qubits	Release Date
Google	N/A	20 qb	2017
Google	N/A	49 qb	2017
Google	Bristlecone	72 qb	5 March 2018
IBM	IBM Q 5 Tenerife	5 qb	2017
IBM	IBM Q 5 Yorktown	5 qb	
IBM	IBM Q 14 Melbourne	14 qb	
IBM	IBM Q 16 Ruschlikon	16 qb	17 May 2017
IBM	IBM Q 17	17 qb	17 May 2017
IBM	IBM Q 20 Tokyo	20 qb	10 November 2017
IBM	IBM Q 20 Austin	20 qb	
IBM	IBM Q 50 prototype	50 qb	
INTEL	17-Qubit Superconducting Test Chip	17 qb	10 October 2017
Intel	Tangle Lake	49 qb	9 January 2018
Rigetti	8Q Agave	8 qb	4 June 2018
Rigetti	16Q Aspen-1	16 qb	30 November 2018
Rigetti	19Q Acorn	!9 qb	17 December 2017

Source: Own elaboration

The main question is, therefore, when the quantum-enhanced ICT will be able to fulfil most of its promises? A truly robust and fault-tolerant quantum computer will need to be equipped with more than dozens of qubits that are currently available. Even if we narrow the analysis to universal quantum computers (gate model), not quantum annealing machines which already can reach more than 5,000 qubits, estimates still vary here significantly. They range from the worst-case scenarios setting the bar on the level of billions of qubits (Fowler, et al. 2012) to moderate estimates of millions of them (Gidney and Ekerå 2019). A research study published in 2019 estimated that to break RSA, one of the best known and most widely used cryptographic algorithm (2048 bit), a quantum computer would need 20 million of qubits and 8 hours. With its present architecture, the current global leader, 72-qubit Bristlecone processor, still lacks the scalability needed for that expansion. On the other hand, last year's developments show that quantum computing might even surpass the momentum of traditional IT Moore's Law which states that computing power doubles every two years or so. Between 2016 and 2018, we witnessed boom in universal quantum processors moving the capacity from 5 to 72 qubits. This makes many experts, investors and even politicians to believe that a full-blown universal quantum computer might become a reality during the next decade or two.

#QuantumDefence

The Achilles' heel of modern digital systems is data security. Every piece of information encrypted in the best possible manner available today might be captured, stored and wait safely just before the point in time in which humanity will invent technology able to break this specific encryption (for example, the RSA algorithm). Quantum communication solves this fundamental problem with the help of the laws of physics. The application of the principles of quantum physics in a cryptographic protocol ensures that information in the process of communication between a sender and a receiver will not be stolen, changed or eavesdropped. If this kind of attempt happens, the whole process can be disrupted and terminated. In other words, Quantum Key Distribution (QKD) secures the information with the help of mathematics and the laws of physics at the same time. The risk of eavesdropping decreases dramatically in the quantum internet due to the entanglement principle, and a Man-in-the-Middle attack, or any other false substitution is unlikely to happen since qubits cannot be copied.

Generally speaking, there are presently two forms of quantum communication:

1. The use of QKD across nodes interconnected by traditional fibre,
2. QKD in a so-called "free space" (e.g. open air) on the ground or even between Earth and a satellite.

The United States, with its Los Alamos National Laboratory, has been one of the pioneers in the field of experimental QKD dating back to the beginning of 21st century. In the last years, the European Union with its funding initiative "Quantum Flagship" and active engagement of the European Space Agency have also been one of the leading actors in developing scientific fundaments for QKD infrastructure (ESA 2019). Nevertheless, currently it is China that leads globally in terms of developing and funding quantum commutation infrastructure on a large scale. In 2017, it inaugurated a quantum-secure communication line between the cities of Shanghai and Beijing (Xinhua 2007) using fibre-optic. The network works along the quantum key-distribution scheme in which both an emitter and a receiver share the same key to decode information supported by China's quantum-satellite Micius. Although the network cannot be fully considered a quantum internet network as its users still lack access to a quantum computer and the fact it is embedded in classical infrastructure, it provides a solution to the distance dilemma. As information is stored in quantum units (photons), the longer the distance, the highest the chances of losing the photon and, by extension, the information it contains. The 2,000-km line uses 32 nodes to approach photons and continue connection. Nevertheless, nodes convert the quantum key information into classical one and do not avoid potential eavesdropping (Courtland 2016).

The aforementioned example shows the important truth – every sophisticated technological solution, even quantum communication infrastructure, is not immune to a wide range of possible pitfalls. In short, unbreakable cryptography does not mean total security. Although real-real QKD systems can significantly raise the level of digital data security, they will never eliminate all the weak spots of communication systems that can range from numerous technological problems such as side channel attacks (Cai 2006) to an ordinary human-error.

THE END OF CYBERSPACE AS WE KNOW IT?

With the arrival of robust and usable quantum computers, cybersecurity we know today will become obsolete. Internet communication we use, apps we download, emails we exchange – all of that is protected by traditional methods using the RSA algorithm and elliptic curve cryptography The innate characteristic of these algorithms is their breakability — it is only a matter of time and the necessary computing power to do so. In the 1980s or 1990s, when these systems were developed and introduced, it was not a problem because of the technological limits of computing power available back then. Even now it is estimated that the breaking of the 2048-bit RSA algorithm with the use of a standard desktop computer will take 6.4 quadrillion years. But quantum technologies might turn the table.

In 1994, Peter Shor created his eponymous algorithm based on two specific computational problems – namely, integer factorization and discrete logarithm. His algorithm showed that certain computational problems could be solved more efficiently and exponentially faster using a quantum computer rather than an ordinary computer (Grumbling and Horowitz 2001). This striking discovery also evidenced that anyone with a real-world quantum computer could theoretically break most of the traditional and generally used cryptosystems.

Most recent developments in quantum computing indicate to have a significant impact on the security and privacy of people. From online communications to implanted medical devices, cryptography plays a very important role by ensuring that today's most secure communication systems remain unbreakable. However, the dynamic growth of the quantum computing industry has brought along significant threats to information protection systems (also known as cryptosystems), as shown in Table 2.

Table 2. Modern cryptosystems and their vulnerability to quantum algorithms

Cryptosystem	Impact	Comment
RSA	Broken	Shor algorithm describes an exponential speed-up for solving classically difficult number theory problems, such as factoring large prime numbers and solving discrete logarithms. The latest RSA version which has been broken was RSA-240 (795 bits), factored in November 2019.
Diffie-Hellman	Broken	-
Elliptical Curve	Broken	-
Code-based	Not yet broken	These cryptosystems were introduced in the late 1970s, and their security has been thoroughly studied. They are not known to be vulnerable to quantum computing advancements.
Hash-based	Not yet broken	-
Lattice-based	Not yet broken	These cryptosystems were introduced in the 1990s and are believed to be secure against quantum computing advancements.
Multivariate	Not yet broken	-
One-time pad (OTP)	Proven unbreakable	Claude Shannon proved the OTP to have perfect secrecy, meaning it is not vulnerable to advancements in quantum computing. Despite being immune to cryptanalysis, stringent keying requirements limits the OTP's implementation.

Source: (Mailloux, Lewis II, et al. 2016)

Any entity in possession of a large-scale quantum computer could jeopardize, in a blink of an eye, some of today's asymmetric cryptosystems, including global public key infrastructure which is a cornerstone of the Internet as we know it (Mailloux, Lewis II, et al. 2016).

This could not only impact modern communication systems by revealing encrypted secrets of countries, companies, and individuals, but also cripple critical infrastructure and financial systems worldwide. More specifically, a quantum computer could efficiently act with brute-force methods to disrupt each of the three cryptographic principles: confidentiality, integrity and authentication. This would mean that with a quantum computer, any third party could understand what is being sent, could modify the messages without being detected or even impersonate one of the communicating parties (O'Connor, et al. 2018, 8). With such potential, a quantum computer could break some security protocols and cryptographic algorithms that are vulnerable to quantum cryptanalysis attacks, severely affecting the handling of message formatting, key management and a plethora of other areas (ETSI White Paper No. 8. 2015, 9).

Although the aforementioned attacks are yet to become practical, institutions worldwide are already working on post-quantum cryptographic standards in order to avoid the materialization of the described catastrophic scenarios. The National Institute of Standards and Technology (NIST), European Telecommunications Standards Institute (ETSI) as well as the International Telecommunication Union are some of the leading organizations in that matter. Having a long-standing history in open cryptographic standards, NIST has been monitoring advancements in quantum computing and working to improve the current cryptography standards by identifying new quantum-resistant algorithms (see Annex 1) which not only remain resistant to all the known methods of classical attacks, but also to new quantum attacks (O'Connor, et al. 2018). However, the transition to quantum-resistant cryptography is likely to take years since most post-quantum algorithms require significantly larger key sizes than the existing public key algorithms. For instance, the call of an increased RSA key size from 1024- to 2048-bit took four years to implement. Although these 2048-bit keys are sufficient until roughly the year 2030, the need for new quantum-resistant algorithms will continue (Faux, 2018).

POST-QUANTUM INTERNATIONAL SECURITY

Although cryptography is currently the most discussed topic when it comes to security implications of quantum technologies, quantum-enhanced computation as well as quantum infrastructure will transform cybersecurity, national security and the international landscape well beyond cryptosystems. In the next decade, we will witness the emergence of Post-Quantum International Security. The main characteristics of this paradigm will include:

- *Few vs many* – the split between two categories of actors in global cyberspace: those few possessing quantum machines and infrastructure versus many others solely equipped with traditional ICT resources.
- *Evolution of the Internet* – segmentation and gradual change from the trust-based open public network to a platform operating separate secure channels in an unsecure environment.
- *Fulfilment of the digital data value chain* – thanks to the advancement of quantum computing as well as machine learning, Internet of Things (IoT) and 5/6G, the global digital data value chain is slowly becoming a reality. This will trigger direct and indirect economic and political implications.

Few vs many

By adding the temporality layer to post-quantum era, we can distinguish between the initial quantum phase and the widespread quantum momentum. The initial stage presumes that the first quantum computer has been successfully built and that some early adopters have acquired that technology. At the same time, only a few countries have been able to build and maintain operational quantum communication infrastructure on the ground and with the use of space components. Since the development and operational usage of quantum technologies require a vast amount of resources, it is very likely that they will be built into an ecosystem combining public-private cooperation, thus reducing the number of actors to publicly sponsored industries. Taking into account the need for the wide fundamental research and huge high-risk investments, state support does not always have to take the form of direct funding, like for example in China. Yet, in the long run, the state and state-backed technological corporations will play a crucial role. Therefore, the initial stage of robust quantum computer implementation and development of scalable QKD infrastructure will create a global oligopoly – a few big actors (corporate and state) being the only stakeholders capable of possessing and operating these technologies. Of course, the ownership and management of robust quantum computers should not be equalled to the exclusive ability to use them. In times of cloud computing, quantum-services are already appearing on the commercial market. This, however, is not changing the fact that the owner of a robust quantum computing machine will ultimately decide what will be available commercially, for whom, and on what kind of terms.

This situation, especially in the context of quantum machines, will somehow mirror the history of traditional computers. Mark I or ENIAC, machines developed through the 1940s and 1950s of the 20th century by and for the United States Military, were primarily used to support calculations needed to set ballistic weapons trajectories, or speed up research in the Manhattan Project. The crucial difference here is that first computers operated in their closed ecosystems. In contrast, quantum machines have the ability to not only be connected via quantum infrastructure, but also to exchange information with the traditional cyberspace, such as the Internet we use on our traditional computers. The situation in which a quantum-backed system operates on one side and our laptop on the other, creates a huge disparity with serious security implications.

Evolution of the Internet

The fundamental principle of the currently known Internet allows us to establish a remote, trusted connection between a sender and a receiver by using public, global in reach infrastructure independent from its users. Enabled by the Public Key Infrastructure (PKI) and cryptography hidden in the numerous parts of the data transmission process such as HTTPS, SSL, TLS and others, the Internet allows us to send messages, download applications and do online banking. What if we were not able to trust certificates and cryptography we currently use for the needs of PKI anymore? How would we verify the identity of the receiver, sender or creator of the data in case quantum computers should be able to break every RSA/ elliptic curve cryptography we are using for the needs of the current Internet?

An obvious solution would be a mass application of quantum-resistant algorithms, such as those searched by NIST (see Annex 1). But as already mentioned, taking into account both technological as well as organizational obstacles (PKI has hardly changed since its origin in 1970s), this will take time. In the meantime, we will witness the division of the World Wide Web, or to be more precise – "the heterogenization of the Internet". Secure but limited in range and accessibility, "quantum internet" (infrastructure based solely or partly on transporting qubits) will exist next to and work simultaneously with the traditional Internet infrastructure which is already flawed with a lower level of security and the diminished trust of its users. This lower level of security will be patched *ad hoc* by applying other solutions such as blockchain-based systems or variations of the one-time pad technique. In short, we will observe increasing segmentation and gradual change of the Internet from the trust-based open public network to a platform operating separate secure channels in a still usable but unsecure environment.

Fulfilment of the digital data value chain and its geopolitical implications

In the past, nations and tribes traditionally waged wars to take over lands, people, trade routes, natural minerals and fossil fuels such as coal or oil. They did so because those resources allowed nations to develop, prosper and, in the long run, rule, if not militarily, then economically by taking a higher place in the regional or the global value chain and division of labour.

In 2017, for the first time in history, the value of the biggest oil companies was lower than that of technological giants. We are witnessing a major shift which is spurred by the introduction of the global digital data value chain and all geopolitical changes that are accompanying that. Digital data is now the most prospective resource: who owns data – rules.

All of that is possible thanks to the unprecedented development of ICT, including not only traditional and cloud computing, but also machine learning (AI) and other key elements such as 5/6G networks. Quantum technologies are one of the key pieces of the puzzle which will speed up this process in the coming years. But make no mistake, it is not about technology – it is all about data. Just like it was not the trade routes themselves that made nations rich and powerful, but the trade itself which was possible thanks to them.

Fulfilling the digital data value chain will not only solidify and confirm the post-Westphalian international system, but it will also grant a new status for the global technological giants. Similarly to the Dutch East India Company or the British East India Company who monopolized global sea trade routes in the 17th and 18th century, tech companies are entering the international relations arena with their distinctive status and complicated relations, both with their home countries as well as their biggest markets.

WHEN PHYSICS RESHAPES INTERNATIONAL RELATIONS

One more time, like in the case of nuclear weapons, physics is rapidly reshaping the international security arena. The key differences between nuclear technologies and quantum mechanics are that the latter, apart from obvious offensive implications, creates also advanced defensive capabilities.

As described in this article, when it comes to #QuantumOffence, robust quantum computers will be able to not only compromise traditional cryptosystems, but also to carry out more nuanced and novel cyberattacks. This new offensive use of quantum mechanics for ICT might be aimed at both hardware components of the cyberspace, for example through side channel attacks, as well as the software layer, for example with the use of quantum multiplied attacks (Wallden and Kashefi 2019). Simultaneously, international actors who are building #QuantumDefence and operating quantum-based communication networks will secure their own information exchange with the help of such solutions as Quantum Key Distribution. All of that thanks to the quantum physics principles, and billions of dollars invested worldwide in quantum technologies in the coming years.

BIBLIOGRAPHY

National Institute of Standards and Technology - NIST. 2016. April. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

Cai, Qingyu. 2006. "Eavesdropping on the two-way quantum communication protocols with invisible photons." *Physics Letters A*, February: 23-25.

Courtland, Rachel. 2016. "China's 2,000-km quantum link is almost complete." *IEEE Spectrum* 53 (11): 11-12.

ESA. 2019. *European quantum communications network takes shape*. https://www.esa.int/Applications/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape.

E-Spin Corporation. 2018. *The advantages and disadvantage of Quantum Computing*. https://www.e-spincorp.com/the-advantages-and-disadvantage-of-quantum-computing/.

ETSI White Paper No.8. 2015. *Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenge.* Sophia Antipolis: European Telecommunications Standards Institute - ETSI.

Faux, Roberta. 2018. "The State of Post-Quantum Cryptography." *Cloud Security Alliance* 6-8.

Fowler, Austin G., Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. 2012. "Surface codes: Towards practical large-scale quantum computation." *Physical Review D.*

Gidney, Craig, and Martin Ekerå. 2019. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits." *arXiv*. https://arxiv.org/abs/1905.09749.

Google AI. 2018. *A Preview of Bristlecone, Google's New Quantum Processor.* 5 marzo. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

Grumbling, Emily, and Mark Horowitz. 2001. *Quantum Computing: Progress and Prospects.* Washington, D.C: The National Academies Press.

Harris, Mark. 2018. *MIT Technology Review.* November 5. https://www.technologyreview.com/s/612381/google-has-enlisted-nasa-to-help-it-prove-quantum-supremacy-within-months/.

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

Herman, Arthur, and Idalia Friedson. 2018. *Quantum Computing: How to Address the National Security Risk.* Washington, D.C: Hudson Institute.

IBM. n.d. *IBM Q.* https://www.research.ibm.com/ibm-q/learn/what-is-ibm-q/.

Kuhn, Thomas S. 1971. "The Relations between History and History of Science." *Daedalus* (The MIT Press) 100 (2): 271-304.

Mailloux, Logan O., Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila. 2016. "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals." *IT Professional*, September-October: 42-47.

Mailloux, Logan O., Charlton D. Lewis II, Casey Riggs, and Michael R. Grimaila. 2016. *Post-Quantum Cryptography: What Advancements in Quantum Computing mean for IT Professionals.* Washington, D.C.: IEEE Computer Society.

Markets and Markets. 2019. *Quantum Computing Market worth $283 million by 2024.* https://www.marketsandmarkets.com/PressReleases/quantum-computing.asp.

Ministry of Science and Technology. 2017. "Quantum Control and Quantum Information Key Special Project 2017 Program Application Guidance." www.gov.cn/xinw-en/2016-10/11/5117251/files/9466f710b972426386489511b 7f727f9.pdf.

Mosca, Michele. 2016. "A Quantum of Prevention for our Cybersecurity." *Global Risk Institute.* https://globalriskinstitute.org/research/cyber-security-fraud/.

O'Connor, Lisa, Carl Dukatz, Louis DiValentin, and Nahid Farhady. 2018. *Cryptography in a Post-Quantum World: Preparing intelligent enterprises now for a secure future.* Accenture.

2018. *Quantum Computing Report.* https://quantumcomputingreport.com/our-take/how-to-explain-quantum-to-your-classical-friends/leveraging-the-quantum-mechanical-principles-of-superposition-and-entanglement/.

QuTech. 2019. *Quantum Internet.* Delft: Technological University of Delft. https://issuu.com/tudelft-mediasolutions/docs/quantum_magazine_june_2019.

US Congress. 2018. "National Quantum Initiative Act." Washington DC, District of Columbia, 3 enero. https://www.congress.gov/115/bills/hr6227/BILLS-115hr6227enr.pdf.

Wallden, Petros, and Elham Kashefi. 2019. "Cyber Security in the Quantum Era." *Communications of the ACM*, April.

Xinhua. 2007. "China opens 2,000-km quantum communication line." http://www.xinhuanet.com//english/2017-09/30/c_136649826.htm.

Annex 1

Main companies developing quantum solutions in the field of computation

Country	Company	Technology
Canada	1QBit	Hardware
	D-Wave	Metrics & simulation
	Quantum Benchmark	Hardware
	Xanadu	Quantum Computer
United States	AT&T	Quantum Internet
	Atom Computing	Quantum Computer
	Google	Processors & algorithms
	HP	Hardware
	Honeywell	Information & simulation
	Intel	Quantum computing
	MagiQ	Post-quantum cryptography
	Microsoft	Quantum communications
	QC Ware	Cloud solutions
	IBM	Quantum computer
	QxBranch	Software
China	Alibaba	Hardware
	Baidu	Quantum AI
	Huawei	Cloud & simulation
United Kingdom	Oxford Quantum Circuits	Hardware
European Union	Airbus	Metrics & communications
	Atos	Quantum AI
	InfiniQuant	Communications
	QuTech	Quantum Internet
	QNTM	Simulation
Japan	Fujitsu	Quantum computer
	Hitachi	Quantum computer
	RIKEN	Theory
	Toshiba	Post-quantum cryptography
Switzerland	ID Quantique	Post-quantum cryptography
	R QUANTECH	Algorithms

Annex 2

NIST finalist second round post-quantum algorithms

NIST Candidate post-quantum cryptography algorithms (January 2019)	
Name	**Type**
CRYSTALS-KYBER	Lattice-based cryptography
FrodoKEM	Lattice-based cryptography
LAC	Lattice-based cryptography
NewHope	Lattice-based cryptography
NTRU	Lattice-based cryptography
NTRU Prime	Lattice-based cryptography
Round5	Lattice-based cryptography
SABER	Lattice-based cryptography
ThreeBears	Lattice-based cryptography
Classic McEliece	Code-based cryptography
NTS-KEM	Code-based cryptography
BIKE	Code-based cryptography
HQC	Code-based cryptography
LEDAcrypt	Code-based cryptography
Rollo	Lattice-based cryptography
RQC	Lattice-based cryptography
SIKE	Supersingular elliptic curve isogeny cryptography
CRYSTALS-DILITHIUM	Lattice-based cryptography
FALCON	Lattice-based cryptography
qTesla	Lattice-based cryptography
GeMSS	Multivariate cryptography
LUOV	Multivariate cryptography
MQDSS	Multivariate cryptography
Rainbow	Multivariate cryptography
Picnic	Hash-based cryptography
SPHINCS+	Hash-based cryptography

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.
The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.
The Kosciuszko Institute organizes the European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.
More on the European Cybersecurity Forum: http://cybersecforum.eu/
More on the European Cybersecurity Journal: https://cybersecforum.eu/en/about-ecj/.
Office: Wilhelma Feldmana 4/9-10, 31-130 Kraków, Polska, tel.: +48 12 632 97 24,
www.ik.org.pl, e-mail: instytut@ik.org.pl