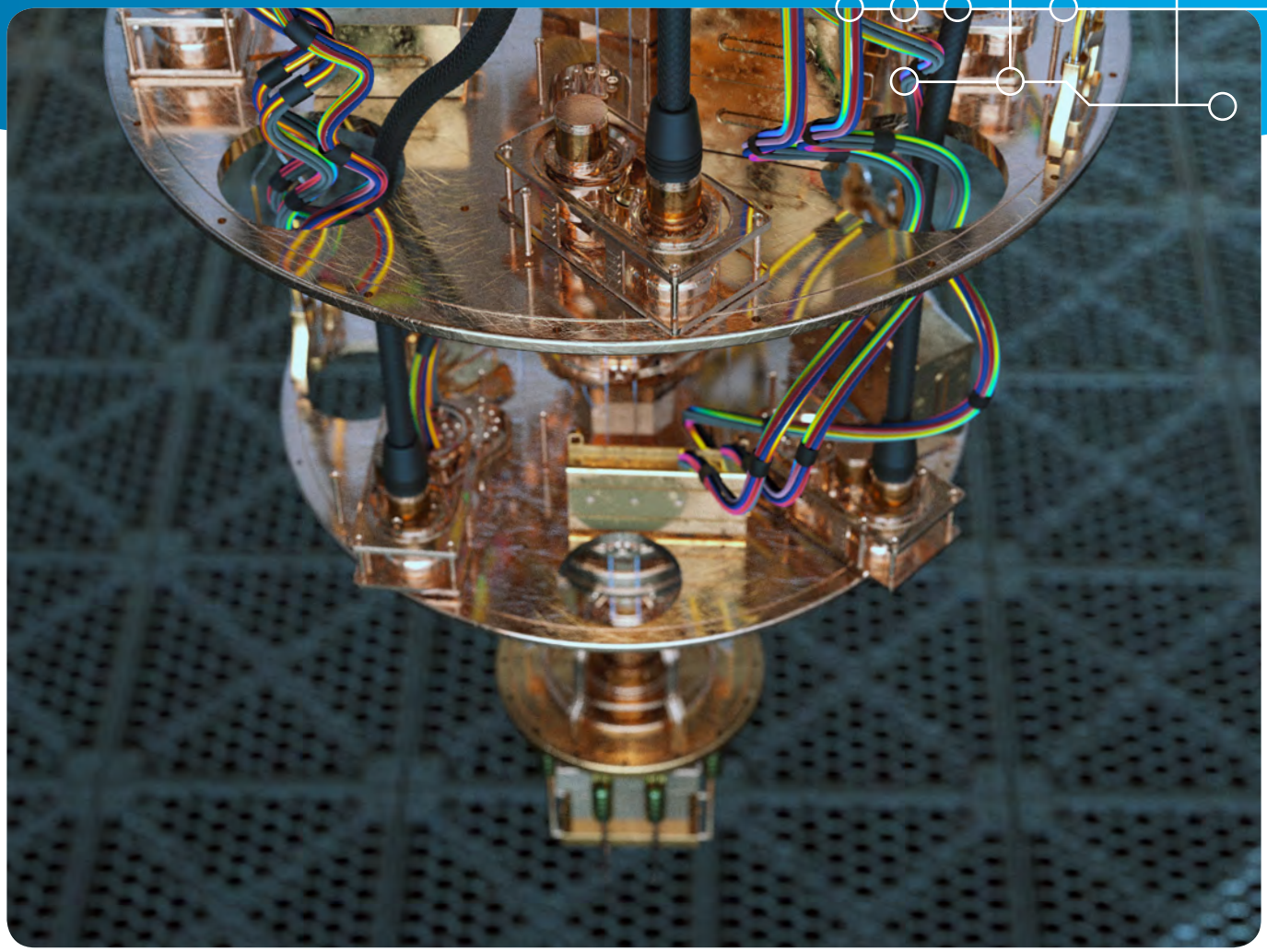
Understanding the Strategic and Technical Significance of Technology for Security

Implications of Quantum Computing within the Cybersecurity Domain



HSD
The Hague Security Delta

Understanding the Strategic and Technical Significance of Technology for Security

Implications of Quantum Computing within the Cybersecurity Domain

The Hague **Security Delta**

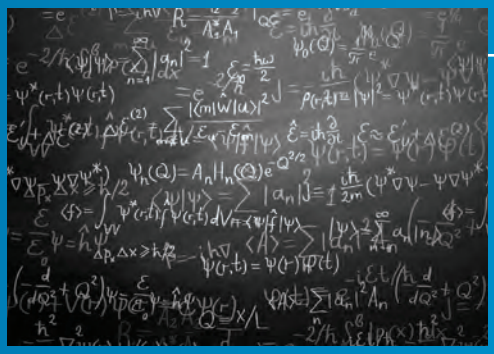


Table of Contents

1 – Introduction: Technology and Cybersecurity

Our society is undergoing a digital transformation. The characteristics of this transformation are determined by the convergence of technologies and social activities that blur the boundaries between physical, digital and biological systems. Moreover, the speed of this transformation is dizzying. Developments such as 'big data', 'cyber crime', 'blockchain', 'autonomous systems', artificial intelligence (AI), and 'smart cities and societies' will soon be replaced by another pantheon of terms and themes.

These technological breakthroughs result in major societal, social and economic changes, leading to considerable challenges, not in the least related to security, such as:

- How do we establish safe and secure access to and use of the Internet?
- How do we prevent the loss of legitimacy and integrity of digital activities?
- How do we stimulate the use of accountable and explainable algorithms?
- How do we define and protect privacy of citizens?
- How do we balance individual, societal, economic and ethical interests?

In 2018, the Dutch government presented a new innovation policy framework which focuses on achieving mission-oriented innovation to provide answers to these challenges and make use of the opportunities.[1]

The policy is based on setting up collaboration, already initiated within the Top Sectors[2], in four central themes:

- energy transition and sustainability;
- health care;
- agriculture, food, and climate; and
- security.

Innovations in these fields require dedicated investments that need to translate into applicable technological breakthroughs. Thus, the Dutch Cabinet intends to heavily invest in development of key technologies such as photonics, artificial intelligence, and nano-, quantum and biotechnology. All in all, societal and economic possibilities for the security domain seem ample.

Still, recent publications (Cybersecurity Beeld Nederland 2018 [CSBN2018],[3] the third National Cybersecurity Research Agenda [NCSRA III])[4] and discussions in existing environments (e.g., HSD) show that insufficient use is made of these opportunities, often as a result of lack of awareness, and that security concerns – one of the main themes of the Dutch Cabinet – are not a top priority.

1 Kamerbrief over innovatie beleid en bevordering van innovatie: naar missiegedreven innovatiebeleid met impact, Parliamentary brief on innovation policy and innovation incentives, 13 July 2018

2 In February 2011, the Dutch government announced the Top Sectors approach, a form of industrial policy which focuses public resources on specific sectors and promotes coordination of activities in these areas by businesses, government and knowledge institutes. The nine sectors chosen are: horticulture and propagation materials, agri-food, water, life sciences and health, chemicals, high tech, energy, logistics, creative industries. See: "OECD Reviews of Innovation Policy: Netherlands."

3 NCTV, Cybersecuritybeeld Nederland, Cyber Security Assessment Netherlands 2018.

4 dcypher, National Cybersecurity Research Agenda, July 2018

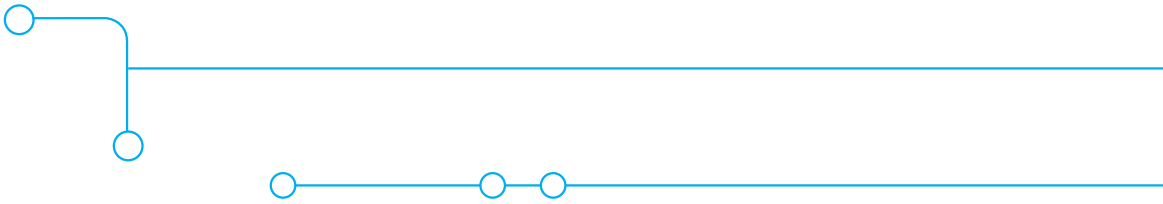

TouchNTuff

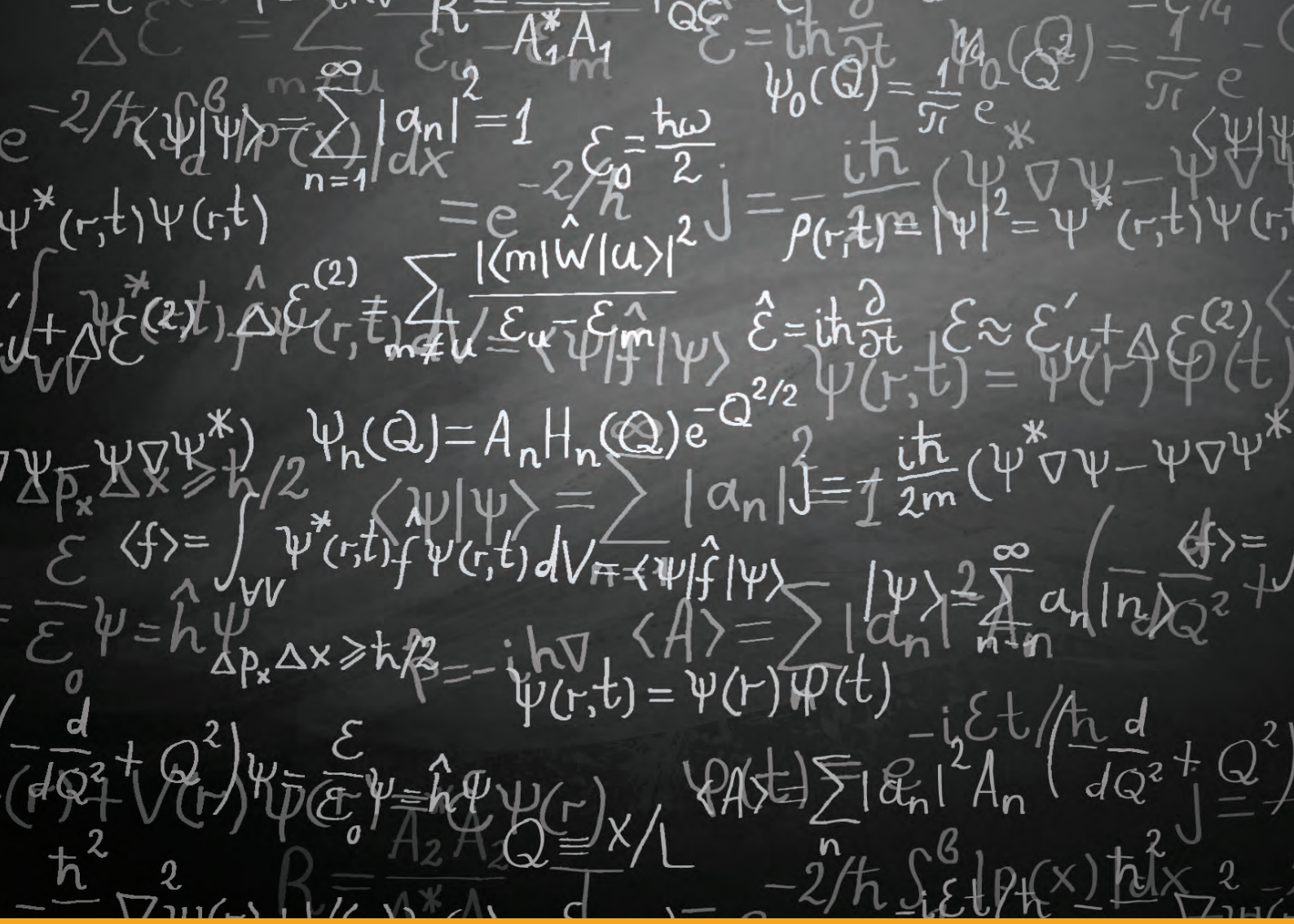
Members within the HSD community have requested to raise attention to a number of these developments that could intrinsically improve the cybersecurity landscape, in the short or longer term:

1 the short-term potential of specific data diode technology.
2 unsupervised learning within the domain of artificial intelligence on the mid- to long-term.
3 the longer-term potential of quantum technology.

This paper addresses the third topic and provides an overview of current developments and expectations in this broad field, while keeping with the following overarching question in mind: **what is the effect of the further developments of quantum computing on current levels of security and within what time frame are they likely to occur?** In addition, this research examines ways to anticipate these effects and to further opportunities in the quantum computing domain.

We conducted our analysis primarily on the basis of existing literature (such as policy documents, academic articles, consultancy reports, statistical data). Having identified our knowledge gaps, desk research was supplemented by a limited number of interviews with relevant stakeholders in the Netherlands. The interviews contribute towards a better understanding of policy, economic, and scientific developments related to quantum computing, encryption as well as existing partnerships and collaborative initiatives. For the interview questionnaire and the list of interviewed people, see **Annex 2**.





2 – The Concept of 'Quantum'

In the opening years of the 20th century, there was a consensus among scientists that physics was complete, that: *"There is nothing new to be discovered in physics, all that remains is more and more precise measurements."*[5] There were only some minor issues, quirks of physics, and scientific loose ends to be tied together; yet one of those loose threads ended up breaking a century's worth of physics, giving birth to the fundamentally new concept of quantum mechanics.

Since its introduction, quantum mechanics has directed physics down a scientific path that led to nuclear weapons, semiconductors, and lasers. Where the 20th century was defined by the advent of computer bit, the future of computing may lie in the quantum bit, or qubit. Quantum computers are widely seen as a potential breakthrough technology, especially when employed in disciplines like artificial intelligence, cryptography, and big data analytics. Yet, with the undeniable promise of quantum computing come vast amounts of hype and confusion, ranging from what a quantum computer precisely entails, to when one can expect a quantum computer, to what sort of applications it might offer.

2.1 Quantum Terminology

Quantum mechanics by its nature is a topic that is complex and confusing, with a wide variety of terminology that is relevant and often used interchangeably. As such, a concise set of definitions is required to ensure consistency, create a basic understanding of some of the quantum phenomena, and provide the context for discussing quantum computing.

While these phenomena obviously guide most of the technological development that is taking place, the focus of this paper will not be on providing a deep understanding of the technical underpinnings of quantum technology. However, given that they are a great part of the discussion, we have listed the three main concepts below.

Key Quantum Concepts

Quantum computing involves making active use of quantum effects, which often challenge traditional conceptions on how the physical world works. Here, we mention two properties of particles that create the quantum effects, superposition and entanglement.[6]

Superposition: A particle can exist in a combination of different states at once. For example, it can behave as if it is spinning both clockwise and counterclockwise at the same time. Once it is measured or interacts with its environment, it settles into a single state, probabilistically adopting either a clockwise or counterclockwise spin.

Entanglement: Two (or more) particles can become intrinsically related, or entangled, so that they can no longer be described as separate entities. This means that a measurement made on one particle will determine the outcome of a similar measurement made on the other particle, even over great distances.

Qubits: Conventional computers store data in 'bits' that can exist in only one of two states (0 or 1); different combinations of 0s and 1s are used to represent letters and numbers. A quantum computer would store data in 'qubits', which, due to quantum superposition, could be both 0 and 1 at once up to the moment they are observed. Quantum computers will need multiple qubits to operate.[7]

A qubit is the unit of quantum information. The more (stable) qubits there are, the more powerful quantum computing will become. This number of stable qubits is currently the center of attention in the debate about the feasibility of quantum computing. Scientists consider the

5 This quote is often misattributed to Lord Kelvin. It most likely is a paraphrasing of a speech made by Nobel Prize winner Albert A. Michelson in 1894.

6 There are more properties that are relevant such as interference. As we will not refer to these in later sections, we have chosen to not elaborate on them here.

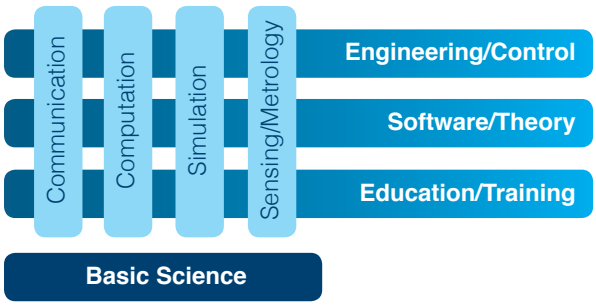
7 The current state of the art on quantum computers is 72 qubits, with roadmaps on scalability that put the number of qubits in the range of several hundreds.

possibility of storing and verifying information in at least 50 stable and error-free qubits as an significant landmark. A collection of qubits makes up a quantum computer, which is physical hardware that makes use of quantum effects in its computations.[8] Within quantum computing there is a distinction between a *narrow quantum computer* and a *universal quantum computer*. The latter is a computer that is, in principle, capable of performing any calculation, given enough time and memory. Current generation quantum computers are all narrow quantum computers, meaning they are able to solve only a specific set of computations.

2.2 Emerging Quantum Scientific Fields

Quantum mechanics has driven scientific development in many fields. As with other R&D domains, it can be delineated in more than one way. The domain of quantum information science is a field that encompasses many different research disciplines and traditions.

The final report of the High-Level Steering Committee on the European QT Flagship Initiative sketched the research field of quantum technologies as follows:



The larger set of research known as quantum information science operates on the intersection between quantum mechanics and information theory, which includes quantum computing, quantum communications, and more.

Quantum Communications: The generation and use of quantum states and resources for communication protocols. Its main applications are in provably secure communication, long-term secure storage, cloud computing, and other cryptography-related tasks, as well as a secure 'quantum web'. Quantum Cryptography is the related field of research dedicated towards exploiting quantum mechanical properties to perform cryptographic tasks.

Quantum Computation: The active use of quantum effects to solve a computational problem.

Quantum Simulation: The use of simple models of quantum hardware and systems to understand more complex systems.

Quantum Metrology/Sensing/Imaging: Quantum systems whose extreme sensitivity to environmental disturbances can be exploited in order to measure important physical properties with more precision than is possible with classical technologies.

Basic Science: The examination of quantum related foundational scientific problems, the investigation of alternative yet unproven approaches, and the furthering of the basic understanding of quantum technologies.

Engineering/Control: The engineering element of constructing a quantum computer that is practical and affordable in its application.

Software/Theory: The research field dedicated towards the utilization of quantum chips that would require drastically different software and algorithms.

Education/Training: The raising of awareness among and improving skills and expertise of potential future stakeholders, decisionmakers, and educators, as well as preparation for outreach to the general public.

8 This is the strict interpretation of a quantum computer, in which the computational device makes use of qubits. Other devices, such as D-Wave, have also been called quantum computers, although this definition is contested.

2.3 The Potential of Quantum Technology

2.3.1 Quantum Supremacy

The promise that quantum computing offers can be summarized into a single concept: quantum supremacy. Simply put, this refers to the ability of quantum computers to outperform classical computers.

This can be either because quantum computers are *able to perform the task in a much faster and more efficient way* than classical computers ever could, or because the quantum computer is *able to compute a task that is not possible on currently available classical platforms*. An example of the latter is quantum simulation that would allow for a more accurate understanding of the intricacies of protein folding, paving the way for more efficient pharmaceutical research. In the case of the former, it might be through applications such as unstructured search, where classical computers would have to sift through entries one by one, while quantum computers may process all search results simultaneously. While several organizations have been working to demonstrate quantum supremacy (see also next section), this milestone has not yet been reached.

While the potential of quantum computers has already been demonstrated in the context of specific areas, the use case for a universal quantum computer is less clear. Universal computers are computational devices that are able to solve any computational problem – current digital computers are examples of universal computers. However, universal computers are not by definition able to solve any problem in a practical timescale, such as prime number factorization. Quantum computers are not considered to be a replacement of classical computers.

A common misconception about quantum computers is that they are simply super-powered conventional computers. However, quantum computers are only applicable in a very specific class of problems, and even within that class only limited applications exist where quantum computers offer significant benefits.[9]

Generally, quantum computers excel in problems where there are many different solutions that need to be tested. Quantum computers can test the validity of each solution simultaneously, whereas a traditional computer would have to test each solution one by one.

As is the case in many young fields of research and development, the expected possibilities of quantum technologies, and quantum computing specifically, range from none to all and from now to never. An often-heard example is improving the efficiency of producing fertilizer, which could generate enormous cost savings and decrease greenhouse gas emissions. There are three broad dimensions along which the utility of any quantum technology may be evaluated, as described below.

Dimension	Description	Current state
Functionality	Any quantum computer developed should be able to perform a wide variety of tasks, meaning it must move beyond niche applications and towards a universal computing platform.	Limited applicability of quantum computing beyond very specific problems. While a universal quantum computer is possible, it would require significant advances in scientific and engineering expertise.
Range	The distance across which quantum communication is possible should be extended, and should in principle be scalable to arbitrary ranges.	Quantum communication for terrestrial application is currently limited (~100 km). Space-based applications have significantly greater range (~2000 km), but come with prohibitively high costs.
Accessibility	The use of any quantum device or service should be practical and cost-efficient, and be accessible to multiple users without significant additional cost.	Quantum computers cost anywhere from $1–10 billion[10] and require highly specialized infrastructure.

Table 1 **Dimensions of the utility of quantum technology**

9 Observation substantiated by expert interviews conducted within the scope of this study.

10 We use billion here to mean a thousand million (1.000.000.000)

2.3.2 Barriers

Some experts consider quantum computing impossible, at least based on the current understanding of quantum mechanics.[11] Some warn for a complete overhaul of current society similar to what IT did in the 20th century. Whatever the final verdict is, efforts towards answering the outstanding questions on the technical and practical feasibility of quantum computers is ongoing. There is, however, no guarantee that a universal quantum computer is practically possible, even though large amounts of funding and research are directed towards overcoming already identified barriers.

Some of the most significant technical barriers and drawbacks are:

Decoherence: Qubits are only able to perform calculations as long as they maintain their quantum-like behavior. Decoherence is the phenomenon whereby qubits degenerate into regular particles, losing their ability to perform quantum calculations. The technical challenge is to extend the longevity of qubits, with a longer *decoherence time* meaning more computational time. This problem pertains to the functionality aspect of quantum computing.

Quantum algorithms: The number of quantum-fit algorithms (a step-by-step procedure for solving a problem on a quantum computer) is still very limited. This obviously limits the usability of quantum computing at the moment. There is a widespread misconception that quantum supremacy can be assumed within a field once a universal quantum computer is developed. However, fields like machine learning will require significant efforts to ensure that current algorithms are able to utilize quantum computing devices. As such, research fields like quantum machine learning are, as of yet, fields of theoretical research rather than of practical implementation. This problem also pertains primarily to the functionality aspect of quantum computing.

Engineering environment: The temperature constraints for quantum computing, requiring near absolute zero temperatures, which are exceedingly difficult, expensive, and impractical to reach and maintain. Another aspect is the cost of various components for quantum infrastructures, with the current range for terrestrial quantum communication networks being limited to 100 km. While some of these problems may be overcome through solutions like space-based quantum networks, these typically come at prohibitively high cost and with other significant drawbacks. This problem relates to both the range and accessibility components of quantum computing.

Lack of standardization: Quantum computers are currently not standardized, with organizations like the National Institute of Standards and Technology (NIST) leading the way on such efforts. Current estimations on the timeframe for the development of quantum computing hardware generally converge on 1–5 years, with the likely price tag floating around US$1–10 billion.[12] This issue centers primarily around the accessibility aspect of quantum computing.

2.4 Timescale

Due to the significant barriers, major breakthroughs in quantum computing technology come very slowly and take considerable investment in terms of time, money, and human resources. Reaching quantum supremacy will be an important milestone in demonstrating the viability of quantum computers, and estimations are that this will happen in a matter of years.[13] For more universal applications this timeframe is considerably longer. Achieving the ultimate breakthrough that leads to a universal quantum computer will be the slowest of all, and some experts say that it may not happen before 2030, if at all.

The development of quantum computers may be divided into three categories:[14]

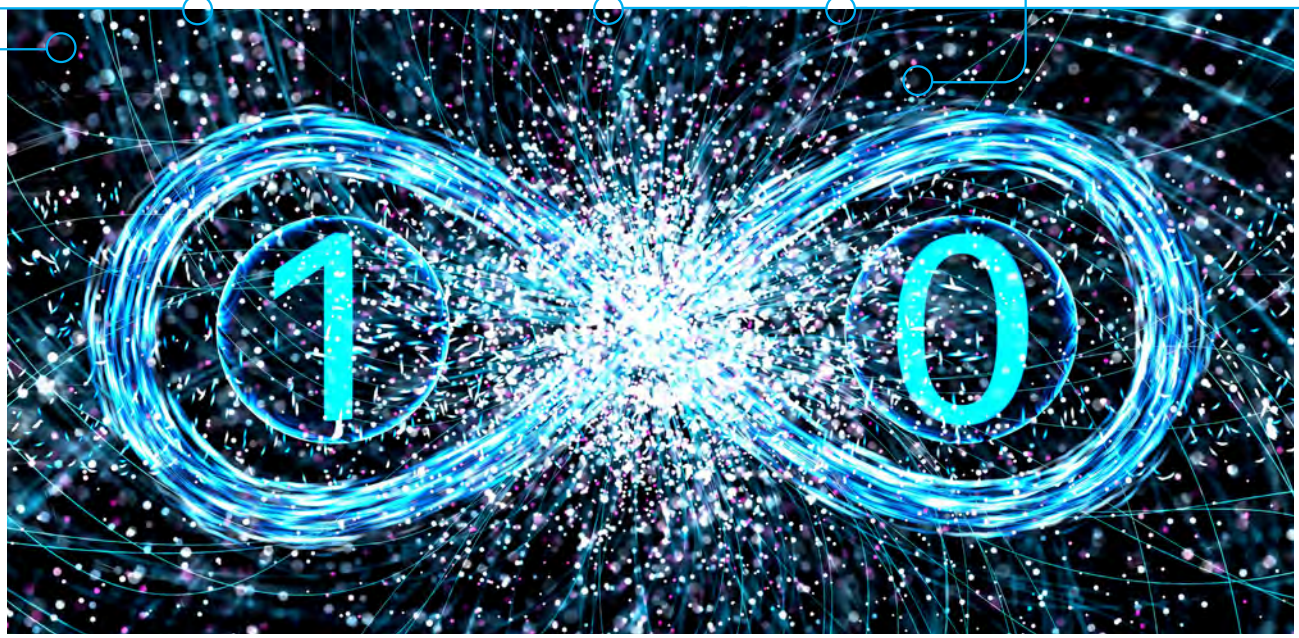
First generation quantum computers: Application of quantum computers will be largely within specific non-commercial applications of low to medium complexity. This period would be characterized by significant upfront costs that are primarily dedicated to proof of concept type research. Limited-scope quantum decryption would start being feasible, but only to those actors that possess the necessary quantum hardware.

11 See for instance, Gil Kalai, one of the prominent skeptics: https://www.quantamagazine.org/gil-kalais-argument-against-quantum-computers-20180207/

12 National Institute for Science and Technology (NIST), Post-Quantum Cryptography, 2016, p.2

13 Mosca, 2015, Cybersecurity in a Quantum World, p. 24

14 Based on a compilation of various sources, such as research done by the Boston Consulting Group; E. Grumbling and M. Horowitz (eds), Quantum Computing, Prospects and progress, National Academies Press, Washington, DC, 2018; expert interviews conducted within the scope of this study.



Second generation quantum computers: Having solved many of the fundamental engineering problems underlying quantum computers, this phase would be oriented towards the first commercial applications, with research directed towards improving scalability of quantum solutions. The renting out of quantum computing power, much like the super computer business case, would start being feasible.

Third generation quantum computers: The development of universal quantum computers will render quantum supremacy feasible across a wide variety of (non-)commercial applications. Research will largely be directed towards implementing quantum applications, which at this point will significantly outperform classical computing in various areas. In addition, the greater accessibility of quantum computers will allow for the rapid development of novel applications. Quantum computing startups are likely to be feasible at this point, as the costs of quantum hardware will have come down significantly.

Timescale[15]	Achievement	Significance	Generation
2018 – 2020	Academic application of quantum computing	The use of quantum computers on some narrowly defined problem with little commercial significance. This would be a technical achievement that could pave the way for further investment.	First generation
2020	Physical limitations on microprocessors herald the end of Moore's Law	More research dedicated towards increasing performance out of current existing hardware. However, long-term scalability of chips can no longer be assumed for classical computing.	First generation
2020	European–Asian quantum-encrypted network	China aims to complete its QUESS Micius satellite program by 2020, creating a quantum-encrypted connection between Europe and Asia.	Second generation
2023	Narrow commercial application	Possibility for large corporations to make use of quantum computers in narrowly defined problems.	Second generation
2030	Global quantum-encrypted network	China aims to expand its quantum-encrypted network to cover the entire globe	Third generation
2030+	Broad commercial application	Quantum solutions become feasible and confer significant commercial competitive advantage towards adopters	Third generation

Table 2 **Predicted development of quantum computers**

15 See footnote 13

3 – Actor Landscape

Across the globe, there is a diverse set of players active in the field of quantum computing and quantum encryption. While academic research, as presented in the introduction of this paper, goes back to the beginning of the 20th century, more recent advances in understanding quantum effects have led to the field of Quantum 2.0 (also known as the second quantum revolution), resulting in the development of hard and soft quantum technologies at various levels of maturity.

Increasingly, the business sector has become involved, funding the development and aiming to deliver the technology to the scale needed for economies. Some estimates for the quantum computing market place its value at $2 billion by 2035 and in excess of $260 billion by 2050.[16] Various collaborative efforts have been set up that cross between government, academia and business: US based businesses Microsoft and Intel that collaborate with Delft University of Technology; the Chinese Academy and Sciences – Alibaba consortium establishing an algorithm-focused lab in Bellevue, Washington, the US National Lab Los Alamos collaborating with the University of New South Wales and University of Maryland, and so on.

The position of quantum computing has been raised on the policy agenda in a number of countries, notably China, member states of the EU, and the United States. Each player has its own set of domestic concerns driving development, as well as varying levels of ambition, technological capacity and funding. In the following section, we highlight the policy, corporate, and research developments in the US, China, and in Europe.

3.1 Major Quantum Computing and Communications Actors

The table on the next page provides a summary of the most prominent plans, programs, and organizations currently related to quantum science and technology.

While efforts are being made towards quantum computing across the world, there are differences between the largest regional players on the world stage, specifically between the United States, China and European Union. In the following sections, we will focus on policy, commercial, and research developments in each of these regions.

3.2 United States

The United States has long been a leader in quantum information technology, especially concerning the hardware dimension of quantum computing. Its tech giants have powerful portfolios and are investing heavily in quantum developments across the globe. At the same time, policymakers feel that R&D levels are unstable and fragmented and that the strategic dimension of quantum technology has been underemphasized in the past.

3.2.1 US Policy

The role of US government agencies has been relatively limited, although it is difficult to assess what happens in the classified research domain. In September 2018, the US Congress introduced the U.S. National Quantum Initiative Act, which, once it is formally accepted, will allocate $1.275 billion towards quantum information science over the next 10 years. This will be directed to support the United States' leadership in the research and development of quantum science and technology.

The two overarching aims of these bills is to strengthen the country's quantum science research capabilities and workforce, as well as improve Federal planning and coordination of quantum science as it is used by the government. In addition, more initiatives are being drafted that put additional importance on the development of quantum R&D in the US. Agencies like NASA make use of Canadian D-wave computing devices, which significantly deviate from the universal computer type chips that corporate parties are pursuing.[17]Organizations like DARPA and the National Science Foundation (NSF) have allocated relatively modest amounts of funding, specifically into secure quantum communication.

16 BCG Henderson Institute, The Coming Quantum Leap in Computing, May 2018

17 EEITimes, Is D-Wave a Quantum Computer?, May 2015

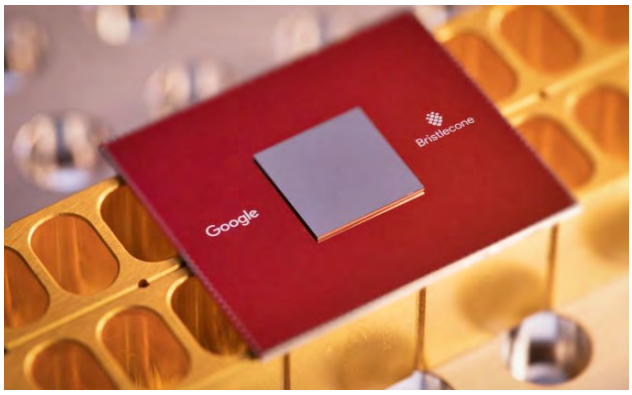
	Policy	Business	Research
United States	10-year National Quantum Initiative Program, Sept. 2018, $1.275 bln.	Google, IBM, Intel, Microsoft	Leading in quantum computing
China	Hefei National Laboratory for Quantum Information Sciences, $10 bln	Alibaba, Tencent, Baidu (Quantum Internet); Qasky, QuantumCTek, and Shenzhou Quantum focused on QKD	Leading in quantum communications (space)
EU	Quantum Technology Flagship Program, 10-year, Oct 2018, €1 bln	Bosch, BT Telecom, Nokia	Leading in quantum communications (ground)
Germany	Quantum technologies – from basics to markets, Sept. 2018, 4-year program, €650 mln	Bosch, Volkswagen (conceptually)	Leading in EU research efforts
UK	UK National Quantum Technologies Programme, 2014, 4-year, £270 mln	BT Telecom	World-leading quantum research capabilities
NL	Topsectorenbeleid – key technologies	Smaller supporting equipment manufacturers: Leiden Cryogenics, Delft Circuits, Single Quantum. KPN and Amsterdam Internet Exchange are involved in setting up quantum internet in Randstad.	Strong in hardware; quantum internet (QuTech), and algorithm development (QuSoft). Also, some PQC protocols submitted to NIST (KUN)
Rest of the World	Japan (2017), Canada (2018), and Australia have set up major quantum research policy initiatives	Japanese (NEC, Fujitsu, NTT) and South Korean (ST Telekom) companies are active in quantum communications; D-Wave (Ca) in quantum annealers (computing)	CQC2T (Aus), National Institute of informatics (Japan)

Table 3 **Actor landscape – countries**

3.2.2 US Business

The innovation landscape within the United States is dominated by large multinational corporations, specifically Intel, IBM, Microsoft and Google. Each of these corporations has dedicated significant levels of funding towards the development of quantum computers that exist in varying states of maturity. In March of 2018, Google unveiled the Bristlecone chip (see image), a 72 qubit, superconducting circuit chip. As of the writing of this paper, the Bristlecone is the largest quantum chip known to the public. While Google has said it is 'cautiously optimistic' about achieving quantum supremacy in the near future, the viability of the Bristlecone as a general purpose quantum chip is disputed. Similar efforts are being made by Intel, currently at 49 qubits, and IBM, currently at 50 qubits.

The role of US government agencies is relatively limited; in September, 2018, the US Congress allocated $1.275 billion towards quantum information science over the next 10 years. Organizations like DARPA and the National Science Foundation (NSF) have allocated relatively modest amounts of funding, specifically into secure quantum communication.



Google's Bristlecone quantum chip

3.2.3 US Research

There are major efforts in quantum computing at several national laboratories, such as the Los Alamos National Lab Quantum Institute and NASA's Ames research center. In addition, R&D is conducted at non-profit organizations receiving public funding, such as the Entanglement Research Institute or Berkeley Quantum Information Science. Based on 2015 figures of non-classified quantum technology research spending, the US invest a little less than 25% of worldwide spending. Given the recent surge in quantum computing research however, the US' relative share is likely to have decreased, with China taking the lead.

Research partnerships between large companies and top universities are forming, most notably between Google and the University of California-Santa Barbara, and Lockheed Martin and the University of Maryland. Interestingly enough, both Intel and Microsoft have invested heavily into collaboration with a non-US research entity, the Delft University of Technology.

3.3 China

China is aiming to become the global leader in innovation in 2035, which would mark the end of dependency on foreign technology. In its current 5-year plan, quantum computing and quantum communications feature prominently. Government-led investments in infrastructure, prototypes, and simulators are expected to exceed billions of Euro in years to come. Given China's political system, the interests of policy, economy, and science are closely monitored and coordinated.

3.3.1 China Policy

There is a widespread sentiment that, if quantum communication technology is considered an arms race, Chinese prospects look increasingly promising. In terms of both funding and vision, the Chinese are setting an ambitious agenda that has thus far been unmatched by Western actors. Overall innovation is driven in large part by government direction, which may contribute to a better coordinated research allocation as compared to the various US corporate parties.

In recent years, China has emerged as one of the primary innovators on quantum information science. While there is little information available on overall spending in China on quantum information science, the new National Laboratory for Quantum Information Sciences in Hefei is set to cost $10 billion. The consistency and scope of funding dedicated towards quantum information science, together with the protectionist measures applied on keeping the technology in China has propelled it as the global leader on space-based quantum technology. The Chinese have also indicated an interest in expanding the reach of the quantum satellite network (Micius) to Europe, with initial academic collaborations already occurring between Austria and China[18].

According to the US China Economic and Security Review Commission: *"China has closed the technological gap with the United States in quantum information science – a sector the United States has long dominated – due to a concerted strategy by the Chinese government and inconsistent and unstable levels of R&D funding" (in the US).*[19]

3.3.2 China Business

In 2015 the Chinese Academy of Sciences and Alibaba established the Alibaba Quantum Labs (AQL). It currently holds offices with interdisciplinary and international team in Hangzhou (Hardware and Systems), Beijing (Applications), and Bellevue, USA (Algorithms). AQL has released an ambitious 15-year roadmap. By 2025, it expects to have built quantum computers that will be the world's fastest by today's measure. By 2030, AQL hopes to achieve a universal quantum computing prototype. Also, in the field of quantum communications, Chinese companies such as Qasky, QuantumCTek, and Shenzhou Quantum have been building enormous patent portfolios in quantum technology applications, outnumbering other countries by significant orders of magnitude.

3.4 European Union

The European Union (EU) has considered quantum technology as critical in its key technologies approach for over the past two decades. In addition to the initiatives within individual member states, EU support for quantum research and development has been a priority. As a result, Europe is holding a strong global position in research. At the same time, a strong economic base that can make us of this leading position, still needs to be developed

3.4.1 EU Policy

To some extent, Europe charts a middle path between China and the United States, with some limited involvement from government and corporate parties. Academia is the driving force between the technical advancements on quantum computing/communication in the European context.

The European Commission has launched a 10-year flagship program with an expected budget of €1 billion.[20] The Quantum Technologies Flagship is a large-scale, long-term research initiative that brings together research institutions, industry and public funders, consolidating

18 Austrian Academy of Sciences, Austrian and Chinese Academies of Sciences Successfully Conducted Inter-Continental Quantum Video Call, September 2017

19 US-China Economic and Security Review Commission, 2018 Report to Congress, Chapter 4, November 2018

20 Website may be found at https://qt.eu/

and expanding European scientific leadership and excellence in this field. Funding for the Flagship is expected to continue in Horizon Europe, the EU's new research framework program.

In its ramp-up phase (October 2018-September 2021), it will provide EUR 132 million of funding for 20 projects in four application areas:

- quantum communication
- quantum simulation
- quantum computation
- quantum metrology and sensing

While funding is still quite modest from the EU level, these investments are additional to various member state efforts. Nonetheless, European efforts have been particularly strong on the system level design surrounding the hardware required for quantum computers, such as quantum algorithmic research and quantum infrastructure.

Various experts have indicated that Europe is also uniquely positioned to influence quantum communications through legal means, by setting standards and legal precedents for the use of quantum technology. This would be in the same vein as the GDPR, where adoption of legislation by the European Union can force external actors to conform to the European standards. Furthermore, stakeholders we interviewed demonstrated a recurrent sentiment that protectionist measures should be applied to quantum technology, including keeping technology in Europe and limiting infrastructure integration with other actors. If not, Europe's leading research positions would soon fade away.

3.4.2 European Union Business Sector

Europe lacks major companies that are able or ready to invest additional funds for innovation. As such, it risks that the many leading researchers and talents that it currently houses move to those environments that provide the greatest intellectual challenges and that smaller, innovative startups are bought by larger multinational companies. Some SMEs such as one of the leading quantum safe technology companies in Europe, ID Quantique, is already being repeatedly courted by South Korea Telekom, having most recently received a 60 million investment.

3.4.3 European Union Research

Europe is particularly strong in terrestrial based quantum communication, having both the know-how and the industrial capacity to craft the components required for the construction of quantum communication infrastructure.[21] While China is making leaps and bounds on developing the domestic capacity to produce components, for the moment the EU maintains its advantages. If the current trajectory will continue, however, it is likely Europe will be overtaken by the Chinese in the near future.

3.5 The Netherlands

3.5.1 Netherlands Policy

In its approach to technology, the Netherlands government has a policy tradition of avoiding to pick winners or losers, as some of them could turn out to be. It aims to leave these choices to the science, technology and innovation field itself. Instead it focuses on creating conditions to level the playing field. As a result, the Netherlands looks at strengthening structural advantages, such as a business friendly environment, expertise on triple helix construction and a strong ICT infrastructure, as can be witnessed by two large internet exchange organizations.

Against this broader policy background, the Netherlands has acknowledged the specific role that certain key technologies, including quantum technology, can play. Back in 2015, six parties signed an agreement to invest €135 million in QuTech, the institute for quantum technology located in Delft, over a period of 10 years.[22] The NWO research council awarded an €18.8 million grant from the Gravitation Programme 2016-2017 to the Quantum Software Consortium, a collaboration between scientists from Delft, Leiden and Amsterdam, stressing the need for integrative efforts between the hardware and software aspects of quantum.

Mid 2018, Dutch innovation policy formally stated its focus to be on the development of key technologies such as photonics, artificial intelligence and nano, quantum and biotechnology. Specific funding programs for these key technologies have, however, not been published yet. In more recent policy debates, the strategic dimension of these technologies has been ascertained. That is, the desirability has been expressed to remain independent from technology developments outside the EU, from China to the US, to avoid geo-political dependencies.

21 Website may be found at http://quantum-internet.team/

22 The Actors involved are the Ministries of Economic Affairs and Climate (EZK) and Education, Culture and Science (OCW), the research councils Netherlands Organisation for Scientific Research (NWO), STW, and FOM, and the research institutes TNO, TU Delft, and the Top Sector HTSM.

The long term bends inexorably towards those nations that have dedicated large and consistent amounts of funding towards quantum information science.

Also in that perspective, the path forward for the Netherlands is largely in line with the path the European Union might follow. For the moment, the Netherlands, holds a strong competitive advantage and has a deep stock of experts, engineering knowledge and future talent. As a country, it has received one of the largest parts of research funds related to quantum technology among all member states. If EU collaboration can be maintained and financial commitments ensured, Europe and the Netherlands can maintain and expand its advantage.

3.5.2 Netherlands Business

As discussed, given the relative paucity of tech giants in Europe, there are no Dutch corporations that are actively involved in the funding of quantum computer development. Obviously, QuTech is active in developing and supported by Microsoft and Intel. While there is business interest, the current use case is still relatively limited. That is expected to change within the coming 10 years as application domains will diversify (e.g., health, agriculture, security). Still, the focus might be on niche markets and specific problems.

Organizations such as KPN are, maybe reluctantly, involving themselves in the development aspects of quantum technology by investing and participating in research (e.g., Horizon2020) and prototype activities. There are a number of smaller Dutch companies active in providing engineering solutions to the challenges currently faced in the quantum computing, such as cryogenic devices (Delft Circuits, Leiden Cryogenics) and other supporting material (Delft Circuits, SingleQuantum).

3.5.3 Netherlands Research

The Netherlands is well regarded internationally, with academic institutions like TU Delft and CWI being considered leaders on quantum computing and quantum algorithms respectively.

From a research perspective, the Netherlands has a tradition of working on the forefront of integration between software and hardware, an area that had been left behind in the first internet revolution in the late 90s. The Netherlands might offer expertise by filling in the research gaps that surround the American efforts to develop the hardware. In addition, various applications of quantum infrastructure are being developed by institutions like the European Quantum Internet Alliance, coordinated by Dutch QuTech, which has recently been awarded €10 million toward the development of a quantum internet.[23] The direction of Dutch research into quantum computing leans towards public service applications, such as quantum internet and its associated algorithmic applications.[24] The European strength in terrestrial quantum infrastructure is largely attributable towards Dutch research efforts and European funding.

23 TU Delft, EU Awards ten million euro to European Quantum Internet Alliance to Speed up Development of Quantum Internet, October 2018

24 QUTech, Quantum Internet and Networked Computing

4 – Quantum Computing and Cybersecurity

As indicated above, there is still considerable uncertainty about the feasibility, timescale and sustainability of quantum computing. Thus, it is difficult to assess the scope and scale of its effects on the broader domain of cybersecurity. However, there is agreement that quantum computing will first and foremost have a major impact on the field of encryption, one of the main protection mechanisms of our current day digital information storage and exchange.

Quantum computing advances might interact and speed up developments of other emerging technologies that are relevant to the cybersecurity domain such as machine learning, big data analytics, and blockchain.[25]

For example, Amazon recently introduced a Quantum Ledger Database, that would record a log of transactions and be able to automatically scale and execute two to three times more transactions than already existing products.

Both the potential vulnerability of digital information now and in the future and its potential virtuous interaction with other technologies, makes quantum technology a strategic domain. Some Western commentators indicate that, for instance, the Chinese government's sheer level of quantum technology investments is sufficient reason for national security concerns. They argue that being the first in the development of quantum computers will provide an enormous strategic advantage with significant political and economic benefits attached to it. Others advocate that open collaboration will provide the fastest path to significant breakthroughs to the benefit of participating parties.

At the core of all of this is the effect that quantum computing could have on the encryption of stored and communicated data. Large amounts of data, such as used in financial transactions, email communication, critical infrastructure operations and transportation systems, are encrypted. There are four major purposes for which encryption is currently used:

Purpose	Meaning	Cryptography required
Secrecy/Confidentiality	Only sender and receiver can read (= decrypt) the message, and no one else can.	Symmetric encryption Public-key encryption
Authentication	Receiver can firmly establish that the message comes from sender.	Symmetric authentication Public-key signatures
Integrity	The message is unaltered	Symmetric encryption
Non-repudiation	Sender cannot deny having sent the message.	Public-key signatures

Table 4 **Purposes of encryption**[26]

Thus, the need for encryption arises from the desire to store and to communicate securely on the one hand and from the ability to access stored or communicated data through internet cables or wireless on the other.

25 A blockchain is a digital tool that uses cryptography techniques to protect information from unauthorized changes.

26 Hughes, 1995, Quantum Cryptography: Contemporary Physics

4.1 How encryption is applied

The basic principle behind encryption entails transforming information in such a way that is difficult to interpret without knowing exactly which transformation was used. More specifically, encryption researchers search for algorithms that are easily computed in one direction, but difficult to compute in the other direction. Such algorithms are known as *one-way functions,* on account of this directionality. All encryption techniques result in an *encryption key*, typically a long string of numbers that are used to transform the data. The most commonly used method of encryption, the so called RSA encryption protocol, makes use of a one-way function known as factorization, explained below.

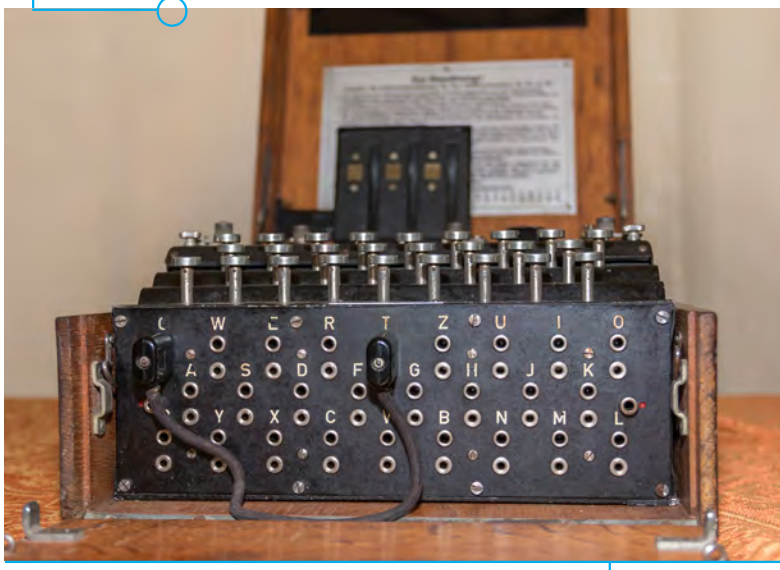
The factorization problem

Current encryption protocol (RSA) is centered around the use of the factorization problem. It consists of the sender using a key based on the multiplication of two large numbers, and the receiver only being able to decrypt the message if they know the two numbers. This problem is easy to compute in one direction, but difficult in the other direction.

For a simplified example, multiplying the numbers 6 and 8 together yields 48, a simple calculation.[27] Yet testing all possible combinations that together make up 48 is a considerably longer list: (1*48), (2*24), (3*16), (4*12), (6*8), (8*6), (4*12), (16*3), (24*2) and (48*1).

Should one want to decrypt the message, that person would need to deduce which two numbers were used to create the key, meaning each one of these combinations should be tested.

This process is laborious and slow on classical computers, but very quick on quantum computers. Current RSA protocol makes use of this simplified example, where two very large prime numbers are multiplied, typically resulting in numbers that are in excess of 750 digits long.



These problems are particularly hard for classical computers because they required each solution is tested one by one, resulting a very slow process. Estimates on how long a state of the art supercomputer would need to crack the highest level of RSA encryption exceed the lifetime of the universe. By contrast, a quantum computer could compute this problem in a matter of hours, if not minutes.

4.2 The effect of an algorithm

In 1994, applied mathematician Peter Shor showed that several important computational problems could, in principle, be solved significantly more efficiently using a quantum computer. Shor's algorithm on quantum factorization will greatly reduce the required computation time to extract the private key required to decrypt current Internet traffic and stored encrypted data.

As a result, quantum computing could threaten cryptographic schemes such as the widely applied RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). These schemes protect government classified data, businesses' intellectual property, and citizen's privacy as well as all communications across these entities.

27 The simplification lies primarily in the fact that we use two non-prime numbers here to make the calculation easier to follow. As stated further, usually factorization uses prime numbers.

Cryptographic Algorithm	Type	Purpose	Impact of large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table 5 **Quantum secureness of cryptographic schemes**[28]

The lack of protection will obviously become relevant once advancements of quantum computing allow for the breaking of the vulnerable encryption schemes. However, the possibility that encrypted information is retroactively decryptable in the future poses a significant challenge today. Hackers, whether private, state sponsored or nation states themselves, might currently be harvesting sensitive data, knowing that they will be able to decrypt this information when a universal quantum computer materializes.

For corporations, it has profound privacy implications, as data stored must not only be encrypted to match the best contemporary standard, but must also be future proof against quantum algorithms. For national governments, there are numerous issues around the possibility of, for example, diplomatic cables or military intelligence being retroactively decrypted which could have significant geo-political and diplomatic ramifications.

In short, companies and governments cannot afford to have their private communications decrypted in the future, even if that future is 30 years away. If data fidelity is to be preserved through the application of quantum computing, actions must be taken now.

4.3 Sense of urgency

As such, there is a degree of urgency in the drive towards creating a cryptography that is resistant to quantum computing. Such schemes are commonly referred to as quantum-proof cryptography. There is a need to begin the transition as soon as possible, especially since it takes over a decade to make existing Web standards obsolete. Asymmetric cryptographic algorithms used in key exchange protocols appear to be the most vulnerable to compromise by known quantum algorithms, specifically by Shor's algorithm.

There is strong public and commercial interest in developing and deploying quantum-proof cryptography. As a matter of fact, various companies have already taken steps to secure smaller firm-critical datasets in new quantum-proof encryption protocols to avoid the risk of retroactive decryption.

Overall, there are two approaches to achieve quantum-proof cryptography. Both are critical fields of research and innovation and both are required for a quantum proof cryptography:

- Post-quantum cryptography (PQC): Developing new encryption algorithms that are where quantum computers have no advantage in computational speed
- Quantum Key Distribution (QKD) Making use of quantum effects in the process of key establishment and key distribution.

In addition to these two primary research fields, there are quantum-random-number generators (QRNG) that can improve the current workings of encryption schemes. QRNG is available and in use in some specific sectors, such as the financial sector.

28 Adopted from National Institute of Standards and Technology (NIST), Report on Post-Quantum Cryptography, April 2016

4.4 Post Quantum Cryptography

Post-quantum cryptography solutions follow an algorithmic approach. Meaning they involve finding mathematical functions where quantum algorithms have no comparative advantage. In essence PQC algorithms are algorithms where *quantum supremacy* offers no tangible benefit. As discussed, the factorization problem happens to be one of the quite rare instances where quantum supremacy has been proven. As such it is deeply problematic, since it forms the basis for the currently used RSA encryption protocol.

4.4.1 Use case for post-quantum encryption

Post-quantum encryption primarily finds it application in the distribution of public keys, meaning that its application answers the factorization problem directly in the form of replacing current RSA protocols. This means that it does not require fundamentally new infrastructure, like the later discussed QKD might. In addition, the theoretical work surrounding PQC is already quite advanced, with numerous different examples of possible quantum resistant encryption already available. In the views of various experts, the question is not whether PQC is a viable option, but rather how it should be implemented and standardized. This latter issue remains a work in progress, with organizations like the National Institute for Science and Technology (NIST) being actively involved in standardization efforts. Being the most advanced, most widely application for public keys and having relatively low costs, PQC appears to be the most straightforward solution for developing quantum resistant encryption.

4.4.2 Current efforts on post quantum encryption

In 2016, the US National Institute for Standards and Technology (NIST) has initiated a process to solicit, evaluate and standardize one or more quantum-resistant public-key cryptographic algorithms.[29] This process is projected to last until approximately 2022 after which the standardization process should be finalized, which could take an additional two years.

Thus, steps are being made towards a realistic new protocol. However, there are significant leaps to be made before any PQC can be considered as a sufficient replacement for factorization-based keys. The three main problems that most PQC protocols suffer from are *confidence*, *efficiency*, and *usability*.

Encryption protocols go through many trials before they are considered secure enough. Encrypted information can be stored for decryption later, so if a protocol that was assumed safe turns out to be decryptable, information that was encrypted with said protocol becomes publicly available. Many methods proposed have only seen little attention to them, so there is the risk that they prove insecure with more people attempting to break the protocols. The *confidence* in these methods is not (yet) very high.

Most of these methods require very long key sizes, meaning there is a lack of efficiency. That is an issue for some users, such as for commercial usage and information exchange through the Internet, because it will take more time to load web pages for example or be too expensive to apply. If new PQCs are less *efficient*, it will not be suitable for modern information exchange. Finally, if a new method has the confidence to be secure and is efficient enough to be a ubiquitous protocol, its *usability* is not trivial. Modern communication protocols on the web such as TLS and IKE need to be adapted to these standards, and this takes considerable time to develop. Indeed, should an adequate encryption protocol be found it will have to be standardized and implemented globally for it to be optimal.

29 Project Overview Post-Quantum Cryptography Standardization

Below is an overview of some of four groups for which PQC algorithms are currently under development.

Method	Confidence	Efficiency	Usability
Lattice-based cryptography	Worst case reduction, meaning high level of confidence	Needs secure improvements in its efficiency.	Successfully implemented in communication protocols, possible candidate for PQC public key encryption
Code-based cryptography	Confidence is high	Requires large key sizes	Good for public key encryption, not so much for signatures
Multivariate polynomial cryptography	Systems have been proposed, but many have also been broken.		Good for digital signatures
Hash-based signatures	Security well understood	Work intensive, one time use only	Quite successful for one-way traffic and authentication (signatures)

Table 6 **Proposed methods for PQC**[30,31]

4.5 Quantum Key Distribution

Where PQC is recognizably the same approach as current cryptography, quantum key distribution (QKD) seeks to make active use of quantum effects in creating encryption keys. Simply put, it involves making use of several quantum properties to ensure that a key is transferred between sender and receiver, and that any information intercepted is fundamentally useless. More precisely, QKD works by sending individual quantum particles from sender to receiver and that together will make up the encryption key, intercepting the particle would result in 'corruption' of that particle. Hence, QKD is utilized to generate a *one-time pad*, a unique key that is sent in advance of the actual data transfer. While the technical details of QKD are beyond the scope of this paper, some of its critical features are:

- QKD ensures that the key transfer cannot be intercepted
- QKD operates based on laws of physics rather than computational complexity, rendering it future proof[32]
- Guaranteed confidentiality and integrity

4.5.1 Use case for quantum key distribution

Quantum key distribution requires a quantum infrastructure, meaning expensive and delicate equipment are necessary. As such, the implementation cost for QKD is high, likely ensuring that its application will remain relatively limited in public sector encryption. Instead, the use case for QKD centers on creating guaranteed safe channels for ultra-secret information such as military intelligence, national security purposes or corporate secrets. Making use of QKD is only feasible in cases where the information is of such sensitivity that it outweighs any financial or practical considerations. The Micius satellite, developed by the People's Republic of China government, allows for real-time communication between Beijing and Urumqi, the capital of Xinjiang province[33]. It is by definition impossible to intercept, crack or decrypt such a channel, as any information intercept will effectively self-destruct. Despite the current limitations, the underlying physics in QKD could have profound applications, with a significant amount of research being directed towards quantum teleportation. As such, QKD is a technology that has an application in encryption but is likely to have much broader applications in the future.

30 National Institute for Science and Technology (NIST), Post-Quantum Cryptography, 2016, 3-4

31 Alkim et al., Post-quantum Key Exchange - A New Hope, 2016

32 Zhou et al., Quantum Cryptography for the Future Internet and Security Analysis, 2018

33 Phys.org, Real-world Intercontinental Quantum Communications Enabled by Micius Satellite, January 2018

4.5.2 Current efforts on quantum key distribution

Active research is ongoing on making QKD more practical and less expensive. Broadly speaking there are three significant problems areas within QKD:

- Key generation rate: Quantum key distribution typically requires a very large key size as only a small section of the original key transmission will be utilized. This causes a lack of efficiency in information exchange. Despite recent breakthroughs, the current key generation rates are orders of magnitude slower than current classical generation methods.
- Distance: QKD is currently optimized for metropolitan distances[34], its effective range is highly limited, especially on terrestrial networks. QKD requires high-grade fiber optic cables and complex constructions to avoid increased noise levels that would destroy the qubits[35]. Increasing distance would require some sort of amplification. Given this lack of noise-free amplification, there are significant constraints on even the theoretical range of quantum networks. Range limitations are substantially less for space based quantum networks with the Micius satellite transferring to a range of 2000 km. While this is a significant achievement, space based networks have significant drawbacks[36].
- Cost and robustness: The past few years there have been significant engineering advancements on QKD systems[37]. Nonetheless, numerous technical challenges remain and QKD systems are both expensive and fragile.

Despite these challenges, QKD has been successfully executed on several occasions. In 2007, QKD was applied in elections in Geneva, and in 2009 and 2010, different research groups established secure video conferencing and voice calls through QKD. Significant efforts are directed towards the establishment of a terrestrial quantum internet, especially in Europe where QuTech has been making advances in producing a prototype.

Recently, the European Union closed a call for proposals on the establishment of a Quantum Key Distribution testbed (within the focus area of boosting the effectiveness of the Security Union) closed with an available budget up to 15 million. The aim of this effort is "Building an experimental platform to test and validate the concept of end-to-end security, providing quantum key distribution as a service. Proposals should develop an open, robust, reliable and fully monitored metropolitan area testbed network (ring or mesh configuration). The aim is to integrate equipment, components, protocols and network technologies with QKD systems and current digital security and communication networks."

4.6 Deployment requirements

As stated before, the time schedule for deploying new quantum-proof encryption does not merely depend on the occurrence of quantum computers to crack current schemes. Data that is encrypted now but which can be decrypted later is vulnerable when captured now and of value at the time of decryption. To limit the negative consequences of this, organizations that estimate that they are vulnerable need to take action as soon as possible.

Having said that, the situation will per definition become more prominent as the occurrence of quantum computers draws nearer. At the same time that investments in quantum computing are increasing, new solutions and implementation trajectories need to be pushed. Depending on the situation governments and business can take various types of actions, ranging from raising awareness, assessing vulnerabilities, pushing for standardization and/or coordination, and financing transition processes.

34 Islam et al., Provably secure and high-rate quantum key distribution with time-bin qudits, 2017

35 Any external interaction with the quantum particle degrades the quantum state.

36 Requiring a line of sight between targets to communicate and being unable to operate in sunlight

37 Nature, Practical Challenges in Quantum Key Distribution, November 2016

In essence, there are four factors of importance to determine the timescale of action.

- a fully functional quantum computer with the ability to run Shor's algorithm
- the development and standardization of quantum-proof encryption
- the implementation of it in real-time operations: the design of new security architectures and the systematic roll out of new algorithms
- the value of the encrypted data: there is a wide range of encrypted data. Some of it might lose it value in the shortest of time frames, other data remains valuable for decades.

For each of these factors, time indications can be given. We have already indicated the broad range of uncertainty related to the introduction of a fully functional quantum computer. On the one hand, it could be argued that developments in the past decade or so have been faster than anticipated. There might also be a tendency in the research community to be cautious about ambitious predictions. On the other hand, as even the feasibility of quantum computing is still under discussion, a timeline of, for example, 15 years might be overly optimistic.

The NIST competition for PQC algorithms, which has received more than 50 credible entries, is the driving factor for the development and standardization of quantum safe encryption. Here, the provided timeline is somewhere between 2022-2024.

The major hurdle appears to be the introduction and roll out of new algorithms in the current infrastructure and architecture. Experience with 'retired' algorithms in the past show that 5-10 years are often required for the complete implementation of a new algorithm.

Finally, the shelf time of information determines the ability to act. Given the wide range of data that is encrypted, the time that data needs to be protected ranges accordingly. For some, regulatory obligations determine how long information must be kept, as is the case with some financial information. Other information might be kept classified for an indefinite period of time. Obviously, all of this is dependent on the condition that information is captured or intercepted and that the encrypted information can be broken by a quantum computer.

5 – Conclusion

The pursuit of scalable, error free and practical quantum computing will require significant advances and is likely to face both breakthroughs and setbacks. That being said, the challenge of developing quantum computing is matched only by the immense competitive advantages that it could deliver. Both the threats and opportunities offered by quantum are significant. Breakthroughs in the health sector could be achieved, by applying quantum simulation to model molecular structure, dramatically speeding up the development of new pharmaceuticals.

The promise of a fully-fledged universal quantum computer is alluring, but there is no guarantee that it is possible. A minority of scholars even hold that such a quantum computer is not possible, even in principle. Given the vast amount of unknowns and the scope of technical challenges, few experts are willing to make a concrete time estimate of when a universal quantum computer will be available. Estimates on narrow application quantum computers, mostly falling in the first generation type, are more concrete. Concrete investments are also being made by the larger corporate parties towards the development of second generation quantum computing, following the super computer business model. Overall the field of quantum computing is characterized by insecurity about the feasibility of the ultimate goal of a universal quantum computer. At the same time, the continuous process of working toward this goal has helped to solve smaller pieces of the puzzle.

The vast potential and threat of a universal quantum computer is driving ambition across the globe, as various actors are starting to position themselves to be at the forefront of quantum computing. The United States, a longstanding leader in the super and quantum computing area, has led many developments through its large entrepreneurial sector, but is now in the process of setting up a bigger government propelled quantum strategy.

China has decided to massively invest in quantum technology. It aims to become a world leader in the field, and has the capabilities, ambition and funding to make that a reality. While there is still relative parity in what may be interpreted as an arms race, Europe especially must step up its ambition and put forward bold vision, lest it increasingly falls behind in the development of quantum computing.

Steps have been taken by the European Union to establish a flagship program, but they fall short in scope and ambition when compared to their overseas equivalents. In addition, various national initiatives are undertaken by countries such as Germany and the UK, as increasing attention and funding is being directed towards a quantum vision. Despite such efforts however, Europe lacks major companies that are willing to invest additional funds into the development of a quantum computer. While there is no shortage of European domestic talent, there is a risk that leading researchers and talents move to those environments that provide the greatest intellectual challenges and that smaller, innovative startups are bought by larger multinational companies. As it stands, those environments are found primarily overseas; China's commercial actors are smaller than those found in the US, but enjoy long term systematic support from their government. The US parties are the leaders in the development of the actual hardware on quantum computing and wield investments that are significantly larger than anything found in Europe.

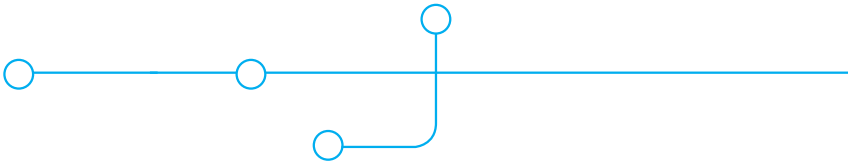
It is possible that Europe could walk some middle path, blending best practices from both the government-oriented Chinese approach and the market-driven American approach. Should Europe fall behind on a technological level, there is still the possibility to force conformity by passing legislation concerning quantum computing. Much like the GDPR has forced (US) multinationals to adjust their practices, a strong legal interpretation on the use of quantum communications and computing can help shape the landscape.

Furthermore, while small, the Netherlands is a known quantity in the quantum computing world, with numerous highly-reputed research organizations, such as QuTech and QuSoft. These organizations have received government support and contributions from the private sector, even though the investments do not match the volume of other tech-giants'. While quantum is mentioned in the coalition agreement, and is identified as a key technology, high-level strategic direction is not yet provided and left to the European Commission. Despite the EU's Flagship Quantum Program and the funds that are involved in that, member states tend to invest significantly more in their national R&D programs.

To summarize, the threat to cybersecurity is concrete and potentially imminent. Developments in quantum computing pose a real threat, as widely used methods to protect the confidentiality, integrity and availability of data might soon be rendered void. While quantum secure encryption might seem like a future problem, information stored now will be decryptable retroactively, opening up potentially huge liabilities for both governmental and corporate parties. Post-quantum encryption is relatively advanced in its development, with a variety of PQC protocols already being evaluated by NIST. Focusing on only PQC however would be short sighted, as there is great potential in the application of quantum key distribution that moves beyond simply mitigation the threat of retroactive decryption.

As the field of quantum information science matures, various technologies might be developed that have not yet found a use case, yet over time confer substantial innovation and commercial applications. While the era of classical computers is not over yet, we are running into the physical limitations of microprocessors.

As Moore's law starts slowing down, a new scalable variant of computing will be needed, giving research into quantum computing a sense of urgency. The co-existence of quantum computers and classical computers is more likely than a full replacement of the current infrastructure and the application of quantum cryptography will most likely remain a narrow field. That in itself might require considerable and coordinated investments in infrastructure (a quantum internet), hardware (from quantum chips to quantum controller processors), algorithms and software (building applications to be used on the hardware), and training and education. For the foreseeable future we are likely to remain in a transition scenario, where the application of quantum computing is not yet fully manifest, but the limitations of classical computing are starting to become apparent.



6 – Recommendations

Based on the analysis in this paper, three main objectives should be envisioned:

- Protecting encrypted information that is already vulnerable
- Preparing for new quantum-safe encryption schemes
- Exploiting the potential benefits of quantum technology

For each of these objectives, we provide recommendations at various levels. As indicated in earlier chapters, these objectives are not mutually exclusive as advancements in quantum technology might put pressure on reaching protection objectives.

6.1 Protecting encrypted information that is already vulnerable

6.1.1 Creating awareness about vulnerable encryption schemes

The cryptography community is very well familiar with the security and insecurity of specific encryption schemes, such as RSA and ECC. However, beyond this community the knowledge of the problem seems to be haphazard at best. Increasingly more attention is being paid in public papers and statements, but awareness is lacking, letting alone a sense of urgency. Given that the vulnerable information is generally strategic of nature, the potential repercussions reach out far above the level of individual organizations. As such, looking at how the anticipated Y2K problems and at the approaches taken at that time and assessing their appropriateness for encryption concerns might be a useful first step.

6.1.2 Identifying the magnitude of the problem in The Netherlands and the EU

As repercussions of vulnerable encrypted information do not stop at the Dutch or European borders, it is clear that concerted solutions will have to be found. At the same time, concrete steps need to be taken in the near term already. In that sense, identifying where and which encryption schemes are used and who are using them is crucial. Internet exchanges, network operators, certification authorities, CSIRTs, software developers, data centers and the like might be able to provide an initial overview of this.

Concomitantly, it is important to assess how much strategic information might be affected. This would need to be done at various levels. At the data level, individual organizations need to assess what they consider to be strategic information. This can be information relevant to an organization's own operations, but also personal information collected from others. The public sector as a whole may be affected disproportionately high, given the levels of classified and privacy-sensitive data that is stored and exchanged.

6.1.3 Supporting the adoption, use and application of short-term remedies

Sporadically, organizations are implementing short-term and small-scale fixes to encryption vulnerabilities, for example within banking and financial institutions. Until quantum-safe encryption schemes will become fully available, these fixes are important for protecting sensitive information, now and in the future. Communities of practice can help support their use and application as well as identify issues that may arise with them. It will also help move these broader communities into action.

6.2 Preparing for new quantum-safe encryption schemes

6.2.1 Connecting to the development of new quantum safe encryption schemes

The NIST competition has generated various promising post-quantum cryptography schemes. The development of these schemes might still take a number of years, standardization of them a few more. Also, within various EU research and policy groups several recommendations are being put forward. As these developments adjust and mature, it is important to remain aware of them. Given that various Dutch organizations are involved in the NIST competition, open exchange of information should be promoted as much as possible.

6.2.2 Developing transition schemes that help develop longer-term solutions

The most significant effort will have to be dedicated to the implementation of new schemes. Past experiences demonstrate that it takes a long time (up to ten years) to

adapt infrastructure and related protocols to incorporate new encryption schemes. Obviously, this is an effort that goes well beyond the level of individual organizations and needs plenty of coordination and leadership.

6.3 Exploiting the potential benefits of quantum technology

6.3.1 Ensuring quantum computing developments remains focused and goal oriented

In many ways we find ourselves in a new Apollo era, where we must set a bold new vision to guide our path forward. Identifying landmark indicators and achievements to provide an indication of being on track supports the implementation of this vision. It also helps in determining when the need for action to protect vulnerable information becomes more and more prominent.

6.3.2 Keeping the momentum of current European and Dutch research strengths

Europe in general and the Netherlands in particular have established a strong research base in quantum technology. At the same time, there is considerable concern that Chinese and US investments will surpass or simply acquire European knowledge and capabilities. The ideological debate whether to protect the knowledge and capabilities has both its cons and pros. Protecting businesses and interests might help retain assets in Europe, while at the same time obstructing access to new developments. Beyond this, European policymakers can aim to systematize consistent levels of funding and set coherent research objectives and landmarks. The Dutch debate on this will need to be carefully conducted.

6.3.3 Defining and expanding on potential use cases

Development of a niche field that has added value when compared to the other efforts towards quantum computing (ie quantum infrastructure)

The first business application is the direct renting out of quantum computing capacity, and while the actual quantum computer will likely remain non-European, there is a substantial amount of pre-processing that must be done to optimize the computational complexity of a problem. Such a service would not in itself require a quantum computer, but be a quantum related service that may be offered. Given the Netherlands' reputation with research into computational complexity and its favorable location regarding the internet exchange points, this would be a business case that is particularly well suited for the Netherlands.

The second business case is encryption protocols, with companies like KPN having developed expertise on post quantum cryptography. A current business case exists for actors that are looking to re-encrypt their most critical datasets and information streams in protocols that are quantum secure. Various solutions like quantum secure emails or quantum secure VPN networks are already available.

A third application is the development of quantum key distribution hardware, allowing for secure channel communication. This use case is related to quantum internet, and the Netherlands being home to numerous institutions that are at the forefront of such research.

Annexes

Annex 1 – List of Interviewees

Name	Affiliation
Jos Baeten	CWI
Jaya Baloo	KPN
Carlo Beenakker	Universiteit Leiden
Hans Bos	Microsoft
Petra van Schayik	Compumatica
Stephanie Werner	QuTech, TuDelft

Bibliography

Public documents, Journal Articles

Adviesraad voor Wetenschap,Technologie, Innovatie (AWTI), Klaar voor de toekomst? Naar een brede strategie voor ICT, The Hague, September 2015

Adviesraad voor Wetenschap,Technologie, Innovatie (AWTI), Werkprogramma 2019, The Hague, September 2018

Alkim, Erdem & Ducas, Leo & Pöppelmann, Thomas & Schwabe, Peter, Post-quantum key exchange - a new hope. 2015

Birch, Q-campus Background Study (in support of: "Building a Q-Campus – Realising a Quantum Ecosystem in Delft", Driebergen, 2018

Brief aan de Tweede Kamer van de Minister en Staatssecratris van Economische Zaken en Klimaat, NaarMissiegedreven Innovatiebeleid met Impact, Tweede Kamer, vergaderjaar 2017–2018, 33 009, nr. 63

Chen, Lily, et.al, Report on Post-Quantum Cryptography, NIST. IR 8105, National Institute of Standards and Technology, Washington, Dc, April 2016

Cyber Security Assessment Netherlands (CSAN) 2018, Ministry of Justice and Security, August 2018

ETSI, Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges, Sophia Antipolis, 2014

Grumbling, E. and M. Horowitz (eds), Quantum Computing, Prospects and Progress, National Academies Press, Washington, DC, 2018

Herman, Arthur, Idalia Friedson, Quantum Computing: How to Address the National Security Risk, Hudson Institute, Washington, DC, August 2018

Islam, Nurul & Lim, Charles & Cahall, Clinton & Kim, Jungsang & Gauthier, Daniel. (2017). Provably-Secure and High-Rate Quantum Key Distribution with Time-Bin Qudits. Science Advances. 3. 10.1126/sciadv.1701491.

KPN, Technology Book: The technology trends KPN has on its radar, The Hague, April 2018

Mosca, M., Cybersecurity in an era with quantum computers: will we be ready?, Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, 5 November 2015.

NCTV, National Cyber Security Agenda: A cyber secure Netherlands, Ministry of Justice and Security, April 2018

Travagnin, Martino & Ferigato, Carlo & Lewis, Adam, Patenting trends in selected Quantum Technologies, with a view on policy implications, November 2017

U.S. GAO, Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies, Washington, DC, December 2018

U.S.-China Economic and Security Review Commission, USCC 2017 Annual Report to Congress, US GPO, Washington, DC, 2017

Web sources

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

https://ec.europa.eu/digital-single-market/en/policies/quantum-technologies

https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-04-2019.html

https://qutech.nl/roadmap/quantum-internet/

https://scipol.duke.edu/track/s-3143-national-quantum-initiative-act/national-quantum-initiative-act-s-3143-hr-6227-115th

https://uknqt.epsrc.ac.uk/about/quantum-technologies/

https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101

https://www.accenture.com/t20170628T011725Z__w__/nl-en/_acnmedia/PDF-54/Accenture-807510-Quantum-Computing-RGB-V02.pdf#zoom=50

https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

https://www.cbinsights.com/research/quantum-computing-corporations-list/

https://www.cbinsights.com/research/quantum-computing-corporations-list/

https://www.digitalcentre2020.com/news/quantum-computing-use-cases/

https://www.eetimes.com/document.asp?doc_id=1326592

https://www.financialexpress.com/industry/technology/how-microsoft-is-leading-quantum-computer-race-to-unlock-mysteries-around-us/1371279/

https://www.forbes.com/sites/juniper/2017/11/01/cybersecurity-in-the-age-of-quantum-computing/

https://www.foreignaffairs.com/articles/china/2018-09-26/chinas-quantum-future

https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing/

https://www.idquantique.com/random-number-generation/applications/banking/

https://www.laserfocusworld.com/articles/2018/09/650-million-for-quantum-research-in-germany.html

https://www.microsoft.com/en-us/research/group/microsoft-quantum-redmond-quarc/

https://www.microsoft.com/en-us/research/research-area/quantum/

https://www.nature.com/articles/d41586-018-07449-z

https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

https://www.wired.com/story/google-alibaba-spar-over-timeline-for-quantum-supremacy/

Understanding the Strategic and Technical Significance of Technology for Security. Implications of Quantum Computing within the Cybersecurity Domain.

A publication from
The Hague Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Authors
Paul Verhagen, Erik Frinking, Lucie Kattenbroek, Thomas Attema (TNO)

Design
Studio Maartje de Sonnaville by the design of Studio Koelewijn Brüggenwirth

Beeldmateriaal beschikbaar gesteld door QuTech, www.qutech.nl. Fotografie door: Marieke de Lorijn (p. 20, 30) en Pim Top Fotografie (p.6).
Overig beeldmateriaal: iStock

Print
Drukkerij Edauw + Johannissen

This study was commissioned by the Hague Security Delta (HSD). The information and views set out in this study are those of the authors and do not necessarily reflect the official opinion of HSD. HSD does not guarantee the accuracy of the data included in this study. Neither HSD nor any person acting on behalf of HSD may be held responsible for the use which may be made of the information contained therein.

Together we Secure the Future

www.thehaguesecuritydelta.com