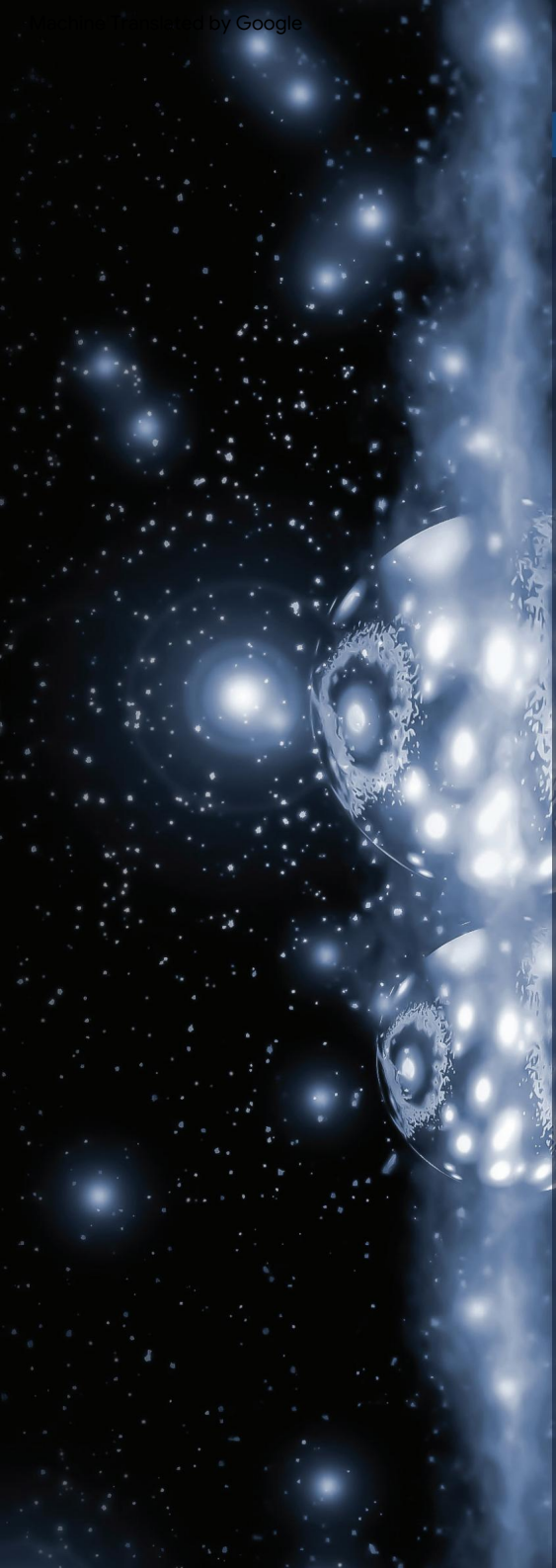

JANUARY 2020

PAULA FORTEZA
Deputy of the French of Latin America and the Caribbean

JEAN-PAUL HERTEMAN
Former CEO of SAFRAN

IORDANIS KERENIDIS
Research Director at CNRS

QUANTUM : TURN TECHNOLOGY THAT FRANCE WILL NOT MISS

37 PROPOSALS FOR A AMBITIOUS NATIONAL STRATEGY

Mission rapporteurs
NEIL ABROUG
THIERRY DAVID
MATTHEW RATIEVILLE
JEAN VANNI MENUS

Mission entrusted

by Prime Minister Édouard Philippe

Parliamentary mission

from April 15, 2019

to October 3, 2019

With the support of:

Marianne Billard • Marion Dos Reis Silva • Jean Éric Michallet • Sébastien Kunz Jacques

Foreword

Paula Forteza

When you have been evolving in the digital ecosystem for several years, it is impossible to miss the quantum. A concept that appears regularly in exchanges between experts, in an almost mystical way: on the one hand the converts, on the other the skeptics. Agnostic on the issue, but always ready to objectify technological debates, I was honored that the Prime Minister entrusted me with this mission.

The quantum is not at the dawn of its first revolution, since from the beginning of the 20th century, quantum physics was already at the origin of many major technological upheavals such as the invention of the transistor or the laser. Today, thanks to new discoveries in fundamental physics, we are again faced with the imminent emergence of new breakthrough innovations, based, this time, on quantum computing.

At the time of writing these few lines, Google would have managed to achieve quantum supremacy, by managing to stabilize 53 *qubits* long enough to carry out in a few minutes a calculation which would have taken 10,000 years to the most powerful of existing supercomputers. The secrecy and the precaution surround this information crumbled in the press, indicator of the strategic character which covers these technologies.

Understanding the nature of these innovations, their catalysts, the obstacles they face, in order to identify opportunities for France and thus build a national strategy, has been our work over the past few months. First observation: faced with the speed and uncertainty of these developments, only countries that have dared to take risks will find a place in this new technological turning point and will therefore be able to guarantee their sovereignty. It is urgent to act.

France has an ecosystem of immense quality, thanks in particular to a network of outstanding academic researchers. But, if the world of research is still mainly at the maneuver of this revolution, it cannot do without industrialists making investments important and testing these new innovations. The main objective of our recommendations is to build bridges between these two worlds, which too often evolve side by side.

I would like to highlight the voluntarism and enthusiasm of this ecosystem. Behind a complex subject, of unequaled technicality, requiring to handle physics and engineering, when it is not advanced mathematics and computer science, I met accessible, passionate people who are keen to raise awareness widely. We will be able to count on them, as the awareness of the issues related to quantum is one of the conditions for the success of our national strategy.

I particularly welcome the presence of many women in this field. Faced with a world of research and digital technology that is still very masculine, they have established themselves thanks to their professionalism and the quality of their work. I am thinking in particu

Vinet, to Alexia Auffèves, Pascale Senellart, Elham Kashefi, Eleni Diamanti, or even Hélène Perrin whom I congratulate and thank for having inspired me throughout this mission.

Last but not least, a word about my co-bearers, from whom I learned a lot. Iordanis Kerenidis, expert in quantum algorithms and worthy representative of the world of research, knew how to be our compass so as not to omit anything on the technical level. Jean-Paul Herteman, for his part, was able to bring his expertise from the business world and his feedback from previous comparable technological upheavals, particularly in aeronautics.

In addition to the participation of the joint sponsors and the expertise of the French ecosystem, the success of this mission owes a lot to the dedication shown by the administration demonstrate to accompany us in the construction of this strategy. Special thanks to Neil Abroug for his perseverance. And finally my team, within which Marianne Billard and Marion Dos Reis Silva have been able to coordinate this collective work admirably.

Entering the international and European game of quantum technologies is possible provided that we trigger a movement fast. Today, the human and intellectual resources are ready; we can rely on them, but we must mobilize the necessary means. Thanks to an ambitious national strategy, quantum technologies are called upon to make our country a key player on the international scene.

Our report invites you to reflect on this.

Jean-Paul Herteman

I accepted with great interest to contribute to this mission relating to quantum computing as the subject seemed both exciting and strategic to the engineer and business manager that I was. This interest has not been denied, quite the contrary, over the course of the hearings and our work. And I hope you will share it as you read this report.

This technology is a real breakthrough. Its applications can revolutionize industrial branches such as chemistry, pharmacology, energy, metallurgy, aeronautics or communications. The term and scope of its development are not yet known with certainty, but it is now or never that the decisive orientations must be taken.

I have had the chance to devote my career to an industry - aeronautics - of which France can be proud and which owes its success to a constant strategy of scientific and technological innovation and to the prevailing demand for industrial excellence. among its engineers, technicians and companions.

I also remember how decisive the industrial policy of the "Pompidou years" was in restoring our industry to the leading position in the world that the Second World War had obscured.

The situation of quantum computing, which is more disruptive and more complex, is different today, but the issues are at least of the same order, as is our country's ability to act and succeed.

Our recommendations aim to give us the means to achieve this success.

In terms of organization and methods, we recommend grouping scientific and technological actors into "campuses", setting up steering of the scientific, technological and industrial research policy, closely coordinated between the public authorities, the research and business.

It will also be necessary to ensure that training is put in place in anticipation of key needs.

In terms of development themes, the ambition is to build an inclusive industry controlling the entire value chain, from the basic material to software optimized for the application sectors, including the production of quantum chips, the integration of computers and their specific algorithms, without forgetting the enabling technologies (cryogenics, lasers, etc.) which are the real strength of an industrial fabric.

This obviously requires significant but unavoidable public funding because the logic of the market alone does not allow the start of such disruptions and all the major global players, in one way or another, devote the essential strategic investment to it.

I am personally convinced that this effort (which, to be concrete, will represent around a few euros per Frenchman and Frenchwoman for perhaps 5 to 10 years) will be very largely repaid and will greatly contribute to the development of our country.

Iordanis Kerenidis

My first encounter with quantum algorithms dates back more than twenty years, when, as a young student in Greece, I discovered the existence of Peter Shor's factorization algorithm. Although I did not have a very clear idea of the repercussions that this work could have, it seemed obvious to me that this was a revolution. This discovery also convinced me to prepare a thesis in quantum computing at Berkeley (University of California) and to apply after my doctorate for a research position at MIT, at a time when this science was still an essentially theoretical field of study, without application. immediate, due to the lack of quantum hardware.

In fact, even during the following decade, when I had joined the ranks of the CNRS, in Paris, since 2006, the idea of having an operational quantum computer remained a distant dream shared by a few rare scientists. This is no longer the case today. In recent years, we have seen this dream become that of an entire generation, a possibility of a total paradigm shift in the field of information and communication technologies, a promise of unprecedented computing and communication capabilities.

As with any dream, the road to realizing the promise of quantum technologies is long and arduous, but it is also fraught with rewards, namely the acquisition of new scientific knowledge and unexpected technological benefits. It should also be noted that we have already made considerable progress in this area: Google announced that it had reached "quantum supremacy" at a time when

As we were finishing this report, new applications in chemistry, optimization and machine learning *have* dramatically increased the impact

potential of quantum computing, and quantum communication satellites are currently orbiting the earth. It's time for optimism, tinged with caution. The time has also come to recognize the potential of this field of study and to invest in what constitutes one of the most promising paths to scientific discovery, technological progress and economic and societal benefits. Quantum technologies bring remarkable advantages in chemical and physical simulations, with potential applications in agriculture, drug discovery and battery design; quantum algorithms enable dramatic accelerations in optimization and machine learning applications, especially in the fields of finance, energy, automotive and environmental sciences; quantum communication networks can improve the long-term security of sensitive data. The quantum revolution could well be born and it is incumbent on us to see it through. It is also for this reason that in 2014 we created the " *Paris Center for Quantum*

Computing " (PCQC), an interdisciplinary research center at the forefront of quantum technologies in Europe.

When I was asked to take part in the parliamentary mission responsible for proposing a national strategy in

When it comes to quantum technologies, I quite naturally felt a great deal of emotion, firstly because France had decided to explore quantum technologies more actively and, secondly, because I was aware of the responsibility that such a stain.

As a scientist, my goal is to help create, through the progress of science, a better world for everyone, a more equitable, more ethical and more respectful world for the environment. To achieve this goal, it is important to join forces and create alliances with all partners at even to promote these transformations: the public sector, the private sector, the scientific community, industrialists, investors, the media, citizens and political decision-makers.

I am convinced that our recommendations are a first step towards the creation of a healthy and dynamic quantum ecosystem involving all stakeholders, which will make it possible to realize the disruptive potential of quantum technologies and to establish the leadership role of the France and the European Union in this area.

Glossary

QUBIT	**In quantum computing, a qubit or " *quantum bit* " is the smallest quantum information storage unit. It is the quantum analogue of the bit in classical computing.**
OVERLAY	**A classic bit is always either in the state or in the state. In the general case, a qubit is found in a superposition of these two states, which can be described by a linear combination of the two states: ÿ ÿ . The coefficients bibs and bibs being two complex numbers verifying the bibs relationship bibs**
INTRICATION	**Quantum entanglement, or quantum entanglement, is a phenomenon in which two particles (or groups of particles) form a linked system and exhibit quantum states that are dependent on each other regardless of the distance between them. Such a state is said to be "entangled" because there are correlations between the observed physical properties of these distinct particles. Thus, two entangled objects and are not independent even separated by a large distance, and it is necessary to consider like a unique system.**
NON-CLONING	**Another peculiarity of the qubit compared to a conventional bit is that it cannot be duplicated. Indeed, to duplicate it, it would be necessary to be able to measure the amplitudes fics and fics of the initial single qubit, while preserving its state, so as to prepare another qubit in ÿ ÿ . this is the same state fics ÿ doubly impossible because of the theorem of "non- cloning »**
NISQ	NISQ " ***Noisy Intermediate-Scale Quantum*** " **quantum computers have been available in Cloud access for a few years.** 50-100 ***qubit*** **quantum computers will be able to perform calculations that exceed the capabilities of today's conventional supercomputers. However, noise from quantum gates will limit the size of quantum circuits that can be reliably executed. The NISQ devices will explore many-body quantum physics and may have other useful applications, but the 100-qubit quantum computer wo *n't* change the world right away.**
LSQ	**LSQ "Large Scale Quantum" quantum computers are not expected before 2030. Thanks to a high number of *qubits* and a low noise level, these machines will exceed by several orders of magnitude, our current computing capacities thus representing challenges of major competitiveness *(eg* time to market) and sovereignty *(eg* intelligence and deterrence).**

Supremacy Quantum	**Quantum supremacy refers to a situation where a quantum computer can perform certain calculations inaccessible to current supercomputers in a humanly reasonable time.**
supercomputer	**A supercomputer is a computer designed to achieve the highest performance possible with the technologies available at the time of its design. The science of supercomputing is called "high-performance computing" or "intensive computing" (in English: *"High-Performance Computing"* or HPC). In 2019, supercomputer manufacturers are racing to reach "Exascale", computing power corresponding to one billion billion operations per second.**
Cryogenics and cryostats	**Cryogenics is the study and production of very low temperatures (below ÿ150°C) with the aim of understanding the physical phenomena that occur there. Cryogenics has many applications, particularly in the food, medical, industrial, physical and livestock sectors. Devices that achieve these temperatures are called Cryostats.**
fabless	**The term *fabless,* a contraction of the English words *fabrication* and *less,* refers to a company that designs its products and outsources all of its manufacturing. This model is mainly developed in the semiconductor sector.**
Post-quantum cryptography	**Post-quantum cryptography designates classical encryption mechanisms based on mathematical problems whose difficulty remains intact when faced with a quantum computer.**

Executive summary of the report

Technological background

If the first quantum revolution allowed the invention of the transistor, lasers and GPS, the second revolution in progress, fruit of the control of the phenomena of superposition and entanglement where the particles can take on several states at the same time or the same state in two different places, will exponentially increase our computing power, "teleport" information and perform measurements with unprecedented precision.

Challenges

ECONOMIC GROWTH

Several macroeconomic projections, over the next two decades, attribute to quantum technologies a significant potential contribution to GDP as well as to employment in developed countries. The proposed strategy is therefore in line with the full employment objectives of the "Productive Pact" announced by the President of the Republic on April 25, 2019. The expected benefits concern both the sectors that will industrialize these technologies (microelectronics, photonics, software, *etc.)* than those likely to exploit them, in the short, medium and long term and for which these technologies could induce a disruptive competitive differential (pharmacology, chemistry, materials, pharmacology, petroleum, aeronautics, cyber security, etc.) .

TECHNOLOGICAL SOVEREIGNTY

The evolution of the geopolitical context, as well as the rise of industrial power, which is particularly slow and difficult, encourage global high-tech industries to adopt silo strategies that weaken countries that do not master the entire technological value chain.
Not having its own technological capacities could thus, in the long term, pose difficulties in terms of supply for national needs, with economic and sovereignty impacts, as well as export barriers for industrial products.

Vision

The depth of the disruption that quantum technologies could induce in the coming decades is at least comparable to that resulting from the invention of the transistor in the middle of the 20th century . France, a pioneer in upstream research in quantum physics thanks, in particular, to the presence of several Nobel Prize winners as well as leading researchers, is currently lagging behind in terms of technological and industrial development.
The main major world powers, such as the United States, China, the United Kingdom or Germany, have set up ambitious global national programs in terms of quantum technologies.

By capitalizing on the excellence of its research fabric and its industrial precursors, France will be able, through an ambitious industrial and research policy, to develop a long-term vision coupled with an appropriate risk management strategy. Thus, France will confirm its place as a leading industrial power and European leader, by developing, before the end of the

decade, a world-class technological offer in terms of quantum technologies like what it has succeeded in developing for nuclear and aerospace.

ambitions

BECOME ONE OF THE WORLD LEADERS IN QUANTUM TOLERANT COMPUTERS FAULTS (LSQ)

The development of fault-tolerant quantum computers (LSQ) aims to make possible calculations and modeling several orders of magnitude more complex than what is possible today with traditional supercomputers. Developing LSQ machines requires making millions of good quality *qubits* . Silicon, one of the few materials that can eventually allow such a transition to scale, benefits in France from cutting-edge research and a solid industrial base in micro-electronics, despite a delay of a few years compared to - vis-à-vis other countries whose progress seems otherwise slow.

France could thus adopt the ambition of creating, before the end of the decade, the first European ***fabless*** company **offering silicon-based quantum processors in close association with its upstream value chain whose technological, industrial and geostrategic criticality will be major.**

BECOME THE EUROPEAN LEADER IN NOISE QUANTUM SIZE COMPUTERS INTERMEDIATE (NISQ)

Without waiting for the arrival of LSQ calculators, NISQ calculators could lead to disruptive uses in the shorter term in the chemical, logistics and artificial intelligence sectors.
By benefiting from the skills of its supercomputing manufacturers and various European startups that are developing NISQ processors, France could develop and distribute, from 2023, the first European quantum acceleration offer for the supercomputing market, in line with the European agenda on the acquisition of Exascale supercomputers.

BECOME ONE OF THE WORLD LEADERS IN BUSINESS SOFTWARE

Without software development tools specifically adapted to the very specific behavior of quantum processors, the use of quantum computing will find it difficult to establish itself in downstream sectors. Traditionally, the French software offer is characterized by its less generic positioning but with higher added value than what is developed across the Atlantic.
As the first developments of NISQ machines primarily impact specific businesses, France could capitalize on its algorithmic researchers and software manufacturers to position itself as a world-class player in business software using quantum computing by offering, from 2023, with the support of Germany, the first "turnkey" business quantum software offer for the fields of chemistry, pharmacology, advanced materials, logistics and AI learning.

ENJOY BROAD INDUSTRIAL AUTONOMY ON ENABLING TECHNOLOGIES

The enabling technologies for quantum computing (cryogenics, ultra-high vacuum, lasers, wiring, *etc.)* are a prerequisite for the development of the various quantum technologies and call for particularly rare and cutting-edge know-how. They are thus very sensitive to the risk of embargo on the part of the countries that control them.
With the exception of a few limited cases, French players in quantum technologies are currently sourcing from abroad.
France could aim to become, before the end of the decade, one of the world's leading suppliers of enabling technologies for quantum computing, in particular for cryogenics and lasers.

Due to their performance and complexity, these technologies can naturally find outlets in other highly technological sectors.

ENJOY WIDE INDUSTRIAL AUTONOMY ON IMPURITY-BASED SENSORS IN THE DIAMOND

Quantum sensors based on impurities in diamond have the advantage of being able to scale up easily to an industrial scale.
On the strength of its industrial players positioned downstream in the value chain, France could aim, by taking advantage on the one hand of the withdrawal of certain historical foreign players, and on the other of the skills and know-how of its laboratories to become a leading global supplier of diamonds for impurity-in-diamond sensors by 2026, and thus cover the entire industrial value chain of quantum sensors.

MAINTAINING STRATEGIC INDEPENDENCE ON CRYPTOGRAPHY TECHNOLOGIES

The possible advent of sufficiently powerful quantum computers (LSQ) to break current encryption schemes *(eg* RSA), even if this will only happen in the relatively long term, calls for immediate action in terms of securing sensitive communications.
With a community of world-class cryptographers and leading security manufacturers, France could aim to develop, as early as 2022, the first post-quantum cryptography offer for high-performance security devices with resources of limited computing (cryptographic modules, smart cards, routers *etc.).*
In the longer term, France could consider proposing, within 5 years, the first quantum encryption key distribution solution, deployable at marginal infrastructure cost and resistant to side channel and denial of service attacks.

Mission recommendations

A CUTTING-EDGE INFRASTRUCTURE FOR RESEARCH AND INDUSTRY

The establishment, on French soil, of a world-class infrastructure, integrating various quantum emulators and accelerators based on various technological principles, will represent a strong lever for action making it possible to develop the software ecosystem and the uses and develop the legitimacy and influence of France internationally; A
rapprochement with Germany could make it possible to develop a common offer and a common portal allowing access to all European quantum computing technologies.

A TECHNOLOGICAL DEVELOPMENT SUPPORT PROGRAM

With research and technological development programs bringing together public and private players by combining " ***top-down*** **" and "** ***bottom-up*** **" approaches , France will provide itself with the necessary means to remove the various scientific and technological obstacles punctuating the development of the quantum computers, as well as cryptographic devices needed to secure sensitive communications in the quantum era.**
In terms of " ***bottom-up*** **" systems, France could strengthen existing systems and include priorities on quantum technologies: calls for ANR projects, innovation competitions, PSPC (Structuring Projects for Competitiveness),** ***etc.***
In terms of " ***top-down*** **" devices, the Grands-Défis as well as actions of the Future Investment Plan will make it possible to achieve French ambitions in terms of quantum computers, software and cryogenics.**

A SUPPORT PROGRAM FOR THE DEVELOPMENT OF USES

"Quantum challenges" associating sectors of use and technological sectors, both in the field of quantum computing and in the field of quantum sensors will make it possible to strengthen the competitiveness of downstream sectors while securing short-term outlets for technological sectors.

AN EFFECTIVE INNOVATION ENVIRONMENT

The creation of three ***"Quantum Hubs"*** **will be a decisive lever for the interdisciplinary mixing necessary to lift the locks marking out the objectives of the national strategy. The development of skills and access to risk capital will make it possible to remove the obstacles to innovation and the creation of start-ups, an essential vector for the transfer of technologies to the economic fabric.**

AN ADAPTED ECONOMIC SECURITY STRATEGY

France's position in terms of quantum technologies encourages certain organizations or States to take an interest in the French ecosystem and to target the most vulnerable players, at the forefront at the global level. The protection of scientific and technological heritage and economic diplomacy will be the pillars of an effective economic intelligence strategy.

EFFECTIVE GOVERNANCE

Given the high level of uncertainty relating to certain paths of development of quantum technologies, the long time horizons of the actions to be taken and the capital intensity required, the State will need agile governance endowed with power. decision-making.

List of 37 proposals

Transversal proposals

Proposal 5	*Renew, from 2021, the calls for projects (AAPR) of the "Quantum Technologies" axis of the National Research Agency (ANR) aimed at funding twenty exploratory projects annually for an overall annual envelope of €10 million.*
Proposal 6	*Reinforce the "Quantum Technologies" axis of the ANR with a specific annual envelope aimed at financing three exploratory projects targeting the priority technological paths identified.*
Proposal 7	*Encourage French laboratories and companies to respond to European Flagship "Quantum Technologies" calls for projects.*
Proposition 8	*Include a priority on quantum technologies in future PSPC calls and Innovation Competitions.*
Proposal 26	*Create, in Paris, Saclay and Grenoble, three "Quantum Hubs" bringing together researchers in quantum physics, researchers in theoretical and applied computer science, engineers, industrialists from technological sectors, and end users.*
Proposal 27	*Include an evaluation criterion relating to interdisciplinarity in calls for collaborative projects by the ANR and the BPI.*
Proposal 28	*Include 6 ECTS of quantum algorithms in the twenty main engineering cycles in computer science and 6 ECTS of post-quantum and quantum cryptography in the cryptography masters.*
Proposition 29	*Design training courses with a specialization in engineering and quantum computing and anticipate the growing need for engineers and technicians in industrial sectors.*
Proposition 30	*Raise awareness among ecosystem players of the new provisions of the PACTE law relating to the mobility of researchers and access to laboratory resources by start-ups.*
Proposal 31	*Support the creation of around fifty quantum startups until 2024.*
Proposal 32	*Create a trustworthy "late-stage" investment fund of €300-500 million dedicated to quantum startups.*
Proposition 33	*Raise awareness among the various most strategic players of the risks of technological looting and of the tools available to deal with them.*

Proposition 34	*Identify and monitor strategic assets and activities and deploy, if necessary, the Scientific and Technological Potential Protection system (PPST).*
Proposition 35	*Identify areas of cooperation and possible synergies with France's international partners in the field of quantum technologies.*
Proposal 36	*Set up a Strategic Committee responsible for taking decisions on the orientation of research actions.*
Proposition 37	*Appoint an interministerial coordinator of the national plan, responsible for ensuring the overall consistency of the actions of the various public and private actors at the national level.*

Proposals relating to quantum computing

Proposal 1	*Hosting, at the "Very Large Computing Center" (TGCC), a diversified, scalable and accessible Quantum Computing platform for communities of researchers and academic and industrial developers.*
Proposal 2	*Open a permanent call for contributions to French and European startups and laboratories developing quantum acceleration processors for integration into the computing infrastructure.*
Proposal 3	*Develop a competitive public-private QCaaS or "Quantum Computing as a Service" offer.*
Proposition 9	*Reinforce the Grenoble microelectronics teams with skills in computing software and architectures.*
Proposal 10	*Deploy agile project management to gradually reduce uncertainty and costs throughout the project.*
Proposition 11	*Deploy, through an action of the PIA and the PPR, an R&D-Capitalization program aimed at developing scalable quantum accelerators.*
Proposal 12	*Support, through the AAPRs of the ANR's "Quantum Technologies" axis, a research program aimed at exploring bold silicon avenues*
Proposal 13	*Set up, in 2019, a Great Innovation Challenge "NISQ" aimed at developing, before 2023, an interoperable business software stack for the chemical, logistics and AI sectors.*
Proposal 14	*Include the Grand Challenge in a framework of bilateral collaborations with other European countries.*

Proposition 15	*Strengthen research resources in algorithms and software in the field of quantum computing.*
Proposal 16	*Set up, in 2022, an Innovation Grand Challenge aimed at developing a complete quantum computing solution, subject to convincing intermediate results for the "NISQ" Grand Challenge and for the PIA "quantum accelerators" action.*
Proposition 17	*Include specifications for the acquisition of experimental quantum accelerators in certain GENCI calls for tenders relating to the acquisition, renewal and extension of the French supercomputer fleet.*
Proposal 24	*Disseminate the use of quantum computing, through "Challenges" and "Hackathons" proposed by manufacturers in the most advanced application sectors. The "Airbus Quantum Computing Challenge" could be taken as a model.*

Proposals for quantum sensors

Proposition 18	*Structuring, through a succession of i-Lab, i-Nov and PSPC-Region projects, an industrial value chain for the production of sensors based on diamond impurities.*
Proposition 25	*Accompany, through "Challenges" proposed by the application sectors, the manufacturers of quantum sensors in the search for outlets with the application sectors.*

Proposals relating to post-quantum and quantum cryptography

Proposal 4	***Deploy a test platform for different quantum communications devices.***
Proposition 19	***Support, through the i-Nov competitions and the innovation support and acceleration mechanisms of the ministries concerned, the development, before 2022, of a competitive post-quantum cryptography offer for systems with limited computing resources.***
Proposal 20	***Develop an evaluation strategy for QKD systems based on the French and European certification scheme.***
Proposition 21	***Support, through the AAPRs of the "Quantum Technologies" axis of the ANR, a research action relating to the maturation of QKD technology (systems with continuous variables and discrete variables, quantum relays, satellite links, etc.) involving quantum communications experts, cyber security experts and telecom equipment manufacturers.***

Enabling Technology Proposals

Proposal 22	***Support, through i-Lab competitions, i-Nov competitions and PSPC projects, the development of a competitive French offer in the field of compact ultra-high vacuum and cryogenics for temperatures from 1 to 40 K.***
Proposition 23	***Support, through i-Lab competitions, i-Nov competitions, PSPC projects and the innovation support and acceleration mechanisms of the ministries concerned, or a PIA action, the development of an offer competitive French company in terms of extreme cryogenics for sub-K temperatures.***

Contents

I. Introduction to quantum technologies

I.1 Quantum Computing

In the 1980s, Richard Feynman, one of the most influential physicists of the second half of the 20th century and Nobel laureate in physics, laid the foundations for a new computational paradigm based on the amazing properties of quantum physics that are entanglement and superimposition. He then proposed quantum computing as a means of simplifying chemical modeling calculations at the atomic and molecular scale.

To date, quantum computing represents the only known computational model capable of freeing us from the slowdown of Moore's law and of offering an exponential acceleration, economically tenable, compared to conventional computers and supercomputers.

Interest in this field increased in the 1990s with the introduction of *Shor's algorithm,* which showed that a quantum computer would exponentially speed up the solving of an important class of cryptanalysis problems. potentially threatening the main asymmetric encryption methods used to protect communications. This period is also characterized by the discovery of ***Grover*** **'s algorithm which, if implemented, could quadratically speed up the search, in an unordered list, for a specific element.**

Cryptanalysis is the study of ciphertexts and cipher systems with the aim of understanding how they work and identifying and improving techniques for deciphering them.

These accelerations result from the capacity of quantum computers to carry out several calculations simultaneously. The basic unit of classical computers is the *bit,* which can only take one state at a time, 0 or 1, whereas quantum ***bits* , or *qubits,* basic units of quantum computers can be in both in state 0 and 1. The concept that qubits *can* exist in multiple states at the same time is called superposition, which means that something can be "here" and "there" or "up" and "down " simultaneously. The concept according to which two *qubits* can have correlated states is called entanglement: knowing the state of one makes it possible to know the state of the other even if it is geographically far from it. Superposition allows a *qubit* to encode several pieces of information in parallel, while entanglement makes it possible, using logic gates, to make qubits interact *with* each other and process information simultaneously. Although confusing, these principles allow 2 *qubits* to represent the equivalent of 4 *bits,* 3 *qubits* the equivalent of 8 *bits,* and n *qubits* the equivalent of 2n *bits* at the same time. The calculation parallelization capabilities of a quantum computer therefore increase exponentially with the number of *qubits,* allowing quantum computers to perform calculation operations that are physically inaccessible to the most powerful of supercomputers.**

Intel co-founder Gordon Moore claimed in 1965 that the number of transistors per circuit of the same size would double, at constant prices, every eighteen months. He deduced that the power of computers would grow exponentially, and this for years. His law, based on empirical observation, has been verified until today.
In 1997, He predicted that this growth would come up against around 2020 at the limit the size of atoms.

Nevertheless, the effective exploitation of this power is not trivial and requires the development of new algorithmic methods and development tools.

Long confined to the sphere of theoretical computing, the first functional quantum computers could not be developed and built until 30 years after Feynman's proposal. Today, the number of companies building quantum computers based on different technologies and materials is constantly growing. It is worth mentioning: D WAVE, IBM, RIGETTI, Google, IonQ, PASQAL (France), PsiQuantum, Honeywell, *etc.*

The production of *qubits* is based either on physical systems such as atoms, photons and ions, or on artificial systems based on supra and semiconductors (see Figure 1).

These so-called "physical" *qubits* are vulnerable to noise. **To create fault-tolerant *qubits* ,** also called logic ***qubits* , behaving exactly like their mathematical models, it is necessary to use error correction and fault-tolerance methods, which use several** physical ***qubits* to create a logic *qubit* .**

A quantum computer can be emulated without providing any tangible speed-up on a conventional computer, for which the number of (logical) *qubits* to be emulated is limited by the computer's memory. The largest emulation to date required a supercomputer with several petabytes of memory to represent 46 *qubits (Jülich).* On a corporate server, the record is 41 *qubits* (Atos QLM).
A true quantum computer of 50 *qubits* would make it possible to carry out in a reasonable time calculations requiring thousands of years on a supercomputer. **This threshold of 50 *qubits* corresponds roughly to that of "quantum supremacy".**
From a few hundred *qubits,* several practical applications could be envisaged: predicting the interactions between a protein and a new drug, predicting the macroscopic properties of a new material, *etc.*

This results in two main types of quantum computers :

- **A "universal" quantum computer of significant power called "LSQ" for " *Large Scale Quantum* " which would be composed of thousands of logical *qubits*** and would have the possibility of carrying out any type of quantum calculation. **This type of calculator would exponentially outperform the most powerful of today's supercomputers for a large number of applications. The first "LSQ" calculators are not expected before 2030.**
- **A "noisy" quantum computer of intermediate size called "NISQ" for " *Noisy Intermediate Scale Quantum* ", which would, *on the contrary,* be composed of a few hundred** physical ***qubits* allowing a certain number of specific calculations to be carried out. This type of calculator was born a few years ago in machines developed, in particular, by IBM, Google, and RIGETTI with a few dozen qubits .**

Despite its promise of unequaled computing power, a quantum computer is not intended to replace a conventional computer or even a supercomputer because it only presents an advantage for certain problems. The quantum computer must be seen as a " *Quantum Processing Unit* " or *QPU1* coprocessor **which will accelerate certain very specific calculations in the same way as a *GPU* (graphics processor) or an *NPU* (IA processor).**
On the other hand, for this type of calculation, the time saved will be exponential (going from several thousands of years to a few hours), making certain calculations accessible that cannot be carried out in practice to date: simulating the folding of a protein, designing a catalyst for the manufacture of nitrogenous fertilizers at low temperature, designing a catalyst to store CO2 , simulating complex systems (climate, meteorology, aviation), factoring large numbers, *etc.*

1 It is also called a quantum accelerator

	supra-conducteurs	Si spin CMOS	ions piégés Yt ou Ca	photons	impuretés diamants	fermions de Majorana	atomes froids
qubits	supraconducteurs + effet Josephson	spin d'électrons dans semi-conducteur	ions piégés magnéti-quement	photons	spin d'électron dans cavité diamant + azote	quasi-particules faites de paires d'anyons	niveau d'énergie de la cavité
état	phase de résonnance ou sens du courant	spins d'électrons	niveau énergétique de l'ion piégé	polarisation, temps, espace, couleur	niveau d'énergie de la cavité	sens de l'anyon	niveau orbital d'électron
portes	micro-ondes 5 GHz et effet Josephson	micro-ondes	laser	interférence quantique	laser	inversions 2D d'anyons	micro-ondes, émission de photons
mesure	magnétomètre	consersion spins to charge	fluorescence	détecteur de photons	fluorescence	fusion d'anyons	ionisation et recueil d'électron
# max de qubits	53 qubits (IBM et Google)	49 qubits (Intel)	79 (IonQ)	20 (Chine)	6 qubits (QDTI)	0	<20

en rouge : chipsets non caractérisés et benchmarkés.

source : Olivier Ezratty, « Comprendre l'informatique quantique »

Figure 1: overview of qubit manufacturing technologies - credit: O. Ezratty

I.2 Quantum sensors By exploiting

the extreme sensitivity of quantum states, quantum sensors achieve unparalleled measurement precision. These sensors exploit the entanglement properties of quantum objects (atoms, molecules, photons, *etc.)* to improve the sensitivity, reproducibility and accuracy of measurements.

It is necessary to distinguish two main categories of quantum sensors whose maturity allows applications today or in the short term:

- **Atoms and ions cooled by laser: this technology makes it possible to prepare a quantum system with almost ideal properties for different types of precision measurement. In particular, it makes it possible to carry out very high performance inertial measurements, and is of great interest for the development of a new generation of gravimeters, gravity gradiometers, accelerometers and gyroscopes as well as for ultimate time-frequency measurements allowing have clocks of remarkable stability.**

- **Impurities in the diamond: this technology has several intrinsic advantages related on the one hand to performance (consistency, resolution, sensitivity) and on the other hand to ease of implementation (solid state, operation at room temperature, handling while optical).**

A 3rd way, quantum illumination, which aims to exploit the entanglement of pairs of photons to improve the performance of detection or active imaging of objects at a distance, is also the subject of research but its level of maturity more low, at the concept stage or the first laboratory experiments, does not allow considering industrial applications in the short term.

I.3 Quantum and Post-Quantum Cryptography

Quantum communications are technologies exploiting the properties of entanglement and non-cloning and aim to reinforce the security or the efficiency of te

Quantum key distribution, often abbreviated as *QKD* for *"quantum key distribution",* is a communication method that implements a classic symmetric cryptography protocol but exploits the properties of entanglement and non-cloning. It allows two individuals to produce a random secret key shared by a quantum channel, known only to them and which can then be used to encrypt and decrypt messages using traditional channels, thus ensuring their integrity and preventing their modification. by a third party *(cf.*

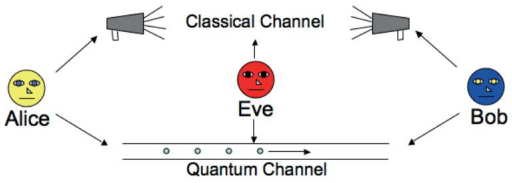

Figure 2: Principle of quantum key distribution

Figure 2). Quantum key distribution makes it possible to ensure, under certain implementation assumptions, that the common key obtained could not be intercepted, which is almost impossible to guarantee in classical cryptography. The originality of this technology is that this assurance does not depend on the computing power or the mathematical know-how of an attacker, contrary to what happens in traditional cryptography.
On the other hand, it is based on the postulates of quantum mechanics (non-cloning theorem, uncertainty principle), and on the quality of its practical realization. QKD is sometimes presented as made necessary by the advent of the quantum computer, in the

in the sense that it makes it possible to replace classical cryptography primitives which are threatened by quantum computers.

Post-quantum cryptography is another possible response to the cryptanalysis (decryption of an encrypted message) capabilities of a quantum computer. This term refers to classical asymmetric encryption mechanisms based on mathematical problems whose difficulty remains intact when faced with a quantum computer.

International competitions, under the aegis of the *"National Institute of Standards and Technology"* (NIST), the main standards body in the United States, are currently in the process of identifying such mechanisms, and standardizing the most promising. This approach is similar to that which standardized the encryption algorithms based on the discrete logarithm and the factorization used today2.

In symmetric cryptography, the sender and the receiver of the message share the same key to encrypt and decrypt the information. The problem with this cipher is that it requires a secure means of transmitting the key but is currently the most secure means of encryption.
Asymmetric encryption relies on two keys. Anyone can encode with the first (public) key, but only the receiver can decode with the second (private) key. The private key is never transmitted.
The security of asymmetric encryption is based on the difficulty of solving certain mathematical problems (factorization of prime numbers, elliptic curves, *etc.)*

I.4 Global ecosystems

With an ecosystem already structured around 40 startups, 50 venture capital funds, 4 large technology companies (Google, IBM, Intel, Microsoft) and 3 government agencies operating $1.3 billion in public money, the USA has a significant lead over other countries.

Across the Rhine, Germany has a 5-year national program with a budget of 650M€.

Across the Channel, the United Kingdom is devoting £270 million to its "Quantum Technologies" industrial program.

On the strength of its pioneering scientific discoveries, France also has several assets to become a serious industrial competitor in IT, in particular thanks to its positioning :

- **its public research organizations, CNRS, CEA, and INRIA on various quantum technologies, which at this stage of maturity offers appropriate risk management,**

- **its large industrial groups that use intensive computing, such as Total, Airbus and Edf, which provide concrete problems that can benefit from quantum acceleration, - its large** industrial **groups that are pioneers in the use of quantum technologies which infuse a strong dynamism in the French ecosystem, such as Thalès and Atos, - its major industrial groups established in the technological field and which have the potential to exploit and support quantum innovations, such as SOITEC, STMicrolectronics, Air Liquide, Orano, etc. - several startups that are already using quantum image technologies**

by Pasqal, Muquans, Quandela and VeriQloud,

- the " ***Quantonation*** " **venture capital fund specializing in quantum technologies.**

2 These two classes of algorithms are today known to be vulnerable to quantum cryptanalysis

II. Challenges of quantum technologies

II.1 Quantum Computing

Issue 1 **Distribute, as of today, the use of quantum computing in priority application sectors (chemistry, logistics, artificial intelligence, etc.) in order to anticipate the breakthrough that this technology will eventually bring in terms of marketing**

In recent years, noisy machines of intermediate size or " *NISQ* " for " *Noisy Intermediate-Scale Quantum* " and commercially exploitable quantum simulators (analog machines specialized in the simulation of molecular chemistry) have become a reality. These machines are, as of today, tools for learning quantum computing. Seizing, as of today, learning tools for quantum computing, will confer, in the medium term, a strategic advantage to industrial players in several fields: pharmacology, advanced materials, fertilizers, catalysts, logistics, finance, *etc.*

Main short-term applications of Quantum Computing

ÿ **Chemistry :**

Quantum Computing could allow the quantum simulation of molecular chemistry, which made it possible to develop new chemical processes with substantial efficiency gains: the development of a new catalyst for the manufacture of fertilizers could potentially make it possible to reduce 5% of global energy consumption.

ÿ **Materials Science :** Quantum

Computing could be used to analyze complex physico-chemical interactions, allowing faster discovery of new disruptive materials in several economic sectors. The creation of **patentable materials** is a **potential source of significant profits** for early end users in key industries. ÿ **Personalized medicine:**

Quantum Computing could be used to model chemical reactions at the molecular level to more accurately predict **protein-drug interaction,** leading to **new pharmaceutical methodologies** that would speed the time-to-market of new personalized drugs. ÿ **Biology:**

Quantum Computing could be used for the simulation of processes such as photosynthesis or for the modeling of energy systems. It would accelerate the development of **new fertilizers** or the improvement of existing fertilizers, thereby helping to improve global food sources.

ÿ **Optimization and logistics**

Quantum Computing would make it possible to speed up the resolution of complex optimization problems, in particular for energy distribution, traffic control and re-routing, and task planning. ÿ **Learning for Artificial Intelligence :** Quantum Computing could

significantly accelerate **learning from complex differential models :** aeronautics, energy systems, etc.

Issue 2 Guard against excessive dependence on a single player and on a single technological path

Experts believe that 200 physical ***qubits*** **is the threshold at which NISQ machines will take advantage of traditional chemical modeling techniques. However, very highly integrated ecosystems are being formed, today, around machines of 50** physical ***qubits*** **which, although they do not confer a proven quantum advantage, make it possible to anticipate future disruptions and federate and retain an ecosystem. developers around *Hardware-dependent*** development tools **(depending on the hardware).**

The quantum advantage refers to the situation in which the use of quantum processors provides, compared to a conventional solution, for a given application, an economic advantage in terms of cost, computing time, energy consumption, *etc.*

Today, these vertical integration strategies constitute a brake on the adoption of quantum computing by downstream sectors which fear the risk of dependence on a technological path that does not succeed in the long term. This challenge is accompanied by an opportunity to develop predictive models that can extrapolate the results of different technological approaches and predict their performance in advance.

Challenge 3 Guarantee, in the future, a capacity for the development and supply of "LSQ" computers

Beyond the "NISQ" machines, the prospects of an error-corrected quantum computer "LSQ" or " *Large Scale Quantum* " promise :

- **a qualitative leap of several orders of magnitude in the various fields mentioned more high ;**
- **risks of compromise on all the information encrypted today by asymmetric cryptography ;**
- **still unsuspected uses with the discovery of new algorithms that can take concrete advantage of these machines.**

Given the dual nature linked in particular to the cryptanalysis applications permitted by the “LSQ” machines, the very exclusive club of countries equipped with the technology could decide to prohibit the export of the most efficient machines. Such technological retention would offer these countries gains of several points in their trade balance and GDP, while the rest of the world would be under the threat of a generalized compromise of its communications with the obligation to deploy in the urgency for more secure means of encryption.

The trajectory leading to the "LSQ" machines is much more uncertain than for the "NISQ" machines, in particular because of the extreme conditions in which these machines operate: it is necessary, in fact, to fight against the natural tendency of quantum objects to be disturbed by their environment.

Three scenarios could then be envisaged : - An unexpected discovery could occur at any time in little explored ways, like the “topological” approaches defended mainly by Microsoft and Nokia ;

- **“LSQ” machines arise over the next two decades thanks to advances in technologies known to be “scalable” ;**
- **The “LSQ” machines never see the light of day.**

The first two scenarios raise the same issues of building an industrial ecosystem as in the case of the NISQs, with in particular the need to have appropriate industrial and supply strategies allowing France to guarantee its strategic interests.

In the event that the "LSQ" calculators never see the light of day, the effort made would not be in vain. The obstacles lifted will have created positive externalities irrigating several French technological sectors (microelectronics, photonics, industrial vacuum and cold, wiring, industrial gases, *etc.).* By way of illustration, it should be remembered that the efforts made to produce the Concorde ultimately made it possible to develop the technologies of the current Airbus airliners. The ITER nuclear fusion project is another illustration, which, although to date not yet operational, has made it possible to remove obstacles in several technological sectors whose impacts are already palpable (eg electromagnets, superconductors , materials etc.).

On September 20, 2019, the *Financial Times* claimed that Google had achieved "quantum supremacy": performing, in a few minutes, a calculation that would have taken 10,000 years on a supercomp If the information is confirmed, it will be a big step towards "LSQ" machines.

Furthermore, research on quantum computers has already had a significant impact on classical computing, where the concepts and techniques developed have made it possible to invent new classical algorithms in the fields of chemistry, logistics and IA, or to develop new specialized calculation processors, particularly in combinatorial optimization *(ie* the *"Digital Annealer "3* from *Fujitsu).*

[3] ***"Digital Annealer* ", whose design is "inspired by quantum phenomena" according to its designers, is a classic computing chip which claims to be a direct competitor of the D-Wave processing unit, and aims in the same way solve combinatorial optimization problems.**

II.2 Quantum Sensors

Issue 4 Ensure an operational capacity to supply quantum sensor technologies

Quantum sensors have several promising applications in the defense field: navigation, interception, detection, seismography, etc.
Due to their dual nature, they could eventually be subject to the same export constraints as quantum computers.

Main Defense Applications of Quantum Sensors

ÿ **Browsing :**

Embedded accelerometers, magnetometers and quantum gravimeters could address the reliance of critical navigation systems on GPS system satellite signals, which can be jammed or spoofed by an attacker, rendering navigation systems unusable. An airplane could make a transoceanic flight and arrive at its destination with an accuracy of a few meters without using the GPS signal.

Quantum navigation sensors precisely measure the variations of certain physical properties of the terrestrial globe (electromagnetic fields, gravitational fields, *etc.)* for which a very high definition cartography is available, thus allowing them to position themselves precisely without having recourse to elements. external as satellites.
Navigation sensors can be based either on the atoms cooled by laser, or on the impurities in the diamond *(cf.* I.2). ÿ **Electromagnetic**

interception : Sensors based on impurities in

diamond *(see* I.2) could make it possible to carry out spectral analyzes of electromagnetic signals several orders of magnitude finer than current technologies. In a context of electronic warfare and listening to radiofrequency signals, these devices could increase the performance of interception systems.

ÿ **Remote sensing :**

Quantum radar is an emerging remote sensing technology based on quantum illumination *(see* I.2). If successfully developed, it will detect stealth aircraft, filter out deliberate jamming attempts, and work in areas with high background noise.

Issue 5 Ensure the long-term economic viability of quantum sensor technologies developed in France

Among the different families of quantum technologies, quantum sensors have the greatest technological maturity, but suffer from difficulties in being industrialized in civilian application sectors. The complexity of their implementation and the extreme environment often necessary for their operation today limit outlets to very specific markets, which compromises the long-term viability of the companies that produce them. The defense sector alone will not be able to ensure the economic viability of the companies that develop them.

In civil applications, quantum sensors, even if they promise increased performance or functionality, are in competition with "classical" sensors, whose performance is constantly increasing, either intrinsically or through networking and advances in data processing.

II.3 Quantum and Post-Quantum Cryptography

Issue 6 Guarantee, even in the remote event of the advent of a sufficiently efficient quantum computer, retroactive integrity over 50 years of communications and sensitive information.

Although it is unlikely in the short term, the advent after 2030 of an "LSQ" machine, capable of decrypting data protected by public key algorithms, is not excluded. To deal with this risk, the priority of the French authorities is to guarantee the integrity of the State's information and communications systems retroactively, by :

ANSSI is now able to label security solutions including “hybrid” cryptography mechanisms combining a proven asymmetric mechanism and a new asymmetric mechanism offering a perspective of post-quantum resistance.

- **developing and deploying asymmetric cryptographic schemes, belonging to “post quantum cryptography”, resistant to quantum cryptanalysis. These cryptography schemes can be added to the current schemes without replacing them, in a hybrid system. Such a system, combining the security of a current mechanism and a post-quantum mechanism, makes it possible to guard against any risk of regression in the face of classical cryptanalysis, caused by the introduction of new and still incompletely studied algorithms.**

- **deploying, in suitable contexts, classic symmetric cryptography schemes with appropriate key sizes, on which an “LSQ” machine has no known impact for the most sensitive communications.**

Issue 7 Protect against the introduction, in the infrastructures of communication, of quantum cryptography components mastered only by non-European players.

Although post-quantum asymmetric cryptography and symmetric cryptography provide, in the opinion of the competent authorities, a ***priori*** sufficient **guarantees vis-à-vis quantum cryptanalysis, disengaging from research in quantum communications could be perilous. .**

Indeed, there is a worldwide craze for the deployment of quantum cryptography in addition to post-quantum schemes4. We could therefore find ourselves, in fact, with components of quantum cryptography in the global internet networks. Three scenarios can therefore be envisaged :

- **France is developing, with the help of French manufacturers, its own operational QKD solution, certified by ANSSI. The risk of loss of sovereignty would be negligible and the industrialists involved could have interesting export outlets for the technologies developed.**

- **France ensures that a European QKD solution emerges with a limited French contribution. The risk of sovereignty, shifted to the European level, remains limited.**

4 Quantum cryptanalysis is a relatively new field studied by a small community of researchers. The post-quantum cryptographic primitives considered to date could be vulnerable to new classes of quantum algorithms.

- **France is divesting itself of the subject, and solutions developed outside Europe are becoming the de facto standard. In this case, components not mastered in Europe are introduced into the communications infrastructure5.**

5 This scenario is particularly critical, especially since the current deployment of 5G illustrates, as of today, the risks in terms of the possibility of compromise of the core network, of a loss of know-how in Europe.

III. Obstacles to the development of quantum technologies

III.1 Technological obstacles

III.1.1 Quantum calculation

Obstacle 1 The development of an “LSQ” computer requires a technology for manufacturing qubits with low variability.

For a system with a large number of *qubits,* the dimensions, the surface qualities, the purity of the materials and other physico-chemical parameters must have a sufficient level of reproducibility for two *qubits* to behave nominally identically. The ***qubits*** **' domains of operation are outside the usual scope of mass production technologies. A significant technological effort will be required to move to large-volume *qubit*** production.

Obstacle 2 An “LSQ” computer requires, beyond the hardware aspect, the development of high-performance error correction codes.

With the exception of the “topological” path explored in particular by Microsoft and Nokia, *qubits,* all technologies combined, do not have the intrinsic capacity to reject external disturbances which can distort the results of calculations. The rejection of these disturbances is carried out by special low-level algorithms called “error correction codes”. The increase in the number of *qubits,* all technologies combined, also increases their sensitivity to noise, further complicating the realization of efficient error-correcting codes6.

Conceptually, error correction consists of entangling a large number of physical ***qubits*** **so that the disturbance of one marginally influences the state of the others. The performance of error-correcting codes is measured by the minimum number of physical *qubits*** needed to create a **logical *qubit* . The ratio depends on the quality of the** physical ***qubits*** **and is currently several thousand. For a practical realization of an "LSQ" calculator, it will be necessary to reduce this ratio.**

Lock 3 The most efficient qubit technologies are difficult to scale and the most scalable technologies display noise levels that are too high to allow effective implementation of error-correcting codes.

However, the production of "LSQ" computers will continue to require a large number of physical ***qubits* , which presupposes an ability to manufacture them using existing industrial processes or to create new industrial tools that will have to be amortized.**
However, the technological paths capable of scaling up thanks to an already amortized industrial tool, like silicon, suffer from a low level of maturity because they started later than the approaches that could be explored with laboratory techniques. To date, this path displays noise levels that are too high () for an effective implementation of error-correcting codes. Ideally, the noise level should be improved to reach . The most advanced technological pathways, such as superconducting, also suffer from a high level of noise and seem to struggle to scale beyond a few tens of qubits .

6 INRIA is one of the world's specialists in error correction.

Lock 4 The more a qubit technology is robust to external disturbances, the more difficult it is to create logic gates and vice versa.

Another obstacle to the realization of "LSQ" machines lies in the fact that the sensitivity to external disturbances and the quality of the logic gates are actually two manifestations of the entanglement phenomenon (cf. I.1) *which* characterizes the ability to a *qubit* to interact with its neighbor.
The improvement in the quality of the logic gates is systematically accompanied by a deterioration in the rejection of external disturbances and vice versa. There is therefore a compromise to be found between the speed of manipulation and the duration of preservation of the quantum information.

To date, only the technological path of topological *qubits* claims the ability to overcome the noise problem.

The feasibility of topological *qubits* has not yet been demonstrated.

This lock, known as "decoherence", is generally little addressed by the marketing communications of technology companies which only announce the number of *qubits,* more laudatory, without addressing the subject of the quality of these *qubits :* their sensitivity to noise compared to the quality of their logic gates. Removing this lock will require work on improving the trade-off between qubit manipulation capability *and* decoherence, in order to increase the number of operations that can be performed before quantum information is lost.

Barrier 5 The absence of a known protocol allowing an efficient transfer of massive data to a quantum computer is hampering the breakthrough of quantum accelerators, including NISQ, in the field of High Performance Computing (HPC).

Although a quantum computer derives its power from its ability to use a small number of *qubits* to represent an exponentially larger amount of data, there is currently no known method to efficiently transcribe a large set of classical data into a single quantum state.

As a result, for problems that require large amounts of input data, the time required to initialize the quantum computer becomes preponderant over the computation time, thus reducing the quantum advantage. This limit opens the way to innovations in terms of protocols and interfaces between the software and the hardware implementation.

Obstacle 6 The lack of development tools and standards of efficient and interoperable programming hinders adoption by the application sectors.

Quantum algorithms constitute an important programming paradigm shift compared to classical algorithms. Indeed, the “non-cloning” properties of quantum states prevent any possibility of reading quantum information more than once, without forgetting that quantum information “collapses” into a classical state as soon as it is read. Because of this property, basic classical operations such as “iteration loops”, “intermediate results”, “copies”, “breakpoints”, or even “step executions” n make more sense in quantum algorithms.

Exploiting the power of quantum computing will therefore require rethinking algorithmic development paradigms and methods. New software stacks, programming languages, and development environments will have to be developed. Several initiatives are beginning to address this subject, such as

the quantum emulation environment of Atos *QLM* based on the *AQASM* language or the integration of the *Q#* language into *Visual Studio* by Microsoft.

In general, lifting the various locks related to quantum computing will require the support of several areas of expertise such as theoretical computer science, quantum physics, system engineering, process engineering, materials and control-command.

III.1.2 Quantum sensors

Lock 7 Quantum sensors must be integrated into systems where their added value compared to conventional sensors is tangible.

Due to their maturity, the main technological locks related to quantum sensors as components have been removed. The remaining technological obstacles are at the level of integration into existing systems with a view to fulfilling a metrological function: replacing a set of antennas with a single sensor based on diamond impurities for electromagnetic detection needs, developing a geolocation system without GPS based on cold atom sensors, *etc.*

III.1.3 Quantum and Post-Quantum Cryptography

III.1.3.1 Post-Quantum Cryptography

Traditionally, trust in cryptographic schemes increases over time: the fewer attacks on a scheme, the greater the trust placed in it.
Some post-quantum schemes, which have been around for some time, are well accepted and considered mature enough to deploy.

Lock 8 In the absence of sufficiently powerful quantum computers, the confidence in post-quantum schemes can only be established on the basis of a theoretical model of the quantum computer.

Post-quantum algorithms also need to be evaluated against an attack using quantum computers. However, there is, to date, no quantum computer powerful enough for practical analysis of quantum cryptanalysis. Consequently, estimates on the security of post-quantum systems with respect to quantum computers are purely theoretical, which causes two problems :

- **if the power of quantum computers is underestimated, the chosen security measures risk being too weak and the patterns will be broken with the appearance of sufficiently powerful quantum computers;**
- **if the power of quantum computers is overestimated, the security measures chosen will also be overestimated, which will hamper their efficiency and their large-scale deployment.**

Lock 9 Post-quantum cryptography algorithms being evaluated increase the time and storage resources required by one or more orders of magnitude compared to current algorithms.

Currently envisioned post-quantum algorithms typically leverage keys at least 10 times longer than their current counterparts. This larger size

is accompanied by a greater calculation time, as well as by higher memory requirements for the devices that implement them. These changes pose relatively little difficulty for devices with large amounts of computing power and memory, such as smartphones or desktop computers. For devices with limited resources, such as smart cards, specialized circuits aimed at securely accelerating the calculations linked to these new algorithms will have to be developed. This work can begin when the standardized algorithms are known or strongly anticipated. Several academic works, in progress, aim to develop the calculation bricks necessary for some of the proposed algorithms.

Lock 10 The actual deployment of new cryptographic systems, and therefore post-quantum algorithms, will be a slow process.

Deploying post-quantum algorithms to replace current asymmetric algorithms will be a slow process based on what has been observed in the past for the deployment of current asymmetric algorithms. A decade will probably be necessary for a good penetration of these algorithms. In general, applications requiring a hardware or semi-hardware implementation of algorithms evolve over longer times. These time estimates depend on the pressure that will be exerted on the evolution. In the event of proven vulnerability of current algorithms due to the development of quantum cryptanalysis algorithms, the deployment of post-quantum algorithms could be significantly accelerated.

III.1.3.2 Quantum Cryptography

Before a generalization of QKD is possible, several challenges must be addressed :

- The distance: the loss of photons and the noise limit the transmission distance. Exceeding these limits requires traditional reliable relays inducing security problems because of the unprotected information which circulates there, quantum relays which require quantum memories, and satellites, with the associated cost.
- Integration into telecommunications infrastructures: QKD generally requires the deployment of dedicated infrastructures, which limits its adoption, where post-quantum cryptography is satisfied with existing infrastructures. QKD with continuous variables, a technology invented in France, has the advantage of being able to better reuse existing terrestrial telecommunications equipment, and therefore of being able to be deployed more easily. However, it suffers at this stage from a greater sensitivity to losses.

Lock 11 Core QKD Technologies Require Deployment specific infrastructure, the cost of which is high compared to the service rendered.

- **Trust in the cryptographic solution: to be adopted in practice, a QKD solution must provide cybersecurity guarantees for a given security target. As the maturity of QKD is low with respect to threat categories such as side channels or denial of service (DoS) attacks, it will be necessary to design adequate countermeasures for this type of attack, before consider possible use to handle sensitive information. The countermeasures used for classical communications, mostly based on redundancy mechanisms, are not applicable as they stand, due to the constraints of non-cloning of quantum states.**

A side channel attack refers to an attack that exploits flaws in the implementation of a security method through electromagnetic analysis, consumption, time, acoustics, *etc.*

A DoS attack aims to prevent the legitimate use of a service, by saturating it with illegitimate requests.

Lock 12 **The QKD today lacks maturity in terms of cyber-security, particularly with regard to trust relays and side-channel and denial-of-service attacks.**

These different axes of development constitute the framework of a possible certification of a QKD system allowing its use to manipulate sensitive information.

III.1.4 Enabling Technologies

Lock 13 **Quantum sensors and computers require complex, bulky service equipment with form factors that are not conducive to system integration**

Enabling technologies are non-quantum components that are essential for the proper functioning of quantum sensors and computers: cryostats, lasers, ultra-high vacuum, *etc.*

One of the main obstacles linked to these technologies lies in their size and their form factor.

Figure 3: 70°K cryostat

Thus, if a cryostat at 70°K as developed for infrared imagers today fits in the palm of a hand *(see* Figure 3), this feat could only materialize thanks to a research effort and consequent development on the part of industrialists.

While a sensor or a quantum processor takes up less than a cm3 , the control electronics and the cooling system capable of reaching temperatures of a few milli Kelvins occupy, to date, no less than ten cubic meters including dilution refrigerators, control bay and accessories *(see* Figure 4).

Moreover, these cryogenic machines, designed for generic uses in the laboratory, do not, to date, allow the integration of quantum devices into their system environment. Technological development must improve the integration of the system and the optimization of the allocated spaces.

Figure 4: Dilution Cryostat

Thus, with regard to sensors, control and cooling systems will have to become more compact before these devices can be widely distributed.

When it comes to quantum computers, the R&D effort in enabling technologies will need to address both compactness as well as form factor. Cylindrical one-cubic-meter cryostats will struggle to fit, as-is, into a data center in a *plug-and-play* fashion like GPU or NPU-based acceleration blades .

Close collaboration between the cryogenics and ultra-high vacuum sectors and the developers of quantum technologies will be necessary to overcome these obstacles.

III.2 Non-technological obstacles

III.2.1 Coordination and efficiency of the ecosystem

Obstacle 14 **The functioning in silos of the different communities of physicists, algorithmicists, engineers, cryptographers, and end users limits major breakthroughs and high-impact lock releases in quantum computing.**

Major advances in quantum sensors have been achieved through the sole effort of the community of physicists, a subject significantly less complex than computation and communications.

Regarding quantum computing and quantum communications, operating in silos is much more detrimental to the lifting of high-impact locks, insofar as these technologies are much more complex and multidisciplinary. Several biases explain these functionings in silos.

Thus, in terms of quantum computing, the community of physicists, mainly motivated by a detailed understanding of physical phenomena, tends to be skeptical about possible technological advances as long as this understanding is not full and complete. However, technical progress has generally preceded a detailed understanding of the laws of nature. Humans created the first alloys five millennia before understanding the sciences of materials, and the steam engine a century before understanding the laws of thermodynamics.

Computer and electronics communities, generally endowed with a strong technical culture, tend to minimize certain conceptual and fundamental difficulties.
It is thus observed that certain models are simplified to the extreme and run up, during the practical realizations, with physical locks not taken into account initially.

A second bias lies in a general tendency to favor techno-push approaches, and to consider uses last. If this approach is relevant when the end uses are diversified, in the case of quantum computing, which targets specific sectors, the association of end users from the start is essential. From these uses can derive the right computing architectures, and the right compromises on the technical performance of the qubits.

When it comes to quantum cryptography, the physics community tends to be more interested in performing a quantum communication task than performing a cryptography function with proof of security. This bias is natural, insofar as researchers in this field are more intellectually stimulated by discovery and scientific experimentation than by the production of turnkey devices, which is more a matter of engineering.

Finally, the cryptographic community, more involved in the engineering of security devices, expresses, for its part, a certain skepticism as to the real contribution of quantum communications in terms of security. If this skepticism is based on legitimate reasons related to implementation vulnerabilities not addressed by the physical community, the lack of exchange between these two communities has been exacerbated in recent years by the promises of "absolute security" of claimed quantum communications. a few years ago on the one hand, and its "practical uselessness" on the other. Technological breakthroughs in quantum communication will undeniably require the cooperation of both communities.

III.2.2 Skills development

Lock 15 The increase in the number of engineers, start-ups and familiar with the logic and development process in quantum computing is a necessary condition for the dissemination of quantum computing in the application sectors.

Aware of the breakthroughs linked to quantum computing, several companies in different application sectors are beginning to explore the contribution of this technology to their sector. However, they face a lack of cutting-edge skills on the job market. This observation concerns engineers, masters graduates or doctors on leaving higher education as well as software startups and consulting companies.

Unlike other technologies such as artificial intelligence, the number of algorithmicians and developers familiar with quantum logic does not exceed a few dozen across the country.

The constitution of an ecosystem of developers in quantum computing is a strong expectation of industrialists. An increase in the skills of developers in the field of quantum computing has become a necessary condition for the dissemination of quantum computing in the application sectors.

III.2.3 Market Size and Hype Cycles

Obstacle 16 Maintaining a long-term Public-Private " *cash-flow* " aimed at companies involved in the development of quantum technologies is a necessary condition for overcoming a "valley of death" which could last nearly ten years.

The learning curve in the field of quantum technologies will be particularly slow and will therefore require numerous successive technological redeployments and significant reinvestments by the technological sectors. At the level of the downstream sectors, the market will also be slow to develop due to the shortage of specialists in quantum technologies within the current employment market. The confidence of decision-makers will therefore be slow to achieve because of the countless hazards encountered *(see* Figure 5).

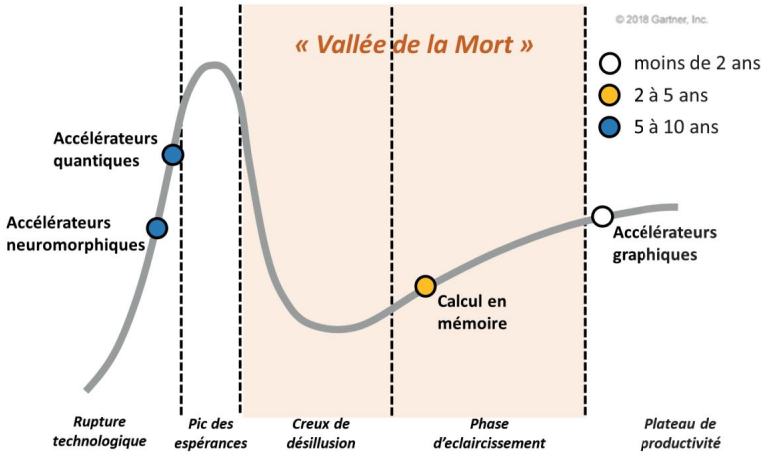

Figure 5: Compute Technology "Hype" Cycle – credit Gartner

It will therefore be necessary, in the same way as what is practiced by the largest global players, to ensure the viability of our emerging players through a sufficient flow of orders and appropriate continuity and visibility. This flow of orders could be done either within the framework of the various European initiatives in terms of digital sovereignty, or from the angle of the imperatives of sovereignty or even national security.

Finally, this order flow will constitute an important lever in order to reassure capital investors whose contribution to the viability of emerging players is essential, insofar as these players could, while gaining significant market shares, not generate profit over the next five to ten years.

IV. France's ambitions in terms of quantum technologies

IV.1 Quantum Computing

IV.1.1 Become one of the world leaders in "LSQ" computers

In terms of "LSQ" machines, Silicon technology enjoys a capacity for scaling up greater than that of other technological paths, in particular thanks to the billions of euros invested worldwide in industrial production capacities, but currently shows lower performance levels.

Ambition 1 Create, before 2025, the first fabless/hybrid company **European company offering silicon-based quantum processors.**

France is one of the rare countries in the world to have, thanks to the CNRS-Institut Néel, the CEA-LETI, the CEA-IRIG and STMicroelectronics, a base of skills in upstream and technological research, as well as of the industrial tool making it possible to seriously explore the Silicon route. Indeed, the realization of Silicon ***qubits*** **is satisfied with an engraving fineness of 28 nm, which suggests a production in the long term on the industrial site of STMicroelectronics in Crolles.**

Nevertheless, quantum processors will remain a relatively low-volume market at the global level, comparable to that of supercomputing requiring the development of appropriate business models.

Also, a preferred option to enable the development of a national industrial sector is the creation of a company *(NewCo)* capable of bringing technological developments to the market through a *fabless* approach **like Nvidia or hybrid image by Lynred (formerly Sofradir).**

Whatever business model is chosen, *NewCo* will have to provide a software development kit including a set of basic instructions and a high quality compiler. Indeed, the distribution of CPUs and GPUs from Intel and Nvidia would not be the one we know today without the associated X86 and CUDA instruction sets and the community of developers that goes with it.

IV.1.2 Become the European leader in “NISQ” calculators

In terms of “NISQ” machines and quantum simulators, the first machines began to emerge two years ago. Leaving aside the problems of scaling up, several technological paths currently cohabit in the available offers: superconductors, trapped ions, cold atoms, photonics, *etc.*

France has a critical mass of researchers (CNRS and Institut d'Optique) and support from sector unions in the field of photonics and cold atoms.
The research effort of recent years has made it possible, among other things, to spin off the first French start-up in quantum simulation: Pasqal. At the European level, Austria has a substantial technological lead in the field of trapped ions, another promising avenue that it is exploring with Atos as part of a European ***flagship*** project .

Ambition 2 **Develop and distribute the first European commercial offer quantum acceleration for the supercomputing market.**

By capitalizing on Atos' expertise in the design and integration of supercomputers, France could become the leading supplier of "quantum computing blades" for the supercomputing market. These computing blades will be able to incorporate quantum emulators and accelerators available or under development in France and Europe (cold atoms, trapped ions, superconductors, silicon, *etc.).*

IV.1.3 Become one of the world leaders in business software

While the technological offer in quantum computing is today dominated by Americans, the main groups interested in the use of quantum computing are European. It would be desirable under these conditions to reclaim the value at the European level. Becoming a world leader in quantum computing relies, in addition to hardware development, on the ability to identify impactful industrial applications where the available hardware provides a tangible "quantum advantage".

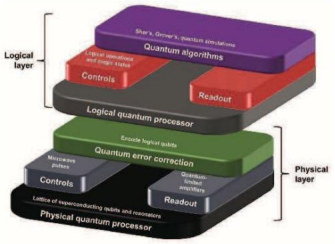

Figure 6: Technological building blocks of quantum computing

The identification of these applications requires a large number of other technological bricks *(see* Figure 6), in particular relevant use cases, powerful and robust algorithms, optimized software stacks, good integration with conventional supercomputing systems , optimal problem decomposition for efficient execution on NISQ quantum accelerators, high-performance compilers and error-correcting codes, and *more* .

Ambition 3 **Propose, in 2023, with the help of other European partners, the first "turnkey" business software offer, benefiting from quantum acceleration, for the fields of chemistry, pharmacology, logistics and learning in AI.**

Starting from the principle that quantum computing only effectively solves a specific category of problems, France could capitalize on its know-how in the development of business software to develop, with the help of its European partners, in particular Germany, a business software offering quantum acceleration dedicated to the fields of chemical modelling, logistics and AI learning. This offer would include hardware abstraction layers (error correction codes, assembly languages, and compilers), development environments and programming languages dedicated to the identified fields.

To develop such an offer, France will be able to capitalize on :

- **past developments of Atos in terms of interoperable low-level programming languages (AQASM software kit) and integration of quantum computing in an HPC environment (quantum computer emulator "Quantum Learning Machine"), - know - how and INRIA's ability to access the market in terms of software stacks and IA[7] ,**

7 In AI, the SciKitLearn library developed by INRIA ranks 3rd in number of users in the world.

- **CNRS skills in quantum algorithms,** - **CEA-LIST skills in software and systems architectures,** - **Dassault Système's know-how and ability to access the market in modeling software chemicals and the German SAP in terms of logistics modeling software,**

- **the business specifications of French and European end-users such as TOTAL, Airbus, Dassault Aviation, EDF, SANOFI, BASF, BAYER and BOSCH.**

IV.2 Quantum Sensors and Enabling Technologies

IV.2.1 Enjoy broad industrial autonomy on enabling technologies

Ambition 4 **To bring out, in 2025, at least two world-class European industrial players, including at least one French, for each of the critical enabling technologies: cryogenics, ultra-high vacuum and lasers.**

In terms of lasers, France has an important industrial history and has several world-class laser manufacturers supplying national and European integrators8.

In terms of cryogenics and ultra-high vacuum, France also has several assets to become a world player in the field. The presence of institutional and industrial players in cryogenics and ultra-high vacuum, such as IRIG, the Néel Institute, *CryoConcept, MyCryoFirm, Absolute System, Thales* and *AirLiquide* contributes to lifting the obstacles linked to integration of cryogenic systems into their environment as discussed in the previous chapter.

IV.2.2 Enjoy broad industrial autonomy in impurity-based sensors in the diamond

Sensors based on impurities in diamond are one of the most promising quantum sensor technologies because they allow us to see concrete applications in the short and medium term. There is a very significant effort in this area at the global level (US, China, EU, Australia, *etc.).* France has significant assets in terms of sensors based on diamond impurities but deploys more modest means compared to its main global competitors.

For example, Thales is conducting R&D work aimed at exploring the potential of this new sensor technology and identifying the opportunity to integrate it into future Thales systems.

Ambition 5 **To become a leading global supplier of diamonds to sensors based on diamond impurities, by 2026.**

In France, there are production capacities at the academic level (CEA-LIST, LSPM, *etc.)* which are sufficient for work at a research stage, but do not make it possible to meet industrial demands as they stand.

Support for this sector would make it possible to strengthen it and develop the resulting applications. It could thus be envisaged to take advantage of the ongoing repositioning of the company *Element Six,* to structure a French industrial sector of sensors based on diamond impurities, particularly in terms of the manufacture of high quality diamonds.

To set up such a sector, France will be able to benefit, in addition to Thales, from the expertise of its public laboratories.

8 In terms of lasers, the risk lies in the level of protection of French laser operators against a hostile takeover.

IV.3 Quantum and Post-Quantum Cryptography

IV.3.1 Maintaining strategic independence on the technologies of post-quantum cryptography

Ambition 6 **Propose, in 2022, the first post-quantum cryptography offer for high-performance security devices with limited computing resources.**

France is one of the world's industrial players in cyber-security, particularly in terms of security devices such as HSM9 modules and smart cards. By developing its own post-quantum cryptography products and disseminating them through its existing market access capabilities and an appropriate standardization strategy, France will confirm its position as a world leader in cyber security.

To develop its offer, France will be able to benefit from the technical and commercial know-how of its major groups and start-ups such as Thales, Atos, Orange, Secure- *IC* and *CryptoNext.*

Maintain strategic independence on quantum cryptography technologies

Ambition 7 **Propose, in 2024, the first European QKD solution, deployable at marginal infrastructure cost and resistant to side channel and denial of service attacks.**

In terms of quantum communications, France has a research fabric specialized in quantum communications with continuous variables and discrete variables, which are two technological paths that suggest deployment at marginal infrastructure cost. In the longer term, QKD solutions based on hybrid variables, for which France is one of the pioneer countries, should make it possible to exploit the best of both approaches.

By capitalizing, moreover, on its expertise in cyber-security, France could take the European leadership in the development of robust QKD solutions from the point of view of cyber-security, and not requiring heavy infrastructure investments.

9 An HSM module or " *Hardware Security Module* " is an electronic device, reputed to be inviolable, intended to generate, store and protect cryptographic keys.

V. Mission recommendations for a national strategy

V.1 State-of-the-art infrastructure for research and industry

V.1.1 Quantum Computing

Proposal 1 **Host, at the "Very Large Computing Center" (TGCC), a Quantum Computing platform diversified, scalable and accessible to communities of researchers and academic and industrial developers.**

Through a vision of convergence between quantum computing and HPC, France could host at the TGCC, the main French public computing center, the first infrastructure in the world of quantum accelerators integrated from a software point of view into a system of supercomputers. classic. The establishment, on French soil, of a world-class infrastructure, integrating various emulators and quantum accelerators based on various technological principles, will represent a strong lever for action making it possible to respond to several challenges, obstacles and ambitions addressed in previous chapters :

- **Develop the software ecosystem and uses: The emulation created by making this platform available to a community of researchers and pioneering industrial users like Total or Airbus will make it possible to build an ecosystem of developers familiar with quantum logic and independent of a particular hardware implementation, which meets a strong expectation of industrial users. A dynamic for the creation of start-ups and consulting services taking advantage of the TGCC platform may emerge, similar to what is observed in other countries, notably Canada and the United Kingdom;**

- **Develop France's legitimacy and influence internationally: The diversity of hardware platforms is a** strong ***marketing*** argument **for attracting world leaders in quantum computing to French soil. The capacities for testing, experimentation and comparison between the different technological paths allowed by this infrastructure will contribute to giving France the legitimacy of leadership in the development of a quantum software suite "hardware agnostic ";**

Links between the TGCC and the German computing center *Jülich* could make it possible to develop a common offer and a common portal allowing access to all European quantum computing technologies.

Proposal 2 **Open a permanent call for contributions aimed at French and European startups and laboratories developing quantum acceleration processors for integration into computing infrastructure.**

In order to maintain its legitimacy and its attractiveness, the infrastructure must maintain itself at the highest level of the world state of the art and will therefore have to renew its equipment so as to benefit from the most advanced quantum accelerators (more *qubits,* more operations, less noise *etc.).*

To do this, it will be able to open a call for contributions to French and European startups, laboratories and consortia developing quantum processors and emulators: *Atos, Pasqal, AQT Innsbruck, CEA, CNRS, OpenSuperQ, etc.*
The opportunity to open the infrastructure to suppliers outside Europe could also be studied.

Integration, into the computing infrastructure, of quantum computing blades developed by the various start-ups will not require high technological maturity10 and can be envisaged based on a proof of concept (TRL4) of 5 *qubits* and a sheet performance improvement route validated by a committee of experts.

In the same way as for HPC, the management of the purchase and renewal of quantum accelerator blades could be entrusted to the civil society GENCI.

Proposal 3 Develop a public-private offer of *QCaaS* or " *Quantum Computing as a Service* " competitive.

In order to secure their investments, the majority of end users prefer, as recommended by the consulting firms *Gartner* and *McKinsey,* the use of quantum computing resources in SAAS or " *Software As A Service* " mode to investment in an infrastructure. own. The uniqueness of the proposed infrastructure should be accompanied by an adapted service offer aimed at both the world of research and business.

This offer would consist of shared access to computing resources and an experimentation support service.

Two levels of support could be offered : - A basic level of

support for new users who wish to discover the basics of quantum computing ;

- An advanced level of support aimed at informed users seeking in-depth expertise for a specific subject.

The implementation of this QCaaS offer, which in the first estimate may require around ten full-time engineers given the number of users targeted, as well as the definition of a viable business model may be entrusted to players such as Teratec, Airbus, Atos and INRIA who have experience in HPC ecosystem animation and SaaS offers. A Call for Expression of Interest (AMI) may be launched by the State in order to develop this QCaaS offer.

V.1.2 Quantum communications

Proposal 4 Deploy a test platform for different quantum communication devices.

In order to remove the technological barriers relating to quantum cryptography, academic and industrial researchers will need an experimental infrastructure to validate their various devices. In practice, it is a question of having a means of communication by optical fiber over long distances where researchers can

10 Access to computing infrastructures is via cloud access. The low maturity of a quantum accelerator will mainly result in a higher maintenance cost and a potentially lower availability function. Unavailability for maintenance is observed in commercial quantum computing offers such as the IBM-Q.

test different devices, including continuous and discrete variable systems, classical and quantum relays or possibly interoperability with satellite links. It could be envisaged to exploit the optical fiber infrastructure of the RENATER network linking Paris to Saclay, or to call on a telecommunications operator to deploy new optical fibers to be made available to research teams according to a model of business to be determined.

This infrastructure, as well as the infrastructures present between Nice and Sophia-Antipolis will also allow French researchers to participate more effectively in various European initiatives such as the OpenQKD project or the EuroQCI initiative.

The study of the opportunity to invest in the deployment of a larger-scale quantum communications infrastructure will be conditioned by the lifting of the technological obstacles relating to the use of QKD (cf. Obstacle 11 and Obstacle 12) for handle sensitive information. The interest of a broader infrastructure deployment could be studied by the authorities once these obstacles have been lifted.

V.2 A technological development support program

V.2.1 Transversal support for all quantum technologies

V.2.1.1 Upstream search

Proposal 5 Renew, from 2021, the calls for projects (AAPR) of the axis "Quantum Technologies" of the National Research Agency (ANR) aiming to finance twenty exploratory projects annually.

Quantum technologies do not currently have a long enough development history to allow a given technological path to take precedence over the others. Therefore, it is essential to maintain a sufficient base of exploratory upstream research. This research base concerns both quantum computing technologies and those of quantum sensors and communications.

In order to perpetuate this research base, it may be considered to renew the calls for projects of the ANR's "Quantum Technologies" axis, which will end in 2020.

Proposal 6 Strengthen the "Quantum Technologies" axis of the ANR by financial envelope aimed at supporting three exploratory projects targeting identified priority technological pathways.

In addition to a cross-cutting research base, more targeted support on the technological paths for which France benefits from an advantage in terms of academic and industrial players11, through fewer projects but benefiting from greater funding , will make it possible to reach the critical R&D thresholds necessary to remove the main scientific barriers. Projects to be funded under this modality must include a strong upstream exploratory research component *(flying qubits,* quantum relays, topological insulators, satellite links, Si/SiGe heterojunctions, *etc.)* aimed at strengthening understanding and removing scientific uncertainties around priority technologies12.

Proposal 7 Encourage French laboratories and companies to respond to calls for European projects Flagship "Quantum Technologies".

At the European level, French academic and industrial research teams could be encouraged to submit more proposals to the European ***Flagship*** **"Quantum Technologies" and to the future Horizon Europe and Digital Europe programs, in order to complete the national effort. An objective of 12 to 15 M€ of annual European co-financing would be consistent with the success rates observed so far. An alignment of part of the national aid with the European subsidies obtained could be envisaged.**

11 Cold Atoms, Photonics and Silicon
12 The level of scientific risk-taking must be an evaluation criterion for this call for projects

V.2.1.2 Partnership research

Proposal 8 Include a priority on quantum technologies in future PSPC calls and Innovation Competition.

In addition to support for academic research, various aid instruments for innovation and partnership research between public laboratories and industry could be mobilised :

- **i-Lab Innovation Competition: startup creation competition for researchers.**
- **i-Nov Innovation Competition: competition to help start-ups and SMEs wishing to develop an innovative offer.**
- **PSPC-Region: Collaborative projects aimed at structuring value chains industrial.**

With regard to existing instruments that have proven their effectiveness, consideration could be given to introducing a priority on quantum technologies in future calls for projects.
An objective of supporting fifteen i-Lab competitions, five i-Nov competitions and ten PSPC-Région13 over a period of 5 years could be envisaged.

V.2.2 Support for French ambitions in Quantum Computing

V.2.2.1 Ambitions on "LSQ" computers

A major research effort has been deployed to date by CNRS and CEA teams with a view to developing qubits *based* on semiconductors, in particular on 28Si.

A team of fifty researchers made up of microelectronics engineers (LETI) and quantum physics researchers (NÉEL, IRIG) was formed and made it possible to reach a certain number of milestones relating to the production of qubits and *logic* gates *(see* Figure 7): 6 Gallium Arsenide *qubits* , 1 **Silicon *qubit* ,** 1 2- ***qubit gate, etc.***

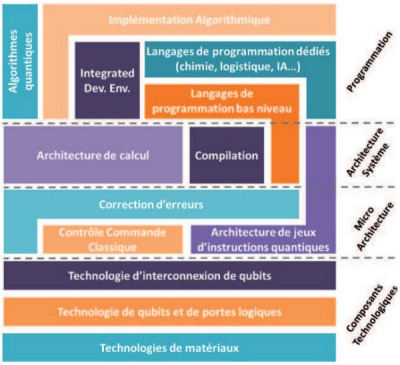

Figure 7: Technological bricks of an "LSQ" computer

Removing the obstacles relating to the production of "LSQ" computers *(cf.* III.1.1) will require, in addition to work on the "Technological Components", to address the "Micro Architecture" and "System Architecture "14 aspects ***(cf.* Figure 7) globally .**

13 PSPCs are best suited to projects with low technological uncertainty. Their use will be limited to projects of this type only. 14 The programming aspect is covered in V.2.2.2

Proposal 9 Strengthen the Grenoble microelectronics teams with skills in computing software and architectures.

It will be essential to strengthen this team while balancing the distribution of skills. Having a critical mass of engineers and researchers distributed in a balanced manner between technological components and architectures is a necessary condition for achieving French ambitions in terms of "LSQ".

Furthermore, the scientific and technological uncertainties that punctuate the production of an "LSQ" calculator require risk management adapted to the long cycle of the project. It will, in fact, be particularly risky to make a single bet on a given technological path.

Proposal 10 Deploy agile project management to gradually reduce uncertainties and costs throughout the project.

" *Fast fail* " risk management reduces uncertainties and costs over time. Thanks to this method, several technological paths can be explored in parallel. The least promising technological options may be phased out.

Proposal 11 Deploy, through a PIA15 action and a *PPR16,* an R&D-Capitalization program aimed at developing scalable quantum accelerators.

Due to the sovereign issues, the uncertainties, the long time horizons, and the capital intensity associated with it, the development of "LSQ" computing capacities will have to be accompanied by dedicated action at State level in partnership with private actors. A "quantum accelerators" action at the national level, to which could be added European co-financing of the ECSEL and EuroHPC JUs, would make it possible to cover the needs in terms of personnel costs and technological lots.

This action could be carried out in coordination with the second phase of the IA plan in order to address the subject of computational accelerators (XPU) in a more global way: quantum, tensorial, neuromorphic accelerators, *etc.*

The financing needs of these additional actions may be the subject of a more in-depth investigation by the State services.

Proposal 12 Support, through the AAPR of the "Quantum Technologies" axis of the ANR, a research program aimed at exploring bold silicon avenues.

In the spirit of Proposal 10, exploratory and ambitious research actions may benefit from the ANR's "Quantum Technologies" AAPR *(cf.* Proposal 6). These actions may, among other things, concern Silicon/Germanium junctions, topological ***qubits*** **on Silicon, hole-doped Silicon, Silicon Nitrides, impurities in Silicon for *qubits* at higher temperatures, electron-photon couplings, *etc.***

These exploratory actions will help reduce the risk of a premature and irreversible commitment to a risky technological path.

[15] **Future Investment Program**
[16] **Research Priority Program**

V.2.2.2 Ambitions on "NISQ" calculators and software

Proposal 13 Set up, in 2020, a Great Innovation Challenge “NISQ” aimed at developing, before 2023, an interoperable business software stack for the chemical, logistics and AI sectors.

In order to guard against heavy dependence on a single player, and to meet France's ambitions for European leadership in NISQ calculators and software, the France may consider setting up a Grand Challenge of the Innovation Council17 relating to the following theme:

"How to use quantum computing to accelerate innovation in chemistry, logistics and artificial intelligence"

This Grand Challenge of the Innovation Council will lead to innovative solutions for the benefit of companies and individuals for :

- **Draw the greatest benefit from quantum accelerators in a more global context of high performance computing by developing hybrid algorithmic solutions, by improving the exchange of data between quantum computers and classical computers and by developing high-performance mixed compilers.**
- **Disseminate the use of quantum computing in priority sectors by developing software stacks and *hardware-agnostic*** development environments **based on programming languages dedicated to the fields of chemistry, logistics and AI *(Domain Specific Languages)* and could eventually become standards.**

This challenge may be based on France's fields of scientific excellence, in terms of quantum algorithms and theoretical computing, as well as on a rich breeding ground for companies and innovation ecosystems, including: - for academics, CNRS

(PCQC, IRIF, LIP6, LORIA, *etc.),* INRIA, and CEA (LIST) ;

- **for large groups, Atos, TOTAL, EDF, SANOFI and AIRBUS ;**
- **for SMEs, PASQAL ;**
- **for the competitiveness clusters and IRT, the Systematic cluster and the IRT SystemX.**

It will be able to rely on certain student communities specializing in quantum computing and organize algorithmic development ***hackathons*** **for key uses;**

It may also rely on the existence of technological platforms available or under construction to test the innovations developed under realistic conditions, in particular at the TGCC *(see* V.1.1).

Proposal 14 Include the Grand Challenge in a framework of collaborations with other European countries.

Finally, this great challenge could find international resonance, whether at European level, in particular through the EuroHPC joint venture, bilaterally with Germany, for example by launching the great challenge jointly with the Germany coming

17 The Innovation Council, a strategic steering body, will guide the Government's action in terms of innovation.

to create its breakthrough innovation agency, or bilaterally with Austria, which has leadership in the design of *qubits* based on trapped ions. This major joint challenge will therefore be able to benefit, on the German and Austrian side, from the expertise of :

- *Innsbruck, Fraunhofer* and *Jülich* for public research ; - BAYER,

BASF, BOSCH and SAP for industrial *end-users.*

Proposal 15 Strengthen research resources in algorithms and software in the field of quantum computing.

As part of its 2019-2023 objectives and performance contract, INRIA has proposed that "quantum algorithms and information" as well as "post-quantum cryptology" be among its priority themes.

As part of this program, INRIA will be able to set up fifteen joint project-teams with academic and industrial partners covering :

- **in the short and medium term: the exploitation of existing hardware through the development of software engineering tools and suitable algorithms;**
- **in the longer term: support for the development of new *hardware (see* V.2.2.1) through the development of error correction codes and the exchange of data between classical and quantum computers.**

Proposal 16 Set up, in 2022, a Great Innovation Challenge aimed at develop a complete quantum computing solution, subject to convincing intermediate results for the "NISQ" Grand Challenge and for the PIA "quantum accelerators" action.

Provided that the Grand Challenge launched in 2019 and the "quantum accelerators" action have provided convincing intermediate results, it may be considered to launch a second Grand Challenge in 2022 aimed at disseminating as widely as possible a complete quantum computing offer including in addition to the " *hardware-agnostic* " software layers, the " *hardware-dependent* " software layers , as well as the most advanced French and European hardware components.

Proposal 17 Include specifications for the acquisition of experimental quantum accelerators in certain GENCI calls for tenders relating to the acquisition, renewal and extension of the French supercomputer fleet.

Subject to satisfactory intermediate results for the "NISQ" Grand Challenge and sufficient maturity (TRL4) of the first quantum acceleration devices *(Pasqal, AQT Innsbruck,* OpenSuperQ consortium , *etc.),* both from a hardware and software and integration in a classic HPC environment, GENCI's various calls for tenders, relating to the acquisition, renewal and extension of supercomputers in the French fleet, may provide an opportunity to include a specification relating to a "sandbox" of quantum accelerators.

V.2.3 Support for French ambitions in Quantum Sensors

Proposal 18 **Structure, by means of a succession of i-Lab, i-Nov and PSPC-Region projects, an industrial value chain for the production of sensors based on diamond impurities.**

In order to respond to French ambitions on sensors based on impurities in diamonds, the creation, based on academic know-how, of a start-up, specializing in the manufacture of high-quality diamonds, will be a privileged vector for the creation of a complete industrial value chain for the production of sensors based on diamond impurities in France. This action will be able to benefit successively from i-Lab and i-Nov aid as well as from a regional PSPC, after the removal of the main technological obstacles.

V.2.4 Support for French ambitions in Cryptography

Proposal 19 **Support, through i-Nov competitions and support schemes and accelerating the innovation of the ministries concerned, the development, before 2022, of a competitive offer of post-quantum cryptography for systems with limited computing resources.**

In order to meet French ambitions in terms of post-quantum cryptography for high-performance security devices with limited computing resources, the i Nov competitions, and more generally the innovation acceleration tools of the ministries concerned, will be able to benefit French industrialists, in particular start-ups, developing these technologies. Calls for projects must include an evaluation criterion related to risk management relating to the schedule of the NIST competition aimed at standardizing a certain number of post-quantum cryptography primitives.

Proposal 20 **Develop an evaluation strategy for QKD systems based on the French and European certification scheme.**

Without certification by the national organizations responsible for the security of information systems, the QKD cannot be used to handle sensitive information.
A certification scheme at national and European level could be developed with different time horizons.

In the short term, the analysis could focus on vulnerabilities of a non-quantum nature. In a second step, the certification scheme may focus on the analysis of the quantum protocols used, the classical cryptography on which they are based, as well as the possibilities of exploiting auxiliary channels.

Proposal 21 **Support, through the AAPRs of the ANR's "Quantum Technologies" axis, a research action relating to the maturation of QKD technology (systems with continuous variables and discrete variables, quantum relays, satellite links, etc. .) involving quantum communications experts, cybersecurity experts and telecom equipment manufacturers.**

The AAPRs of the "Quantum Technologies" axis of the ANR will initially be the preferred vector for removing the technological obstacles relating mainly to the use of QKD with continuous variables and with discrete variables to manipulate information.

devices, as well as the integration of QKD devices, into existing communications networks, without prohibitive infrastructure overhead. In order to maximize the chances of success of this research work, interdisciplinarity should be an important eligibility criterion in the process of evaluating project submissions.

Subject to convincing results, the results of this research may be subject to industrial development through the i-Lab, i-Nov and PSPC competitions.

V.2.5 Support for French ambitions in terms of Enabling Technologies

Proposal 22 Support, through the i-Lab competitions, the i-Nov competitions and PSPC projects, the development of a competitive French offer in the field of compact ultra-high vacuum and cryogenics for temperatures from 1 to 40 K.

Several promising quantum technologies, such as photonics and potentially Silicon18, are satisfied with temperatures above 1 K. At these temperature levels, cryogenic systems are several orders less complex and more compact than those necessary for sub-K cryogenics (below 1 K).

The development of a competitive compact cryogenics offer may be supported by i-Lab competitions, i-Nov competitions and PSPC calls for projects and benefit from the French industrial and research ecosystem in sur-K cryogenics: Thales *CryoConcept, MyCryoFirm, Absolute System,* Institut Néel, , IRIG, *etc.*

Proposal 23 Support, through i-Lab competitions, i-Nov competitions, PSPC projects and the support and innovation acceleration mechanisms of the Ministry of the Armed Forces, or a PIA action, the development of a competitive French offer in extreme cryogenics for sub-K temperatures.

Extreme cryogenics needs are today mainly covered by three global players: *Bluefors* in Finland, *Oxford Instrument* in the United Kingdom and *JANIS* in the United States.
These companies meet the needs of researchers with dilution refrigerators that can reach temperatures of a few mK but with very low cooling powers (~30 µW).

The low power of these machines will ultimately be a limiting factor in the development of quantum computing with a large number of *qubits.* Indeed, this high number of *qubits* will require much greater cooling power (from 100 mW to a few tens or hundreds of W).

An R&D action, associating *AirLiquide,* CEA, CNRS and the ecosystem of French startups will make it possible to anticipate the challenges of the change of scale of quantum computers, and to develop a new generation of refrigerators with a power increased by a factor of 30 or more.

18 Silicon **qubits operate nominally at 100 mK with first evidence of operation at 1 *K.***

V.3 A support program for the development of uses

V.3.1 Quantum Computing

Proposal 24 **Disseminate the use of quantum computing, through "Challenges" and "Hackathons" proposed by manufacturers in the most advanced application sectors. The "Airbus Quantum Computing Challenge" could be taken as a mode**

Like the "AI Challenges", quantum "Challenges" and "Hackathons" could be offered by the most advanced industrial players: Airbus, Atos, Thales, Total, Edf, Bosch, Bayer, SAP, *etc.*

Taking advantage of the TGCC's quantum computing infrastructure and the associated QCaaS offer, startups and service companies will be able to respond to these "Challenges". These actions thus make it possible to develop the quantum development ecosystem, to disseminate and popularize quantum computing, and to encourage researchers in the field of quantum computing to develop start-ups and thus maximize the economic impact of their work. of research.

V.3.2 Quantum Sensors

Proposal 25 **Support, through "Challenges" proposed by the application sectors, manufacturers of quantum sensors in the search for outlets in the application sectors.**

Challenges proposed by industrial end-users could allow start-ups and industrialists offering quantum sensors to find new market outlets. These challenges are particularly critical for the development of the ecosystem of quantum sensors so that this technology finds its place alongside conventional sensors whose performance is constantly increasing.

V.4 An effective innovation environment

V.4.1 Quantum *Hubs*

Proposal 26 **Create, in Paris, Saclay and Grenoble, three *Hubs* Quantics bringing together researchers in quantum physics, researchers in theoretical and applied computer science, engineers, industrialists from technological sectors, and en**

80% of the French quantum ecosystem is divided between central Paris, Saclay and Grenoble. Geographically bringing together the actors of this ecosystem in three Quantum ***Hubs*** **would contribute to the emulation between researchers and industrialists from different disciplines as well as to the visibility and attractiveness of the ecosystem abroad. Indeed, the concentration of resources is a key element of the efficiency of innovation ecosystems.**

Through a land component, supported by the State and local authorities, making it possible to intensify exchanges between actors who usually have very little interaction, as well as an allocation of €23 million/year from 2021, Hubs will be able to :

1. **facilitate collaborative and interdisciplinary research between public bodies and industrial ;**
2. **put fundamental research at the service of the most important technological axes strategic;**
3. **create multi-site international visibility to attract the best talent through international chairs, " *Frenchtech* visas" and cutting-edge infrastructure *(see* V.1);**
4. **bring out and finance the creation phases of startups;**
5. **support business creators;**
6. **facilitate collaboration between startups and industrial customers by bringing out use cases through a " *use-case-driven* " approach rather than " *techno-push* ", in particular through "Challenges" (see V .3);**
7. **provide testing and validation means: quantum programming environment, access to quantum accelerators, quantum communications network prototypes, *etc.***
8. **develop new initial and continuing training courses for researchers, engineers and technicians supporting the quantum ecosystem ;**
9. **publish analyzes and recommendations for the attention of economic decision-makers and public institutions, while increasing awareness among the academic and non-academic population of the issues, skills, *etc.***

At Saclay, the State will be able to support the dynamics already initiated by the University of Paris Sud, research organizations, industrialists like Thales, and the region, aimed at creating a large-scale quantum hub .

In Paris, the PCQC, bringing together since 2014 researchers from the CNRS, Sorbonne University, and University of Paris, in association with INRIA Paris teams, startups and Parisian industrialists, will be able to prefigure the next Quantum Hub in *Paris* .

In Grenoble, the ongoing rapprochement between INRIA, CEA-LETI, CEA-LIST on the theme of computing architectures for AI, in addition to the already very strong synergies between CNRS-NEEL, CEA LETI, CEA- IRIG and UGA as well as the presence of Atos, could prefigure the Grenoble *Hub* .

For the establishment of these *Hubs,* the State may ask the public research organizations, CEA, CNRS and INRIA, to propose a coherent program for the establishment of these *Hubs* making it possible to have three strong and visible sites at the international both in terms of research and transfer to industry.

If the logic of geographical concentration is virtuous for breakthrough innovation and justifies the creation of a limited number of Quantum *Hubs* , the three ***Hubs*** **will be called upon to put in place inclusion strategies making it possible to mobilize all the national competent .**

Proposal 27 Include an evaluation criterion relating to interdisciplinarity in ANR and BPI calls for collaborative projects.

In order to encourage the different communities to work together *(see* Verrou 14) on lifting the scientific and technological obstacles to quantum information, the various calls for projects by the ANR and the BPI relating to quantum technologies may explicitly request that the projects submitted are interdisciplinary: physics and information technologies, physics and engineering, physics and cryptography, *etc.*

The level of interdisciplinarity may be the subject of an evaluation criterion in the process of reviewing the projects submitted.

V.4.2 Skills development

Proposal 28 Include 6 ECTS19 of quantum algorithms in the twenty main cycles of engineers and masters in computer science and 6 ECTS of post-quantum and quantum cryptography in the masters of cryptography.

Without wanting to make all engineers and computer masters graduates experts in quantum computing or all cryptographers experts in post-quantum and quantum cryptography, that the current job market is in any case not able to absorb, an introduction to these disciplines in the main training paths in computer science and cryptography is essential. Indeed, although these disciplines are nascent, we can already observe a difficulty of recruitment in companies wishing to invest in these technologies both in terms of technological development and in terms of use.

Proposal 29 Design training courses with a specialization in engineering and quantum computing and anticipate the growth in the need for engineers and technicians in industrial sectors.

In a more limited number, more specialized training courses could be developed in order to meet the specialized needs of technological companies, in particular start-ups, both in quantum engineering strictly speaking and in enabling technologies such as advanced cryogenics.

19 Credit system developed by the European Union within the framework of the Bologna process

V.4.3 Mobility of researchers

Proposal 30 Make ecosystem players aware of the new provisions of the PACTE law relating to the mobility of researchers and access to laboratory resources by start-ups.

Before the PACTE law, the participation of a CNRS or INRIA researcher in an entrepreneurial project aimed at promoting their research results was accompanied by a major constraint linked to the rules of ethics incumbent on the public service. If he decided to join the entrepreneurial company, the researcher would lose his status as a civil servant and the job security that ensues, as well as access to the research infrastructures of his original laboratory.

These are two major obstacles to the transformation of a breakthrough discovery or invention in the field of quantum technologies into an industrial project and a competitive advantage for the economic fabric.

In other countries, such as the United States, the United Kingdom or Germany, it is common to see researchers creating start-ups while keeping their positions in their home laboratories and universities and while benefiting from the research equipment of the latter, which constitutes an important competitive advantage for the startup.

These two locks were lifted by the PACTE law of May 22, 2019, which introduced flexibility in the terms of cooperation between researchers, startups that value their work and academic laboratories.

The new provisions of the PACTE law and the flexibility it introduces are not yet well known to a majority of researchers in the academic community.

Awareness-raising actions with researchers and laboratory directors, including outside the quantum community, are necessary in order to remove the blockages of researchers wishing to promote their research work but worried about the old provisions of the labor code.

V.4.4 Venture Capital

Proposal 31 Support the creation of around fifty start-ups in the quantum until 2024.

As an extension of the "Deeptech" plan implemented in early 2019, the State may ask the BPI to support the creation of quantum startups at a rate of 5, 10, 10, 15 and 15 startups between 2020 and 2024. This support can be provided either in direct aid to start-ups (i-Lab, i-Nov, Capitalisation, etc.), or through investment by the BPI in "funds of funds". The startups supported will be able to benefit from the excellence of the French research ecosystem to address different markets in computing, sensors and quantum communications.

The creation of software startups will be facilitated by the implementation of the national quantum computing infrastructure *(cf.* Proposal 1) and the associated QCaaS offer *(cf.* Proposal 3). Indeed, it is observed, in the United States and Canada, that since the establishment of Cloud access to IBM and D-Wave computers, the dynamic creation of software startups has accelerated (eg simulation *of* proteins , smart-grid, smart mobility, etc.).

Proposal 32 Create a “late-stage” investment fund from trust of 300-500 M€ dedicated to quantum startups.

As with all French start-ups, series B and C fundraising (50 – 200 M€) generally requires calling on non-European investors with negative impacts on technological sovereignty, thus hampering the emergence of French unicorns . The creation of a **trustworthy** “ ***late stage*** ”20 **investment fund is essential to support French quantum start-ups beyond the *seed* and series A phases (1 – 20 M €). This fund should, however, be separated from funds dedicated to digital, given the different time horizons: 2-3 years for digital, 5-8 years for quantum. This trust fund will be able to raise 300 to 500 M€ from French manufacturers like Atos, Thales, Total, EDF or Airbus, institutions like AXA or BNP as well as from of the BPI.**

20 This fund may be based on the State's "ScaleUp" strategy, announced by the government on September 17, 2019.

V.5 An adapted security and economic intelligence strategy

V.5.1 Protection of scientific and technological heritage

The prospects for evolution announced by quantum technologies encourage certain organizations or States to take an interest in the French ecosystem and to target the most vulnerable players, who are also at the forefront at the global level. The sovereignty issues linked to the development of a quantum technology offer and the profile of the key players in this strategy call for an appropriate economic security strategy.

Proposal 33 Make the various most strategic players aware of the risks of technological looting and the tools available to deal with them.

The protection of scientific heritage is not a notion to which academic researchers are naturally receptive. Actions to raise awareness of economic security will be necessary to deal with the risks of technological looting.

Proposal 34 Identify and monitor strategic assets and activities and deploy, if necessary, the Scientific and Technological Potential Protection system (PPST).

Provisions such as the securing of information systems or the establishment of zones with a restrictive regime may be deployed to protect the most strategic scientific and technological assets, both in public laboratories and in start-ups resulting from public research. Conditioning public funding on membership of the PPST system could be considered.

Other more innovative or restrictive measures are proposed in the IGF report on economic security tools (reimbursement with very heavy penalties of public aid paid in the event of sale to a foreign player, for example). Finally, the generalization of the system of foreign investments in France to the most strategic sectors coupled with the early detection of investments considered problematic contributes to a better defense of this sector.

V.5.2 Economic Diplomacy

Proposal 35 Identify areas of cooperation and possible synergies with France's international partners in the field of quantum technologies.

Several European and non-European countries active in quantum technologies could become France's leading partners in quantum technologies.

Contacts at the right level could make it possible to identify synergies between the national strategies of France and its international partners.

V.6 Effective governance

Proposal 36 Establish a Strategic Committee responsible for making decisions orientation of research actions.

The high level of uncertainty relating to certain paths of development of quantum technologies, the long time horizons of the actions to be taken (2030) and the capital intensity required imply that the State's strategy cannot be immutable and must to redirect, if necessary, its actions over the duration of the national plan. To do this, the state will need agile governance with decision-making power. A similar situation has been observed in the field of aerospace and supercomputing. The State responded to this by setting up strategic committees bringing together representatives of the State, research organizations and industry. Similarly, a Strategic Committee may be set up to steer each of the structuring actions of the PIA.

The Committee may meet once or twice a year and will aim to :

- **stimulate the structuring technological options (support for one technological path rather than another, decide on the development of a technological brick or import it, *etc.) ;***
- **coordinate research actions from fundamental research to TRL6 demonstrators ;**
- **monitor budget execution.**

Proposal 37 Appoint an interministerial coordinator of the national plan, responsible for ensuring the overall consistency of the actions of the various public and private actors at the national level.

In the same way as for the national artificial intelligence strategy, an interministerial coordinator may be appointed. The latter will have a more operational role than the Strategic Committee. In particular, he will be responsible for :

- **ensure the proper execution of the national strategy by the actors ;**
- **ensure the proper structuring of the emerging sector ;**
- **ensure the proper coordination and articulation of the actions carried out by the management bodies the State, research organizations and industrialists.**

The interministerial coordinator will report on his action to the government.

The mission

Paula Forteza LREM MP for French Abroad (2nd constituency)

Aged 33, Paula Forteza was born in Paris to Argentinian parents, and has spent more than 20 years of her life in Latin America. After several experiences within the government of the city of Buenos Aires, the French administration (Etalab), or even in entrepreneurship, she wishes above all to put digital technology, transparency and citizen participation at the heart of the political debate in France.
Since the start of her term of office, Paula Forteza has been involved in particular in the bill for the moralization of political life, the transposition of the general regulations on the protection of personal data (RGPD), as well as in the project to reform the 'National Assembly. She has also contributed to advancing public debate on many other digital-related topics such as the fight against Fake News, net governance, regulation and taxation of web giants, the place of women in digital or again the environmental impact of digital technology.

In April 2019, Paula Forteza was commissioned by the Prime Minister for a four-month mission on quantum technologies.

Jean-Paul Herteman Honorary President of GIFAS,
Chairman and Chief Executive Officer of the SAFRAN Group **between September 2007 and April 2015**

Jean-Paul Herteman began his career as a weapons engineer in 1975 at the Toulouse Aeronautical Test Center (Ceat) and joined Snecma in 1984. Successively Materials Research Manager, Quality Director then Design Office, in 1995 he became Director of CFM 56 programs and Vice-President of CFM International. He was in charge of the Technical Department of Snecma from 1996 to 1999, then was entrusted with the General Management of the Rocket Engines Division until 2002. He was appointed Chairman and Chief Executive Officer of Snecma Moteurs in February 2002. as Deputy Chief Executive Officer of Safran, in charge of the Propulsion Division. He was appointed Chairman and Chief Executive Officer of Sagem Défense Sécurité (2006-2007) and in charge of the Defense Security Branch. In 2007, he became Chairman of the Executive Board of the Safran group, then Chairman and Chief Executive Officer

Iordanis Kerenidis Research Director at CNRS

Iordanis Kerenidis obtained, in 2004, a Ph.D. from the Department of Computer Science at the University of California, Berkeley. After a two-year contract at the Massachusetts Institute of Technology (MIT), he joined the National Center for Scientific Research (CNRS) in Paris as a permanent researcher. He won a Marie Curie European grant, "Young Researchers – Young Researchers" funding from the National Research Agency (ANR) and funding from the European Research Council (ERC Starting Grant). His research in algorithms and quantum communications has been the subject of more than seventy publications in renowned journals and peer-reviewed conference proceedings. His latest work aims to find concrete applications for quantum computers in the fields of optimization and machine learning. He is director of the " *Paris Center for Quantum Computing* ", an interdisciplinary research center which is the spearhead of quantum technologies in Europe.

People interviewed

Adrien Facon • Alain Aspect • Alain Schuhl • Annaïg Andro • Anthony Leverrier • Arnaud Landragin • Bernard Giry • Bernard Hamelin • Bernard Ourghanlian • Bertrand Monthubert • Bruno Sportisse • Charles Beigbeder • Christophe Jurczak • Christophe Strobel • Cyril Allouche • Cyril Baudry • Daniel Estève • Daniel Verwaerde • Delphine Roma • Diane Dufoix-Garnier • Dominique Thomas • Eleni Diamanti • Elisabeth Giacobino • Eric Jaeger • Eric Vacaresse • Florent Muller • Franck Pereira dos Santos • Franck Schlie • François Alter • François Jacq • Frederic Magniez • Frederic Valette • George-Olivier Reymond • Georges Ulzbelger • Gilles Ceyssat • Guillaume Colin de Verdiere • Henri Calandra • Hervé Mouren • Hisham Abou Kandil • Hubert Fraysse • Ivan Testart • Jean-Jacques Rabeyrin • Jean-Charles Faugere • Jean-Christophe Gougeon • Joffrey Célestin-Urbain • Khalil Rouhana • Laure Le Bars • Ludovic Perret • Martine Garnier • Mathieu Landon • Maud Vinet • Nolwenn Rozen • Olivier Ezratty • Pascale Senellart • Patrice Bertet • Philippe Duluc • Philippe Grangier • Pierre Perrot • Raphaël Jammes • Roberto Viola • Romain Alléaume • Sébastien Kunz-Jacques • Sébastien Tanzilli • Serge Haroche • Stéphane Bajard • Thierry Debuisschert • Thierry Lahaye • Thierry Petit • Tristan Meunier • Valérie Gacogne • Valerian Giesz • Vincent Mages • Xavier Vasques • Xavier Waintal • Yannick Devouassoux • Zaki Leght