Our Digital Future

When questionning the digital transformation becomes essential

HOW TO BUILD AN ARTIFICIAL INTELLIGENCE OF TRUST?

WHAT IMPACT WILL DIGITAL HAVE ON HEALTH CARE IN THE FUTURE?

WHAT IS THE INVISIBLE WORLD BEHIND THE INTERNET OF THINGS?

IS CYBERSECURITY JUST A MATTER OF PROTECTION?

WHAT WILL QUANTUM TECHNOLOGIES CHANGE IN THE WORLD ORDER?

Inria

SUMMARY

BRUNO SPORTISSE

INRIA'S CEO

IN AN ERA WHERE DIGITAL TECHNOLOGY IS OMNIPRESENT, WHERE OPPORTUNITIES AND RISKS COEXIST, SOMETIMES INSEPARABLY, AND WHERE ALL AREAS OF SOCIETY ARE LIKELY TO BE TRANSFORMED, WHAT ROLE DOES INRIA INTEND TO PLAY?

To be at the forefront of research and innovation in and through digital technology, driven by the scientific, technological, industrial and societal impact of its projects.

To have a audacious and creative vision of research and innovation. It is in this sense that it is up to us to be a driving force in strategic areas for digital sovereignty, to take up the many current scientific challenges, to know how to anticipate the next ones, and to produce knowledge at the highest level that can respond to them, always with the ambition of having an impact, whatever its form. And it is also up to us to be a player in technological breakthroughs, with our public and private partners, and to encourage and support innovation. To do this, we need to be agile, open to changes in our working methods, and able to move beyond existing models, because our environment is changing very rapidly and our field of action must be at the highest global level.

Inria sees itself as a platform institute, open to exchanges and interfaces, capable of transforming the complexity of digital ecosystems - academic, industrial and entrepreneurial - into an asset, capable of attracting and combining talent and bringing together energies in France and Europe. An institute at the highest scientific level is a requirement. An institute capable of leading technological projects from start to finish to meet our major challenges, with a modern vision of innovation, non-linear and breaking down silos. Our scientific projects, integrated into the heart of the major university clusters, stimulate fruitful partnerships with academic players and with companies, large groups or ETIs, and are also the crucible of technological startups.

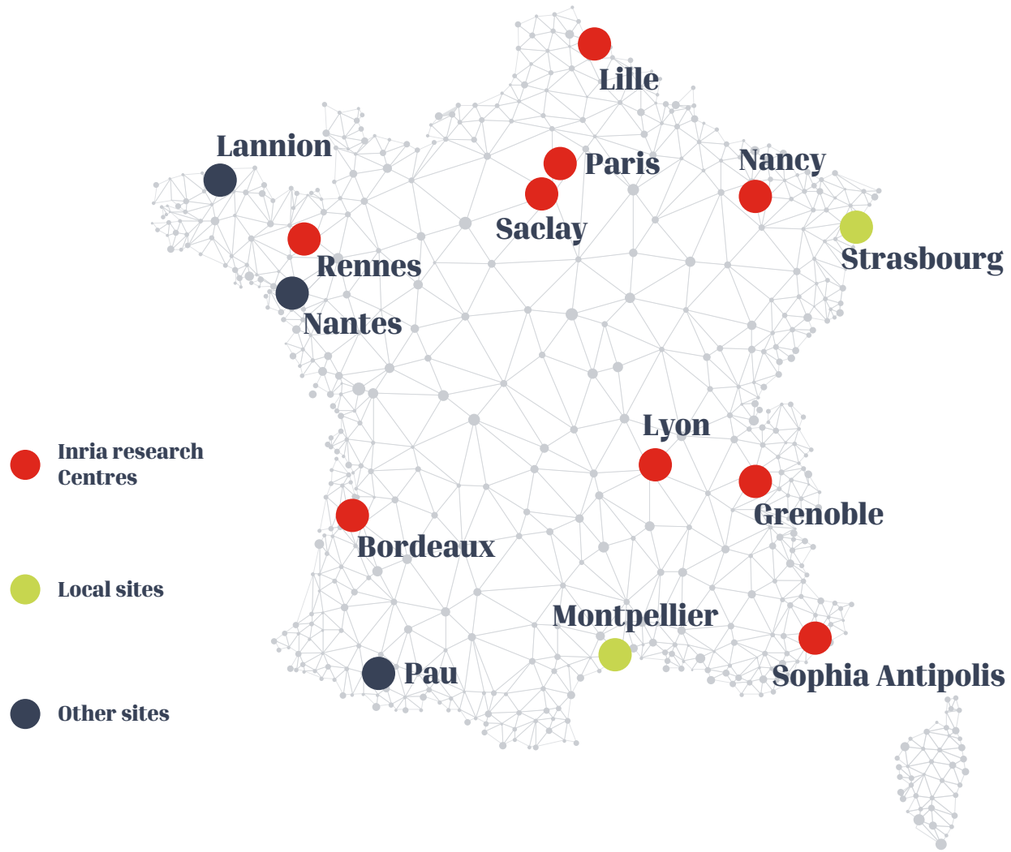
Our institute is firmly committed to supporting public policies and is fully aware of its duties in the areas of skills development, knowledge dissemination and strengthening the dialogue between science, technology and society for and with digital technology. Because mastering our digital destiny requires full awareness of the issues at stake. Because we need to «give meaning to digital technology», as our Foundation aims to do, in order to build a digital society based on trust and innovation, at the service of human beings.

At the forefront, Inria is the public research platform for France's digital power.

> At the forefront, Inria is the public research platform for France's digital power.

Our institute is firmly committed to supporting public policies and is fully aware of its duties in strengthening the dialogue between science, technology and society.

OUR TERRITORIAL STRATEGY



INRIA IS COMMITTED TO BUILDING UNIVERSITY CAMPUSES OF THE FUTURE

Since the first laws on university autonomy, the government's political will has been to create world-class French university research sites. The objective is to meet the challenge of competition from large international campuses by strengthening their attractiveness, their leadership, and their scientific, technological, and industrial impact. Inria is fully committed to this national strategy and is unambiguously committed to strengthening the ecosystems of major university sites in and through digital technology. This new positioning was formalized by the signing of a first strategic partnership between Inria and Sorbonne University in July 2021.

Five other partnerships were signed in the second half of 2021 with the Université Côte d'Azur, the University of Bordeaux, the Institut Polytechnique de Paris, the University of Paris-Saclay and the University of Lille, respectively. These new types of agreements herald the creation of Inria centers at the relevant universities, where the Institute proposes to operate its research and innovation facilities on behalf of its partners as part of a shared strategy and joint implementation. In this way, the Institute is reaffirming the strength of its organizational model and its impact strategy, which is fluidly linked to the models of its partners, for the benefit of all the players on these sites.

How to build an artificial intelligence of trust?

HOW TO BUILD AN ARTIFICIAL INTELLIGENCE OF TRUST?

DECODING

“Why should AI be human-centered?”

WHAT IS AI?

Giving machines actions or behaviours that humans consider intelligent, such as understanding, deducing, imagining, reading or talking. There is a plethora of recent advances but what are the scientific, political and ethical challenges facing the AI of tomorrow? Renaud Vedel, French national coordinator for AI, and Fabien Gandon, director of research at Inria, answer our questions.

WHAT ARE THE STATE'S STRATEGIC FIELDS IN AI?

R.V.: As for all technology, the biggest concern is staying at the forefront. If the hypothesis of AI becoming a general-purpose technology holds true, public policy must encourage the emergence of a strong national ecosystem. The AI dynamic is changing the tools of scientific discovery and the modes of economic production in the design of industrial goods and services, the optimisation of processes and the circular economy, customer relations, etc. In short, in all the relationships between the business and support functions of companies. **Moreover, AI is playing an increasing role in regalian functions such as defence and is integrating weapons systems, becoming a real geopolitical object.** In particular, China is banking on AI to affirm its ambitions for power and challenge American supremacy. Europe should also be concerned about its own technological positioning.

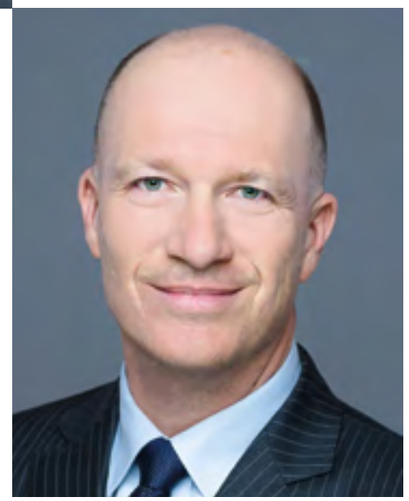
WHAT ARE THE EMERGING ISSUES IN AI?

F.G.: I would say that the biggest issues concern the need to remove the one-way dynamic between AI techniques and users. For example, one issue is being able to obtain and query explanations that are understandable and adapted to users. Another is the challenge raised by the establishment of trust which requires, in particular, the ability to generalise methods and their performance, ensure their robustness and verification, detect and correct biases, secure data and integrate mechanisms allowing users to raise questions and make corrections. There are many more, such as frugality and the distribution of onboard AI methods in multiple objects with very different architectures, capabilities and software environments.
In the short term, we are less at risk of experiencing AI supremacy but more of the blind exaggeration of social biases or the heedless reinforcement of individual behaviour by blinkered algorithmic governmentality. Work in AI must be human centred from the first stages of formulation. To establish trust in AI, it must have an ethical purpose and be technically robust and auditable with sanctions if this is not the case. Resolving these issues will involve adopting a social, political and moral project in cohesion with the scientific projects we are developing.

FABIEN GANDON
RESEARCH DIRECTOR
AT INRIA

WHAT ARE THE RESPECTIVE RESPONSIBILITIES OF THE STATE AND CITIZENS IN A WORLD THAT IS SEEING THE DEVELOPMENT OF INCREASINGLY AUTONOMOUS AI?

R.V.: The State must ensure that community life respects the norms in which technology is used to serve the autonomy of citizens and the correct functioning of institutions, while preserving as much as possible the freedom for entrepreneurship and innovation. The primary responsibility is to avoid all forms of dehumanising algorithmic governance, which means understanding technology and regulating it in such a way as to make sure it remains socially useful and positive.
We can see that certain families of AI, such as machine learning, are statistical in nature and fall through the net of the standard methods of formal validation and verification that have existed until now. Without hindsight on the use of these technologies, developing the necessary regulation is not easy. However, Europe recently made a pioneering commitment in this area with the AI regulation proposed by the Commission in April 2021.
Another major responsibility for the State is building the education and training infrastructure for stakeholders in all fields of the creation and use of AI systems that incorporates the associated challenges.
We need to train a new generation of developers and informed users, who are also informed citizens.
Lastly, there is the question of sovereignty, especially data control, whether in terms of individual privacy or business and industrial secrecy. This concerns the ability to maintain a power balance with big international groups that must not be allowed to impose their own rules in matters of democratic political standards. Europe must accelerate the process of recreating open technological sovereignty! This must be done without rancour but with determination and must preserve collective spaces for global co-construction such as the OECD, the W3C and standardisation bodies.



RENAUD VEDEL
COORDINATOR
OF THE NATIONAL
STRATEGY FOR AI

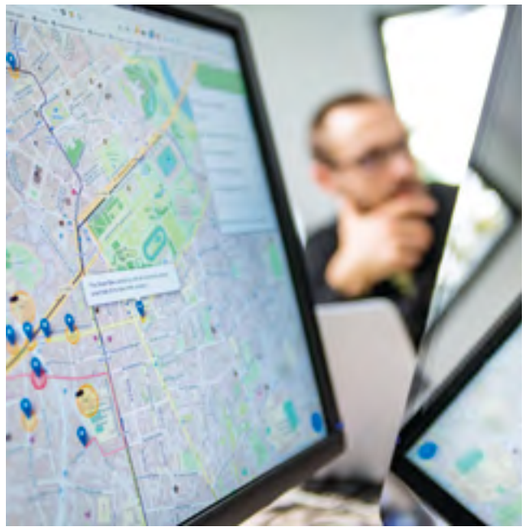
> Europe must accelerate the process of recreating open technological sovereignty!

HOW CAN WE MEET THESE NEEDS AND FIND A BALANCE BETWEEN THE NEEDS FOR REGULATION AND OPENNESS?

F.G.: This is a very broad issue, but there are two international tools for contributing to regulation and openness that immediately spring to mind and which concern the full spectrum of AI (data, software, etc.): standardisation and open source. Standardisation is not limited to national borders and it is therefore important to monitor and contribute to standards, whether they concern data or any other software or hardware aspect. We must not only monitor but also actively participate in international standardisation. Open source software also offers interesting possibilities for transparency: the community has access to elements of a solution that can be used at the individual, communal, corporate, European or even international level!

HOW TO BUILD AN ARTIFICIAL INTELLIGENCE OF TRUST?

2021 REVIEW



TRANSPARENCY

THE *REGALIA* PILOT PROJECT FOR RESPONSIBLE AI

Algorithms are almost everywhere, from advertising recommendations and tax calculations to search engines. They are increasingly shaping our cultural and economic choices and rapidly changing uses and our dependence on them, but the widespread emergence of AI techniques can make them so complex that their use and operation become opaque. How can we make sure that they are not a source of injustice, bias or fraud? This is the aim of the ***Regalia* pilot project**, led by Benoît Rottembourg in partnership with the French Digital Regulation Expertise Platform (PEReN). The project tests regulatory tools to **help or oblige public and private actors to improve the transparency of their algorithms and make the use of AI more responsible.**

GPAI

AI for human rights

Inria's Mission-IA, headed by Isabelle Herlin, was in charge of coordinating the GPAI (Global Partnership on Artificial Intelligence) this year. It aims to promote the responsible development of development of AI based on the principles of human rights, inclusion, diversity, innovation and economic growth. Launched in June 2020, GPAI is an international and multi-stakeholder initiative that currently involves 25 member countries and aims to bridge the gap between theory and practice in AI by supporting research and actions to inform public policy. It brings together leading experts from science, industry, civil society, international organisations and governments. In 2021, the annual GPAI summit was led by Inria and was held on 11 and 12 November in Paris. The aim of the summit was to reflect on the AI of tomorrow within the international community. Four working groups were held, focussing on Responsible AI (with a sub-group on AI and the response to the pandemic), data governance, the future of work and innovation and commercialisation.

LAB IA

How to accelerate the state's digital transformation with AI

To assist the digital transformation of administrative bodies, there is a need for tools that are able to meet the needs of staff and users. This is where *Lab IA* comes in! This structure involves Inria, the Interministerial Directorate for Digital Technology and the Interministerial Directorate for the Transformation of Public Action. It collects and selects the needs of administrative bodies in digital technology and AI and finds companies or research teams able to meet them. The results of the projects are often open source proofs of concept that anyone can use.

TRUST-AI PROJECT

A QUESTION OF TRUST

Artificial intelligence models are known for their efficiency but are often described as "black box" models. The lack of transparency in the way they operate can lead to scepticism or mistrust among users. When AI influences a medical decision, the health professionals and patients concerned need to be able to understand the processes of the algorithms that influenced the decision, both to be reassured but also to plan possible actions to change the outcome. It is in this context that the European project *TRUST-AI* was born: **using cognitive science and genetic programming, which makes it easier to understand and interpret the choices made by an algorithm, the project aims to create a reliable collaborative AI platform.**

STARTUP

AI-assisted medical imaging

What if AI could help improve the detection of suspicious areas in brain imaging data? This is the question addressed by postdoctoral research carried out within the Statify project team. It has led to the creation of the startup Pixyl *and its solution,* **Pixyl.Neuro, *which makes it possible to analyse brain images, identify anomalies and immediately give the radiologist information to help them adapt the proposed treatment for the patient or confirm their diagnosis.*** Pixyl.Neuro *is already used for monitoring neuroinflammatory and neurodegenerative diseases and continues to improve.*

THE *DEEPOMATIC* REVOLUTION: ADAPTING IMAGE RECOGNITION TO BUSINESSES

The real-life needs in image recognition are as varied as the professions that use it. To solve this problem, the startup* Deepomatic*, created in the Inria Paris Centre in 2014, is developing a fully customisable SaaS (Software as a Service) artificial intelligence platform, which allows its clients to design and use their own image recognition solution according to their needs. The idea has met with great success and* Deepomatic *is already used by around fifteen companies including major firms such as Suez, Bouygues Telecom and* Sanofi*, a number which, alongside the list of use cases, continues to grow.

What impact will digital have on health care in the future?

WHAT IMPACT WILL DIGITAL HAVE ON HEALTH CARE IN THE FUTURE?

DECODING

“How can the digital technology help physicians?”

HUGUES BERRY
DEPUTY SCIENTIFIC DIRECTOR IN CHARGE OF DIGITAL BIOLOGY AND HEALTH AT INRIA

TOOLS TO SUPPORT DIAGNOSIS, THE ANALYSIS OF EXAMS, OPTIMISATION AND PERSONALISATION OF TREATMENT, SCREENING OF BIOLOGICALLY ACTIVE MOLECULES, ETC.

In the last 15 years or so, the application of digital science to complex medical data has revolutionised health data processing and promises numerous benefits for patients. Hugues Berry, Deputy Scientific Director in charge of Digital Biology and Health, talks about the future challenges in this area.

WHAT DOES DIGITAL HEALTH INVOLVE?

Digital health is the use of digital technology as a tool for medical research. It also involves digital science research on biological problems and the development of specific healthcare tools.

The main objectives of digital health are to assist doctors in disease diagnosis, prognosis and therapeutic decisions. For example, to treat a cancer there are often several options: digital technology can help the doctor choose between surgery, immunotherapy and chemotherapy, or decide to combine them.
Another aspect is public health: digital technology allows us to spot signs of new diseases or epidemics or analyse their progression. It also allows, for example, larger data sets to be analysed to give a more accurate estimation of the side effects of treatments in the population.

WHAT ARE THE MAIN CHALLENGES OF DIGITAL HEALTH?

Health professionals need to collect large amounts of data with few errors, which requires large infrastructures. Digital research can provide new and efficient methods that also work with less massive, less “clean” data and whose functioning can be explained.
Multiscale models will become key in the challenges for our researchers. **We are starting to be able to simulate systems on specific scales: we can simulate part of a heart cell, or the contraction properties of the entire organ, or the evolution of the patient’s condition according to their lifestyle over twenty years, for example.** However, we are not yet able to make personalised models that incorporate all of these scales (molecule, cell, organ, behaviour). In brain imaging, we have access to images of the patient’s brain but we don’t yet fully understand how to combine their analysis with other data (genetic, lifestyle). We are working on this to be able to make more precise and accurate predictions for individual patients, among other things. Work on digital twins requires this multi-scale capability.
Another major challenge concerns clinical trials, in which methodological constraints make it very difficult to implement them correctly, as we saw with Covid. The creation of dedicated digital methodologies could facilitate their implementation, for example by supplementing them with external data or customising treatment during the trial.

INSERM, APHP and INRIA INSERT

The joint Inserm-Inria team COMPO is based in the cancer research centre of Marseille. It uses maths to optimise different treatments: how can they be combined? How should they be dosed? Should they be alternated? It has several aims: increase efficiency and reduce side effects to provide better care for patients.

The joint HeKA team with Inserm and APHP creates digital phenotyping tools that help personalise the prognosis and management of rare diseases. One of the team’s tools is used to characterise the patient’s hospital pathway by grouping similar pathways. They also work on hospital text data mining. Using automatic language processing, medical concepts can be automatically extracted from reports to allow their automatic analysis.

A PHYSICIAN IN THE CROWD

DIGITAL HEALTH ACCORDING TO ALEXANDRE MEBAZAA

There are huge needs for digital technology in medicine. The recent Covid crisis is illustrative of the management of healthcare and health research since Pasteur: health is a trinomial of disease/dysfunction/medicine. This trinomial has developed in all specialities which have each progressed in silos. We are reaching the limits of this structure because of the growing complexity of patients who are living longer with several pathologies that aggravate each other. Digitalisation can help understand the complexities of the patient, disease and treatment while simplifying the work of health professionals.
One of the challenges of our research is the management of acute care patients who have undergone surgery and for whom the possible complications have not been anticipated. Today, a patient staying in hospital for surgery is treated by several departments which produce different patient data. All this data is lost when the patient changes departments. The patient goes home and sometimes suffers complications. One of our projects involves collecting all the data produced during the hospital stay and using learning software to allow a prognosis of the risks of complications to be made when the patient is discharged. In human terms, it is important to be able to reassure, provide recommendations and, above all, monitor patients on a more long-term basis. The joint Inria/APHP team works on the collection, analysis and cross-referencing of this data. **Twelve million patients undergo operations every year in France. Being able to anticipate complications and provide long-term follow up would generate great savings and be of revolutionary benefit for patients, who would regain a good quality of life after surgery.**
Digital health is also changing medical research. The great researchers of the past discovered diseases, their causes and treatments. Today, we are trying to tackle the problem in a different way by analysing and cross-referencing data: new research avenues, based on statistics in particular, are emerging.

ALEXANDRE MEBAZAA
PROFESSOR OF MEDICINE AT THE UNIVERSITY OF PARIS, HEAD OF THE ANAESTHESIA AND INTENSIVE CARE DEPARTMENT AT LARIBOISIÈRE HOSPITAL

WHAT IMPACT WILL DIGITAL HAVE ON HEALTH CARE IN THE FUTURE?

2021 REVIEW

E-HEALTH

AN INRIA – INSERM TEAM AT PARISANTÉ CAMPUS

The HeKA project team was set up by Inria and Inserm in association with the APHP. It is based at *ParisSantéCampus*, inaugurated in December 2021, which allows it to work in daily contact with university hospital doctors, patient associations, startups and health industry professionals in a conducive environment for the emergence of joint research projects. Created in 2021, HeKA develops models and tools for decision making in medicine. **These can be used to facilitate the diagnosis and prognosis of patients or enhance clinical trials (treatment data, scientific knowledge) to accelerate access to innovative molecules.** The project focuses on cancer and a number of rare paediatric diseases.

SIMCARDIOTEST

Digital simulation is good for the heart

Since the start of 2021, Inria has coordinated the European project SimCardiotest, *involving ten partners from six countries.* ***The aim is to demonstrate the feasibility, efficacy and benefits of* in-silico *(i.e. based on digital simulation) clinical trials for medical devices and heart disease drugs.***
The stakes are high: if the in-silico route proves reliable, fewer clinical trials on animals will be required and human trials can be made shorter and safer, making it less time consuming and costly to develop and bring new devices or drugs to market. SimCardioTest *also aims to strengthen trust in health innovation among patients, care staff and regulation authorities. It will use anonymised medical data.*

MODELLING

MODELLING NEURODEGENERATION TO BETTER FIGHT IT

Stanley Durrleman, winner of the 2020 *Inria – Académie des Sciences* prize, is Head of the Aramis project team at the Brain and Spinal Cord Institute (ICM) where he works on modelling and statistical learning for neurodegenerative diseases. His aim is to detect the early signs of the disease, understand the changes in the brain that it causes and predict its evolution over three or four years. His long-term goal is to better characterise individual patients' development to make therapeutic trials more targeted.

COVID-19

A MODEL TO INFORM HEALTH AUTHORITIES

Inria and the IGN (National Institute for Geographic and Forestry Information) are co-designing a very detailed simulator for epidemic propagation that is specifically adapted to Covid-19. It models a real city with its population and their journeys and compares different scenarios depending on vaccine coverage, rates of teleworking, limited business hours, etc. Its flexibility will later allow it to create models for simulating other epidemics. The ICI project was launched as part of the Inria Covid-19 Mission.

LIVER CANCER

Helping surgeons operate better

For a surgeon, removing a liver tumour is a challenge: the liver is a soft and deformable organ and the images taken before the operation do not always resemble what they discover when they operate and the liver is partially deformed. As part of the European project Hipernav, *fourteen partners, including Inria, have laid the foundations for a precise virtual model of the liver based on images taken before and during surgery. The model will make it easier to "navigate" through the organ, a bit like a GPS, shortening the duration of operations and allowing precise and complete tumour removal.*

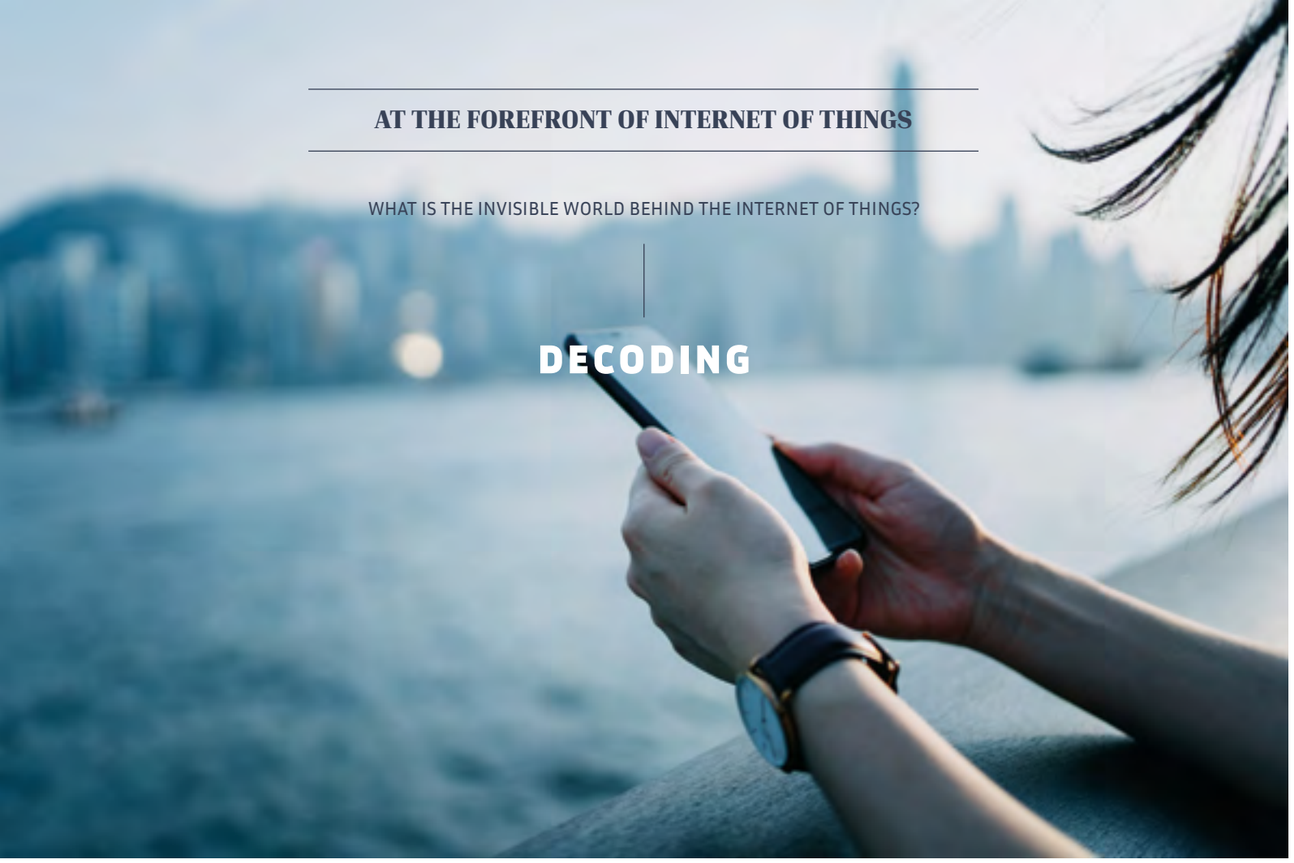
GENETIC DISEASES

DIGITAL TWINS OF LIVING CELLS

Biologists know a lot about the healthy and diseased states of the cells they study. But they don't understand in detail the mechanisms that come into play when a genetic disease occurs. The startup *Vidium*, supported by Inria, offers **a new tool: digital twins of living cells, or digital models of their internal molecular functioning.**

Based on real biological data, they describe cells with a high degree of complexity and seek to predict their evolution according to different mutations. The solution appeals to investors and *Vidium* already raised €1 million in 2021.

What is the invisible world behind the Internet of Things?



WHAT IS THE INVISIBLE WORLD BEHIND THE INTERNET OF THINGS?

DECODING

WHAT WILL THE CONNECTED WORLD OF TOMORROW LOOK LIKE?

ALICE'S DREAMS (extract from the white paper on the Internet of Things published by Inria in December 2021)

ALICE'S DREAM

Freedom is very important for Alice. She can easily connect her devices to other smart devices or remote computing solutions that she selects on the network: this system gives her a sort of personal, cyber-physical cocoon that acts as a "buffer" to her experience of reality, whether she is at home, travelling or at work. To get to the factory, Alice uses a driverless vehicle that interacts with the smart city's infrastructure to automatically choose the least polluting route or find a parking space. The advanced predictive maintenance and real-time environmental monitoring systems that the plant uses ensure workplace safety and productivity, while optimising energy consumption. Most importantly, she remains in control and can trust the system to protect her privacy. Alice uses her cocoon to help her take care of her health with predictive guidance. She can, of course, choose to deactivate the system and delete the recorded data at any time. If she wishes, Alice can choose to share some of her health data with her doctor. What is more, she can already access all these services even though she has just moved to the country!

ALICE'S NIGHTMARE

Alice's driverless taxi hit a tree. The taxi company later explained that its fleet of vehicles had malfunctioned due to spoofed GPS signals. Alice was not seriously injured, but the accident damaged one of her valuable connected implants. As if that wasn't enough, she was forced to pay a hefty «ransom» to hackers who exploited a security hole in one of her implants. Under pressure from her insurance company, she has no choice but to use new devices to monitor her vital signs and have her confidential data sold to third parties. At work, she is constantly spied on by her supervisors who make abusive use of the incredible surveillance capacity of IoT installations, which in turn fall victim to cyberattacks, compromising productivity as well as security. Based on a pilot study, the government is proposing a new policy for the mandatory use of digital cocoon medical sensors, sacrificing the privacy of this data to reduce the country's public debt. Subjected to this omnipresent connectivity and dependence on technology, lost and trapped in her digital cocoon, she wonders what is left of her private life, or even her free will, in this society gone mad.

Nathalie Mitton

Inria Director of research, Head of FUN team-project

INTERPRETS ALICE'S DREAMS

Alice's dream and nightmare illustrate what the world of IoT could be like. Fortunately, the reality will be neither but will be somewhere in between. Alice's dream may not be a universal representation of the uses of the IoT, but it illustrates the major impact it can have on our daily lives, production methods and social developments in general. **The IoT is a powerful tool for facilitating daily life by automating domestic tasks, reducing drudgery at work and, on a larger scale, making the exchanges and processes of our modern world smoother.** Alice's nightmare illustrates the points to watch out for when deploying such solutions, particularly the security of systems and people and data security which, when compromised, is a threat to individual privacy and economic competitiveness. No, we don't live in a world like that, largely because these vulnerabilities have already been identified and, before such systems are deployed, technological, political and legal barriers must be put in place to protect us from such abusive uses. The deployment of these services also requires social acceptance, which may or may not come naturally depending on the culture. But IoT-based services have a much broader scope than what Alice experiences. Today, they are found in many other very varied fields of application such as agriculture, waste management, home automation, factory 4.0, support for emergency services, road and bridge maintenance, etc. In some of these applications, the dangers that Alice faces are not plausible and the systems deployed often provide real added value. For example, better irrigation management for certain crops is all the more important in arid regions, while quality preventive maintenance in the upkeep of bridges and roads reduces work and accidents.
The next step for the deployment of sustainable, safe and responsible IoT systems is the establishment of legal frameworks and technical certifications to ensure the reliability of such systems.
Another major challenge is raising awareness and informing the different groups of people (users, IoT-based solution providers, local authorities, policy makers) about the risks to which they are exposed (cyber-attacks, theft of personal data, etc.) as well as the cost/utility balance of an IoT application.
Take the example of an IoT application for agriculture that aims to protect and preserve the environment by locally adapting the amount of water or nitrate needed for a crop: the benefit is obvious, but the production of IoT components made of precious metals, their transport from production plants and recycling and even the powering of the servers storing and exploiting the data they return each have their own environmental impact. We must find the right balance that provides universal benefits!

WHAT IS THE INVISIBLE WORLD BEHIND THE INTERNET OF THINGS?

2021 REVIEW

WHITE PAPER

Protecting billions of new machines

Over the next few years, the Internet of Things (IoT) and its billions of new communicating machines will impact every sector of our lives: housing, health, transport, agriculture, factories, urban and rural areas, etc. Inria has published a white paper coordinated by Emmanuel Baccelli, Director of Research at Inria, on this ongoing revolution that sometimes defies imagination. The Internet of Things means more comfort and value-added services, but also an increased risk of individual surveillance or vulnerability to cyberattacks.
The document explains the history of IoT from the first RFID (Radio Frequency IDentification) tags in the late 1990s and reviews the social, scientific and technical challenges. It also presents the 11 fields of computer science research concerned by this technology. Inria works in all of them.

INRIA CHALLENGE

IMPROVING THE SECURITY AND TRANSPARENCY OF CONNECTED OBJECTS

An embedded software platform for connected objects with no concessions in terms of cybersecurity or performance, using little in the way of energy or processing? This is the ambitious objective of the RIOT operating system and the Inria RIOT-fp project. With the aim of optimising the way microcontrollers work, this ground-breaking project is based on the continuous improvement of an operating system that is ultra-light but which will remain universal, with open-source programme libraries combining breakthroughs in cryptography, networks and formal verification. ***RIOT heralds the possibility of a secure, high-performance, scalable and energy-efficient "Linux of things".*** *The RIOT-fp project aims to promote the longevity of hardware by preserving batteries and progressively adapting the IoT software used in a microcontroller, as well as its security, in a complex context where uses, needs and standards change very quickly.*

ORANGE – INRIA

If it's not broken, don't fix it!

Orange **and Inria have been research partners since 2015 and are strengthening their collaboration with the creation of a joint laboratory dedicated to the Cloud-IoT continuum. In other words, clouds stretching from largest data centres to the smallest connected objects over vast geographical areas. The research programme includes infrastructure management, application development and experiments.**

TOUCH SENSITY

After the touch screen, sensitive material!

What if the wall of a house, a prosthetic arm or a piece of clothing became a sensitive surface capable of detecting pressure, extension, deformation or damage? This is the vision of the startup Touch Sensity, *created by former Inria engineer Anna Pugach and entrepreneur Mehdi Elhafed. Their technology is robust, flexible and non-invasive. It is based on work conducted at Inria on a connected garment that measures joint angles to prevent musculoskeletal disorders.*

AGRITECH

RFID TAGS: THE WINEMAKER'S MEMO

As they go through their vineyards, winemakers identify damaged stakes, branches to be shredded, leaves impacted by a disease, etc. But, if they install the RFID (Radio Frequency IDentification) tags developed by the startup *AgriBIoT*, hosted by Inria *Startup Studio*, they can make a note of this information using an RFID reader-recorder.

The vineyard employees can recover it in the same way and see where they need to work, without using a telecom network. These "memo" tags can also store other information such as hygrometry, temperature, treatments applied, etc.
In addition, winemakers can rapidly transfer the data to their computer.

Is cybersecurity just a matter of protection?

IS CYBERSECURITY JUST A MATTER OF PROTECTION?

DECODING

“How is public research advancing digital security?”

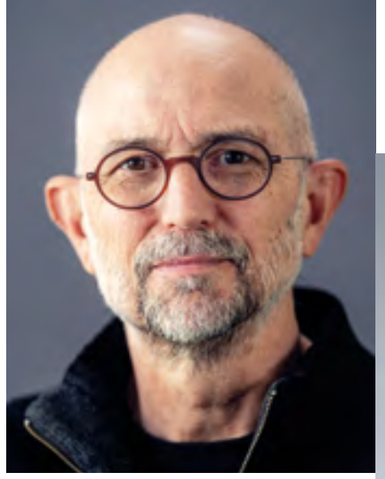
CYBERSECURITY: WHAT IS IT? WHAT IS THE ROLE OF PUBLIC RESEARCH?

Current events are a constant reminder of the extent to which the digital transformation of companies and administrations has placed cybersecurity at the heart of today’s challenges. The aim of cybersecurity is to ensure three properties of information, services and computer infrastructures: confidentiality, integrity and availability. The priority issues are the protection of critical infrastructures (allowing the production of goods and provision of essential services to the nation) and new digital services for the functioning and resilience of our society (financial services, supply chain, online commerce, electronic voting).

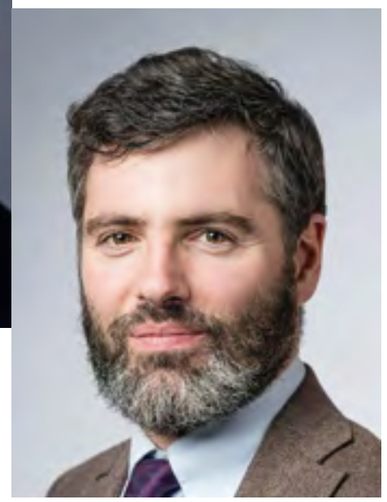
At Inria, the question of the technological and industrial sovereignty of digital technology is at the heart of our strategic outlook: cybersecurity research has been one of the institute’s priorities for the last fifteen years, with around 30 teams working in this field.

As part of the “France Relance” Plan, Inria jointly manages, alongside the CNRS and CEA, the cybersecurity PEPR (Priority Research Programmes and Equipment), structured around two key themes: “Information Security” and “Systems Security”. Inria also implements its Campus Cyber transfer programme on behalf of the academic community as part of the Campus Cyber project and its regional network. With a budget of €40 million over five years, this programme aims to strengthen research and the transfer of skills and technology from public research to all local cybersecurity ecosystems and encourage joint projects between stakeholders (academic, industrial or governmental).

HUBERT DUAULT
HEAD OF THE CYBERSECURITY PROGRAMME AT INRIA



LUDOVIC MÉ
DEPUTY SCIENTIFIC DIRECTOR IN CHARGE OF CYBERSECURITY AT INRIA



GEOFFROY HERMANN,
REFERENT FOR RESEARCH AT THE FRENCH NATIONAL CYBERSECURITY AGENCY (ANSSI)

Interview with Ludovic Mé and Geoffroy Hermann

WHAT ARE THE PRIORITY AREAS FOR ANSSI AND INRIA IN THE FIELD OF CYBERSECURITY?

G.H.: The priority areas and their associated collaborative approaches have been defined through joint reflection by the teams of ANSSI and Inria between 2019 and 2021. We have identified a list of research topics for potential cooperation and a range of possible forms of collaboration (PhDs, joint challenges, etc.) Current discussions between our teams concern a subset of these topics in line with our priorities for 2022.

We want to focus in particular on interactive theorem proving to automate the development of proofs of properties which can be used in security, for example to prove that a certain program does not leak information. These tools are complex and a high level of expertise is required in order to use them. This needs our collaboration on the following questions: how can these tools give us a full view of security issues? How can they be better understood and used?

Another current issue is “applied” cryptography and its implementation in the context of the Internet of Things. In this case, our involvement is required to address the significant increase in the attack surface that will be generated by the widespread use of objects.

L.M.: We also want to progress in the creation of secure processors using RISC-V architecture, because even if we achieve a much better level of software security than what we have today, if the software is running on an insecure platform with vulnerabilities, the protection is ineffective. A PhD has already been started on this topic and has led to the development of a mechanism for protecting the stored return address of a procedure, for example against “overflow” attacks, and the formal definition of the related security properties.

Security supervision and intrusion detection are also central themes of our collaboration. Due to the inadequacy of protection alone, an issue which is illustrated on an almost daily basis, we need to monitor information systems to detect, ideally in real time, attacks targeting them.

Lastly, our areas of cooperation also include other related themes, such as trusted AI in connection with security supervision. Machine learning is one of the most frequently used techniques in this field, although there is significant improvement to be made in the results obtained and there is still the obvious question of how much we can trust these techniques which sometimes have a “black box” aspect and are not invulnerable to attack. Security mechanisms therefore need to be integrated throughout the “machine learning pipeline”, from learning to operation, to prevent specific attacks. **For example, we know that a virus can be masked and disguised to trick a machine-learning based antivirus, so we need to increase the robustness of recognition mechanisms.**

WHAT ARE THE AIMS OF THE COOPERATION BETWEEN THE TWO AGENCIES AND INSTITUTES?

L.M.: As we explained in answer to the first question, our primary objective is to work together on issues that we have jointly identified as important and requiring answers as quickly as possible to increase the security of our future information systems. A similar objective is to be able to benefit simultaneously from the knowledge and scientific and technical culture of ANSSI staff and Inria researchers in the design of solutions. This knowledge and culture are often similar but due to their respective missions, Inria researchers master certain theoretical tools or are aware of certain very recent scientific advances while ANSSI staff have a more precise and up to date vision of the needs in the field and can direct research according to their knowledge of security incidents actually observed. Of course, there is a great deal of overlap between the two.

G.H.: When working on current issues such as those illustrated above, one of our objectives is to build a long-term vision and anticipate future fields of work. **When we are aware of certain attacks or proofs of concept developed in laboratories, without knowing whether these attacks will ever actually occur, we need to assess the likelihood of this becoming a reality and, above all, design potential protective countermeasures.** Finally, another challenge of our joint work is preparing for the possible technology transfer of our discoveries.

IS CYBERSECURITY JUST A MATTER OF PROTECTION?

2021 REVIEW

PUBLIC POLICY
THE SECURITY-DEFENSE MISSION IN SUPPORT OF THE ARMY

In 2020, the Security-Defense Mission was created at Inria under the responsibility of under the responsibility of Frédérique Segond, aimed at supporting public public policies in the field of intelligence by serving as an interface serving as an interface between the science and technology of our project teams and the actors of the sector. Two years later, many partnerships have been structured around this mission mission, with the ANSSI (*Agence nationale de la sécurité des systèmes d'information*), the DGA (*Direction générale de l'armement*), the DRM (*Direction du renseignement militaire*), and the Agence Innovation Agency (AID). Their common objective: to meet to meet the needs of these organizations in terms of cybersecurity and high digital technologies. Other partnerships have also been developed with companies in the defense industrial base. industrial base. Demonstrators, as well as a simulation and experimentation simulation and experimentation center, have been or will be created... so that the technologies developed can then be transferred to so that the technologies developed can then be transferred to the projects concerned.

PREVENTION

The LHS aims to anticipate the cyberattacks of tomorrow

The High Security Laboratory (LHS) was set up by engineers at the Inria Nancy-Grand Est Centre and Loria and is a sort of unusual library of malicious software. It has collected over 35 million entries since its creation in 2008! Once the software has been captured, researchers analyse it and observe the evolution of targets and techniques over time in order to prevent attacks. ***A project called* ThreatPredict*, led by the Resist project team and Carnegie Mellon, has led to the creation of an algorithm designed to predict the types of breaches likely to be of interest to attackers in the near future by combining data from the dark net (the hidden part of the Internet), social networks and social and geopolitical events****. Even in cyber security, prevention is better than cure!*

THE SECUREIOT PROJECT
STRENGTHENING THE SECURITY OF CONNECTED OBJECTS

The Internet of Things (IoT) allows a large number of machines to communicate with each other and, as a network in its own right, is potentially vulnerable. Faced with this problem, the European project *SecureIoT* aims to strengthen the security of connected objects and has led to the creation of a knowledge base that lists known vulnerabilities and the development of solutions to detect and predict attacks against driverless vehicles or domestic robots. The project also recently led to the creation of a startup called *CybAI*.

W3PROOF

Increasing trust in software

How can we make sure a software program does what it is supposed to do? By producing a formal proof using mathematical logic. ***The challenge is to use cryptographic tools to standardise and certify the proofs developed so that they can be reused from one program to another and between different countries.*** *This is the aim of the* W3Proof *exploratory action led by Inria.*

MALIZEN

A CYBER INVESTIGATION KIT

Whenever a new software attack occurs, security analysts carry out a real investigation to find the source of the problem and its consequences. The good news is that there is now a tool to make things easier for them: *ZeroKit*. Created in 2021 by the startup *Malizen* (the result of a collaboration between Inria and CentraleSupélec), this software recovers the activity logs of the infected computer and displays all the information likely to help the expert make a diagnosis. This is a valuable time-saver which could go even further, as *ZeroKit* will soon be offering direct advice to experts.

ANTIVIRUS
DASPREN BLOCKS RANSOMWARE WITH PARAD

Ransonware attacks can cost millions to organisations who fall victim to them. While known ware can be blocked by antiviruses, there has been no means of defence against new ones... until now. The startup Daspren, incubated in Inria's *Startup Studio*, proposes a new solution: Parad. The solution consists of producing a model representing the data in its normal state and putting in place a security mechanism as soon as a suspicious change occurs. *Parad* thus prevents any alteration of the data and preserves its integrity. In other words, it blocks ransomware without even having to identify it.

What will quantum technologies change in the world order?

QUANTUM COMPUTING: AN ONGOING REVOLUTION

BORN IN THE 1980S, QUANTUM COMPUTING AIMS TO INCREASE COMPUTATIONAL EFFICIENCY BY USING THE LAWS OF QUANTUM MECHANICS INSTEAD OF THOSE OF CLASSICAL MECHANICS.

HAROLD OLLIVIER
HEAD OF
QUANTUMTECH@INRIA

In the 1990s, the first algorithms were developed that offered an improvement on their classical counterparts. This encouraged many experimental groups to start building systems to show the feasibility of this kind of processing. Thirty years on, prototypes are beginning to reach sufficient size to outperform classical machines significantly in solving specific tasks.
However, there are still many obstacles to overcome before quantum algorithms can enter production. Inria and its teams are working to resolve some of these issues. Undoubtedly, the first is to broaden the spectrum of quantum algorithms able to offer an advantage over classical computing (speed, precision, reliability, etc.).
Several quantum computing models currently exist, each with their own strengths and weaknesses and, above all, their own specificities, particularly in the nature of the elementary gates and their topological constraints. **Work on quantum languages should remove most of these differences and automate the optimisation processes necessary to allow these machines to function correctly. This work will make programming easier and more accessible to end users in research and industry.**
Finally, the scaling up of these machines is still problematic because of the accumulation of uncorrected errors. Several techniques currently exist to resolve this, namely fault tolerance and auto-correction, which must be further developed and implemented in complete architectures. They should make it possible to calculate reliably for a long time and with enough qubits, which are the conditions necessary for benefiting from the advantages offered by quantum technology.

Quantum computing in Europe: the Union holds its own

By nature, research in the field of quantum computing is highly interdisciplinary, involving multiple sectors and implying a strong need for collaboration. Having top-level research in Europe is crucial because the mastery of emerging quantum technologies may determine the strategic autonomy of states and the competitiveness of their industries in critical sectors. **To avoid excessive fragmentation and the duplication of initiatives, mobilise the necessary investments to achieve critical mass and make Europe a leader in the quantum field, we must ensure that efforts undertaken by the member states are coordinated at European level.** The competition is global, and Europe has already put in place initiatives to support European cutting-edge research, such as the Quantum Technologies Flagship to offer scientific governance and, more recently, the construction of a European Quantum Communication Infrastructure (EuroQCI).

MARIE-HÉLÈNE PAUTRAT
DIRECTOR OF EUROPEAN PARTNERSHIPS AT INRIA

CÉCILE VIGOUROUX
DIRECTOR OF INTERNATIONAL RELATIONS AT INRIA

The question of quantum technology has become a major scientific and geopolitical issue in recent years. During the joint science and technology committee meetings held in 2021 between France and the United States and France and Singapore, and during meetings on the matter with Canada, the topic was central to discussions to outline future bilateral collaborations, the aim being to open alternative avenues to that of a quantum polarisation between North America and China. At Inria, the International Chairs programme is hosting Thomas Vidick, a researcher from Caltech specialised in quantum cryptography who has joined the COSMIQ project team for a period of four years from 2020 to 2024. It is through such high-level exchanges that international regulation in quantum science will be achieved.

PROJECT FOCUS

The European EuroHPC initiative works on the development of simulators and quantum computers for 2027. Inria teams are taking part in the HPCQS (High Performance Computer and Quantum Simulator hybrid) project, which will integrate two quantum simulators into the supercomputers of two European HPC centres. This is a first step towards a European infrastructure for quantum computing and simulation.

WHAT WILL QUANTUM TECHNOLOGIES CHANGE IN THE WORLD ORDER?

2021 REVIEW

CRYPTOGRAPHY

A unique and undecodable digital signature

A paper co-authored by five researchers, Antonin Leroux (Inria), Luca De Feo (IBM Research), David Kohel (IMM), Christophe Petit (Free University of Brussels) and Benjamin Wesolowsk (Inria), has received a Best Paper Award at the international Asiacrypt conference. The authors propose a digital signature protocol able to withstand attacks from the quantum supercomputers of tomorrow. To add a signature to a message, the sender generates a specific sequence of characters that only they can create, allowing the recipients to verify the identity of the sender. The work anticipates the arrival of quantum computers in ten to twenty years. Much more powerful than our current machines, they will revolutionise the cryptography methods currently used to protect our communications and personal data.

QUANTUMTECH@INRIA

QUANTUM COMPUTING: AFFIRMING OUR AMBITIONS

The first work on quantum computing at Inria dates back to 2001. Since then, the Institute has become increasingly active in the field. It now has five leading project teams, collaborates with startups and has signed several industrial partnerships with major technology companies. **In April 2021, the *QuantumTech@Inria* programme was created to define and accelerate the deployment of the Institute's strategy in this area.** It also plays an important role in the implementation of the national quantum strategy: the France Relance plan includes an ambitious Quantum Plan with a budget of €1.8 billion, to which Inria is fully committed. With the CEA and the CNRS, it jointly manages a PEPR (Priority Research Programmes and Equipment) and the national hybrid quantum computing platform.

PARTNERSHIP

Atos makes its move in research

Atos is present in 71 countries and employs 105,000 staff. In April 2021, the company signed a strategic partnership with Inria to structure and strengthen its relationship with the world of computer science research. The joint results will ultimately be integrated into the industrial player's solutions. The agreement covers six scientific themes including quantum computing, with work focusing on high-level programming languages and error-correcting codes.

CRYPTANALYSIS

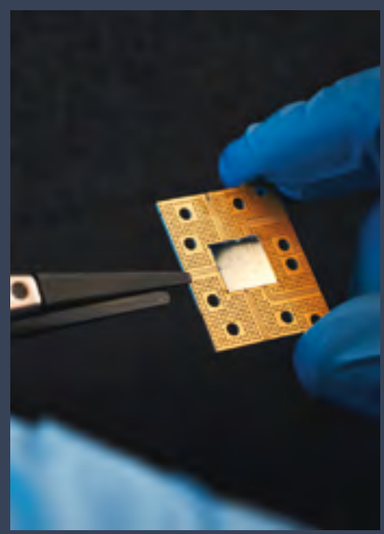
GABRIELLE DE MICHELI, *L'ORÉAL-UNESCO AWARD*

American by birth, Italian by her father and French by her mother, Gabrielle de Michelli is a young scientist of the highest calibre. Her speciality is cryptanalysis, i.e. encryption of sensitive data using specific algorithms. She dedicated a PhD to the subject, which she began in the United States and then mainly conducted at the Inria Nancy - Grand Est centre. **For three years she has been working on discrete logarithms, which are complex mathematical problems that secure communications on the Internet.** Her career recently earned her a L'Oréal - Unesco Young Talent Award France 2021.

STARTUP

SEARCHING FOR THE IDEAL QUBIT

Théau Perronin and Raphaël Lescanne, two former PhD students in a joint Inria - ENS team, founded the startup Alice & Bob in 2020. They are developing a revolutionary quantum computer that gets around one of the biggest stumbling blocks today: the multiple errors generated by quantum bits (qubits). While Google and IBM are trying to solve the problem by increasing the number of qubits, the two entrepreneurs are exploring a path in the opposite direction: designing "ideal" superconducting qubits capable of partially correcting errors themselves.



PHD

Long live virtuous errors!

Thomas Debris-Alazard, a researcher in the Grace project team, was recently awarded the Gilles Kahn prize for his PhD on cryptography based on error-correcting codes. ***The principle is to encrypt messages using these codes which modify the content in a very specific way that is impossible to reproduce.*** *The recipient can identify the sender and verify that the original content has not been modified.*

Meeting with

Philippe Durance

A TIME FOR FORESIGHT

PHILIPPE DURANCE IS AN ECONOMIST.

He is a professor at the Conservatoire National des Arts & Métiers (CNAM) and researcher at the Interdisciplinary research center in action-oriented science (LIRSA).

Holder of the Chair of Foresight and Sustainable Development, President of the Institute of Desirable Futures and author, in 2014, of the book* Strategic foresight in action, *Philippe Durance is a specialist in foresight. He works with numerous public and private organizations in their prospective and strategic thinking.

Foresight was born from an observation: our societies are too focused on the past. Decisions are taken mainly on the basis of established laws or models based on the observation of regularities. The advantage of this approach is the ability to make forecasts: knowledge of the past provides knowledge of the future. In a stable world, this way of thinking is entirely possible. In an uncertain world, however, in which change is the norm and forms part of everyday experience, organisations are faced with ever-changing situations. Established models no longer work and forecasting cannot effectively inform decision making.

Based on this observation, there are two possible approaches. The first consists in reviewing the existing models thoroughly to adapt them to the new reality and thus renew their ability to forecast. In this case, the fundamental question is: how to determine at what point a model must be revised? What events could indicate that the reality has sufficiently changed, that it is beyond the scope of our analytical grids and that these must imperatively be modified? This issue is now of concern to economists[1]. Few crises have caused a rethink of the fundamental principles of economic theory: the Great Depression of 1929, for example, prompted the development of Keynesian economics. The 2008 crisis, meanwhile, although still fresh in our minds, did not require a reconstruction of the standard theoretical framework to understand what had happened; it was enough to adjust the existing model to incorporate a few new elements. In this precise case, however, economic forecasts failed and left politicians to deal with the situation in an emergency. **Today, some feel that there is a need for a new economic theory, particularly in view of climate change. All that is certain is that it will resemble neither that of the past nor that of the present[2].**

The second approach sees the future as a territory to be explored. It is no longer a question of forecasting, but of foresight. The idea is not to project the past into the future but to analyse possible futures systematically and methodically to question the present and pave the way for a desirable future. **Foresight is therefore different to the principle of predicting the future, which is often implied by forecasting. It considers that the future is not written in advance but is the result of human decision.** This approach offers an unparalleled opportunity because tomorrow depends on us. But it is also a heavy burden:

it means that the people of today have a responsibility to future generations, because the decisions taken (or not) today will define the reality of tomorrow.

Foresight emerged through a realisation: human beings are capable of designing technologies of which the potential uses and their consequences are far from predictable. The initial objective pursued by its founder, the philosopher Gaston Berger, was to **reconcile wisdom (science) and power (politics) so that decisions would include, ex ante, an ethical reflection on the future.** This principle still holds true today as networks, artificial intelligence and quantum technology, among other things, open up new and unexplored worlds.

1. See the article by winner of the Nobel Prix in Economics Paul Krugman, "When Do We Need New Economic Theories?" *published in* The New York Times *on 8 February 2022.*
2. See the interview with Stephen Marglin, Professor of Economics at Harvard, Le Monde, *18 February 2022.*

FINANCIAL REPORT

ANNUAL BUDGET REPORT FOR THE 2021 FINANCIAL YEAR

Inria's initial budget for 2021, which was voted on in December 2020, was €259.8 million for resources and €264.2 million for expenses.

With regard to the execution of the 2021 budget and in terms of income, the **Public Service Grant** (SCSP) stood at €189.7 million, compared to €178 million in 2020 and €176.6 million in 2019. This accounts for 72% of all income for the 2021 financial year.

Own resources received stood at €74.8 million, giving a budget execution rate of 83% in relation to the figures outlined in the last amended budget. This accounts for 28% of all the Institute's resources for 2021.

Total resources received stood at **€264.4 million** in 2021, giving an execution rate in relation to the amended budget of **96%**.

Expenses can be broken down as follows: €188.7 million for personnel expenses (76.5% of total expenses), €138.2 million of which was spent on Contract Staff Payroll and €50.5 million on permanent personnel payroll.

In terms of personnel "below the threshold" (paid through the Public Service Grant), there were 1,516.6 full-time equivalents compared to 1,604.5 in 2020 and 1,605 in 2019, while the initial budget forecast for 2021 was 1,551.4 full-time equivalents.

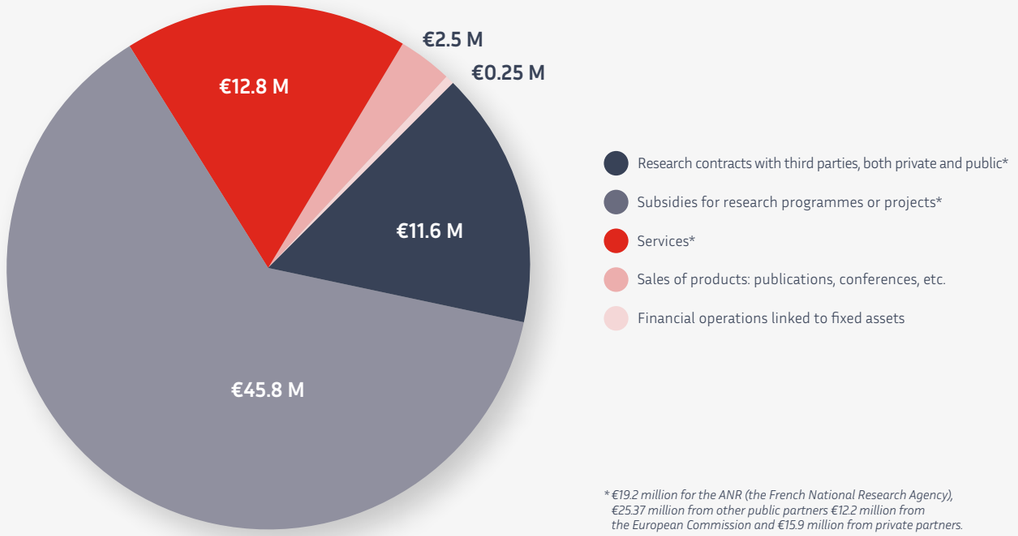
In terms of personnel "above the threshold" (paid through own resources) there were 1,091.8 full-time equivalents, compared to 848.6 in 2020 and 765.8 in 2019.

- €52.5 million on **non-scheduled operating and investment expenses**;
- €5.5 million on **expenses linked to scheduled investment operations**.

Overall expenses for 2021 stood at €246.8 million against an initial forecast of **€264.2 million**, giving a budget execution rate of 93%.

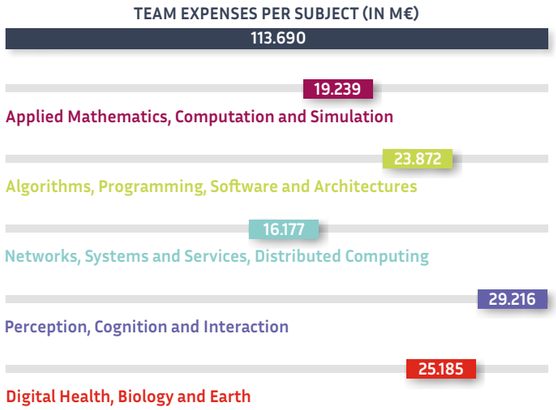
2021 expenses can be broken down as follows:
- €160 million on scientific activity for Research Centres (aggregate 1), 65% of total expenses for 2021;
- €21.7 million on joint research initiatives (aggregate 2), 9% of total expenses;
- €65 million on support functions (aggregate 3), 26% of total expenses.

THE PRIMARY ORIGINS OF OWN RESOURCES WERE AS FOLLOWS



** €19.2 million for the ANR (the French National Research Agency), €25.37 million from other public partners €12.2 million from the European Commission and €15.9 million from private partners.*

The scientific subjects corresponding to the Institute's main objectives are outlined in the table below, factoring in all expenses irrespective of their source of funding and including all aggregates.



CERTIFICATION OF THE FINANCIAL ACCOUNTS

As has been the case since 2010, the 2021 accounts were certified by two statutory auditors. The accounts for the 2021 financial year were certified without reservation by both independent auditors (Ernst & Young and KPMG).

2021 was marked by the continuation of actions to achieve the aims of the 2019-2023 Objectives and Performance Contract, despite the continuing health crisis that is still having an impact on the financial results which therefore remain atypical, as in 2020.

The 2021 financial account shows a profit of €5.6 million (compared to €9.3 million the previous year).

In 2021, operating income increased by 10.1% (+ €15.2 million), mainly due to:

- an increase of 6.6% in the subsidy for public service expenses (+ €11.7 million), which can be explained in particular by additional credits for the AI plan (+ €3.3 million), but also, in its basic component, by a sum of €4 million paid in December 2021 as an advance on the objectives and means contract, scheduled for 2022;

- a significant increase in direct income from activity (+ €15.2 million), mainly explained by the impact of the Institute's activities in support of public policies, including the project management assistance contract signed with the DGS for the deployment of the TousAntiCovid application: this increase in income is nevertheless counterbalanced and ultimately neutralised when account is taken of subcontracting expenses for an almost equivalent amount (see detail below).

Operating expenses were also up on the previous year, by 12.0% (+ €29.6 million), due in particular to the following factors:

- the impact of the Institute's activities in support of public policies, including the contract for the *TousAntiCovid* project mentioned above, leading to an increase in expenses for the year of €16.2 million;

- other external expenses ("use of supplies, works and services"), which broadly remain at a similar level to that of 2020, with in particular a low level of assignment and hosting expenses which reflects the ongoing travel restrictions caused by the health crisis;

- personnel expenses increased by 6.7% (+ €11.1 million), due to an overall increase in staff numbers (+ 6.5%), and to the revaluation of certain bonuses (research bonus, IFSE, PEDR), in particular in connection with the implementation of the Salaries and Careers Agreement of 12 October 2020.

The balance sheet total (assets and liabilities) stood at €319.4 million in 2021 compared to €286.1 million in 2020.

EDITOR IN CHIEF
BRUNO SPORTISSE

COMMUNICATIONS DIRECTOR
LAURENT STENCEL

EDITORIAL MANAGER
ARIANE BEAUVILLARD

GRAPHIC DESIGN AND EDITORIAL
TERRE DE SIENNE

WRITING
INRIA AND MÉDIATHÉNA

PHOTOS CREDITS
© Inria / M. Magnin p. 4, 34
© Inria / C. Morel p. 6-7, 10, 17, 23, 24-25, 28
© Inria / B. Fourrier p. 10, 18-19, 20, 27, 28, 33, 35, 36-37
Shutterstock / NicoElNino p. 11
© Inria / É. Garault p. 11
© Inria / H. Raguet p. 12
© Inria / G. Scagnelli p. 15, 16, 33
© Inria / F. Nussbaumer – Signatures p. 16
© G. Guerout p. 21
© Inria / R. de Bengy p. 22
© Inria / D. Betzinger p. 22
@pixabay p. 23
© J.-C. Caslot p. 33
© N. Hoppenot p. 33

Private collection / Fabien Gandon p. 9 ; Renaud Vedel p. 9 ;
Alexandre Mebazaa p. 15 ; Hubert Duault p. 26 ;
Geoffroy Hermann p. 27 ; Harold Ollivier p. 32

Getty Images
iStock

Inria.fr

Inria