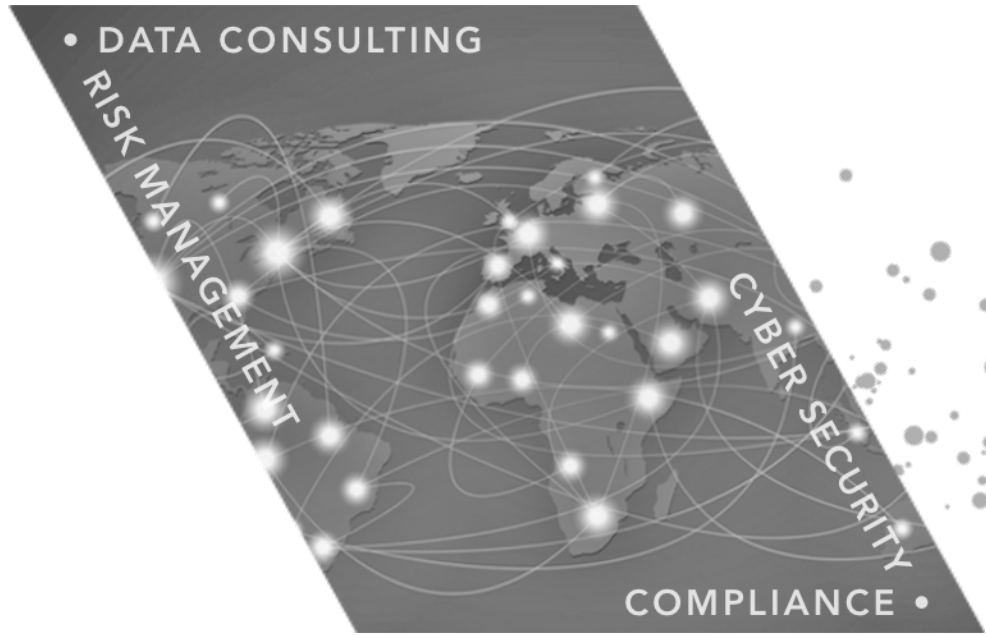


Janvier 2021

NOVAMINDS

La **Cybersécurité** face au développement de l'informatique quantique

NOVAMINDS
Create trust, build performance.

LE LAB'

R&D

Une activité de R&D au service de nos Clients à forte valeur ajoutée

- Novaminds se positionne comme un **Acteur de référence** pour les institutions financières.
- Novaminds dispose d'une **activité de Recherche** centrée sur son cœur de Métier, pour **anticiper les mutations** réglementaires, économiques, sociétales et technologiques.
- Cette activité de R&D, portée par notre **Laboratoire de Recherche et d'Innovation,** vient nourrir nos Réflexions, nos Publications, nos Enquêtes et nos Dossiers thématiques et nous permet de **fournir à nos Clients des services de pointe à forte valeur ajoutée**.
- Nos collaborateurs sont partie prenante dans les travaux de R&D afin de permettre de **développer de nouveaux savoirs**.
- Novaminds est accompagné par un **Cabinet accrédité** spécialisé dans le financement de l'innovation. Notre partenaire accompagne toutes les phases de la R&D avec la mobilisation de **Docteurs en Sciences** et d'**Experts financiers**.

État de l'art & Limites	Verrous & Incertitudes scientifiques
Concepts existants sur la gouvernance de la donnée anciens et n'ont pas été revus à la lumière du phénomène Big Data Pas de méthodologie de cartographie et de taxonomie de la donnée actuelle **Pas de culture de la donnée suffisante dans les établissements financiers**	Développement d'un modèle opérationnel global de pilotage de la donnée et cohérence des différents éléments constitutifs du modèle Organisation de la gouvernance transversale de la donnée avec la prise en compte du **Big Data, de l'IA, de la robotisation et des bockchains** La méthodologie d'analyse des éléments constitutifs du modèle
Démarche expérimentale	**Apport de connaissances**
Caractérisation des référentiels d'analyse des thématiques constitutives du Pilotage de la donnée Développement des éléments d'un modèle organisationnel et d'un modèle opérationnel pour un dispositif intégré de Pilotage de la donnée **Expérimentation d'une méthodologie d'analyse de risques de plateformes Big Data**	Améliorer la compréhension des différents éléments du modèle de pilotage de la données (gouvernance et organisation, méthodologies, processus, systèmes) Compréhension de la catégorisation des données et les règles d'accès dans le secteur financier **Nécessité d'une coordination transversale du pilotage de la donné**

PROJET D'INNOVATION

1 **Difficultés scientifique ou technique pour mener à bien le projet ?**

ÉTAT DE L'ART

2 **Les connaissances accessibles permettent-elles de résoudre les difficultés ?**

ACTIVITÉ R&D

CONNAISSANCES MANQUANTES

3 **Formulation des verrous scientifiques et techniques bloquant le projet**

Nos axes de Recherche & Développement

- Sciences financières
- Risques émergents
- Data science
- Conformité réglementaire
- Cybersécurité
- Résilience
- Outsourcing

Notre déclinaison dans le secteur financier

- Modèle unifié de gestion des Risques et des Contrôles
- Développement agile de la culture Cybersécurité
- Apport des nouvelles technologies pour le KYC
- Nouveaux modèles de gestion holistique de la donnée
- Organisation unifiée pour la Cyber-Résilience

Notre rayonnement Scientifique & Technique

- Publications dans la presse spécialisée
- Chroniques d'expert Conférences de Place
- Groupes de Réflexion organisés avec nos clients
- Benchmark et sectoriel de haut niveau
- Actions de notoriété …

Veille des tendances et orientations du secteur financier

Analyse du niveau de maturité des institutions financières

Anticipation des mutations sécuritaires et réglementaires


La donnée et les nouvelles technologies : quels enjeux pour la conformité ?

Les nouveaux enjeux de l'externalisation : un dispositif ad hoc au 30 septembre 2019

LA DONNÉE AU CŒUR DES ORGANISATIONS

CHIEF DATA OFFICER : POSITIONNEMENTS, MISSIONS ET MOYENS D'UNE FONCTION EN PLEINE ÉVOLUTION

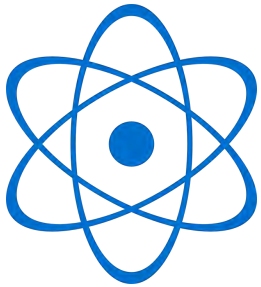
SÉCURITÉ DES DONNÉES ET LUTTE CONTRE LA CYBERCRIMINALITÉ

IL EST TEMPS D'INNOVER !

Introduction

« La première révolution quantique, menée au début du XXe siècle par de jeunes européens, comme Einstein, Heisenberg, Pauli ou Schrödinger, a donné naissance au fil des années à des inventions majeures, telles que la supraconductivité, le transistor, le laser, les communications par fibre optique, l'IRM, le GPS, etc. De nos jours, grâce à notre expertise en supercalculateurs et en cybersécurité, nous nous engageons pleinement dans la seconde révolution quantique. […] Ceux qui ont aimé l'évolution du numérique vont adorer la révolution quantique. »

Thierry Breton, PDG d'Atos



« L'innovation est bien souvent basée sur des technologies existantes ou dont les fondements sont, sinon maîtrisés, **a minima** ***compréhensibles.***

L'informatique quantique n'est pas cela. »

Informatique quantique : comprendre le quantum computing pour se préparer à l'inattendu**, CIGREF**

// AGENDA

1. **Qu’est-ce que l’informatique quantique ?**
2. Pourquoi s’en préoccuper dès aujourd’hui ?
3. Les pistes de réponse à la menace
4. Enjeux et hypothèses d’évolution

Create trust,
build performance

Les bases du quantique

« Un ordinateur quantique utilise les caractéristiques inhabituelles de la mécanique quantique – le comportement contre-intuitif de très petites particules – pour réaliser des calculs de façon différente des ordinateurs actuels ». *Rapport 2018 des National Academies of Sciences, Engineering and Medicine*

Cette discipline est fondée sur plusieurs phénomènes propres à la physique quantique :

L'intrication

Phénomène dans lequel deux particules ou groupes de particules forment un système lié et présentent des états quantiques dépendants l'un de l'autre, quelle que soit la distance qui les sépare.

La superposition

Un même état quantique peut posséder plusieurs valeurs pour une certaine quantité observable. Exemple : un électron gravitant autour d'un atome peut se trouver à la fois dans un état neutre et un état excité.

L'indétermination

Phénomène impliquant qu'un corps puisse occuper plusieurs positions à la fois. En physique quantique, il est possible soit de mesurer la position d'un corps, soit sa vitesse, mais pas les deux à la fois.

Une application : les Qubits

C'est l'unité de base en informatique quantique. Contrairement aux bits en informatique classiques, qui peuvent se trouver en état 1 ou 0, les qubits (quantic bits) peuvent représenter à la fois 0 et 1, voire un dosage de 0 et de 1 grâce au phénomène de « superposition ».

Principe de fonctionnement et usages envisagés

Enjeu principal du processus : découvrir un moyen d'accélérer l'exécution de longues vagues d'instructions.

- Exemple avec une macro Excel : augmentation linéaire des lignes d'instruction = croissance exponentielle du temps de calcul. L'informatique quantique permet de se détacher de cette logique..

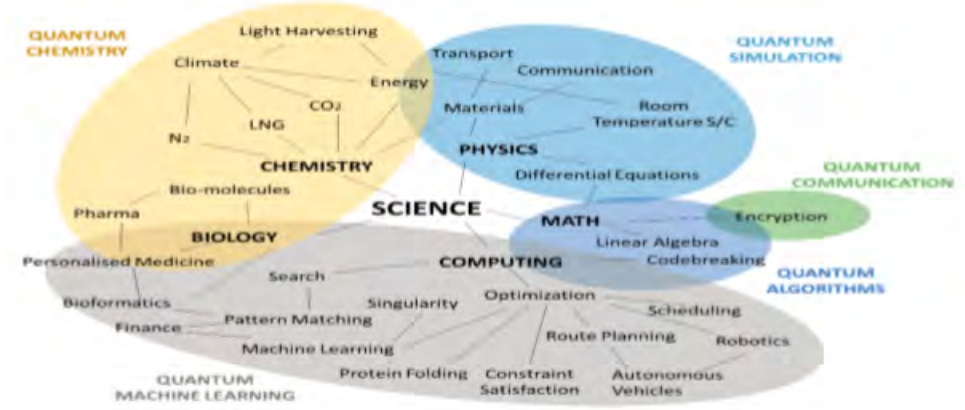
Une rupture technologique

- Traitement simultané de toutes les données
- Algorithmes probabilistes : réponses inexactes

→ Mise à l'échelle de la puissance de calcul

→ Réduction importante des durées de calcul

Exemple d'usages



Source : CIGREF

Elaboration de modèles climatiques, sismologiques et GPS
Cybersécurité et machine learning
Avancées médicales et pharmaceutiques

Ces caractéristiques rendent cette technologie idéale pour un éventail de problèmes spécifiques dans les domaines de la gestion des risques, de la finance ou tout domaine présentant un ensemble de probabilités.

Limites

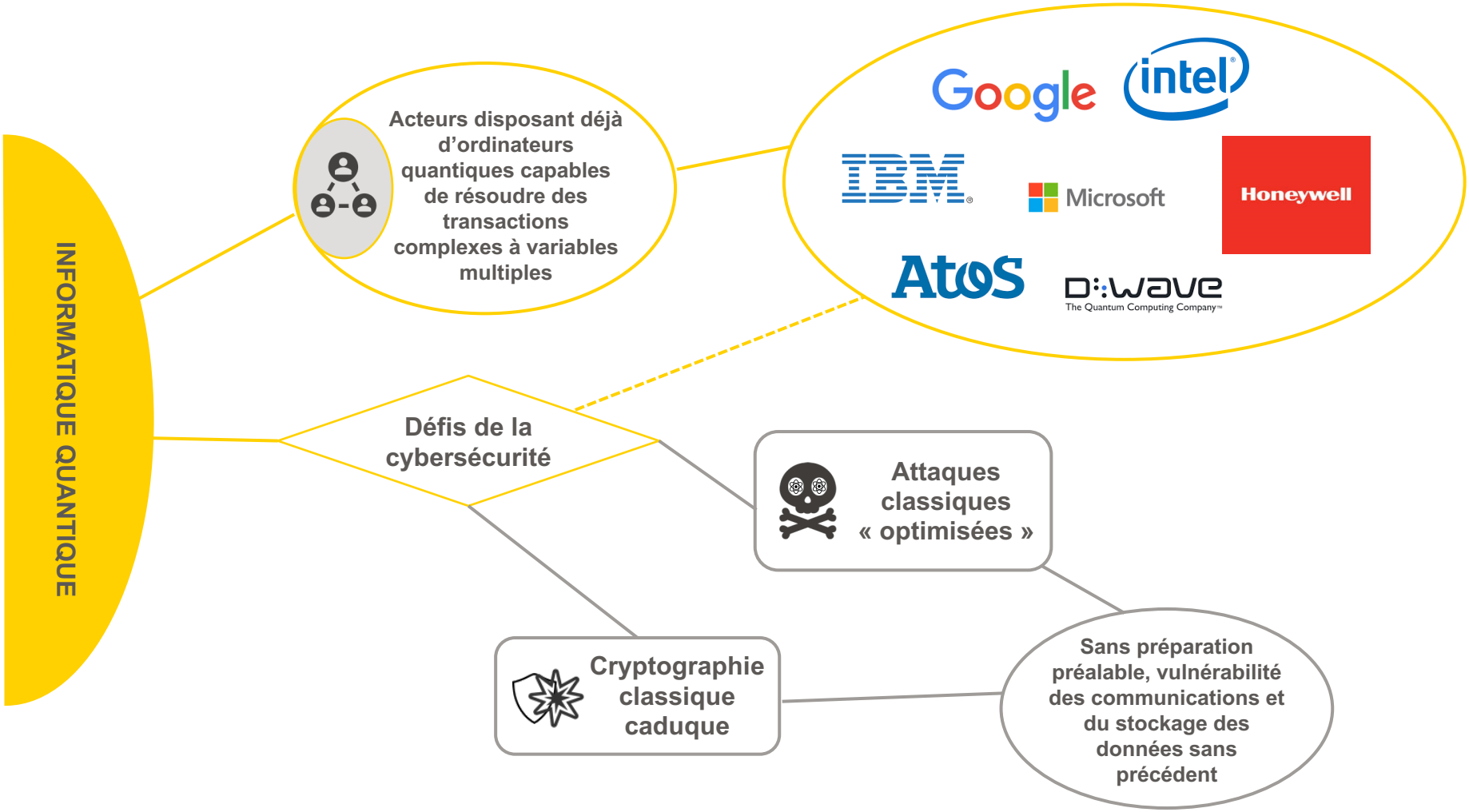
Décohérence	Bruit de fond	Technologie incertaine
Effondrement naturel de l'état quantique	Facteurs extérieurs conduisant à la décohérence	Faible standardisation des Qubits et de la programmation

// AGENDA

1. Qu’est-ce que l’informatique quantique ?
2. **Pourquoi s’en préoccuper dès aujourd’hui ?**
3. Les pistes de réponse à la menace
4. Enjeux et hypothèses d’évolution

Create trust,
build performance

Emergence de l'informatique quantique & Cybersécurité



A terme, les développements de l'informatique quantique auront des implications pour la sécurité nationale en raison de leur capacité à casser les méthodes cryptographiques actuelles.

Une menace en puissance

Une menace majeure

Optimisation sans précédent du décryptage par force brute des algorithmes de chiffrement des communications

Facteurs favorisant l'adoption par les pirates

QaaS
Quantum as a Service
(Azure, AWS, IBM)

Etat-Nations
Course aux armements

Décryptage rétroactif
Faible risque, gain élevé

Quelques chiffres

50 % Taux de chance que l'un des standards cryptographiques majeurs soit brisé dans les 15 prochaines années.

Année à partir de laquelle l'ANSSI ne labellise plus d'entreprise non « quantic resistant ». **2020**

1 MM$ Budget rassemblé par le gouvernement américain pour développer des centres de recherche quantique entre 2021 et 2025.

Temps nécessaire à un ordinateur quantique pour décrypter une clef de chiffrement RSA de 2048 bits (contre 1 MM d'années avec la méthode classique). **100"**

// AGENDA

1. Qu’est-ce que l’informatique quantique ?
2. Pourquoi s’en préoccuper dès aujourd’hui ?
3. **Les pistes de réponse à la menace**
4. Enjeux et hypothèses d’évolution

Create trust,
build performance

Les moyens de défense

Algorithmes à base de treillis : l'ère du *zero knowledge*

Principe : cacher les données à l'intérieur de problèmes mathématiques complexes.

Avantage : possibilité d'effectuer des traitements directement sur les données chiffrées sans avoir à les déchiffrer.

Inconvénient : incertitudes sur la rapidité de l'évolution de la puissance de calcul quantique (loi de Neven).

Communication contrefactuelle : la S-F en marche

Principe : transmission d'une information sans échange de particules (contrairement à la téléportation) grâce à l'effet Zénon.

Avantage : interception physiquement impossible à réaliser.

Inconvénient : ce type de communication exige de maintenir un canal quantique intègre sur la distance qui sépare les interlocuteurs.

Cryptographie post-quantique : faire du neuf avec du vieux

Principe : proposer de nouveaux algorithmes basés sur la cryptographie classique, même pour des ordinateurs quantiques.

Avantage : les algorithmes peuvent être expérimentés sur les ordinateurs traditionnels, selon les procédés cryptographiques déjà existants.

Inconvénient : pour élaborer de tels algorithmes, le plus simple serait d'utiliser des ordinateurs quantiques.

Cryptographie quantique : combattre le feu par le feu

Principe : utiliser les propriétés de la physique quantique et des qubits pour créer des parades, comme la distribution de clefs quantiques (QKD).

Avantage : théoriquement incassable : toute tierce personne essayant d'accéder au message le détruit.

Inconvénient : exige la modification des infrastructures de communication physique, comme la fibre optique.

Vers une cryptographie hybride : *Combiner la cryptographie quantique et la cryptographie post-quantique*

Anticiper les impacts - Gestion du risque d'attaques quantiques

Penser une feuille de route de gestion des risques liés au quantique

Etude du Contexte

Inventaire
Identification des ressources IT concernées.

Parties Prenantes & Expertise
Penser les futurs besoins RH
Se familiariser avec les solutions techniques existantes.

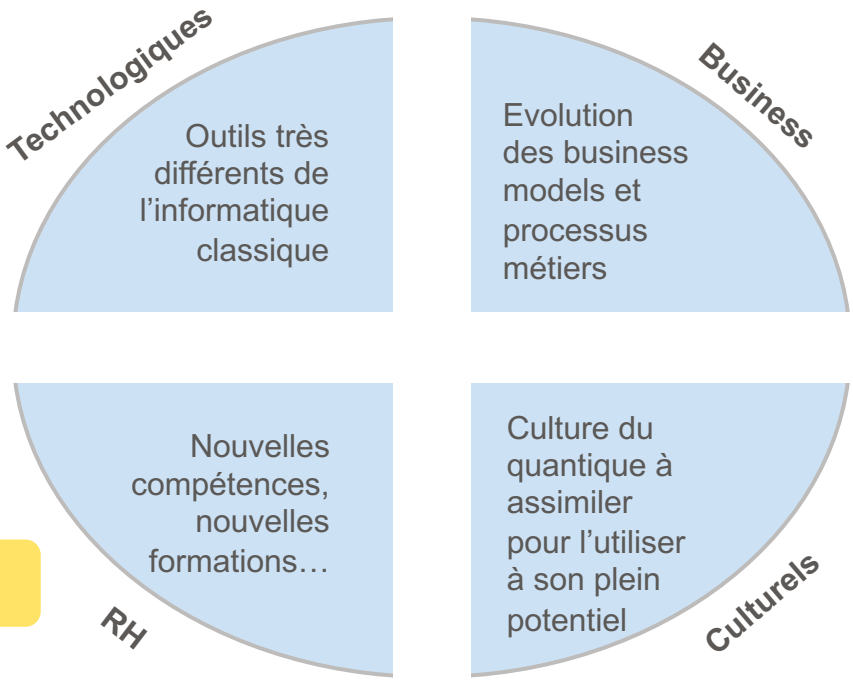
Expression des besoins de sécurité

Etude des menaces

Risques

Mesures de sécurité : alternatives de cybersécurité

4 impacts majeurs



L'agilité et la capacité de résilience des entreprises sera mise à rude épreuve : dans beaucoup de domaines, il pourrait s'agir d'un enjeu aussi crucial que l'adoption d'Internet et des nouveaux usages numériques.

// AGENDA

1. Qu’est-ce que l’informatique quantique ?
2. Pourquoi s’en préoccuper dès aujourd’hui ?
3. Les pistes de réponse à la menace
4. **Enjeux et hypothèses d’évolution**

Create trust,
build performance

Trois constats, trois enjeux majeurs

Crédibilité sociale

UN ENJEU BUSINESS ET DE SOUVERAINETÉ

- Intérêt croissant des grands acteurs du numérique
- Recherche d'un avantage concurrentiel et géopolitique
- Investissement massif dans le domaine

ENJEU

Se positionner en pionnier du secteur, détenir la connaissance pour des raisons économiques, géopolitiques et de prestige

DES DÉFIS TECHNIQUES SURMONTABLES

- Simplification des conditions de fonctionnement
- Méthodes de communication quantique déjà éprouvées
- Hybridation : optimisation des pratiques existantes

Proposer un produit fiable et simple d'utilisation

ENJEU

Crédibilité technique

UN MODÈLE ÉCONOMIQUE À CONCEVOIR

- L'ouverture au grand public est conditionnée à un modèle rentable
- Un modèle de cloud quantique sûrement différent des modalités de cloud classique
- Plusieurs technologies en concurrence à l'heure actuelle

ENJEU

Proposer un modèle économique viable pour ouvrir cette technologie aux organisations privées et permettre un nombre croissant d'investissements

$ Crédibilité économique €

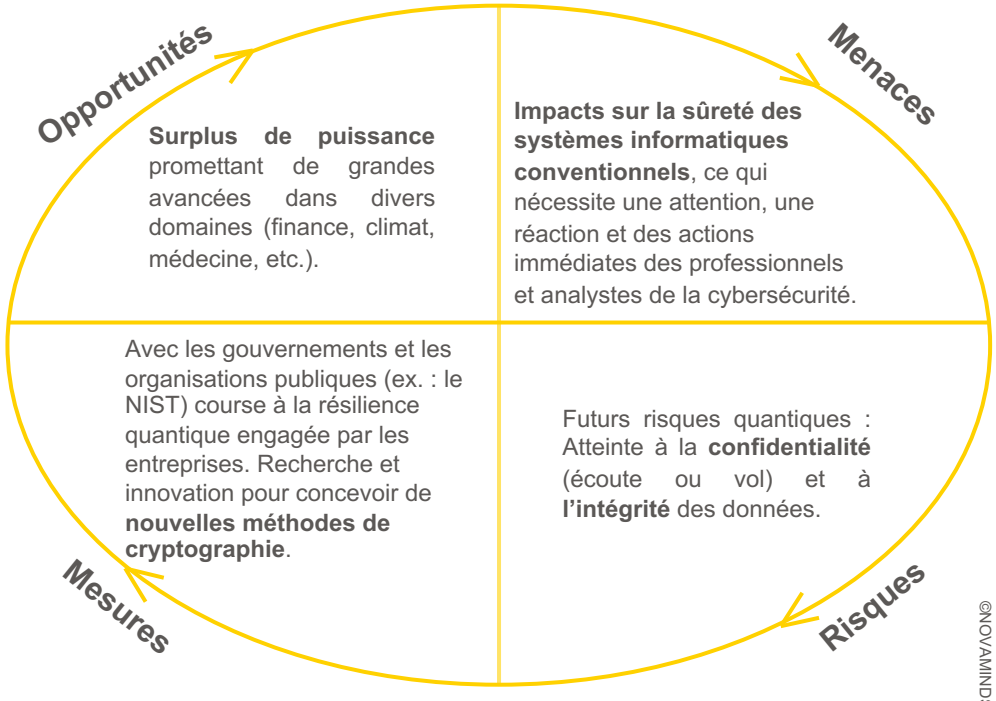
Conclusion : une véritable révolution… en puissance

L'informatique quantique demeure pour le moment une révolution en puissance. Ceci étant dit, que peut-on retenir des attentes et des précautions pour ce domaine ?

A long terme : une véritable révolution dont on ne peut sans doute pas encore percevoir l'ampleur tant les domaines économiques, sociaux et scientifiques qu'elle touche sont variés et nombreux.

A moyen terme : l'informatique traditionnelle sera soumise à une hybridation croissante avec l'informatique quantique. Développement des capacités d'attaque et de défense dans ce nouveau contexte.

A court terme : prise de position et investissement d'acteurs économiques et politiques majeurs. Développement de langages de codes et réflexion sur les moyens de défense face à des attaques quantiques.



Et le secteur bancaire en général ?

Le secteur bancaire en sera le premier bénéficiaire. A titre d'exemple, JPMorgan développe déjà avec IBM des outils quantiques destinés à optimiser les stratégies de trading, la gestion des portefeuilles de titres, l'évaluation des actifs et l'analyse de risques.

Limites

- Domaine d'activité aux contours encore mal définis
- Incertitudes techniques
- Course à la communication et informations parfois contradictoires

// Références

- SD Magazine, « *La révolution quantique : entre stratégie et adoration* », Septembre 2019
- CIGREF, « *Informatique quantique : comprendre le quantum computing pour se préparer à l'inattendu* », Janvier 2020
- ZDNet, « *Tout comprendre à l'informatique quantique* », Septembre 2019
- Communications of the ACM, « *Cyber Security in the Quantum Era* », Avril 2019
- Le MagIT, « *Informatique quantique : pourquoi la cybersécurité doit s'y préparer dès aujourd'hui* », Août 2020
- Cyberguerre par Numerama, « *Comment la cryptographie se prépare à faire face aux cyberattaques quantiques* », Janvier 2020.

// CONTACT

Nicolas VETRIAK

Président Fondateur

Create trust,
build performance