CIM.PP

Et l'avenir !

Nous sommes passés en 60 ans, des machines à cartes perforées aux ordinateurs d'aujourd'hui, aux data-center, à internet, aux smartphones, aux Cloud, aux débuts des objets connectés, en passant par les bandes magnétiques, les énormes disques durs, les disquettes, les cd-rom, etc….

Tenter de se projeter sur les 20 ou 30 années qui viennent serait très risqué, car qui aurait pu dire dans les années 90 où nous en serions aujourd'hui !

L'avenir de l'informatique !

C'est un terme qui revient de plus en plus souvent, il reposerait sur des calculateurs **de type quantique.** Concrètement ces technologies sont censées changer la face du monde, mais il ne s'agit que d'une promesse, car ces technologies ne sont pas encore disponibles, le seront-elles un jour, seront-elles vraiment utiles ?

Qu'est-ce qu'un ordinateur quantique ?

Sous cette appellation se trouve un panel de technologies reposant sur les propriétés quantiques de la matière. Contrairement à un système **numérique dit « normal »** qui s'appuie sur des données codées en chiffres binaires (**les fameux bits 0 et 1**), le calcul quantique utilise un autre élément de base : le qubit ou bit quantique. Celui-ci n'est autre que l'état quantique qui représente la plus petite unité de stockage d'information quantique. Explication :

Un bit classique se trouve toujours **soit à l'état 0, soit à l'état 1**. Il n'a aucune autre possibilité.

Au lieu des bits que les ordinateurs traditionnels utilisent, un ordinateur quantique utilise des bits quantiques, appelés qubits. Pour illustrer cette différence, imaginez-vous une sphère.

Un bit peut exister à l'une ou l'autre des extrémités de cette sphère, mais un qubit peut exister à n'importe quel point de cette sphère.

Cela signifie qu'un ordinateur utilisant les qubits peut stocker une très grande quantité d'informations, tout en utilisant moins d'énergie qu'un ordinateur classique. Dans cet informatique quantique où les lois traditionnelles de la physique ne sont plus, nous pouvons créer des processeurs significativement plus rapides (environ un million de fois plus rapides) que ceux que nous utilisons aujourd'hui. *Fantastique*, direz-vous, mais le challenge repose sur le fait que l'informatique quantique est incroyablement complexe.

Chaque qubit pouvant assumer un tel éventail de valeurs, un petit nombre d'entre eux peut contenir une quantité folle d'informations. Ainsi, une mémoire à qubits diffère significativement d'une mémoire classique.
Exemple : seulement 100 qubits pourraient stocker 1 267 650 600 228 229 401 496 703 205 375 de nombres différents… Aucun ordinateur moderne n'est capable de telles performances.

Pour l'heure, les ordinateurs quantiques ne sont que de l'ordre du rêve, de l'utopie, voire du fantasme. Finalement, pour répondre à cette question :
Est-il possible que l'informatique quantique soit l'avenir de l'ordinateur.

Nous dirons simplement qu'il est encore impossible de le savoir, malgré le potentiel évident de ces technologies. Si avenir il y a, il n'est hélas pas certain que ce soit pour demain ou les 20 ans qui viennent.

Toute la pression repose sur les épaules de l'industrie de informatique, afin de trouver des moyens de le rendre plus efficace, puisque nous avons déjà atteints les limites des méthodes classiques. D'ici **2040**, d'après un rapport de la *Semiconductor Industry Association*, nous ne serons plus en mesure d'alimenter tous les appareils du globe. C'est précisément la raison pour laquelle l'industrie informatique tente actuellement de rendre les ordinateurs quantiques fonctionnels afin de les vendre. Pas un petit exploit, mais un qui apportera énormément de bénéfices.

Comment notre monde va changer avec l'informatique quantique

Il est difficile d'exactement prédire dans quelles mesures l'informatique quantique révolutionnera notre monde, parce qu'il sera appliqué à toutes les industries. Nous nous aventurons dans un domaine absolument inédit de la physique, où des solutions et utilisations n'ont jamais été encore pensées.

Mais lorsque vous songez à la manière dont les ordinateurs classiques ont bouleversé nos sociétés, avec une relative simple utilisation de bits et de 0 et de 1, vous pouvez imaginer quelles possibilités extraordinaires apportera l'informatique quantique dans son pouvoir de traitement par qubits, capable d'effectuer des millions de calculs en même temps.

.

Les objets connectés

« Avec l'Internet des objets (ou *Internet of things – IoT*) les données ne sont plus créées par les internautes mais directement captées par les objets. Elles sont produites par l'environnement et l'activité de ceux qui les possèdent.
L'objectif annoncé de ces produits est la simplification du quotidien des utilisateurs. L'objet réagit de façon autonome, influence son propriétaire et diffuse des comptes rendus sur les réseaux. En 2014, le marché a explosé mais la sécurité n'a pas été la priorité des fabricants et des prestataires, loin s'en faut.

À l'horizon 2015/2016, on peut prédire la multiplication des *thingbot* et des atteintes à la vie privée. Les objets connectés pourraient également devenir de nouveaux outils pour la criminalité dite « classique » et de nouvelles portes d'entrée sur les systèmes d'informations du monde industriel et de la sphère privée (*ransonware* physiques par la paralysie d'objets domestiques). »

Tout ceci est une réalité, un objet connecté diffuse des informations sur les réseaux, ces informations pouvant être interceptées et manipulées. Nous avons dit plus haut que ces nouveautés (au demeurant intéressantes à certains niveaux) allaient poser des problèmes d'une autre nature liée à la **liberté et à l'intimité des individus,** et nous y sommes !

Objets connectés….. avenir des ordinateurs de type quantique (Google serait sur le coup et sûrement d'autres), le rêve informatique risque de devenir cauchemar.

Il y a eu et il y a encore la dictature de certains états, nous risquons d'assister à l'émergence d'un autre type de **dictature, celle des systèmes d'information**.

Comment se protéger des risques liés aux systèmes actuels et futurs ? vaste question lorsque l'on constate les insuffisances actuelles et l'inertie des différents acteurs dont nos politiques……que dire du futur dont on a quelques perceptions à travers les systèmes quantiques qui, en matière de cryptage, de protection par mot de passe ou autres, mettrait toutes nos connaissances actuelles au panier.

Ceci n'est pas sans faire peur car de telles machines de 'guerre' pourraient aisément casser de nombreux systèmes cryptographiques. Imaginons l'avantage pour le pays qui disposerait de ce super pouvoir.

Malheureusement comme dans beaucoup de domaines, il va falloir attendre que des catastrophes se produisent pour tenter de minimiser les risques, or c'est dès maintenant qu'il faut s'en préoccuper en partant du postulat suivant :
Tous les systèmes de protections actuels sont appelés à devenir caduques à plus ou moins brève échéance, et tous les systèmes de protection ont et auront leurs failles, ce qui n'interdit pas de s'en préoccuper.

Qui sait qu'aujourd'hui, une loi sur le renseignement devrait légaliser des gadgets utilisés jusqu'ici…. en douce. Ex :

- **La valise IMSI-Catcher** – Placée dans un lieu public, elle capte tous les téléphones situés dans un rayon de 100 mètres.
- **Les capteurs de puces** – Capables de lire jusqu'à 15 mètres les puces sans contact (cartes de crédit,…), et enregistrer leur contenu.

- **Les mouchards internet** – Posés chez les opérateurs, ils surveillent le comportement des internautes et alertent en cas de ???? heures de connexion, mots clés, chiffrement,….
- **Le smartphone** – Bien qu'éteint un téléphone peut servir de micro espion et capter à distance les conversations.

Nul besoin d'être spécialiste ou expert en sécurité informatique pour comprendre à partir de ces quelques exemples, que tous les systèmes de protection vendus et réputés comme tels ne le sont pas vraiment…… c'est avant tout un business très lucratif. Il est vrai qu'ils ont eu à une certaine époque pas si lointaine leur utilité, mais maintenant leur avenir est compté.

Comme nous l'avons souligné plus haut : **le dernier et ultime rempart est l'utilisateur, celui qui :**

- **est devant son écran,**
- **utilise un téléphone portable,**
- **utilise une carte de crédit,**
- **utilise la technologie des objets connectés**
- **etc…**

La **meilleure protection**, sans pour autant tomber dans la paranoïa, est avant tout **l'information et la vigilance des utilisateurs.**

Les systèmes de protection d'accès :

Comme le nom l'indique, protection d'accès au sens le plus large (bâtiments, pièces particulières, véhicules, ordinateurs, téléphones, tablettes, …)

La reconnaissance par code – la plus ancienne

La reconnaissance faciale – Elle n'est pas nouvelle dans le monde de l'informatique. Objet de tous les fantasmes dans la vie des espions ou dans le quotidien, cette technologie a toujours suscité la méfiance, surtout au moment où elle gagne en précision et en fiabilité. Facebook a de quoi être intéressé, et ses scientifiques travaillent sur le projet DeepFace dont les résultats en termes de reconnaissance faciale dépassent les espérances.

La reconnaissance digitale - Il aura fallu moins de deux jours aux hackers pour venir à bout du mécanisme de reconnaissance des empreintes digitales du nouvel iPhone 5S, présenté par Apple comme ultra sécurisé.

La reconnaissance par l'iris - La biométrie par l'iris est une des technologies (avec la rétine) qui assure un haut niveau de sécurité. L'iris procure une unicité très élevée (1 sur 10 puissance 72) et sa stabilité est étendue jusqu'à la mort des individus, d'où une fiabilité extraordinaire.

Des techniques actuelles de reconnaissance, seules la faciale et par l'iris ont des taux de fiabilité très élevés. Pour le moment les autres semblent avoir vécu.

La sécurité

Les systèmes de sécurité actuels sont conçus (en imageant) comme un réseau de barbelés autour d'une résidence….parfois difficile d'entrer, mais une fois à l'intérieur !!!! la différence avec un ordinateur, c'est que les barbelés (outils de protection) sont à l'intérieur et que les portes sont grandes ouvertes à travers les réseaux.

L'éventuelle émergence des ordinateurs de type quantique va, comme vu plus haut, casser tout les codes de protection connus. Alors, que faire ?

Les systèmes de protection d'accès ne règlent qu'une faible partie des problèmes liés à la sécurité. En effet, comme nous l'avons vu plus haut tout est maintenant connecté sur l'extérieur.

Ca n'est pas être alarmiste que d'être conscient. La technologie évolue, les hackers s'adaptent et ont très souvent '**un coup d'avance'**. Il n'y a pas qu'eux, il y a aussi tout ces grands groupes qui proposent le « Cloud » pour sauvegarder vos données personnelles, les réseaux sociaux, les fournisseurs d'accès, les fournisseurs d'outils en ligne…… tout ce petit monde engrange des tonnes d'informations (volontairement ou à votre insu) et en conserve la maîtrise – il faut souligner aussi que tous grands qu'ils puissent-être, ils ne sont pas à l'abri des pirates (hackers). C'est le serpent qui se mord la queue.

Tous systèmes aussi pointu soit-il a et aura toujours ses failles, la sécurité à 100% n'existe pas. La seule chose que l'on puisse faire, c'est de tenter de limiter la « casse » en tentant de respecter quelques règles élémentaires comme citées plus haut, mais surtout en **étant vigilant quant à l'utilisation de nos ordinateurs**, **tablettes, smartphones, cartes de crédit, etc…**

Comme nombre d'inventions avant elles, la mécanographie puis l'informatique ont fait faire un bond extraordinaire à nos sociétés depuis le début des années 60, mais comme dans toutes les avancées, chaque médaille a son revers et génère à un moment donné d'autres problèmes, et les exemples sont nombreux..

Electricité, énergie nucléaire, moteur à explosion, automobile, médecine, médicaments, chirurgie, vieillissement, démographie, eau, pollution,……

L'informatique n'échappe pas à la règle et risque de devenir notre pire cauchemar. Nos sociétés vont promettre monts et merveilles en matière de protection et de surveillance, à travers lois, décrets, etc… , mais ne feront qu'ajouter des textes à l'arsenal législatif déjà existant sans pour autant solutionner.

La cybercriminalité est là. …. menaces sur les infrastructures nationales (**électricité, nucléaire, distribution d'eau, hôpitaux, transports, l'état, les collectivités locales…**) sont bien réelles –

L'exemple récent (9 avril 2015) du piratage **de TV5** monde étaie malheureusement nos propos. Depuis le début de **l'année 2015 plus de 1500 attaques** ont été recensées visant des sites peu protégés**.**

L'Ansii (Agence nationale se la sécurité des systèmes) dispense tous les conseils pour se protéger – ces conseils sont-ils suivis ? on peut en douter !

Il y a eu les guerres de tranchées, sur mer, dans les airs…… aujourd'hui c'est le numérique qui est devenu un espace de combat et de guerre.

En face de la **cybercriminalité et des cyberterroristes, la cyberdéfense des infrastructures nationales** doit-être une priorité, et cela va coûter très très cher !

Il n'y a pas de solution miracle ! la protection passe avant tout par la prévention**.**

LA SOLUTION, certains services de renseignements étrangers l'on trouvé……. **(papier, crayon, bonne vieille machine à écrire)** pour communiquer sur des informations vitales et stratégiques.

Dans certaines circonstances, le retour en arrière est parfois nécessaire avant de trouver les solutions qui s'imposent.