INSTITUT DE FRANCE
L'ESPRIT EN PROGRES
Conférence Nationale des Académies des Sciences, Lettres et Arts
pp 111 - 125

REVOLUTION INFORMATIQUE et COMMUNICATION

par Denis de BRUCQ
Académie des Sciences, Belles-Lettres et Arts de ROUEN

INTRODUCTION

Dans cet exposé, nous allons préciser des découvertes scientifiques en nous restreignant au rôle de quatre savants, à l'origine de la révolution informatique et de la communication. A la suite de Herbert Marshall MAC LUHAN, spécialiste de l'histoire de la communication connu pour son livre : « La Galaxie Gutenberg », rédigé en 1962, il faut comparer les années que nous vivons avec celles suivant la découverte de l'imprimerie par GUTENBERG. Reprenons une citation de Johannes GUTENBERG en 1455 : « Dieu souffre parce qu'une grande multitude ne peut être atteinte par la parole sacrée. La vérité est captive dans un petit nombre de manuscrits qui renferment des trésors. Brisons le sceau qui les lie, donnons des ailes à la vérité, qu'elle ne soit plus manuscrite à grands frais par des mains qui se fatiguent, mais qu'ils volent multipliés par une machine infatigable et qu'ils atteignent tous les hommes. »

Les découvreurs de sciences nouvelles :
Claude SHANNON qui est mort le 24 février 2001 et qui était lauréat de la National Medal of Science.
Ensuite vient Alan TURING, décédé en 1954. En septembre 2009, le Premier ministre britannique a présenté des regrets au nom du gouvernement britannique pour le traitement qui lui avait été infligé.
Une personne peu connue du grand public Jack KILBY. Il est mort le 20 juin 2005 et il était lauréat de la moitié du prix Nobel de physique de l'an 2000. Il était également lauréat du prix de Kyoto en 1993.
Finalement citons pour des raisons personnelles Rudolph KALMAN. Il est membre de la National Academy of Sciences, de la National Academy of Engineering, de l'American Academy of Arts and Sciences, et membre étranger des Académies des Sciences de Hongrie, de France et de Russie.

Quelles sont les disciplines scientifiques, quels sont les dispositifs inventés par ces savants ?

Sur l'Information,
Claude SHANNON donne la mesure de l'Information indispensable pour les canaux de transmissions (radio, télévision, téléphone portable), pour la reconnaissance des formes, des mots, des visages.

Sur l'Intelligence Artificielle
Alan TURING a défini la calculabilité : le modèle abstrait de tout ordinateur !

Sur les dispositifs de communication
Jack KILBY est le découvreur des circuits intégrés, donc de toutes les puces électroniques. Ses travaux ont été développés par des centaines de laboratoires publics ou privés.

Ces circuits intégrés avec les découvertes précédentes sont indispensables pour :
les ordinateurs de bureau, les ordinateurs centraux
le Web
le codage, le chiffrement, le déchiffrement, le décryptage
et donc les transferts d'argent, les cartes bleues
les moteurs de recherche : Alta Vista, Francité, Google, Yahoo

ainsi que pour :

Les applications
Le filtrage de BUCY-KALMAN d'où notamment le programme APOLLO c'est-à-dire le voyage sur la lune.
La robotique : en milieu hostile, l'industrie nucléaire, la prospection en grandes profondeurs sous marines, en chirurgie.

Nous n'introduirons pas les avancées scientifiques sur le génome humain qui, bien sûr, relèvent de la Révolution Informatique et de la Communication ni des aspects quantiques de ces disciplines. Par contre, nous présenterons
La surveillance électronique fait marquant de la société civile.

Deux collègues Marc ENGEL et Michel HUBIN ce dernier de site web http://michel.hubin.pagesperso-orange.fr/ anciens du Laboratoire Perception, Système et Information de l'Université de Rouen ont eu la gentillesse de relire ce manuscrit et je les en remercie.

EXPOSE

Sur l'Information

Avez-vous pratiqué, enfant, le jeu du portrait : Est-ce un animal ? Oui ? Non ? Est-ce une personne ? Oui ? Non ? Est-ce une chose ? Oui ? Non ? Trois questions d'où 3 bits.
Combien faut-il de questions pour trouver un mot dans un dictionnaire ? Or un dictionnaire présente 50 000 mots, et 2 multiplié par 2 seize fois donc 2 à la puissance 16 vaut 65536 supérieur à 50 000 mots qui lui-même est supérieur à 32768, valeur de 2 à la puissance 15. Ainsi, avec 16 questions tout mot du dictionnaire peut être retrouvé et précisons comment. L'intervalle [1, 50 000] est successivement coupé en 2, seize fois. Le nombre de questions à poser, pour obtenir le mot inconnu, s'appelle la quantité d'information. Une indétermination existait avant de connaître le mot choisi. Cette indétermination s'appelle l'entropie et cette entropie est égale à l'information nécessaire pour obtenir le mot, pour supprimer l'indétermination.
Le cas général peut s'appliquer à toute famille d'événements de même probabilité ou même de probabilité différente !

Comme exemple, reprenons les résultats du premier tour des élections présidentielles du 22 avril 2012.

François Hollande	10.273.582 voix
Nicolas Sarkozy	9.753.844 voix
Marine Le Pen	6.421.773 voix
Jean-Luc Mélenchon	3.985.298 voix
François Bayrou	3.275.349 voix
Eva Joly	828.451 voix
Nicolas Dupont-Aignan	644.086 voix
Philippe Poutou	411.178 voix
Nathalie Arthaud	202.562 voix
Jacques Cheminade	89.572 voix

Un de vos amis avait voté et il vous a indiqué pour qui il avait voté. Quelle information vous a-t-il donnée ? Les pourcentages de voix sont considérés par vous, comme les probabilités pour votre ami de choisir son candidat puisque vous ne connaissiez pas ses idées politiques. Le tableau des probabilités vaut, en faisant le rapport du nombre de voix obtenues sur le nombre de votants :

François Hollande	0.2863
Nicolas Sarkozy	0.2718
Marine Le Pen	0.179
Jean-Luc Mélenchon	0.1111
François Bayrou	0.0913
Eva Joly	0.0231
Nicolas Dupont-Aignan	0.0179
Philippe Poutou	0.0115

Nathalie Arthaud 0.0056
Jacques Cheminade 0.0025

La formule à utiliser pour définir l'indétermination s'écrit :
Entropie = - 0.2863 $\log_2$ (0.2863) - 0. 2718 $\log_2$ (0.2718) - 0.179 $\log_2$ (0.179)
- 0.1111 $\log_2$ (0.1111) - 0.1111 l $\log_2$ (0.1111) - 0.0913 $\log_2$ (0.0913)
- 0.0231 $\log_2$ (0.0231) - 0.0179 $\log_2$ (0. 0179) - 0.0115 $\log_2$ (0.0115)
- 0.0056 $\log_2$ (0.0056) - 0.0025 $\log_2$ (0.0025)
Entropie = 2,5062 bits
Chaque citoyen ne donne que 2,5062 bits d'information mais ce chiffre est à multiplier par 35.885.739, le nombre de votants !

Le vote démocratique fournit donc une information considérable 89 936 840 bits !
Dans un autre domaine celui de l'économie, le libre choix du marché, la réponse libre de tout citoyen pour l'achat ou le refus d'achat de chaque produit fournit plus d'information que n'importe quelle méthode dirigiste de l'économie. Notons que l'efficience des services publics français n'est pas contrôlée par le marché mais par le dirigisme d'état et par la Cour des Comptes (cf Jean-Pierre BRULE L'informatique malade de l'état ed. Les belles lettres août 1993). Notons qu'actuellement le marché s'oriente vers des produits allemands ou des produits chinois sinon asiatiques.

Claude SHANNON
http://mapage.noos.fr/fholvoet/shannon.htm
La théorie de l'information est une théorie probabiliste permettant de quantifier le contenu moyen en information d'un ensemble de messages satisfaisant une distribution probabiliste précise. Ce domaine trouve son origine scientifique avec Claude SHANNON qui en est le père fondateur avec son article A Mathematical Theory of Communications publié en 1948.

Il étudie le génie électrique et les mathématiques à l'Université du Michigan en 1932. Il utilise notamment l'algèbre booléenne, les opérations logiques construites avec les et, ou, non , pour sa maîtrise soutenue en 1938 au Massachusetts Institute of Technology (MIT) à CAMBRIDGE à côté de BOSTON, Massachusetts. Claude SHANNON travaille vingt ans au MIT, de 1958 à 1978. Parallèlement à ses activités académiques, il travaille aussi aux laboratoires Bell de 1941 à 1972.
Souffrant de la maladie d'Alzheimer dans les dernières années de sa vie, Claude SHANNON est mort à 84 ans le 24 février 2001 à Medford dans le Massachusetts.

Pendant la Seconde Guerre mondiale, Claude SHANNON travaille pour les services secrets de l'armée américaine, en cryptographie, chargé de localiser, de manière automatique, dans le code ennemi, cachées au milieu du brouillage, les parties signifiantes. Le traitement du signal extrait l'information du signal reçu après réception de la transmission du signal initial, perturbé par le bruit de milieu transmetteur. La totalité de son travail est exposé dans un rapport secret déclassifié dans les années 1980 seulement. Cependant, après la guerre, un article paru en 1948 puis un livre en 1949 sont centrés autour de la problématique de la transmission du signal.
Le schéma de Claude SHANNON
Pour décrire, la communication entre une source et un destinataire, le schéma suivant :
source → encodeur → signal+ bruit → décodeur → destinataire
modélise la communication entre les machines de la source et celles du destinataire.

Le succès de ce schéma est foudroyant, et il a participé largement à la création des sciences de l'information et de la communication.

L'unité de mesure

Dans l'article comme dans le livre, Claude SHANNON popularise l'utilisation du mot bit (binary digit) comme mesure élémentaire de l'information numérique.

John TUKEY fut néanmoins le premier à utiliser le terme de bit. John TUKEY est né en 1915, à New Bedford (Massachusetts), dans une ville de pêcheurs sur la côte du New Jersey. Ses parents sont tous deux enseignants. Enfant surdoué, il apprend à lire, seul, dès l'âge de trois ans. Il ne fréquente pas l'école, ses parents, prenant en charge, son instruction.
En 1959, il met au point les techniques mathématiques de déconvolutions permettant de repérer les essais nucléaires souterrains.
Dans les années 1970, il est à la tête du comité qui met en garde les autorités américaines contre les effets dévastateurs des aérosols sur la couche d'ozone.

Reprenons le rôle du bit. Celui-ci désigne la quantité d'information nécessaire en nombre binaire pour effectuer un codage. Ainsi, il faut, au moins, un bit pour coder deux états ; par exemple « pile » et « face », ou plus généralement 0 et 1. Il faut deux bits pour coder quatre éléments {00, 01, 10, 11}. Les 26 lettres de l'alphabet, soit 26 éléments, nécessitent au minimum 5 bits puisque :

$2^4 = 16 < 26 < 2^5 = 32$

Plus généralement, si N est le nombre d'éléments à considérer, le nombre de bits minimum k nécessaire pour tous, les coder, vérifie :

$2^{(k-1)} < N <= 2^k$

Dans le cas idéal où toute l'information disponible est utilisée, N vaut 2^k.

Entropie au sens de Claude SHANNON

Un apport essentiel des travaux de Claude SHANNON concerne la notion d'entropie. Si l'on considère I événements de probabilité $p_1, p_2, \ldots, p_I$, incompatibles entre eux, alors leur entropie de Claude SHANNON est définie comme :
Entropie = $- \Sigma_{i=1}^{I} p_i \log_2(p_i)$ exprimée en bits

Cette quantité s'appelle l'entropie de la distribution de probabilité. C'est une mesure du désordre de la répartition de probabilité. Claude SHANNON a par ailleurs établi un rapport entre gain d'information et diminution de l'Entropie de Ludwig BOLTZMANN 1844-1906 en thermodynamique.
Dans l'exemple retenu ci-dessus, dire pour qui, votre ami a voté, supprime un doute, un désordre et il vous a fourni la quantité d'information nécessaire à la levée de ce doute.
Pour résumer, de façon didactique, dans une situation aléatoire, la quantité d'information en bits est le nombre de questions nécessaires pour déterminer la situation.

Théorèmes

Le nom de Claude SHANNON est associé à plusieurs théorèmes :
le Théorème d'échantillonnage de NYQUIST-SHANNON,
un théorème sur la limite théorique de la compression d'information
un théorème sur la capacité d'un canal de transmission.

La découverte du concept d'Entropie a ouvert la voie aux méthodes dites d'entropie maximale, donc au scanner médical, à la reconnaissance automatique des caractères et à l'apprentissage automatique.
Ces méthodes comprennent une représentation partielle de l'état et une fonction de coût. Plus précisément, sur l'exemple de la recherche automatique de document sur Internet, les moteurs de recherche (Google, Yahoo, etc.) conduisent à des listes de sites Internet possibles. Il y a lieu de les classer par crédibilité décroissante ; dans cette classification intervient l'aléatoire.

Sur l'Intelligence Artificielle

Quelles questions faut-il poser et dans quel ordre les poser, pour déterminer une inconnue ?
Est-ce que toute notion est atteignable par des questions ? Oui ? Non ?
Pour le Directeur des Ressources Humaines, quelles questions doit-il poser pour savoir si le candidat à l'embauche sera un personnel performant ?
Existe-t-il un nombre fini de questions pour obtenir comme conclusion l'existence ou la non-existence de DIEU ? Oui ? Non ?
La notion de calculabilité s'introduit ici : tout n'est pas calculable, qu'est-ce qui est calculable ?

Que veut dire faire un calcul ? Que veut dire effectuer un algorithme ?
En 1936, Alan TURING a imaginé un modèle abstrait pour définir une notion qui jusqu'alors était restée intuitive : la calculabilité. Ce modèle abstrait de Alan TURING est aujourd'hui connu sous le nom de machine de TURING et ce modèle est encore utilisé en informatique théorique pour résoudre les problèmes de calculabilité.

<u>Un exemple de Machine de TURING</u>

La machine de TURING qui suit effectue la multiplication par deux et de façon imagée provient de la division de troncs d'arbres en deux. De 3 troncs d'arbres, les bûcherons passent à 6 (demi-)troncs d'arbres. Sommes-nous capables à l'occasion de cet exemple, de déduire la machine comme l'a fait Alan TURING ?
Lors d'une promenade en forêt, vous observez des bûcherons qui coupent en deux des troncs d'arbres. Plus précisément, état q0, une première machine soulève un tronc, le positionne devant une scie puis, état q1, un élévateur dépose le premier morceau dans le premier emplacement vide. L'élévateur état q2 va ensuite vers la droite pour dépasser le dernier tronc d'arbre coupé et déposer la seconde moitié du tronc d'arbre coupé. Ensuite l'élévateur repart en sens contraire vers la gauche, état q3, dépasse les demi-troncs d'arbre et atteint le vide entre les demis troncs et les troncs entiers. L'élévateur se positionne alors immédiatement à gauche en attente du travail de la scie et nous sommes revenus dans l'état q0, la première machine soulève le second tronc d'arbre, le positionne devant une scie. Puis, état q1, l'élévateur pose le premier morceau du second tronc d'arbre dans le premier espace vide. L'élévateur, état q2, va ensuite vers la droite pour dépasser le dernier tronc d'arbre coupé et déposer la seconde moitié du tronc d'arbre coupé. Ensuite l'élévateur repart en sens contraire vers la gauche, état q3, dépasse les demi-troncs d'arbre et atteint le vide entre les demis troncs et les troncs entiers.
Ensuite le processus continue jusqu'à épuisement des troncs à scier ce que fournit l'Index à l'état q0 qui arrêtera les machines dans l'état qf.
Chaque opération décrite est suivie par un Index

Passons maintenant à la description mathématique des opérations
Sont déjà introduits les états de la machine de TURING q0,q1,q2,q3,…qf et un index qui informe sur le déroulement des actions de la machine. Cet index se déplace vers la droite D ou vers la gauche G sur un ruban infini. Cet index repère la situation dans laquelle se trouve la machine de TURING. La machine de TURING utilise donc un index qui est positionné sur un ruban de longueur infinie et qui fournit le chiffre 0 ou 1 dans la case indiqué par l'Index
Dans l'exemple de la multiplication par deux d'une séquence de 3 chiffres « 1 » entourée de deux suites infinies de « 0 », la machine va multiplier le nombre de « 1 » par 2. Lorsque la machine s'arrêtera, le ruban comportera une suite de 6 chiffres « 1 ».
.

0	0	0	1	1	Index 1	0	0	0	0	0	0	0	0	0

Que va faire la machine ?
Tout dépend de l'état dans lequel se trouve la machine et de la valeur sur le ruban à l'endroit de l'Index. Dans l'exemple, la machine comprend 5 états : q0,q1,q2,q3,qf .
Il s'agit de décrire une fonction qui, à un état pris dans {q0,q1,q2,q3,qf } et à un chiffre de {0,1} donné par l'Index, donne un nouvel état modifié, remplace éventuellement le chiffre sur le ruban et déplace l'Index sur le ruban d'une case vers la droite D ou vers la gauche G. Il faut donc introduire un tableau à deux entrées et sur chaque case du tableau, il faut définir trois valeurs !

N'expliquons pas comment il a été possible à partir de l'exemple des bûcherons de fournir le tableau suivant décrivant la Machine de TURING, effectuant la multiplication par 2.

	Symbole lu : «0» sur le ruban	Symbole lu : «1» sur le ruban
État : qo	qf «0» D (ou G)	q1 «0» D
État : q1	q2 «1» D	
État : q2	q3 «1» G	q2 «1» D
État : q3	q0 «0» G	q3 «1» G

Présentons la signification d'une des cases de ce tableau : pour la case (1,2) dans l'état q0 et pour un symbole «1» provenant de la case fournie par l'index, le nouvel état sera q1, le symbole sur le ruban sera mis à «0» et l'index se déplacera d'une case à droite.

A l'origine, la tête de lecture se trouve à la fin des trois «1» «1» «1» et l'état est par hypothèse q0. Dans cette case qo, «1» la valeur q1, «0», D est écrite dans le tableau ce qui fournit la transition.

0	0	0	1	1	qo, «1» : q1, «0»,D	0	0	0	0	0	0	0	0	0

D'où la phase 1 : la Machine remplace l'état qo par l'état q1, le «1» par «0» puis l'index se déplace d'une case vers la droite.
Ainsi q0 «1» donne q1 «0» D puis q1, «0» donne q2, «1», D

0	0	0	1	1	0	q1, «0» : q2,«1»,D	0	0	0	0	0	0	0	0

A partir de ce premier passage, le lecteur intéressé continuera l'algorithme en vérifiant qu'il obtient par vérification avec le document correctement les diverses phases de la multiplication par deux.

Phase 2: la machine remplace l'état q1 par l'état q2, le «0 » par «1» puis l'index se déplace d'une case vers la droite
q1 «0» donne q2 «1» D puis q2 «0» donne q3 «1» G

0	0	0	1	1	0	1	q2,«0» : q3,«1»,G	0	0	0	0	0	0	0

Ensuite, la machine dans l'état q2 constate que sur le ruban se trouve un 0 aussi l'index revient en arrière G en mettant un « 1 » sur la case qu'elle quitte et passe dans l'état q3

0	0	0	1	1	0	q3,«1» : q3,«1»,G	1	0	0	0	0	0	0	0

Ensuite, la machine dans l'état q3 constate que sur le ruban se trouve un 1 aussi l'index revient en arrière G en mettant un « 1 » sur la case qu'elle quitte et reste dans l'état q3

0	0	0	1	1	q3,«0» : q0,«0»,G	1	1	0	0	0	0	0	0	0

Ensuite, la machine dans l'état q3 constate que sur le ruban se trouve un 0 aussi l'index revient en arrière G en mettant un « 0 » sur la case qu'elle quitte et passe dans l'état q0

0	0	0	1	q0,«1» : q1,«0»,D	0	1	1	0	0	0	0	0	0	0

En reprenant le tableau le lecteur persévérant continuera le fonctionnement de la Machine de TURING pour constater l'arrêt dans la situation suivante

0	0	q0,«0» : qf	0	1	1	1	1	1	1	0	0	0	0	0

De nombreux autres exemples sont aisés à construire. L'alphabet {0,1} peut être remplacé par {vide, un élément}, par tout alphabet dont l'alphabet latin {a,b,…,z}. Le nombre d'états q est quelconque mais fini.
Les informaticiens ont introduit les machines de TURING universelles et alors tous les algorithmes, tous les raisonnements mathématiques, tous les ordinateurs peuvent être modélisés par de telles machines de TURING dites universelles ! Sans doute les bouliers chinois inventés entre 2500 et 3000 ans avant Jésus Christ et la machine arithmétique de Pascal dès 1642 sont des précurseurs des ordinateurs mais il fallait modéliser leurs fonctionnements ce qu'a fait Alan TURING.

Oui TURING est à la base de la révolution informatique. Précisons maintenant quelques faits marquant de sa vie.

Le personnage

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=complements/turing

Durant la Seconde Guerre mondiale, Alan TURING dirige en Angleterre les recherches sur les codes secrets générés par la machine Enigma utilisée par les militaires allemands pour communiquer Etat major, Unités Combattantes.

Le travail d'Alan TURING sur le décryptage des messages Enigma lors de l'opération Ultra, fut tenu secret militaire jusque dans les années 1970 ; mêmes les plus proches amis d'Alan TURING n'étaient pas au courant de ces recherches.

Alan TURING par un article « Computing Machinery and Intelligence » (Mind, octobre 1950) se trouve également à l'origine de l'intelligence artificielle. Il développe cette idée par des articles « L'intelligence de la machine, une idée hérétique » « Les calculateurs numériques peuvent-ils penser ? » ou par des discussions avec M.H.A. NEWMAN, Geoffrey JEFFERSON et R.B. BRAITHWAITE les 14 et 23 janvier 1952 sur le thème « Les ordinateurs peuvent-ils penser ? ».

L'homosexualité d'Alan TURING lui valut d'être persécuté et brisa sa carrière après 1945. Lors d'une enquête, la police finit par l'accuser d'« indécence manifeste et de perversion sexuelle » d'après la loi britannique sur la sodomie. Il décide d'assumer son orientation sexuelle. S'ensuit un procès très médiatisé, où lui est donné le choix entre l'incarcération ou une castration chimique, réduisant sa libido.

A partir de 1952, il sera écarté des plus grands projets scientifiques.

En 1954, il se suicide par un empoisonnement au cyanure. Le moyen d'ingestion du poison aurait été une pomme partiellement mangée, retrouvée près du corps de Alan TURING et qui aurait été imbibée de cyanure. Une légende tenace y voit l'origine du logo de la firme Apple.

Cet exposé a pour titre Révolution Informatique et Communication. Cependant la vie de Alan TURING révèle également l'importance d'une autre révolution, celle portant sur les mœurs. L'amour et non la procréation seraient la raison du mariage civil entre deux personnes. Faut-il comparer avec les pays voisins ? Les pays voisins ne sont pas forcément la Belgique, l'Espagne etc. puisque à l'époque de la mondialisation les mondes musulman ou russe sont proches. La Compromis sinon la Vérité reste à trouver !

Les développements de l'Intelligence Artificielle portent également sur une approche pragmatique d'ingénieur c'est-à-dire cherchent à construire des systèmes, de plus en plus autonomes, pour réduire le coût de leur supervision par un être humain.

Ainsi, la machine essaie de simuler l'intelligence de l'homme, elle semble agir comme si elle était intelligente. Certains logiciels d'Intelligence Artificielle parviennent à imiter, plus ou moins bien, les dialogues d'humains face à d'autres humains.

On peut considérer différents dispositifs intervenant, ensemble ou séparément, dans un système d'intelligence artificielle tels que :

les traductions automatiques entre langues, si possible en temps réel

le raisonnement automatique comme les systèmes experts,

l'apprentissage automatique,

l'intégration automatique d'informations provenant de sources hétérogènes, la fusion de données,

la reconnaissance de formes, des visages et la vision en général,

etc.

Les réalisations actuelles de l'Intelligence Artificielle peuvent intervenir dans les fonctions suivantes :
la résolution de problèmes complexes, tels que les problèmes d'allocation de ressources. (l'attribution des salles de classes entre élèves, professeurs)
l'assistance par des machines dans les tâches dangereuses, l'industrie nucléaire, les fonds sous marins, ou demandant une grande précision comme en chirurgie,
l'automatisation de tâches répétitives,
la reconnaissance de la parole,
la reconnaissance de l'écrit,
l'aide à la décision,
l'aide aux diagnostics médicaux.
la robotique.

Sur les dispositifs de communication
Et le passage de l'électronique analogique à l'électronique numérique, il faut citer :
Jack Saint Clair KILBY
http://www.universalis.fr/encyclopedie/jack-st-clair-kilby/
Il est né à Jefferson City, dans l'État du Missouri, le 8 novembre 1923 et il est mort à Dallas au Texas, le 20 juin 2005.
Travaillant pour Texas Instruments, cet ingénieur électricien dépose, le 6 Février 1959, un brevet intitulé « Solid Circuit made of Germanium », le premier circuit intégré, lançant une industrie qui pesait mille milliards de dollars déjà en 2005.
En l'an 2000, il est lauréat du Prix Nobel de Physique pour son innovation : le circuit intégré.
En plus du circuit intégré, Jack KILBY est l'inventeur de la calculatrice de poche, de l'imprimante thermique utilisée dans les caisses enregistreuses, au total, il y a 60 brevets à son nom.

Jack KILBY a la paternité du premier circuit intégré car Robert NOYCE, futur co-fondateur d'INTEL, travaillait sur un dispositif identique à la même époque et proposait un autre dispositif viable : l'interconnexion au moyen d'une couche de métal conductrice mais cette technique n'a pas eu le même avenir.
Pour Jack KILBY, l'extérieur du circuit intégré y accède à travers des connexions réparties à la périphérie du circuit. Ce concept révolutionnaire concentre dans un volume incroyablement réduit, un maximum de fonctions logiques.
Les circuits intégrés numériques, les plus simples, sont des portes logiques (et, ou, non), les plus complexes sont les microprocesseurs et les plus denses sont les mémoires. On trouve de nombreux circuits intégrés dédiés à des applications spécifiques (appelé ASIC pour Application Specific Integrated Circuit), notamment pour le traitement du signal, le traitement d'image et la compression vidéo. Une famille importante de circuits intégrés est celle des composants de logique programmable.
Aujourd'hui plusieurs dizaines de millions de portes représentent un chiffre normal pour un microprocesseur, pour un circuit intégré graphique ou hautement parallèle, de qualité.

Le codage
Dans un ordinateur, au niveau matériel, tout est codé en binaire c'est-à-dire uniquement à partir de 0 et de 1.

D’une façon générale, un codage permet de passer d'une représentation des données vers une autre. Parmi les différents codages utilisés, on trouve :
Le codage de caractères pour représenter informatiquement l'ensemble des caractères, comme par exemple le code ASCII (American Standard Code for Information Interchange).
Tout entier numérique en base 10 s’écrit sans difficulté en base 2. Par exemple, en base 10 le nombre $9= 1*2^3+0*2^2+0*2^1+1*2^0$ est codé 1001 en base 2.
En binaire, 8 bits forme un octet listé 0,1,…,9,A,B,C,D,E,F.

Le codage de source permet de faire de la compression de données.
Les sources sonores analogiques ou les sources vidéo sont mises en format informatique d’où les codes MP3, WMA,… pour le son ou AVI, MP4, VOB …pour les vidéos. Dans ces cas, il ne s'agit plus rigoureusement d'un codage, puisqu’il ne s'agit plus d'opérations réversibles : ces codages conduisent à une perte d’information et les signaux initiaux ne peuvent plus être récupérés. Le passage d'un format audio ou vidéo à un autre peut aussi s'appeler le transcodage.
Les langages de programmation utilisés pour écrire les algorithmes mathématiques, les langages comme le Fortran, le Basic, le C ou le Pascal (DELPHI) sont assez proches du langage courant pour être lisibles; ils sont compilés et stockés sous forme binaire pour pouvoir être exécutés par les ordinateurs.
Le langage HTML (Hypertext Markup Language) est le langage des transmissions Internet.

Le codage canal permet une représentation des données de façon à être résistant aux erreurs de transmission, aux bruits. Ces codages comprennent des digits de contrôles permettant la détection ou même la correction d’erreur de transmission.
Bien qu'il s'agisse également d'un codage, on utilisera le terme de chiffrement quand le codage utilisé, cherche à masquer l'information contenue.
La cryptographie est une discipline assurant confidentialité, authenticité et intégrité des messages en s'aidant souvent de clés. Elle est utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, datent de la fin du XXe siècle. N’écrivez jamais en clair vos diverses clefs de carte bleue, de coffre fort, d’ouverture de compte bancaire (login) sur Internet. Utilisez des codes simples dont la mémorisation est facile pour chiffrer vos clefs avant de les écrire sur votre carnet.
À cause de l'utilisation d'anglicismes puis de la création des chaînes de télévision dites « cryptées », une grande confusion règne concernant les différents termes de la cryptographie :
chiffrement : c’est la transformation à l'aide d'une clé, d'un message en clair, dit texte clair, en un message incompréhensible dit texte
déchiffrement : retrouve le message clair correspondant à un message chiffré, le texte en possédant la clé de déchiffrement
décrypter : retrouve le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.
Il apparaît donc que le terme « crypter » n'a pas de raison d'être. L'Académie Française précise que le mot est à bannir et celui-ci ne figure pas dans son dictionnaire, en tout cas pas dans le sens où on le trouve en général utilisé. Toutefois, l'Office Québécois de la langue française intègre « crypter » au sens de « chiffrer » dans son grand dictionnaire terminologique.

Rudolf KALMAN
http://www.ieeeghn.org/wiki/index.php/Rudolf_E._Kalman

Rudolf KALMAN est né à Budapest en Hongrie le 19 Mai 1930. Il obtient son master's degree en 1954 au MIT, en ingénierie électrique, puis son doctorat en 1957 à l'Université Columbia.
De 1964 à 1971, il est professeur à l'Université Stanford, Californie puis de 1971 à 1992 à l'Université de Floride à Gainesville. Il a été conseiller scientifique pour l'école des Mines de Paris. À partir de 1973, il occupe la chaire de théorie des systèmes mathématiques à l'École polytechnique fédérale de Zurich (EPFZ).
Rudolf KALMAN est membre étranger des Académies des Sciences de Hongrie, de France et de Russie.

Travaux
Rudolf KALMAN est surtout connu pour sa contribution à l'invention du filtre de KALMAN. Cependant, ce filtrage trouve son achèvement en 1961 avec Richard BUCY pour s'appeler le filtrage de BUCY-KALMAN. Richard S. BUCY de l'University of Southern California a contribué à la théorie dans l'article
Kalman, R. E., Bucy R. S., "New Results in Linear Filtering and Prediction Theory", Transactions of the ASME - Journal of Basic Engineering Vol. 83: pp. 95-107 (1961) d'où le filtrage dit de Bucy-Kalman.

La méthodologie comprend deux notions : l'évolution du système et l'observation de celui-ci. Prenons un exemple en Justice pour montrer la généralité de la démarche intellectuelle. Comment se fait un jugement. Le Juge dispose du passé du prévenu et en déduit une possibilité d'acte délictueux pour le jour des faits jugés. Le juge possède également des témoignages, des indices matériels présentés durant le procès. Ensuite, il y a fusion des informations de ces deux sources d'information pour établir le jugement.
Notons l'utilisation des filtres de BUCY-KALMAN pour le programme Apollo. On a marché sur la Lune grâce à KALMAN ! ce que n'a pas dit HERGE.
Pour le pilotage d'un satellite, la mécanique rationnelle fournit les équations permettant à partir du passé, de prévoir la position actuelle du satellite.
Les équations d'Etat, linéarisées, discrétisées et bruitées s'écrivent

$$X(t)= A\,X(t-1) + W(t)$$ avec le temps t, l'état X et le bruit W

Mais de plus, les observations par radar fournissent une seconde estimation de la position X du satellite à l'instant t.
Les équations d'observation s'écrivent

$$Y(t) = BX(t) + V(t)$$ avec Y l'observation provenant de l'état X avec un nouveau bruit V

La connaissance physique des phénomènes fournit les matrices A et B.
Le temps t est échantillonné. A partir de ces deux équations linéarisées, discrétisées et bruitées de la réalité matérielle, le filtre de BUCY-KALMAN définit la meilleure estimation de la position X(t) du satellite à la date t.
Actuellement les équations ne sont plus linéaires et les bruits W et V ne sont plus gaussiens et sur Google, plus de 250 000 articles portent sur ce filtrage de BUCY-KALMAN !

La surveillance électronique
Le risque d'Internet : Tout n'est pas faux sur le site www.syti.net mis en référence, mais SURTOUT tout n'est pas vrai !
Fichiers informatiques, carte de crédit et code barre, téléphones portables, Internet, réseau Echelon, voici des moyens de surveillance électronique.
Etes-vous favorables à la surveillance électronique ? Est-ce que la surveillance électronique est conforme à l'article premier de la loi Informatique et Libertés du 6 janvier 1978 ?

"L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."

Les technologies informatiques ont permis d'augmenter ce que les spécialistes appellent notre traçabilité. Nos activités, nos conversations, nos goûts et nos centres d'intérêts laissent des traces dans les multiples systèmes informatiques qui gèrent notre vie quotidienne. Toutes ces données sont collectées, centralisées et mémorisées par des organisations publiques ou privées qui peuvent connaître à tout moment le profil de chaque individu.

Les fichiers :
Les fichiers des administrations et des sociétés privés rassemblent de nombreuses données personnelles sur des millions de citoyens ou de consommateurs. Ces données sont inoffensives tant qu'elles sont éparses.

La carte de crédit associée au code-barre d'un produit acheté :
Les dépenses effectuées avec une carte de crédit permettent de retracer nos déplacements, mais aussi de connaître très précisément les produits achetés par une personne.
L'association du code-barre et du numéro de carte de crédit signifie l'association automatique de produits identifiés avec des consommateurs identifiés.

Les téléphones portables :
On sait qu'avec un récepteur de type scanner dont l'usage est illégal mais dont la vente est autorisée, il est facile de réaliser des écoutes téléphoniques des messages émis par les portables.
Le portable, même hors-communication, en position de veille, permet de localiser à tout moment son propriétaire.
Le micro du portable peut être activé à distance par les services de police grâce à un simple code de 4 chiffres et cela même quand le portable est éteint.

Internet :
Avec les logiciels adéquats, n'importe qui peut pister les informations consultées par un internaute.
De plus, depuis les attentats du 11 Septembre 2001, la plupart des pays occidentaux ont adopté des lois qui autorisent la surveillance de l'ensemble des communications sur Internet.

Microsoft et Intel :
Le système Windows et son navigateur Internet Explorer, de Microsoft, renferment un numéro d'identification de l'utilisateur, le GUID (Globally Unique Identifier). Ce numéro d'identification est ensuite inscrit dans tous les documents créés avec les applications de Microsoft Office. Il peut être consulté à distance par Internet grâce à des commandes spéciales prévues par Microsoft.

La vidéosurveillance :
Les caméras de surveillance se multiplient dans la plupart des villes. A ces caméras s'ajoutent les appareils photo des radars automatiques sur les routes.
L'identification des individus dans une foule est désormais possible en raccordant les caméras à des logiciels de reconnaissance des visages.

La radio-identification ou puces RFID de l'anglais radio frequency identification device

Les puces RFID sont incorporées par les multinationales dans certains de leurs produits pour en assurer la traçabilité. La puce permet ensuite de localiser le produit pendant sa distribution, mais aussi après son achat.

Les implants - les puces "Digital Angel" et "Verichip"
Fabriquée par la société américaine Applied Digital Solutions, la puce "Digital Angel" permet l'identification et la localisation par satellite des individus. Il s'agit d'une puce électronique de la taille d'un grain de riz et qui est implantée sous la peau. Elle est aussi capable de renvoyer des informations biologiques sur son porteur, température du corps, rythme cardiaque, etc. d'où son utilité en médecine.

Le réseau Echelon :
Le réseau Echelon est un système automatisé d'écoute des communications, quel que soit leur support: téléphone, fax, courriel, satellites.
Le réseau Echelon a été mis en place depuis 20 ans et dans le plus grand secret par 5 pays anglo-saxons: les Etats Unis, la Grande Bretagne, le Canada, l'Australie, et la Nouvelle Zélande. Le réseau Echelon est principalement géré par la NSA, l'agence de renseignement électronique américaine.
L'idée d'Echelon est d'utiliser les technologies de reconnaissance vocale pour repérer automatiquement des mots-clés dans les conversations écoutées. Les mots-clés à repérer sont choisis par les officiers d'Echelon en fonction de l'actualité et des objectifs du moment.

La reconnaissance de formes :
La société AOptix a mis au point un nouveau système de reconnaissance de l'iris et du visage des passagers pour aider les compagnies aériennes à l'embarquement.

Le futur porte-monnaie électronique :
Le porte-monnaie électronique est-il appelé à remplacer totalement l'argent liquide ? Le porte monnaie électronique, combiné avec la disparition de l'argent liquide rendrait les individus totalement dépendants des moyens de paiement électroniques.

Une liste de moyen de surveillance électronique est présentée ; est-elle exhaustive ? Vous pourriez vous reposez la question :
Suis-je favorable à la surveillance électronique ? Est-ce que la surveillance électronique est conforme à l'article premier de la loi Informatique et Libertés du 6 janvier 1978 ?
"L'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."

CONCLUSION
Des faits précis viennent d'être présentés sur la Révolution Informatique et la Communication. Il n'était pas dans ce propos d'avoir un avis éthique sur l'évolution concrète des modes de vie résultant des progrès scientifiques dans ces deux domaines. Depuis la seconde guerre mondiale, les applications liées à la Révolution Informatique et à la Communication modifient, de façon chaque jour plus profonde, le mode de vie des hommes. Ne reprenons ni les recherches ni les développements prévisibles sur la Révolution Informatique et la Communication qui se vivent chaque jour dans les centres de recherche, universitaires ou industriels.
Pour nous, pour tout citoyen, il s'agit de comprendre ces transformations pour s'y adapter et en tirer le meilleur parti : comment se vit la Révolution Informatique et la Communication

dans la région rouennaise. Notons, les forums régionaux du savoir, patronnés à Rouen par Monsieur le Président du Conseil Régional, forums régionaux qui diffusent les connaissances au plus large public possible.
Prenons un seul exemple lié aux Mathématiques, l'exposé du Jeudi 15 Novembre 2012, dans les locaux du Conseil Régional par Monsieur Cédric VILLANI, médaille Fields 2010, Professeur à l'Université de Lyon et directeur de l'Institut Henri Poincaré « Peut-on lire l'avenir des astres dans les lignes de la mathématique ? » :
Nous tous, pouvons retrouver l'intégralité de cet exposé en streaming sur le site : http://streaming.crihan.fr/scienceaction/Forum-2012-Villani-reduit-H.mov.
Oui, par Internet, vous trouverez toutes les conférences des Forums Régionaux du Savoir sur le site :
http://www.scienceaction.asso.fr/Videos/Forums-regionaux-du-savoir-2012
De même, sur le site web de l'Académie des Sciences, Belles-Lettres et Arts de ROUEN se trouvent le programme des travaux de cette Académie ainsi que les textes de plusieurs conférences publiques. Cependant, le précis, texte écrit, reste le document de base pour détailler les travaux de l'Académie des Sciences, Belles-Lettres et Arts de ROUEN.