

Il n'existe pas de solution unique providentielle:
à la recherche d'une coexistence
de modèles, de contre-modèles et d'alter-modèles
dans le monde numérique

Michel Riguidel
michel.riguidel@telecom-paristech.fr

Urbanisation numérique hybride

Fin de l'approche monochrome, mono-technologique



Au-delà de la 3-4G

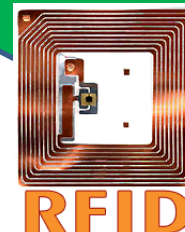
**Web, Services,
Contenus**

Accrochés à plusieurs
infrastructures

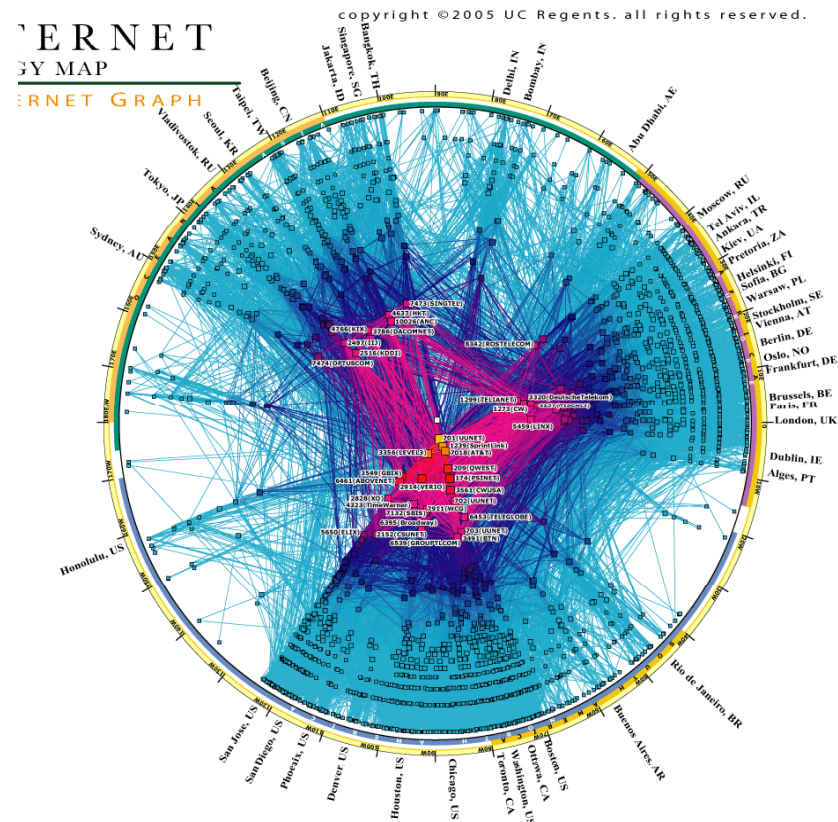
L'Internet actuel
WDM-IPv4/v6-MPLS

Internet des choses

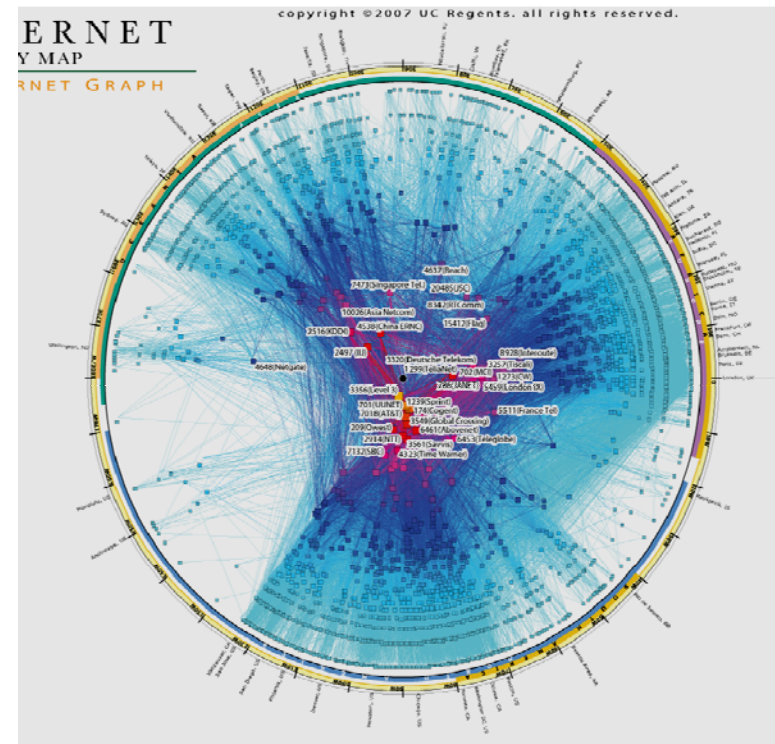
Galileo - Beidou2 - GPS-
horloge et la position



Expansion de l'Univers / Concentration d'Internet



2005



2007

Cryptographie:

Glissement des ressources vers le privé (fermes de serveurs)

Glissement de la compétence vers l'Asie (Inde et Chine)

Échelle hiérarchique traditionnelle de l'Internet actuel

Organisations gouvernementales



28/06/2010

Pirate amateur

Rééquilibrage des forces dans les réseaux du futur (attaques – cryptanalyse)

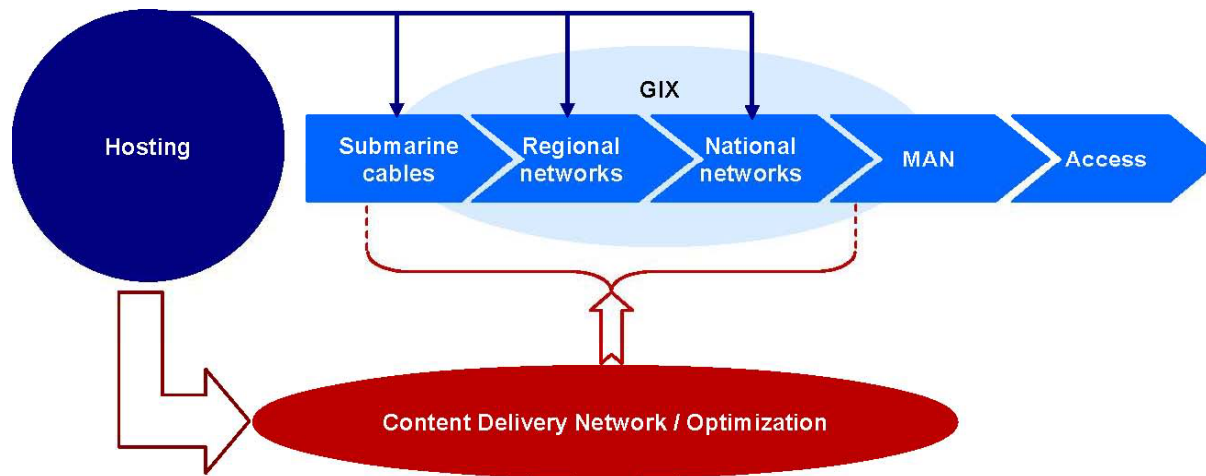
Puissance informatique massive furtive externalisée
exécutant
sur des réseaux anonymes
des calculs illicite confidentiels



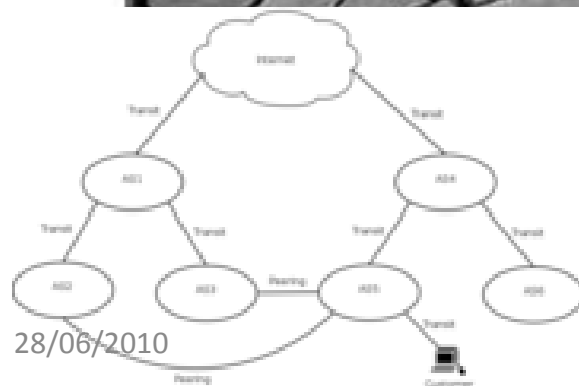
Utilisateur en solo

Nouvelle cryptographie avec des calculs, de l'histoire et de la géographie
Alice et Bob ne sont plus seuls dans ce monde :
ils ont des témoins, des alibis, des itinéraires, ils laissent des traces

Internet : un morcellement en systèmes autonomes



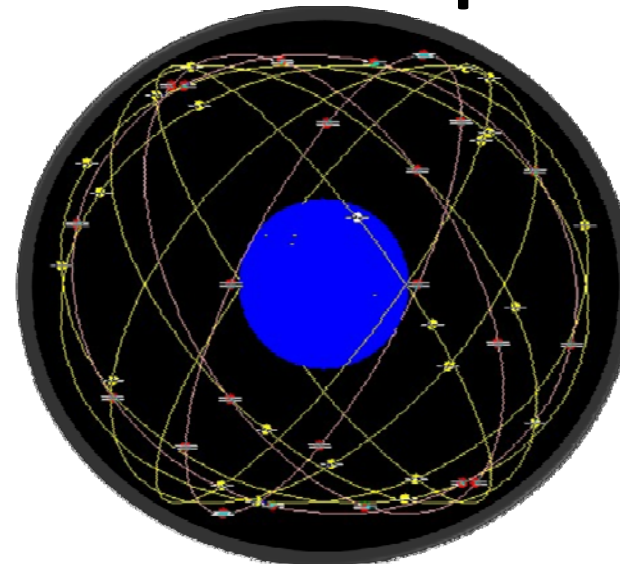
Chaîne de valeur du transport de données sur Internet



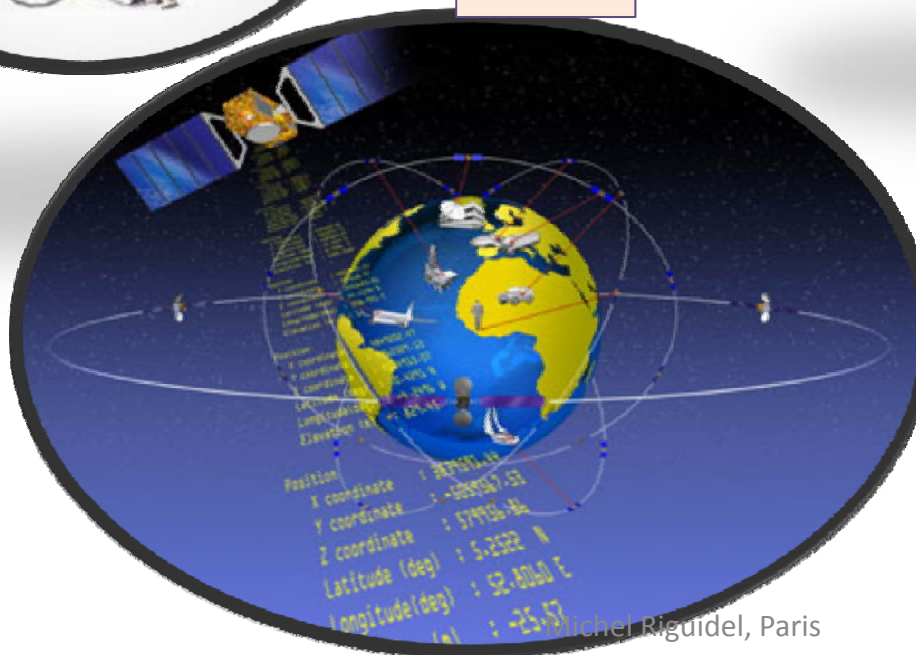
Balkanisation du ciel numérique



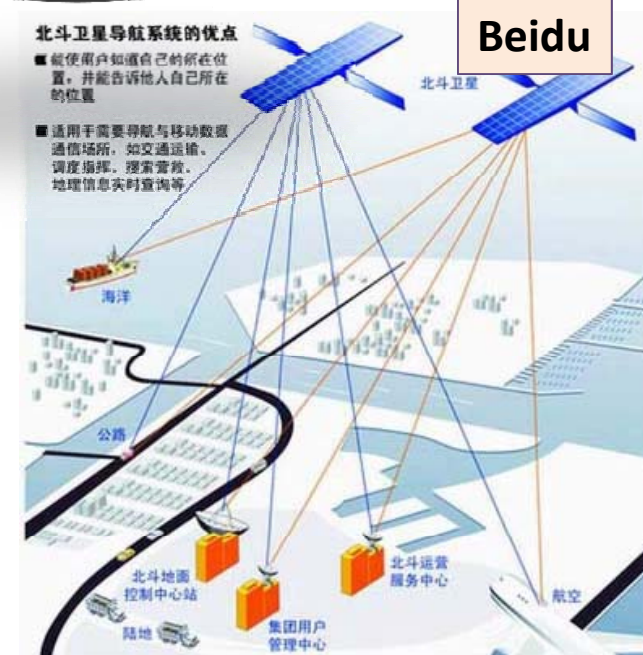
GPS



Glonass



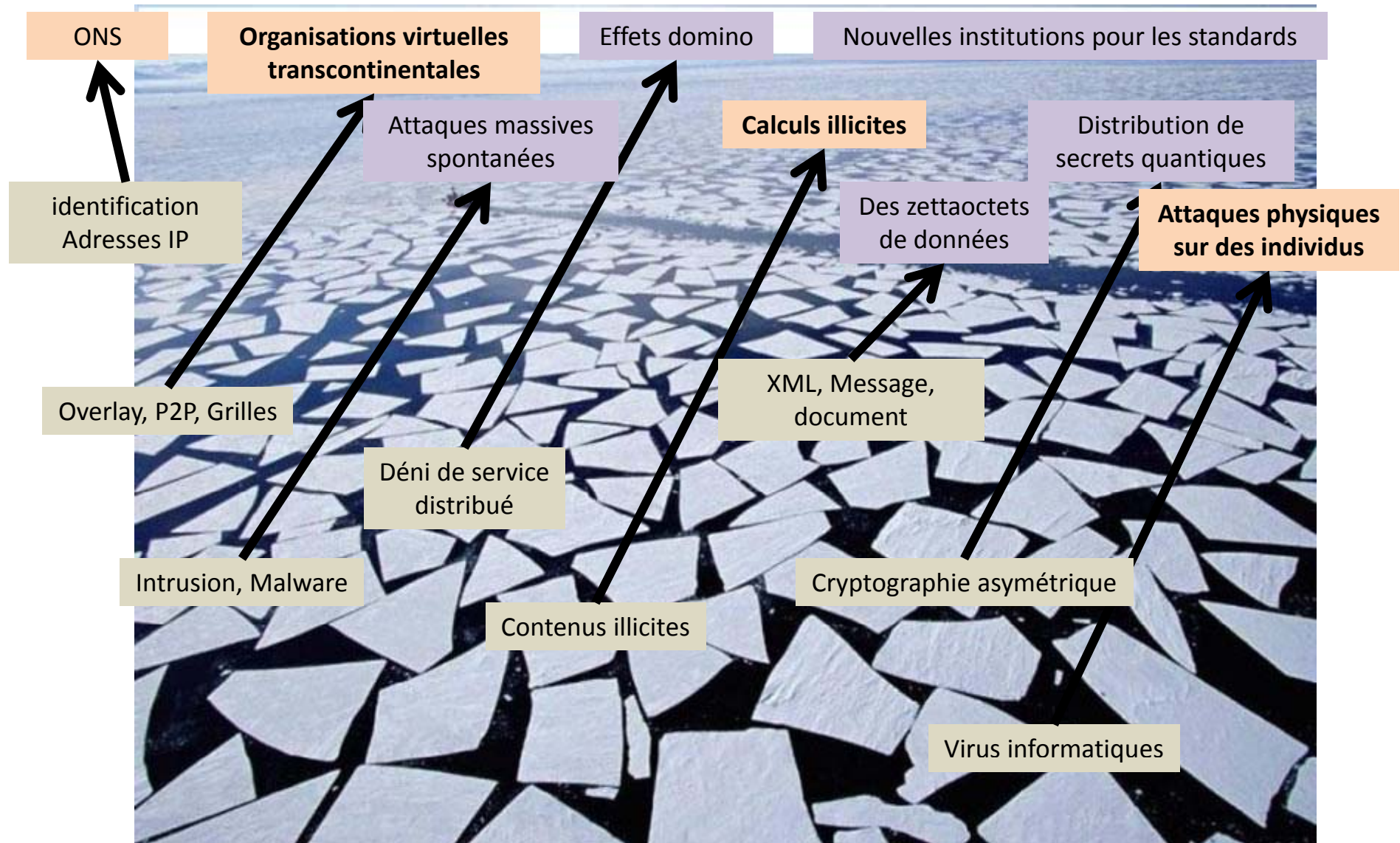
Galileo



Beidu

Les menaces & vulnérabilités à venir

Le cycle de 3 ans des menaces et vulnérabilités



L'Europe exclue du Yalta numérique du XXI^{ème} siècle

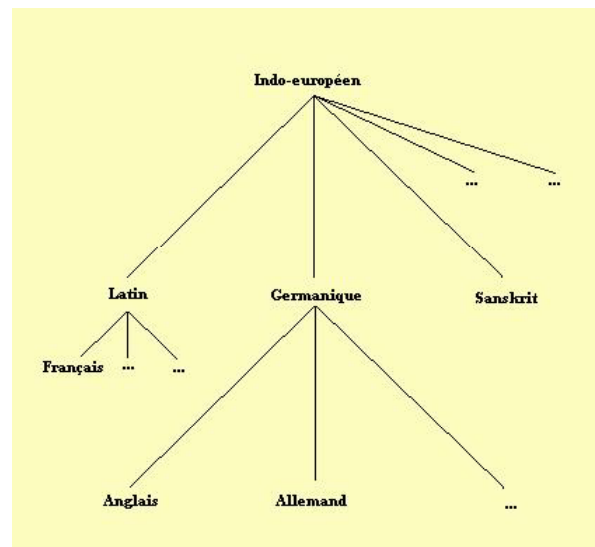
Matériel

Asie (Chine, Corée, Japon)



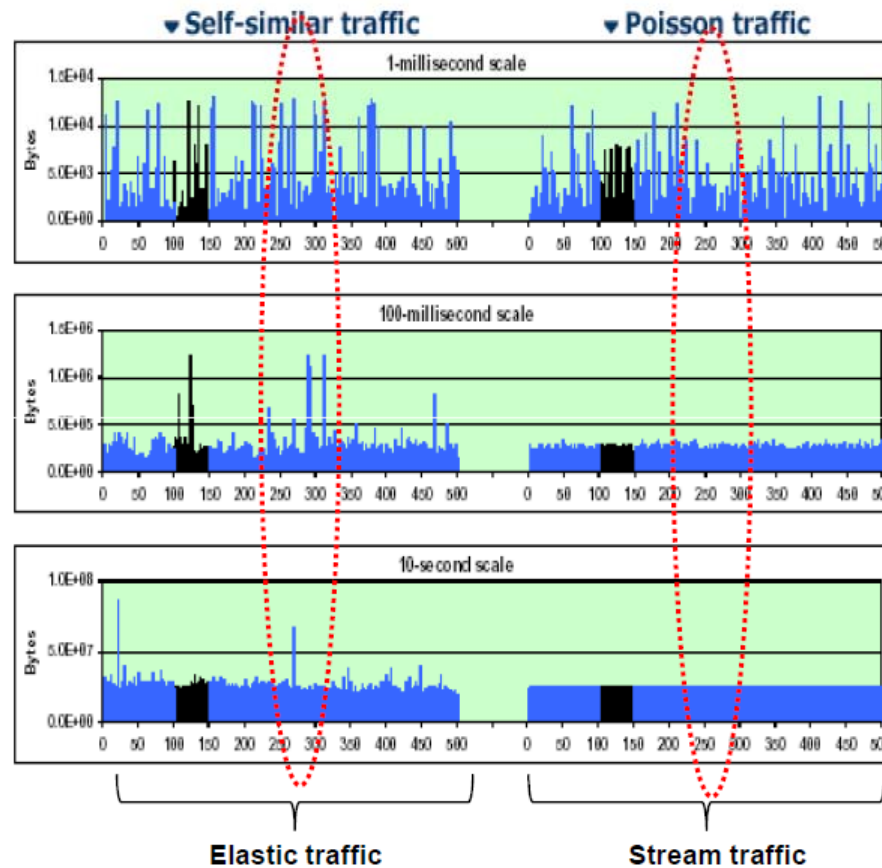
Logiciel

Langue Indo-européenne
(États-Unis, Inde)



Granularités temporelles au niveau du réseau

Self-similar traffic and statistical multiplexing



M Gagnaire, ENST

Le règne numérique : un duo programmes - données



Logiciels opaques,
ouverts dans l'obscurité
Le crochet est dans la lumière



Patrimoine numérique personnel
Éparpillé dans des sphères privées
éclatées

Les verrous de l'intimité numérique

- Sécurité des **communications** (**imputabilité**)
 - Il n'existe pas de fonctions de non-répudiation à l'envoi et à la réception
 - Il n'existe pas d'identification et d'authentification mutuelles, de bout en bout, systématiques
 - Question technologique pourtant résolue
- Sécurité des **contenus en circulation** (**propriété, authenticité, traçabilité**)
 - Il n'existe pas de système de protection des contenus (son, voix, images, vidéo, logiciels, source et exécutable), vraiment fiables et répandus
 - Problème de déploiement d'ingénierie : gestion des droits numériques
- Sécurité des **calculs et traitements** (transparence des opérations / secrets, **signification** des traitements)
 - Il n'existe pas de vérification en temps réel de la sémantique des calculs
 - Ne pas confondre :
 - Conformité des spécifications et/ou de la documentation : « j'obéis strictement, je fais ce que l'on m'a demandé de faire » (conception); « Je dis ce que je fais, je fais ce que je dis » (documentation)
 - Dangereusité de l'exécution : « Je suis inoffensif, je suis dangereux »
 - Fragilité : « je suis vulnérable »
 - Problème scientifique ouvert pour les programmes informatiques

Surmonter les défauts des 2 pôles de réseaux

Le téléphone : architecture de circuits pour des communications synchrones



Internet : architecture de paquets pour des communications asynchrones



```
+++++  
| Version | IHL | Type of Service | Total Length |  
+++++  
| Identification | Flags | Fragment Offset |  
+++++  
| Time to Live | Protocol | Header Checksum |  
+++++  
| Source Address |  
+++++  
| Destination Address |  
+++++  
| Options | Padding |
```

Les 2 rubans de l'ordinateur

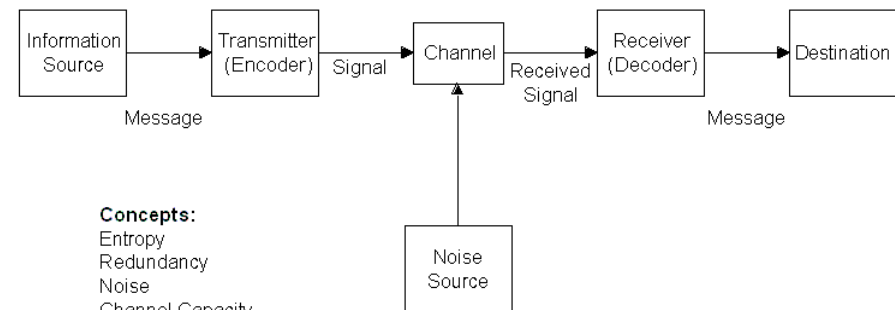
Machine de A Turing



Modèle de C Shannon



The Shannon-Weaver Mathematical Model, 1949



L'écheveau des systèmes numériques



Du fil à retordre pour les informaticiens
Ruban de Turing



Un coup de fil
Ruban de voix sur IP

Un fil(m)
Ruban de pixels

Jean Sébastien Bach (1685 – 1750)



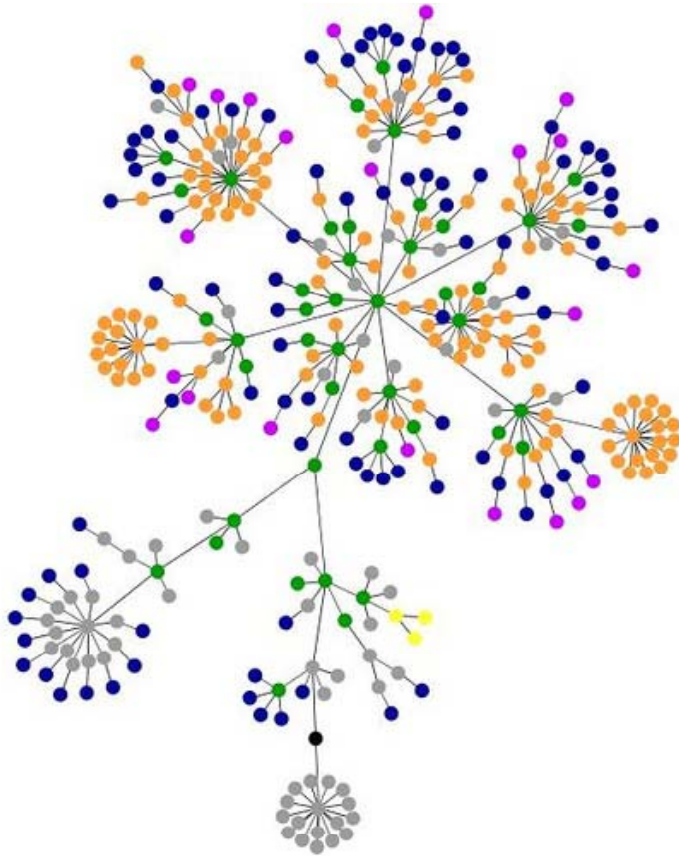
• Le clavier bien tempéré (1722)

- Livre 1 : BWV 846-869
- Livre 2 : BWV 870-893
 - BWV 846 Prélude et fugue, en do majeur
 - BWV 846a Prélude, en do majeur Variante de BWV 846
 - BWV 847 Prélude et fugue, en do mineur
 - BWV 848 Prélude et fugue, en do dièse majeur
 - BWV 849 Prélude et fugue, en do dièse mineur
 - BWV 850 Prélude et fugue, en ré majeur
 - BWV 851 Prélude et fugue, en ré mineur
 - BWV 852 Prélude et fugue, en mi bémol majeur
 - BWV 853 Prélude et fugue, en mi bémol mineur
 - Fugue en ré dièse mineur (dis-moll)
 - BWV 854 Prélude et fugue, en mi majeur
 - BWV 855 Prélude et fugue, en mi mineur
 - BWV 855a Prélude, en mi mineur Variante de BWV 855
 - BWV 856 Prélude et fugue, en fa majeur
 - BWV 857 Prélude et fugue, en fa mineur
 - BWV 858 Prélude et fugue, en fa dièse majeur
 - BWV 859 Prélude et fugue, en fa dièse mineur
 - BWV 860 Prélude et fugue, en sol majeur
 - BWV 861 Prélude et fugue, en sol mineur
 - BWV 862 Prélude et fugue, en la bémol majeur
 - BWV 863 Prélude et fugue, en sol dièse mineur
 - BWV 864 Prélude et fugue, en la majeur
 - BWV 865 Prélude et fugue, en la mineur
 - BWV 866 Prélude et fugue, en si bémol majeur
 - BWV 867 Prélude et fugue, en si bémol mineur
 - BWV 868 Prélude et fugue, en si majeur
 - BWV 869 Prélude et fugue, en si mineur

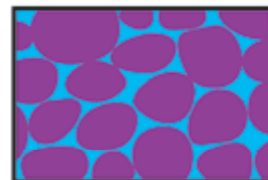
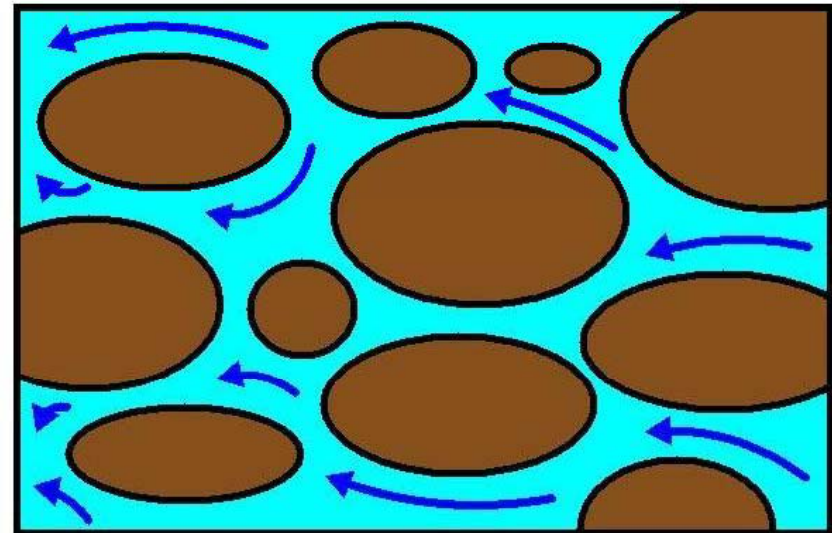


Les modèles de réseaux

Le graphe de nœuds et de liens :
des paquets de bit d'information qui
circulent d'un nœud à un autre



Le réseau en creux :
des entités fluides (trames, paquets, etc)
qui circulent dans un support perméable



Les lois sous-jacentes des modèles de réseaux

Les guichets et les files d'attente
Les lois de Poisson



Le milieu 3D poreux et perméable :
La compressibilité des fluides

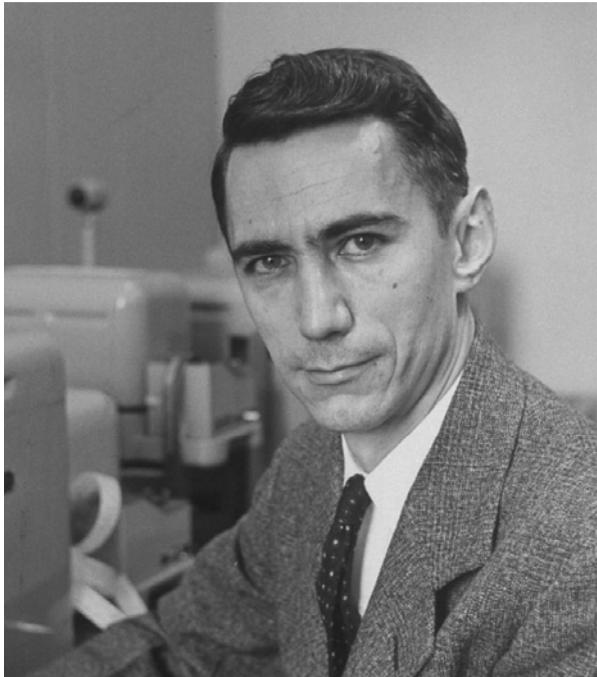
- Les lois de l'écoulement multi-phasique (fichiers, voix, vidéo) dans un milieu poreux (H Darcy)
- Piézométrie : instrument de mesures $U = Ki$

$$\vec{U} = -\frac{k}{\mu} (\vec{\text{grad}} p + \rho g \vec{\text{grad}} z)$$



Les modèles de communication

C Shannon (et Weaver) : 1949
au niveau des bits d'information

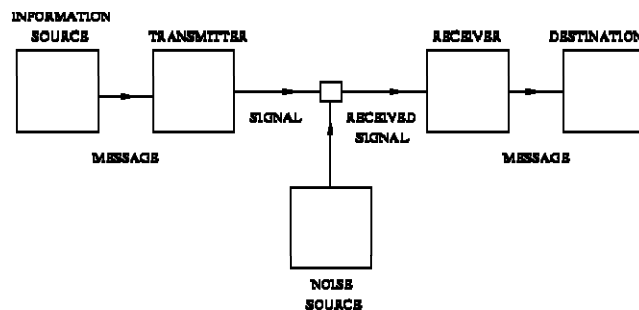


R Barthes : 1960
au niveau du sens et de la rhétorique



Les théories de la communication

C Shannon : La séparation de la source, du canal et du récepteur



R Barthes : la prise en compte de la rhétorique, du sens et de l'utilité

Émetteur : ἔθος => éthique

- Intrusion (profil), agressivité (publicité)
- Contenus, Calculs illicites

Canal : architecture et protocole

=> ῥητορικός

=> Rhétorique (au sens large)

- Épaisseur des signes

Message : λόγος

=> Logos (priorité, utilité)

- Fonctions économiques

Récepteur : πάθος => Pathos

réaction du sujet (individu ou machine)

Évolution des langages informatiques : complexification du typage abstrait

1955

1958

1965

1986

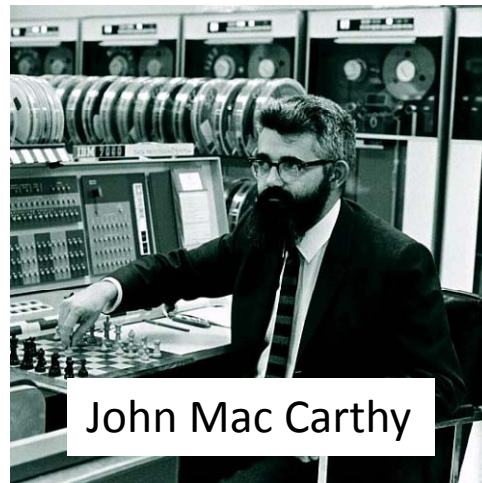
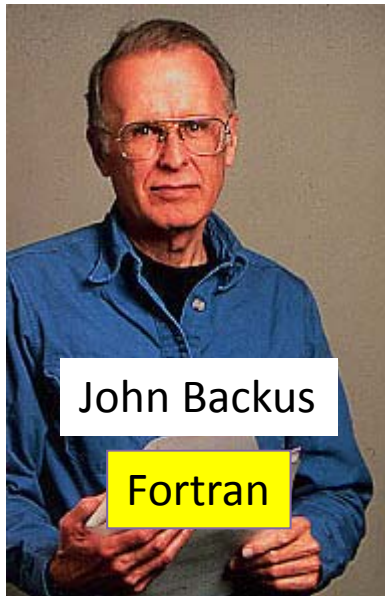
1992

Flottants, Entiers:
Indépendants
dans la mémoire

Listes :
Organisation de la
mémoire en chaînes

Pointeurs:
Structures
statiques
hétérogènes

Pointeurs:
Notions d'objets
Programmes
autonomes
dynamiques



Dennis M. Ritchie

C



Java

Évolution des Réseaux : l'histoire se répète

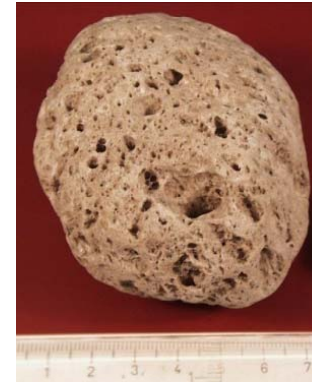
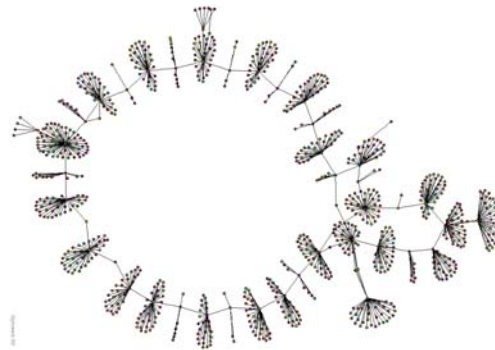
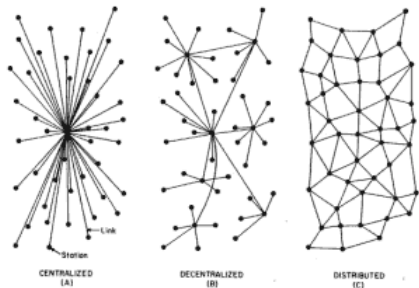
complexification du typage abstrait des liens

1960-2000

2000-2010

2010-2015

2020



Réseau traditionnel
Graphes
de nœuds et de liens

File d'attente,
Markov

Informatique ubiquitaire
Plaque 2D

Topologie (P2P)
Flux de contenus
Géographie

Écosystème
3D Fluide, Plastique

Milieu poreux
Histoire

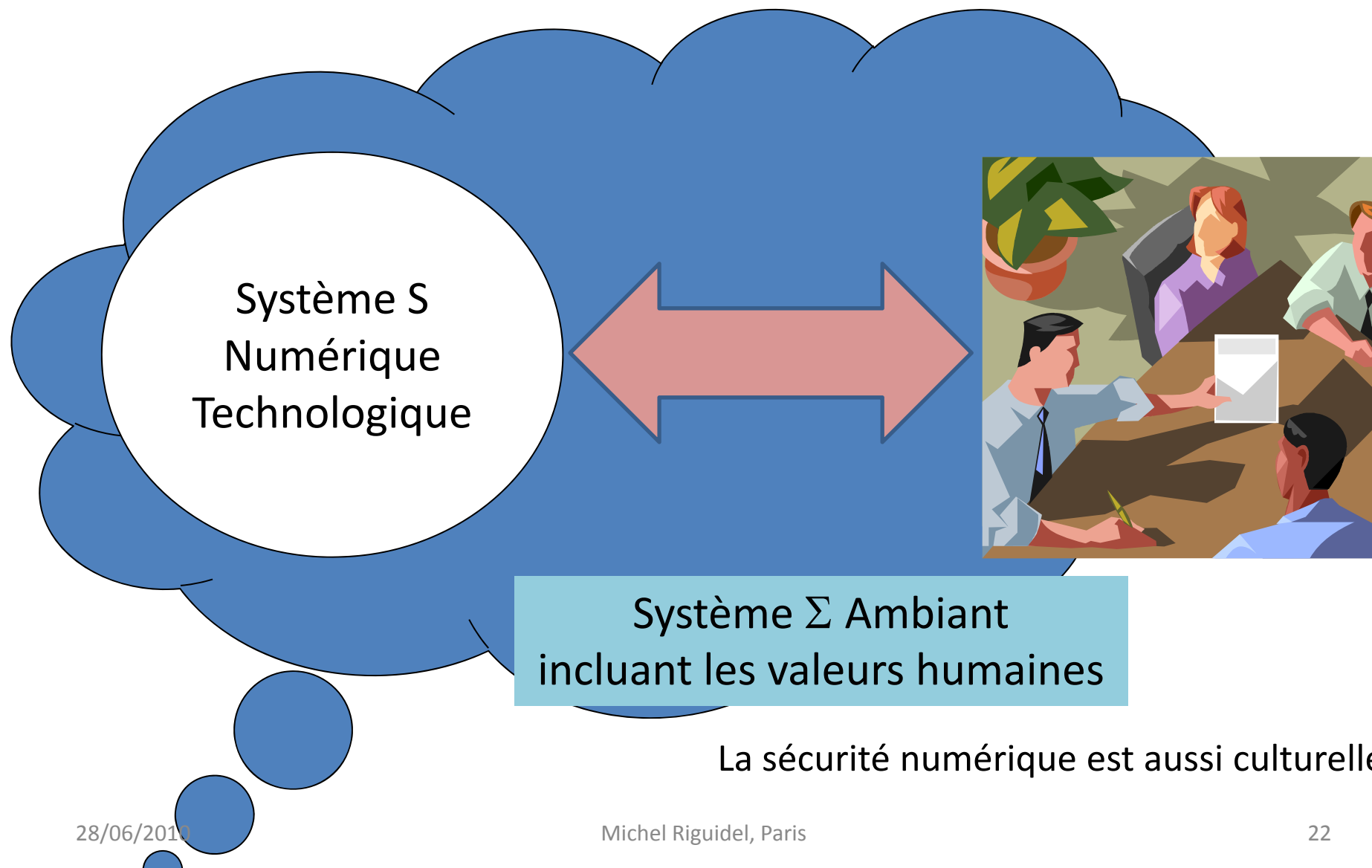
Un espace 3D
Programmable,
dynamique, sémantique
Architecture
programmable



Rigui



La politique de sécurité numérique : souveraineté + dignité



Jean-Jacques Rousseau

Du Contrat Social (1762)

**L'homme est né libre,
et partout il est dans les fers.**

L'ordre social est un droit sacré,
qui sert de base à tous les autres.

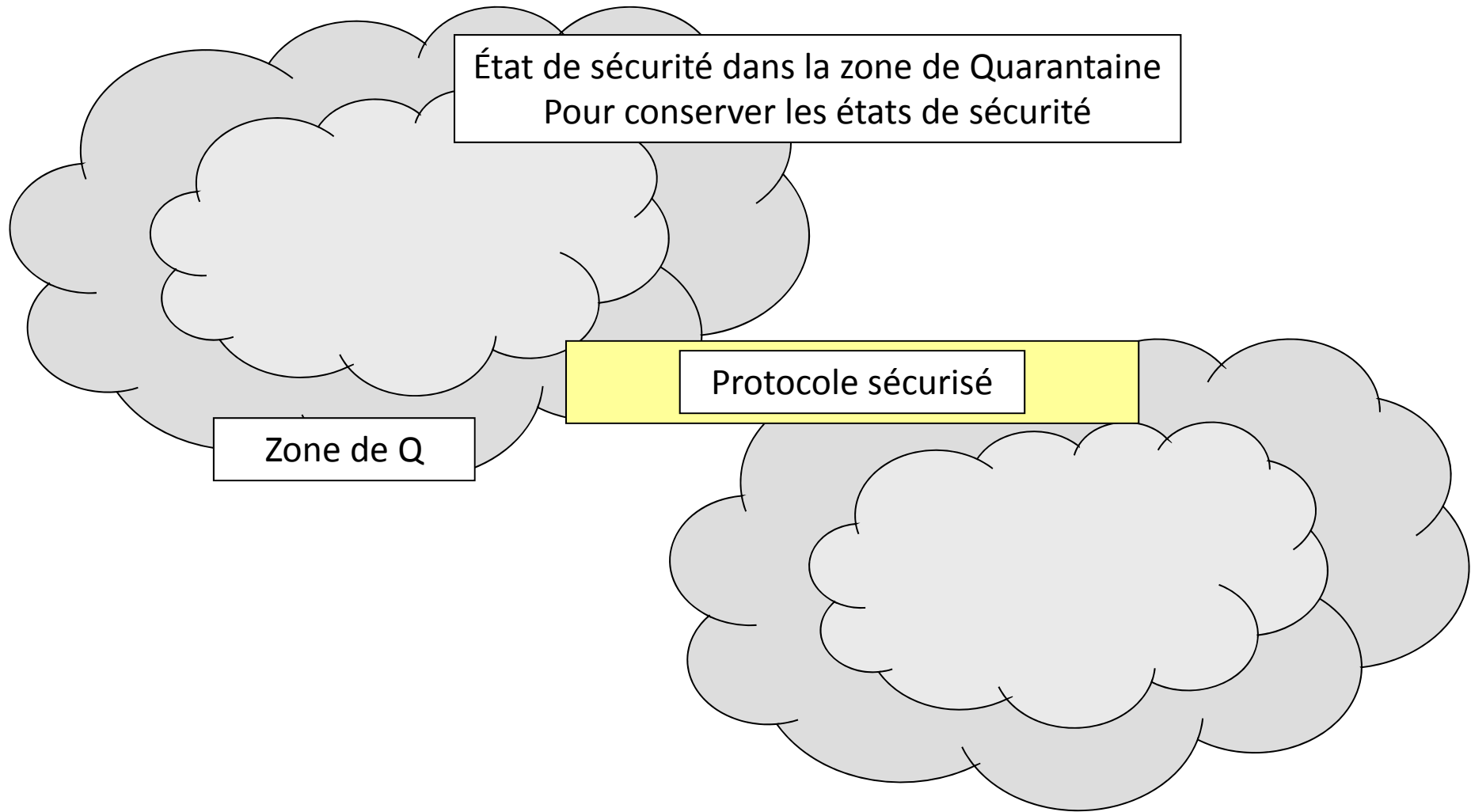
Trouver une **forme d'association**
qui défende et protège de toute
la force commune la personne et
les biens de chaque associé, et
par laquelle chacun s'unissant à
tous n'obéisse pourtant qu'à lui-
même et reste aussi libre
qu'auparavant.



Transposition au monde numérique

- Rédiger un Contrat légitime
 - Constitutif de la vie numérique et de la société numérique dans laquelle nous vivons
 - Refoulant la violence (délinquance informatique et fraude ...) et l'opacité inutile de l'informatique
- Transformant les concepts de départ
 - État de nature de
 - l'informatique originelle, autarcique, comme outil de calcul autonome
 - La vie numérique est perfectible
 - les usages changent, la technologie change, la gouvernance change
 - La loi numérique
 - expression de la volonté générale, règle impérative et universelle
 - Pour gérer les secrets, fixer des règles de gouvernance, des dénominateurs communs d'interopérabilité
 - La souveraineté
 - instance de gouvernance, constituée par toutes les entités responsables
 - une vision multipolaire de l'informatique

Bouclier virtuel dans une sphère privée



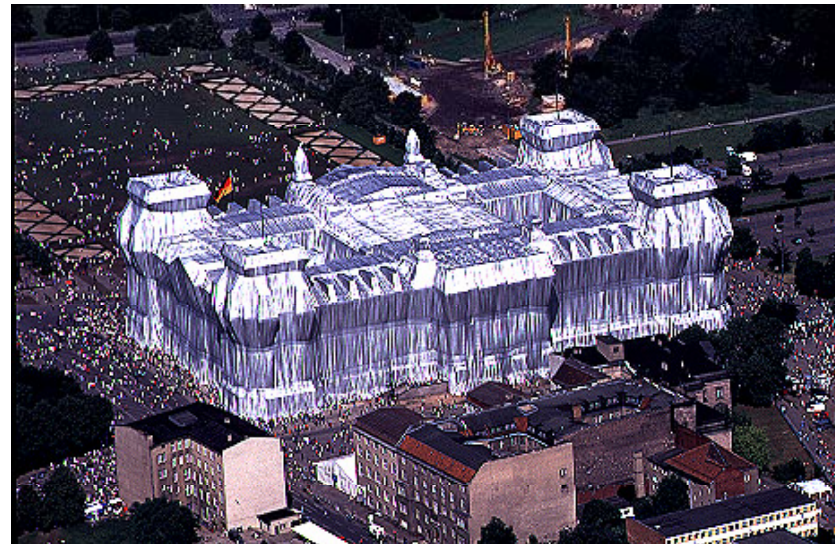
Sécurité des contenus : généralisation des enveloppes qui protègent



Cristo : art éphémère
Pont Neuf & Reichstag

Chaque individu va gérer le cycle de vie des objets de son patrimoine numérique personnel dans son propre réseau virtuel.

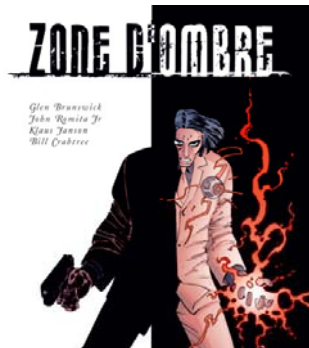
Nécessité d'avoir son **ramasse-miettes** à l'échelle du **réseau** pour effacer ses traces personnelles



La gouvernance dans l'ombre et la lumière

La gestion des secrets

- Sécurité
 - Partage des secrets
 - Sécurité dans l'obscurité
- La gestion de l'identité
 - Cycle de vie, filiation
- Respect de la vie privée
 - Zone d'ombre



La gouvernance de la visibilité

- Confiance
 - Transparence, Sincérité
- Responsabilité
 - Imputabilité
 - Propriété
- Traçabilité, surveillance
 - Les frontières floues
 - Les conflits (filature électronique)



Par delà le bien et le mal schématiques

Le fantôme paranoïaque : Logiciel propriétaire, payant, obscur, fermé, bogué, avec espionite

Le mythe candide : Logiciel libre, gratuit, transparent, ouvert, sans bug, sans porte dérobée

Le monde limité et contraint de l'informatique

- La neutralité : un débat évincé
 - Actuel : sur un support idéal, surdimensionné, avec une nature de communication idéale
 - Non discrimination selon les sources, les destinations, les contenus, les protocoles
 - Évincé : dans un milieu contraint, avec des archétypes de communications réelles
 - Engorgement avec de la voix, de la vidéo, des fichiers, de l'urgence, du prioritaire, de la sécurité, de la sûreté de fonctionnement. La communication est une machine qui a une épaisseur (complexité, entropie, énergie)
- Les réseaux actuels (technologie et gouvernance) ne sont pas neutres
 - Les équations de la couche physique ne sont pas neutres
 - La radio (équations de Maxwell) : diversité des paysages (forêt, zones urbaines)
 - La fibre optique (les lois de l'optique) : fracture géographique
 - Les protocoles ne sont pas neutres
 - IP privilégie les communications asynchrones (transfert de fichiers)
 - MPLS viole le routage IP pour fabriquer des tunnels préférés
 - TCP a été conçu pour les flux élastiques du monde filaire, pas pour un monde sans fil
 - BGP est fragile et dépendant des contrats de peering et des flux d'échanges
 - Les applications (services et contenus) ne sont pas neutres
 - TVHD, télémédecine, diffusion citoyenne d'urgence (collectivités locales) sont exclues de l'Internet
 - La loi de Moore (stricto sensu) est en train de s'émousser : elle favorise en ce moment les portails.
 - L'architecture et la gouvernance des réseaux ne sont pas neutres
 - Gouvernance américaine d'Internet, émiettement des systèmes autonomes.
 - Pressions des opérateurs de télécoms (mobile)

Pour un réseau bien tempéré

Vers des réseaux sobres, équitables, efficaces

- Réaménagement de la gestion du spectre électromagnétique (pas de plage attribuée à 1 service et 1 opérateur)
 - différence entre allocation et utilisation des fréquences
- Une seule infrastructure : réseaux cognitifs (gestion des interférences, service de découvertes, radio logicielle, etc)
 - qui permettent des communications équitables et efficaces
 - avec des réseaux verts : communications économiques et écologiques
 - et une Gouvernance multipolaire, avec de la transparence de la part des opérateurs, pour permettre une vision du point de vue des utilisateurs
- Une virtualisation spatiotemporelle des protocoles applicatifs
 - Réconciliation du filaire avec le sans fil, du paquet avec le circuit
 - Tagguage (IEMML ?) des trames Ethernet pour mettre une intelligence flexible selon les choix des opérateurs et des utilisateurs
 - Flux régionalisés éphémères : « routage sémantique » dans une zone topologique (réconciliation du plan signal et du plan données)

In Port	VLAN ID	Ethernet			IP			TCP	
		SA	DA	Type	SA	DA	Proto	Src	Dst

La réconciliation à partir de la trame Ethernet

du sans fil et du filaire (optique, électrique)

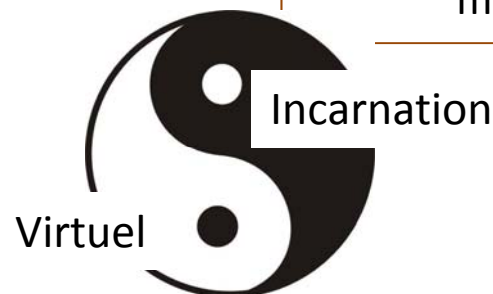
LA VIRTUALISATION SPATIO-TEMPORELLE DES ENTITÉS ET DES LIENS

Une vision globale de la virtualisation
La virtualisation permet de découper en tranches virtuelles toutes les entités et de surmonter l'hétérogénéité

LA VISION TEMPORELLE ET VIRTUELLE DES FLUX (TRAME, PAQUET, CIRCUIT)

Une vision orientée sur les flux

- Intelligence au niveau des flux et trames
 - Tagguage des trames Ethernet par un langage à balises
 - Transparence : visions opérateur mais aussi utilisateur



Nouer

les coutures de la virtualisation et les liens des flux
Sémantique de Typage des Liens pour l'acheminement

**Une prééminence accordée à de nouveaux liens instrumentés
(sémantique des langages)**

Internet de demain: Cortège d' « objets » virtuels mobiles communiquant en « père ou fils à père ou fils »

Pièces du jeu d'échec

Des entités virtuelles
(services, clouds, flux) sur le
réseau avec leur propre
routage
Les entités se découvrent, se
reconnaissent, se composent
et se fédèrent

Abstractions étagées au niveau des entités virtuelles

Vers un nouveau langage
sur le réseau ? De
l'adressage compilé
Vers un routage différencié
et hiérarchique ? Du
routage compilé ou
interprété

Plancher, échiquier

Internet actuel, avec le P2P
classique

