IWT 2011
Rio de Janeiro
Tuesday, May 3rd 2011

New models of communication & security for the Future Internet

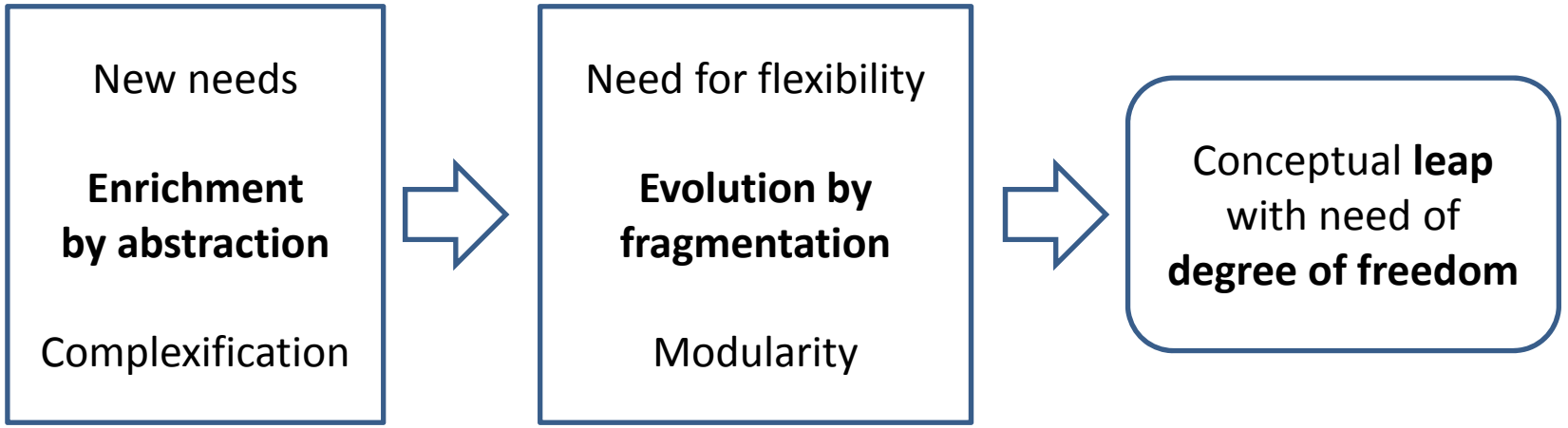
Michel RIGUIDEL
michel.riguidel@telecom-paristech.fr
Paris, France

TELECOM ParisTech

BIC
BUILDING International Cooperation for Trustworthy ICT

The mechanism of IT developments

The condition of the emergence of new paradigms



1 Thickening

2 Fragmentation

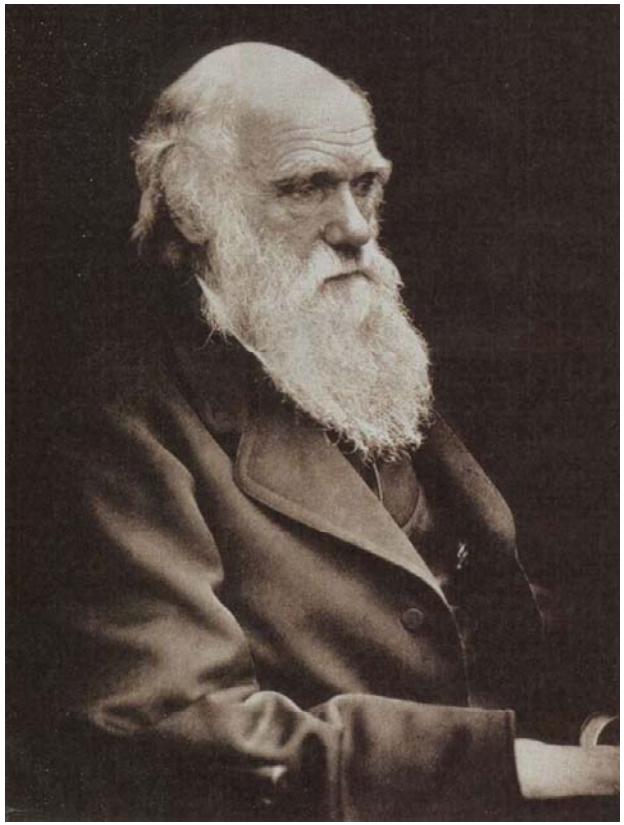
3 New Model

The metamorphosis operates **with slack**

The engines of evolution
Principles for progress in IT

- The principle of enrichment
- The principle of imitation
- The principle of separation
- The principle of fragmentation
- The principle of plasticity
- The principle of action and reaction

A Darwinian ecosystem

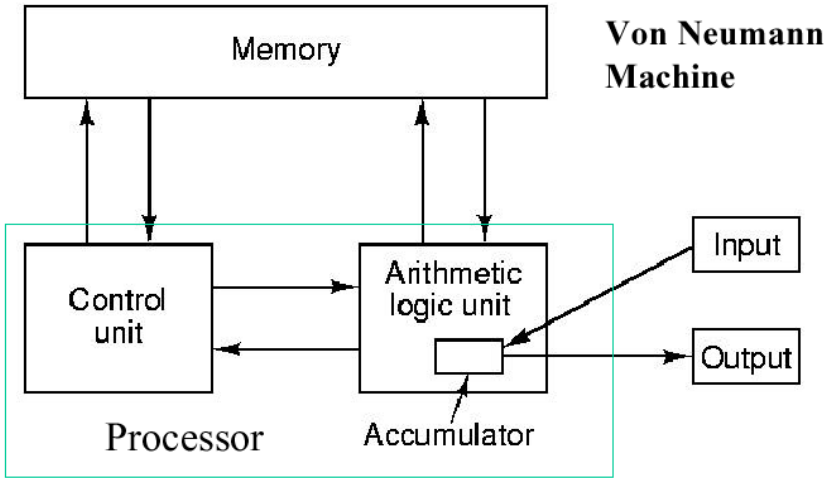


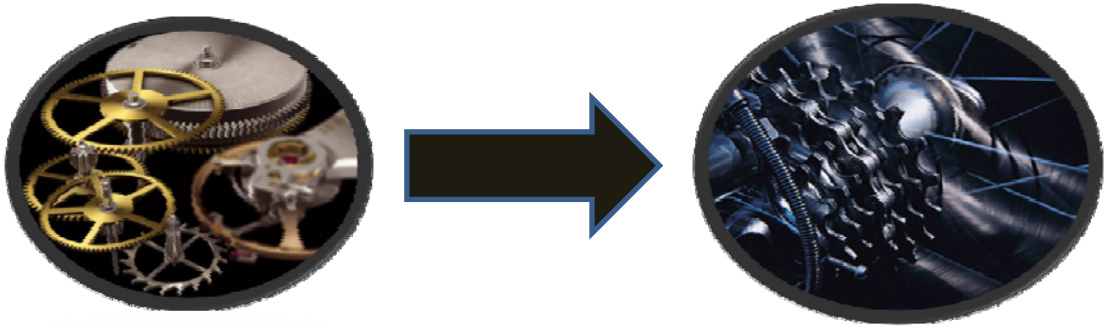
- The principle of **variation**
  - how “copies” of an entity differ from one another (duplicated clones end up being modified)
  - how entities in competition differentiate themselves from each other.
- The principle of **adaptation**
  - products or copies that are the best adapted to their niche survive and find greater deployment
- The principle of **heredity** (or of descent)
  - which posits that advantageous characteristics in a line of products, an architectural family or a conceptual philosophy are transmitted as a hereditary characteristic (with ascendant compatibility)
- => in IT, crucial **questions of interfaces**
  - interoperability more than excellence in the private parts

Loosening :
metamorphosis of paradigms requires a bit of slack

J Von Neumann

Architecture of a computer





To ease up, to leave in a bit of slack into the structures

Tears of the Web

The single whiteboard (1985)

Web pages (1991)

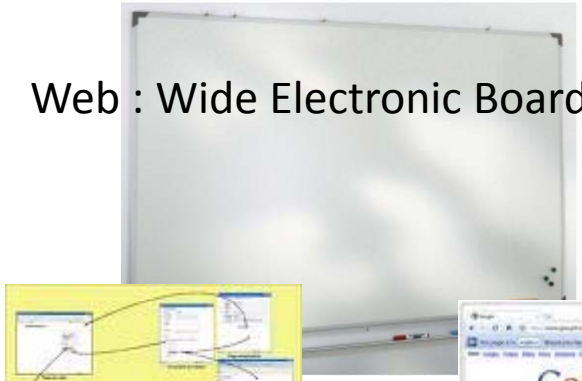
Syndication of flows

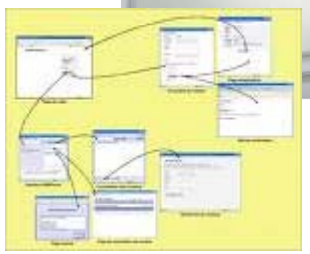
Web 2.0 (2006)

Copernican Web (2015?)

with geography and history

Deepening and widening





Cryptography

Symmetric

Asymmetric

The single key has been broken

+ Prime Numbers

Next Generation

Other Keys + new mathematical approach

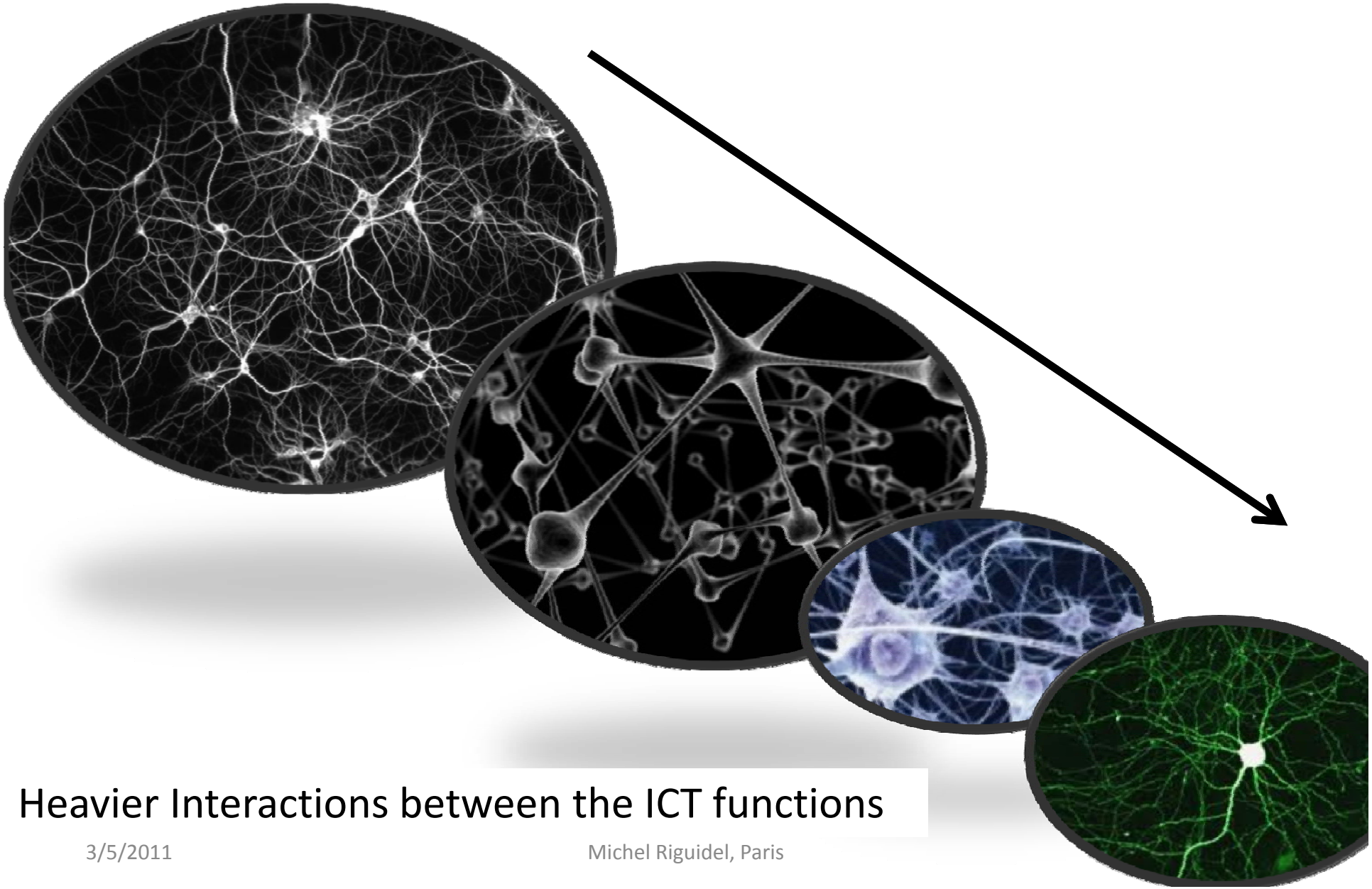
Quantum Communications

The network used to be a graph (nodes and links)

Routing packets into a net

D Poisson Law
A Markov Chain

The network is thickening and lumpy

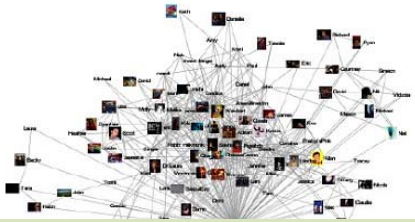


Heavier Interactions between the ICT functions

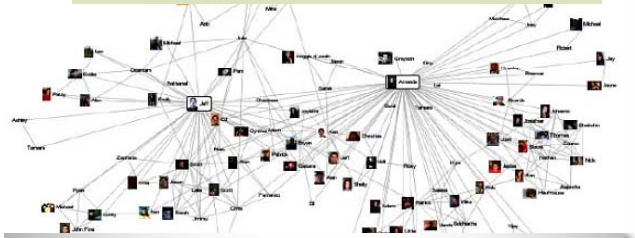
Scansions in IT : accordion-like movements

distribution

concentration



Peer-to-peer Architectures

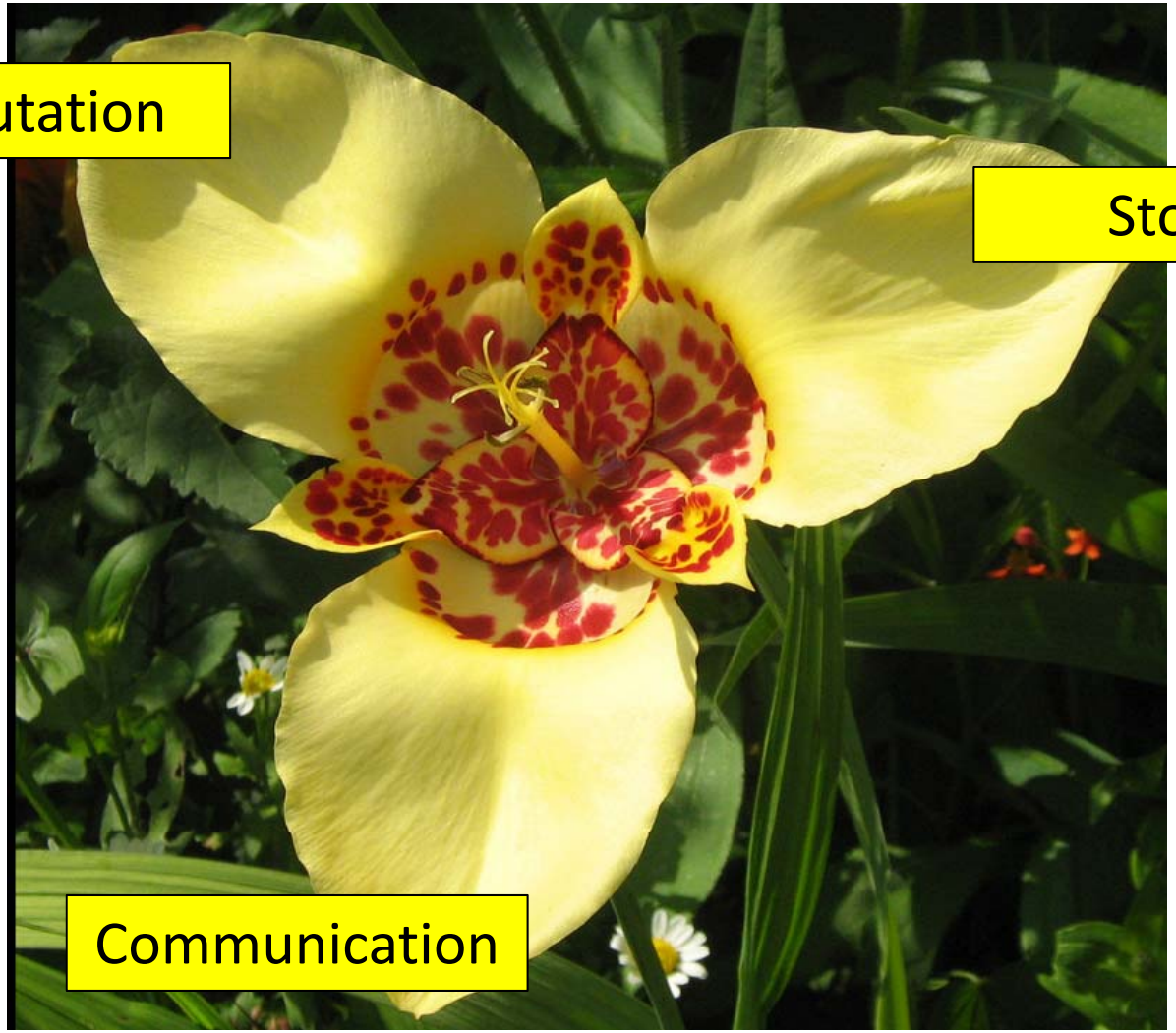


Actio-reactio principle

Serveur farm at Amazon

Arial view of Google's farms

ICT: a flower with 3 petals

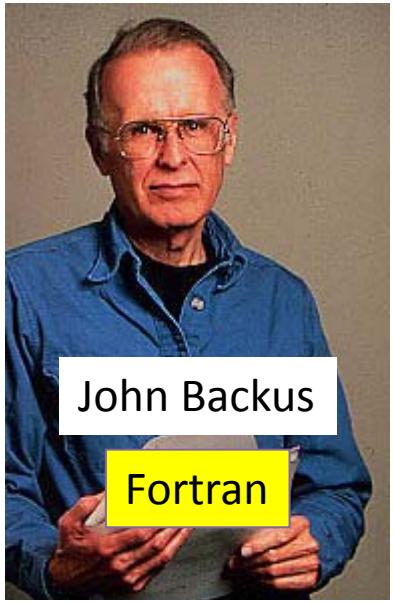
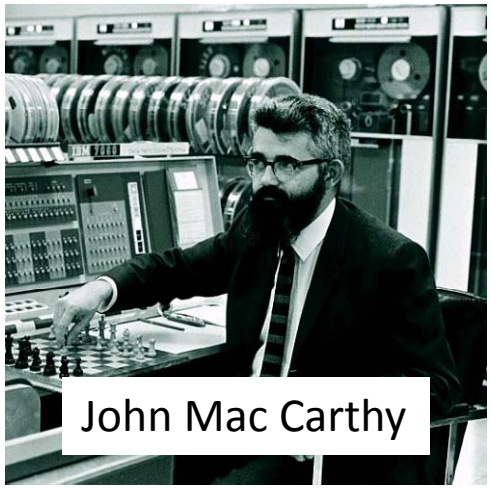
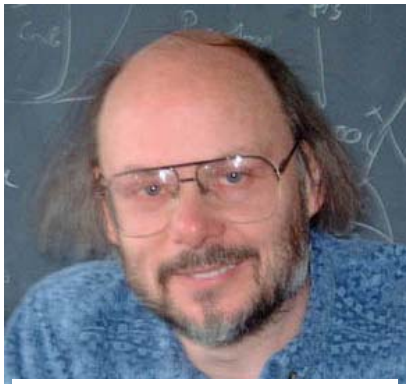


A network: a field of colorful flowers

Evolution of computer languages:

complexification of abstract typing

1955 — 1958 — 1965 — 1986 — 1992

1955	1958	1965	1986	1992
Floatings, Integers: Independent in the memory	Lists : Organization of the memory in chains	Pointers: Static, heterogeneous Structures		Pointers: Notions of objects autonomous dynamic Programs
 John Backus	 John Mac Carthy	 Dennis M. Ritchie	 Bjarne Stroustrup	JAVA™
Fortran	Lisp	C	C++	Java

Evolution of Networks: history repeats itself

complexification of abstract typing links

1960-2000 | 2000-2010 | 2010-2020 | 2020-2030

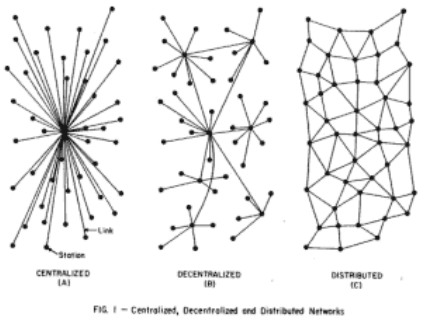
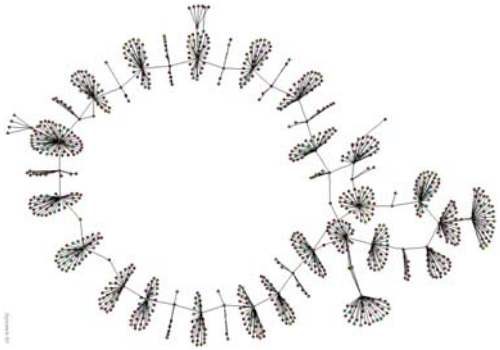
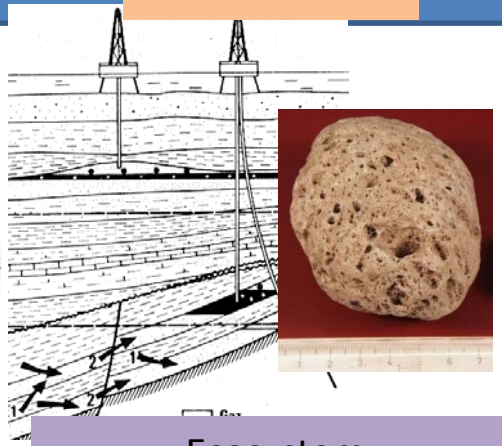


FIG. 1 — Centralized, Decentralized and Distributed Networks





Traditional networks
Graphs
Of nodes and links

Waiting Lists,
Poisson, Markov

Ubiquitous ICT
Plate 2D
Statistics on links
Topology (P2P)
Flow of content
Geography

Ecosystem
3D Fluid, Plastic
Games and rules
Between different players
porous media
History

A programmable 3D space
dynamic, semantic
programmable
Architecture

Two historic parallels

- History of the semantics of programming languages
  - The increasing complexity of **abstract data types**
    - Invention of the compiler: J. Backus's Fortran
    - Organization of memory: L. McCarthy's Lisp
    - Manipulation of pointers & structures: D. Ritchie's C language
    - The abstraction of local programs: the object-oriented class language of A. Kay
- The parallel history of network thinking
  - The **link types** become more complex
    - Before 2000 : The network was a grid of nodes and links
    - 2000 – 2010 : The network is organized to create homogeneous topological links (P2P, Search engines)
    - 2015 -2020 : The network organized to create heterogeneous links
    - Beyond 2020 : The architecture of the network will be programmable

3D environments

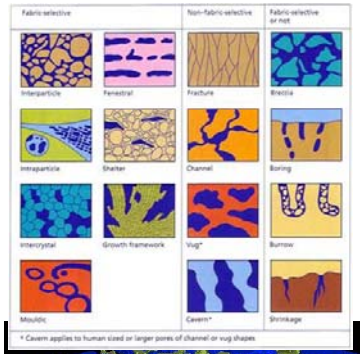
Ubiquitous computing

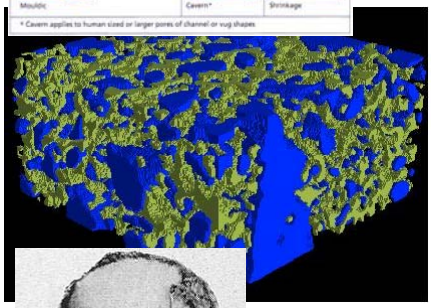
- Ambient Intelligence
- Pervasivity
  - Omnipresence and mobility
  - Reconfiguration and adaptivity

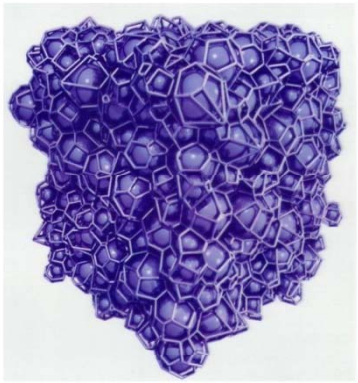
Porous media (permeability laws)

- Heterogeneous geometry
  - Core network
  - Capillarity

  at the periphery

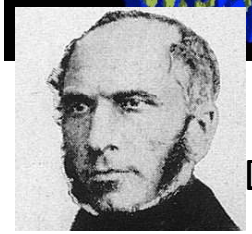






- Flows
  - Multiphasic

  voice, data, video



Darcy

$$U = Ki$$

$$\vec{U} = -\frac{k}{\mu}\left(\overrightarrow{grad}\, p + \rho g\, \overrightarrow{grad}\, z\right)$$

Digital security governance

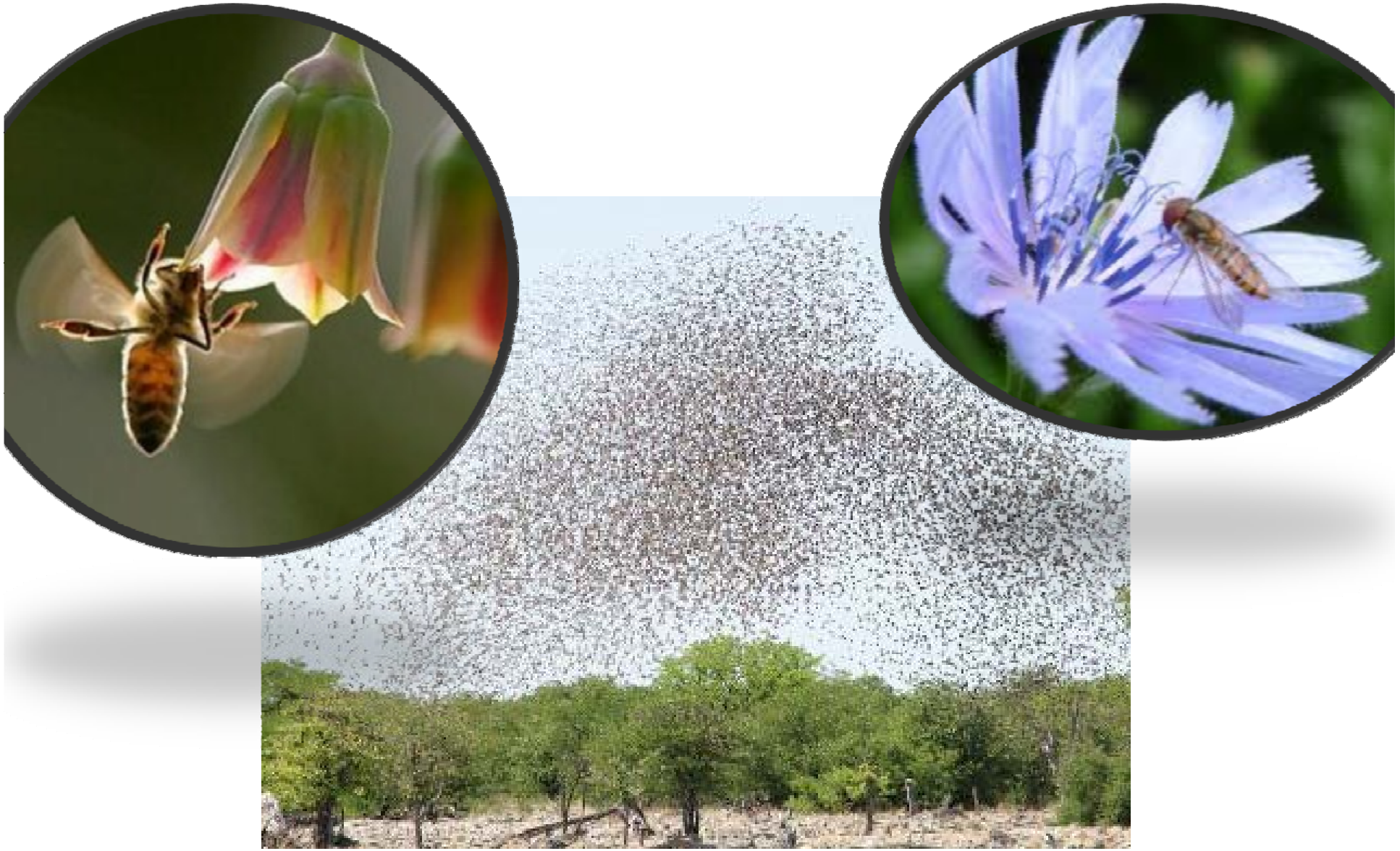
sovereignty + dignity

System S
Digital
Technology

System Σ Ambient
including human value

Digital security is also cultural

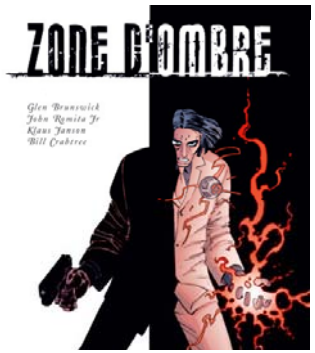
Security of the whole system & all the components



Digital Governance in shadow & light

Secrets' management

- Security
  - Sharing secrets
  - Security in darkness
- Identity management
  - Life cycle, heritage
- Privacy
  - Gray area



Governance of visibility

- Trust
  - Transparency, Sincerity
- Responsibility, Disclaimer
  - Accountability
  - Property
- Traceability, monitoring
  - The blurred boundaries
  - Conflicts (electronic surveillance)

Beyond schematic good and evil

The paranoid fantasy: Proprietary software, expensive, dark, closed, buggy and spying

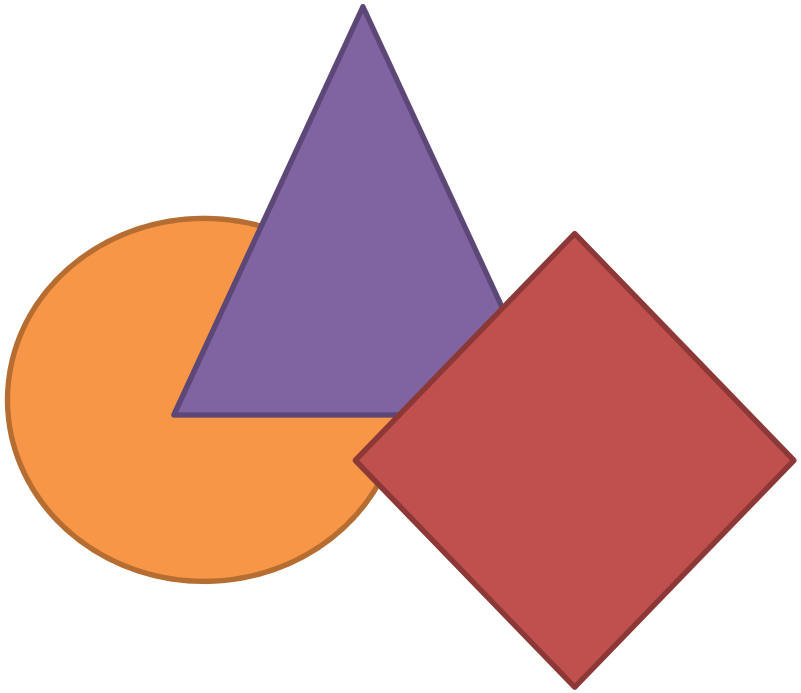
The candid myth : Free software, transparent, open, without bugs, without backdoors

Proprietary entity & openness

Transparency & Trust

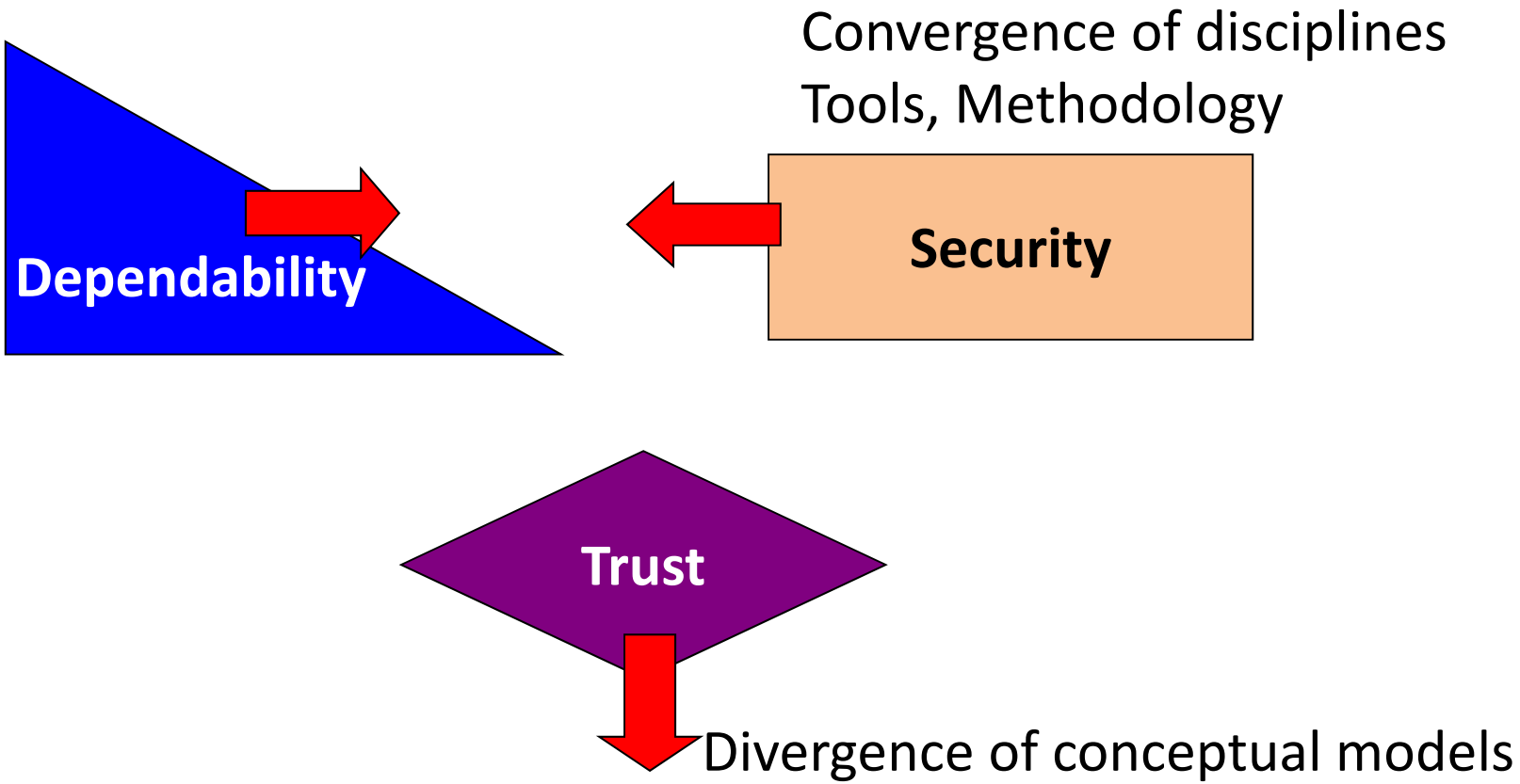
Interoperability & Standardization

Interchangeable, compatible & coexisting

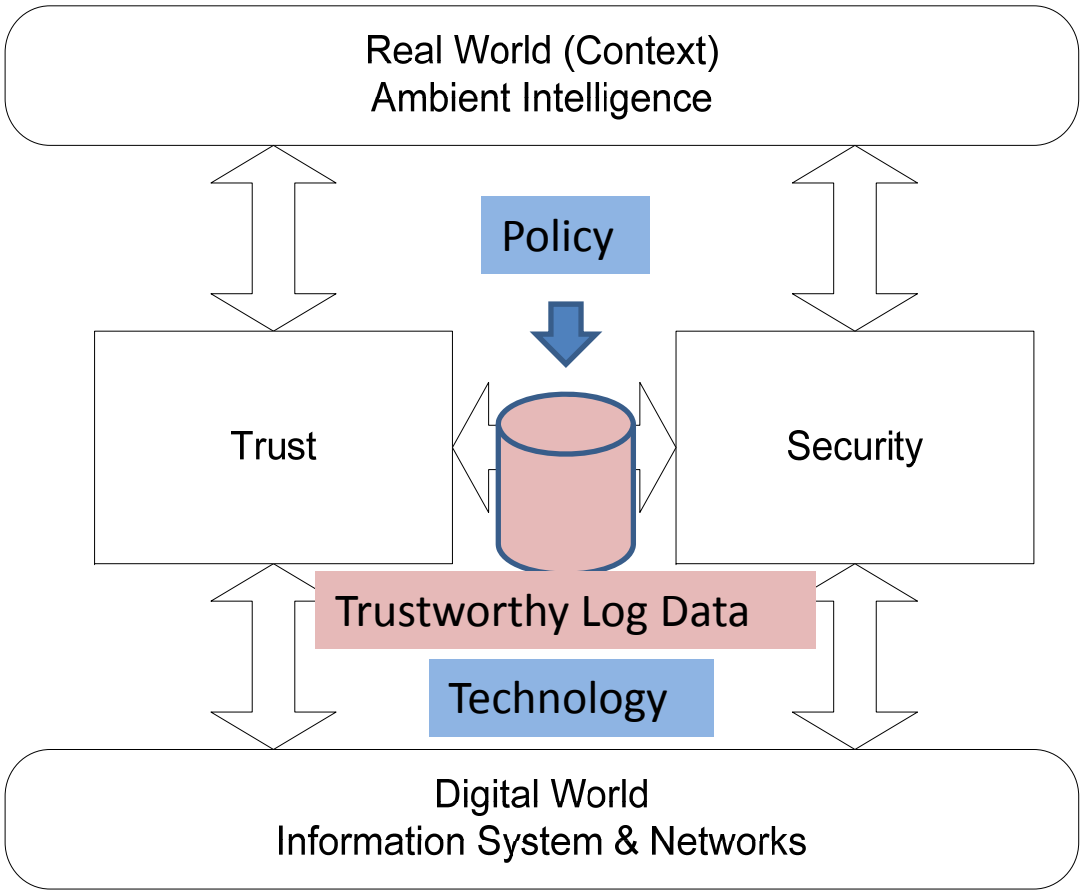


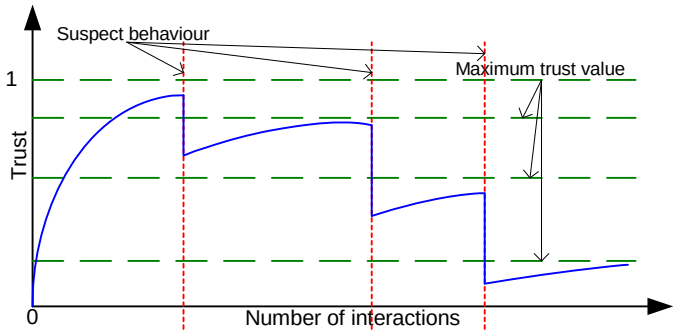
Plates tectonics : Continental drift

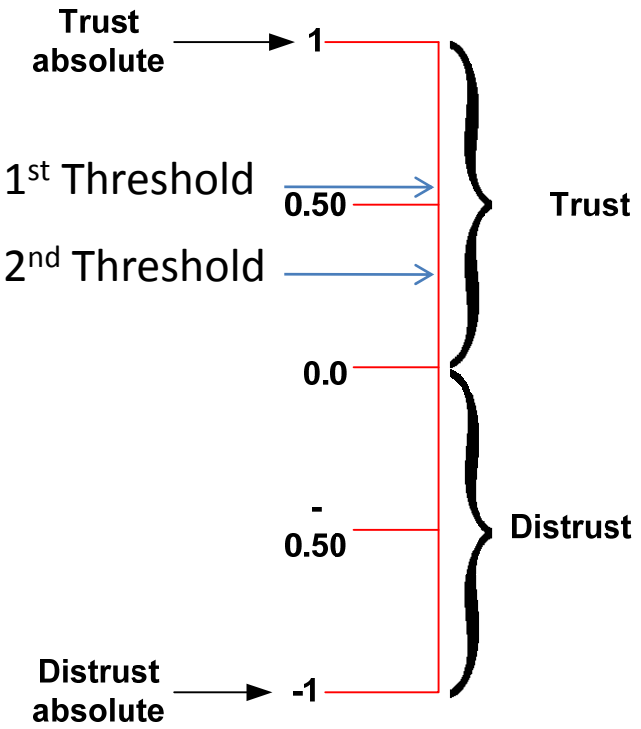
for scientific disciplines



Security & Trust







Dissociation between both Infrastructures/Instrumentations of Trust & Security/Dependability

Trust Continuum

1st Threshold to modify behavior

2nd Threshold to stop interacting

Centrifugal force of data

Data destination

Irreversible process

Data provenance

Source & quality of the information

How can we trust messages or services ?
authentication + non repudiation

Spam?
Spoofed identity?
Valid information?
False rumor?

Privacies :

Compartmented Multi-identities, risk of pulverized identities (napterization)

You have multiple roles:
a citizen, an employee,
a consumer, a provider
a parent, a patient,
a victim, a player …

All these roles have their own privacy

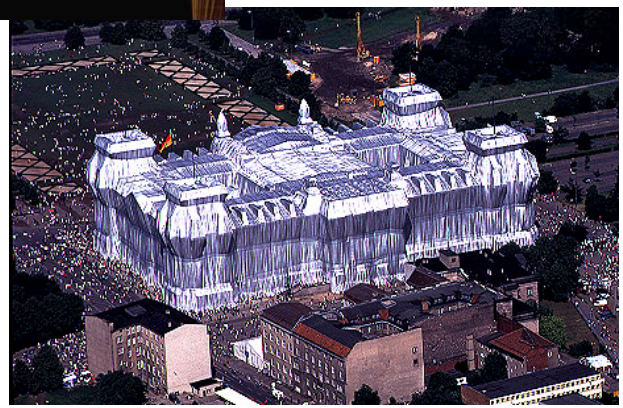
Physical identity(ies) & Cyber identity(ies) must be considered separately and as a whole

Privacy : personal data protection ? NO
the digital reign: duo programs - data

Opaque software,
open in darkness
The hook is in the light

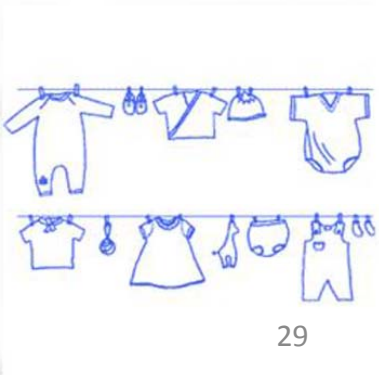
Digital personal patrimony
scattered in private
exploded spheres

Security content:
generalization of protecting envelopes



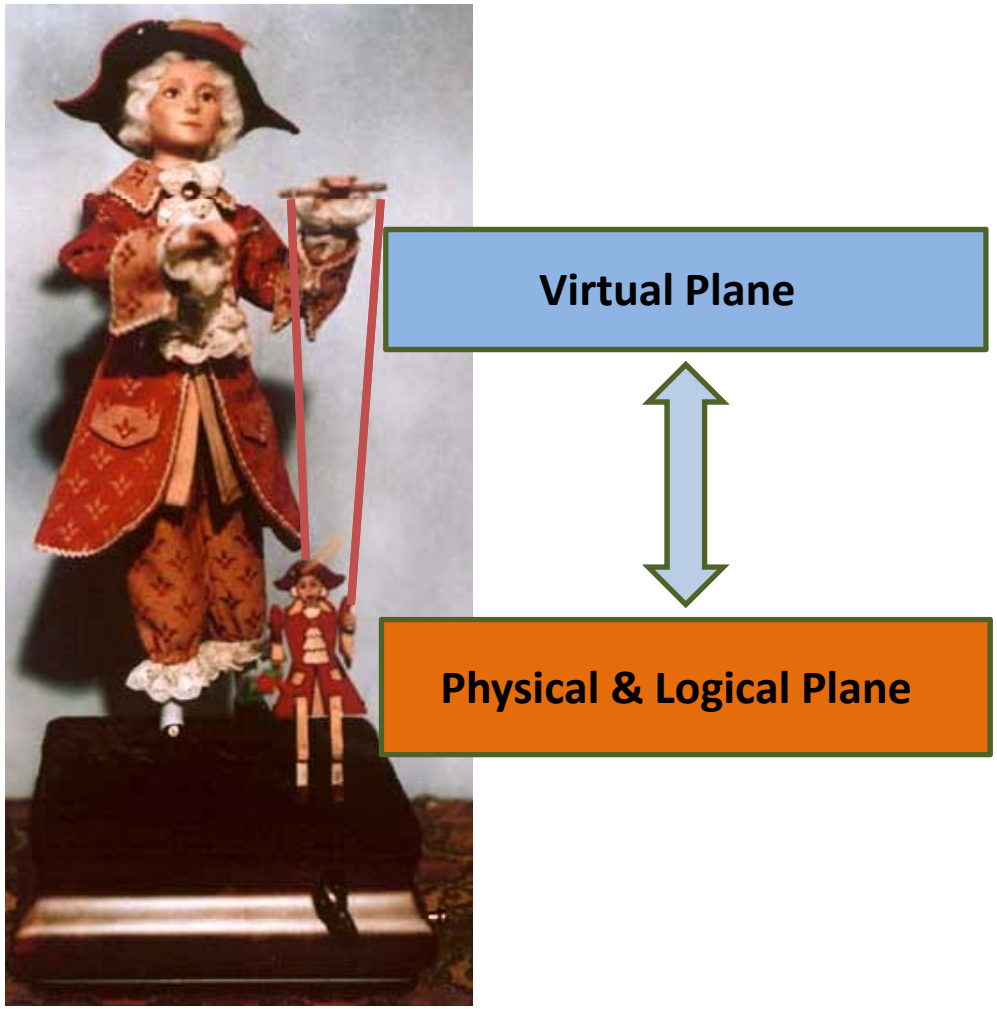
Cristo : ephemeral art
(Pont Neuf & Reichstag)

- Each individual will manage the lifecycle of objects of his personal digital heritage in its own virtual network.
- Right to oblivion
  - Need to have its garbage collector across the network to erase his personal tracks



The invisible seams of the virtual world

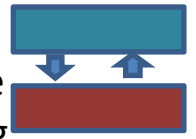
Management of abstractions in protocols and architectures



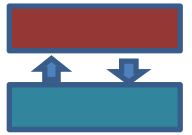
Engineering to override multi-technology complexity

- Mechanisms adapted to reaction speed, to spatial distribution hooking physical and computer science reality

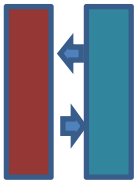
1. Above : **overlays**
   - Overlay Structures / architecture
   - Virtual wires sewed with hashing functions



2. Under : **underlays**
   - Mobility models
   - Physical Landmarks hooked and linked through signal processing and probabilistic models



3. On the sides : **crosslayers**
   - Transgression of OSI layers to react faster
   - Triggers, logical wires to short-cut classical paths to perform rapidly



Digital hybrid urbanization :
Holistic future Internet or Balkanization of networks

No more monochromic, mono-technology security

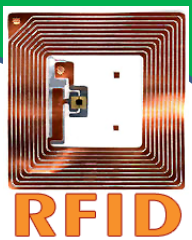
Beyond 3-4G

Current Internet
WDM-IPv4-IPv6-MPLS

Services
Hooked to several infrastructures

Internet of Things

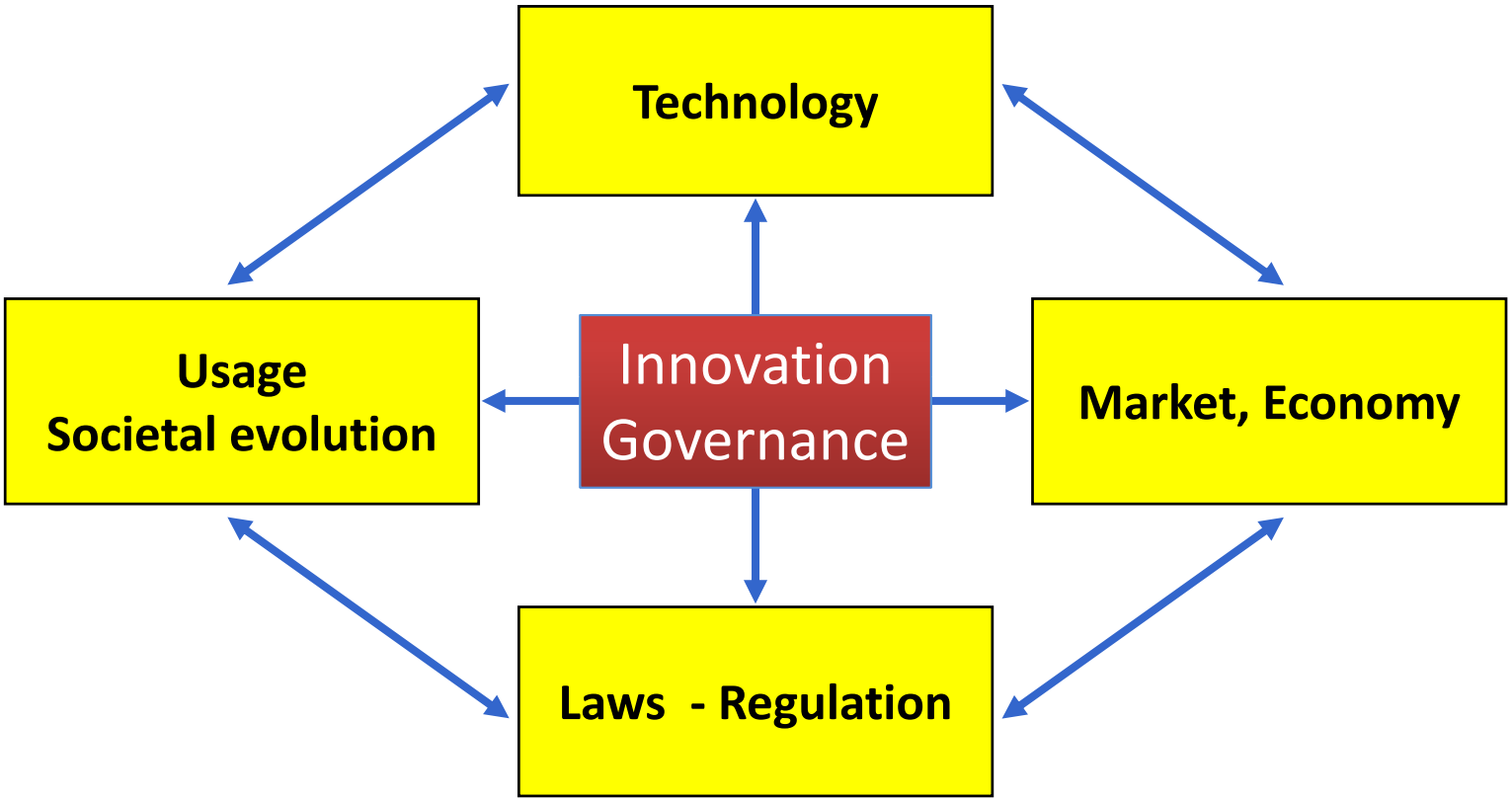
Galileo-GPS-Glonass
Beidu
Clock and Position



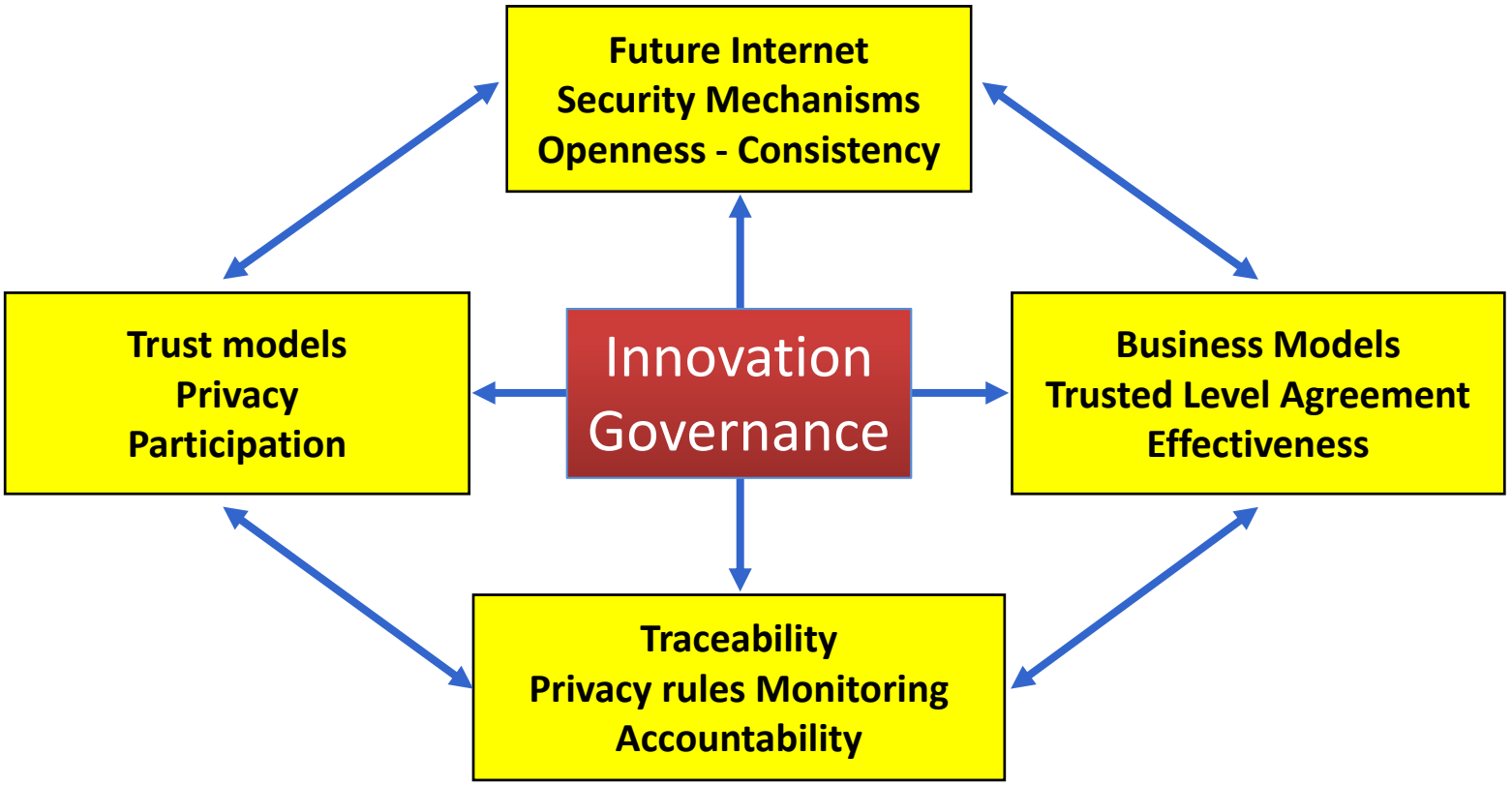
The heterogeneous urbanization of abstract entities of varying granularity

- The first high level of abstractions
  - Programs : executable strings
    - active computing machines
  - Data : static strings
    - passive information which is acted upon by executable services
- The second high level of abstraction
  - Virtualization
    - to reduce complexity
    - to dialogue with remote components
  - Embodiment
    - To be efficient here and now (embedded computer science)
    - Internet of Things
    - Interfaces with the real world

Governance : dialectic aspect of innovation engine



Adaptive built-in security & trust



Security, Privacy & Trust : Technology & Policy

- Security
  - Security information, data sharing, data gathering
    - Within a country and internationally

  => **SPT cyber architectures and models**
    - Transnational data repositories
- Privacy (Individuals, enterprises)
  - anonymity, provenance, transnational storage and dissemination, and ownership of data
- Trust
  - Trust infrastructure =/ security infrastructure
- **Beyond technology** :
  - Today and future security and privacy policies
  - Transnational policies
    - Economical, legal aspects, cultural, psychological, societal considerations
    - Cybercrime

Data sharing across multi-domains

- International collaboration is critical to ensure that solutions can operate **across national and cultural boundaries**
  - Need for expressing national and local policies in order to enable automated comparison, negotiation, and merging across international borders
- Need for R&D of the technical components of **secure and private data repositories**
  - data representation & structure (multilingual)
  - policy representation & understanding (copyright, free)
  - architectures & enforcement
  - development of specific testbeds
- Framework for an International **Cyber Data Exchange System**
  - not only US-EU but expand to support OECD-wide data exchange

Responsibility infrastructure for the Future Internet

- The international research community must work together on mechanisms enabling **accountability**
- Identification and establishment of collaborative, context-specific, automated and non-automated common **trust models** ("virtual organization") in concrete scenarios are needed in order to:
  - provide better understanding of challenges of international data exchange
  - support collaborative research efforts in computer security (malware, attack data)
- Development of models and mechanisms for **information** and **knowledge exchange**, not just data exchange
  - facilitates certain legal and policy requirements
  - necessitates research into ways of automatically extracting and reconstructing information from data in a traceable fashion

Global issues : polymorphic properties

- Not one single providential solution => **governance**
  - Plurality, personalization, scalability, virtualization, embodiment
    - Evolution of standards
  - Security, Privacy & Trust by design at all levels
    - Computer (Cloud…), Services, Software (Web…) and Networks (Post-IP, cognitive networks, sensors…), Internet of Things
  - Security assessment (measurements, formal models)
- Transnational frameworks **across continents**
  - Identity => Accountability
  - Compatibility, interoperability => Openness, Transparency
- Transnational and domestic models => **plurality**, dynamicity, mobility
  - **Trust** (reputation, recommendation, frequentation, delegation)
  - **Privacy** (Anonymity versus Traceability)
  - **Identity Mgt** & Accountability
  - **Cryptography** with statistics, semantics and contexts

Measurements & Governance

- Reciprocity in interoperability
  - Coexistence of several conflicting models
  - Fragmentation, Balkanization
    - Threats: emergence of spontaneous groups
    - Response to openness: opacity of services
    - Birth of feudalism
- Need to dock with common services
  - Identity Management, Management of anonymity
  - Geo-navigation systems and authentication
- Symmetry of exchange and asymmetry of trade relations
- Multipolar governance of systems
  - Monitoring function: essential
  - Transparency (visibility) in governance