Future Internet Security

Michel Riguidel, (Telecom ParisTech, France)
michel.riguidel@telecom-paristech.fr

ITU-T Workshop on
New challenges for Telecom Security Standardizations",
Geneva, 9 (afternoon) to 10 Feb. 2009

Bio & Areas of interest

- Bio
  - Telecom ParisTech – Michel Riguidel (Professor, Department Head)
  - **Michel Riguidel** is the Head of the Department of Computer Science and Networks, at Telecom ParisTech (Ecole Nationale Supérieure des Télécommunications, www.telecom-paristech.fr) in Paris, where he lectures in security and advanced networks.
  - His research is oriented towards security of large Information Systems and Networks and architecture of communication systems (Grids, Security of the Future Internet, Trust and Advanced Networks).
  - In the IST Integrated Project of FP6, he is Key Researcher of the Secoqc Integrated Project (Development of a Global Network for Secure Communication based on Quantum Cryptography), responsible of the Network Architecture.
  - In the FET of the FP6, he was the Security & Dependability Task Group Leader of the Beyond the Horizon Project.
  - In Italy, he is scientific member of the international Think tank on telecommunications ThinkTel (www.thinktel.org).
  - He has several patents in security (firewall, watermarking and protecting CD ROM).
  - He published recently two books “La sécurité à l’ère numérique” (édition Hermès Lavoisier) and “Le téléphone de demain” (édition Le Pommier).
- Areas of Interest
  - He contributes to the FP7 European Project : Inco-trust http://www.inco-trust.eu
  - The future Internet
  - The security, dependability, trust and privacy of the future Internet

Digital hybrid urbanization :

holistic future Internet

No more monochromic, mono-technology security

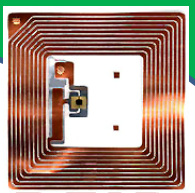
Beyond 3-4G

Current Internet
WDM-IPv4-IPv6-MPLS

Services
Hooked to several infrastructures

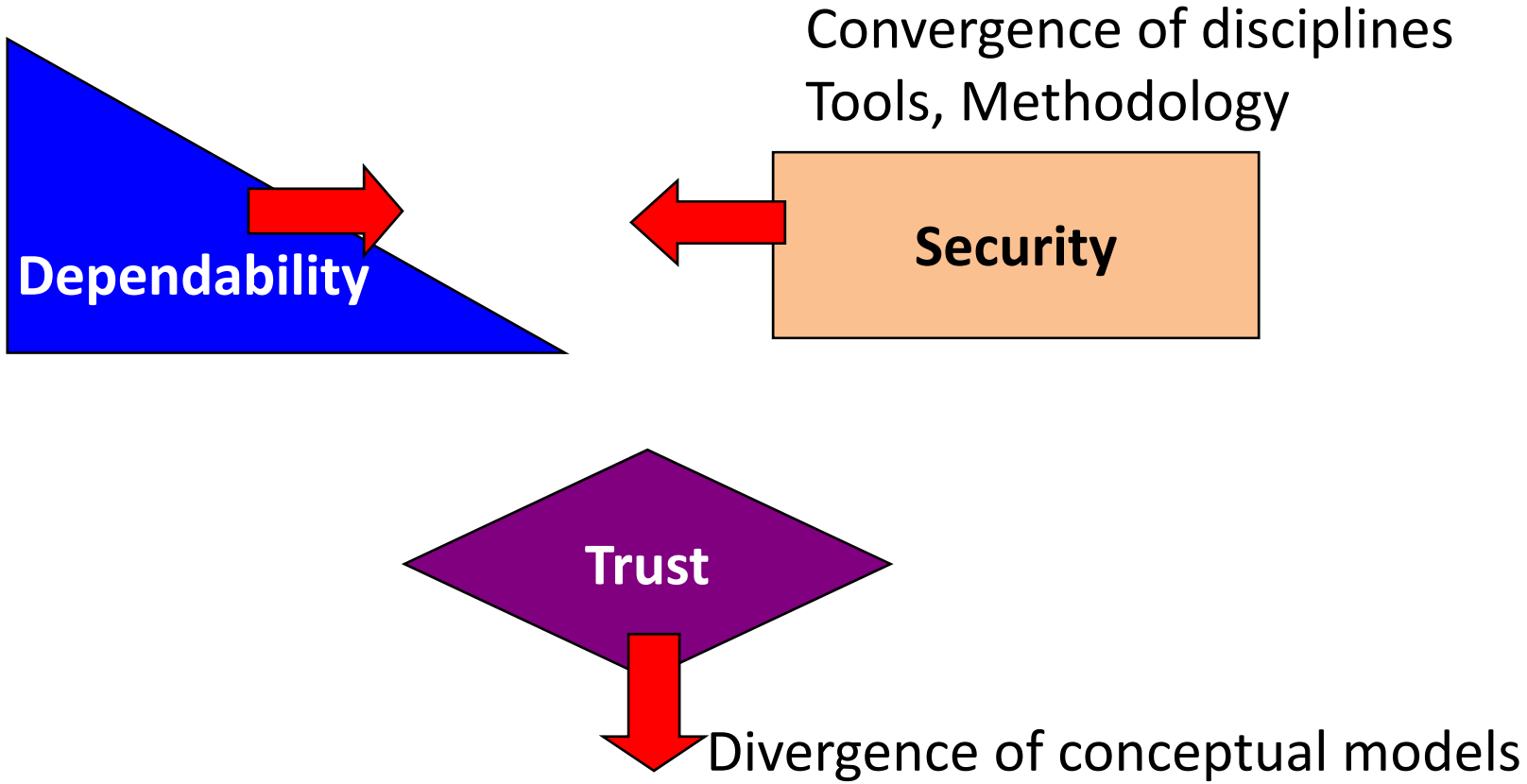
Internet of Things

Galileo-GPS-Glasnos
Clock and Position



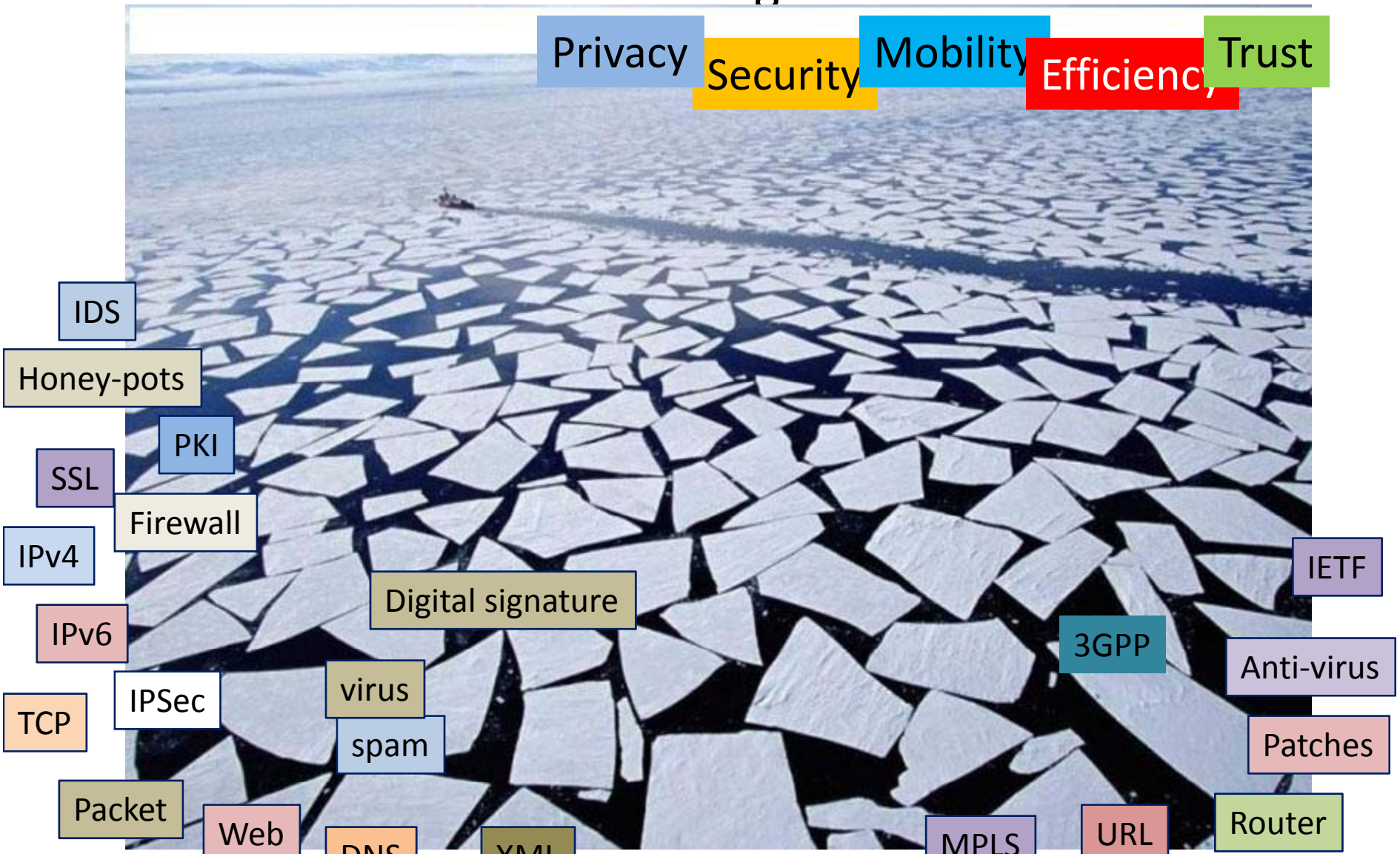
Plates tectonics : Continental drift

for scientific disciplines

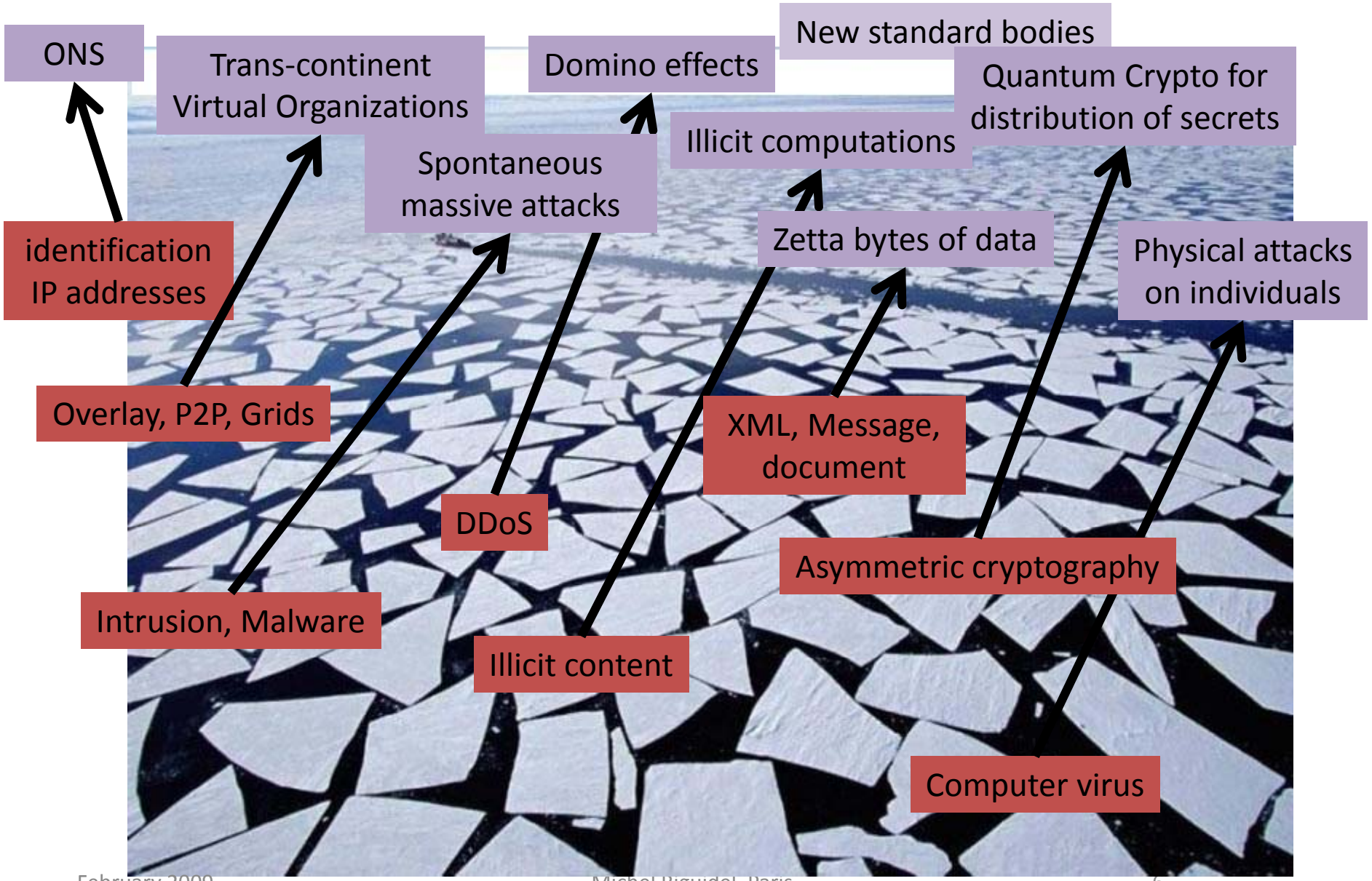


Internet is broken :

how to heal the future fragile communications ?



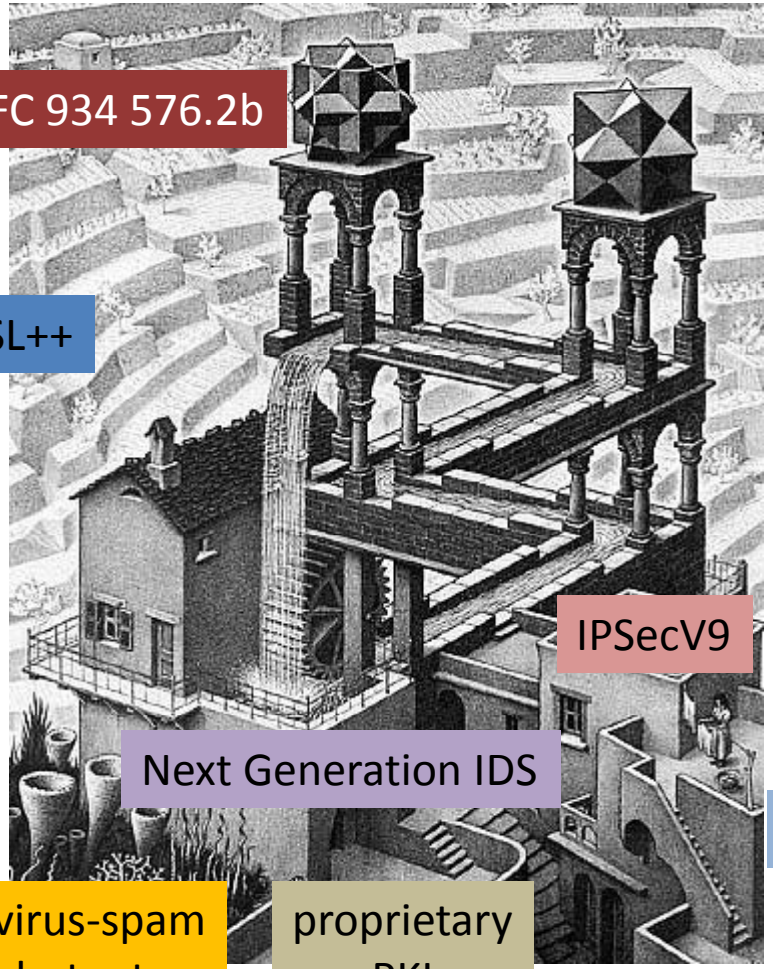
The new landscape in security



Future Internet :

Incremental or Disruptive Approach ?

Upgrade Internet++, B3G++
=> Patch & Go



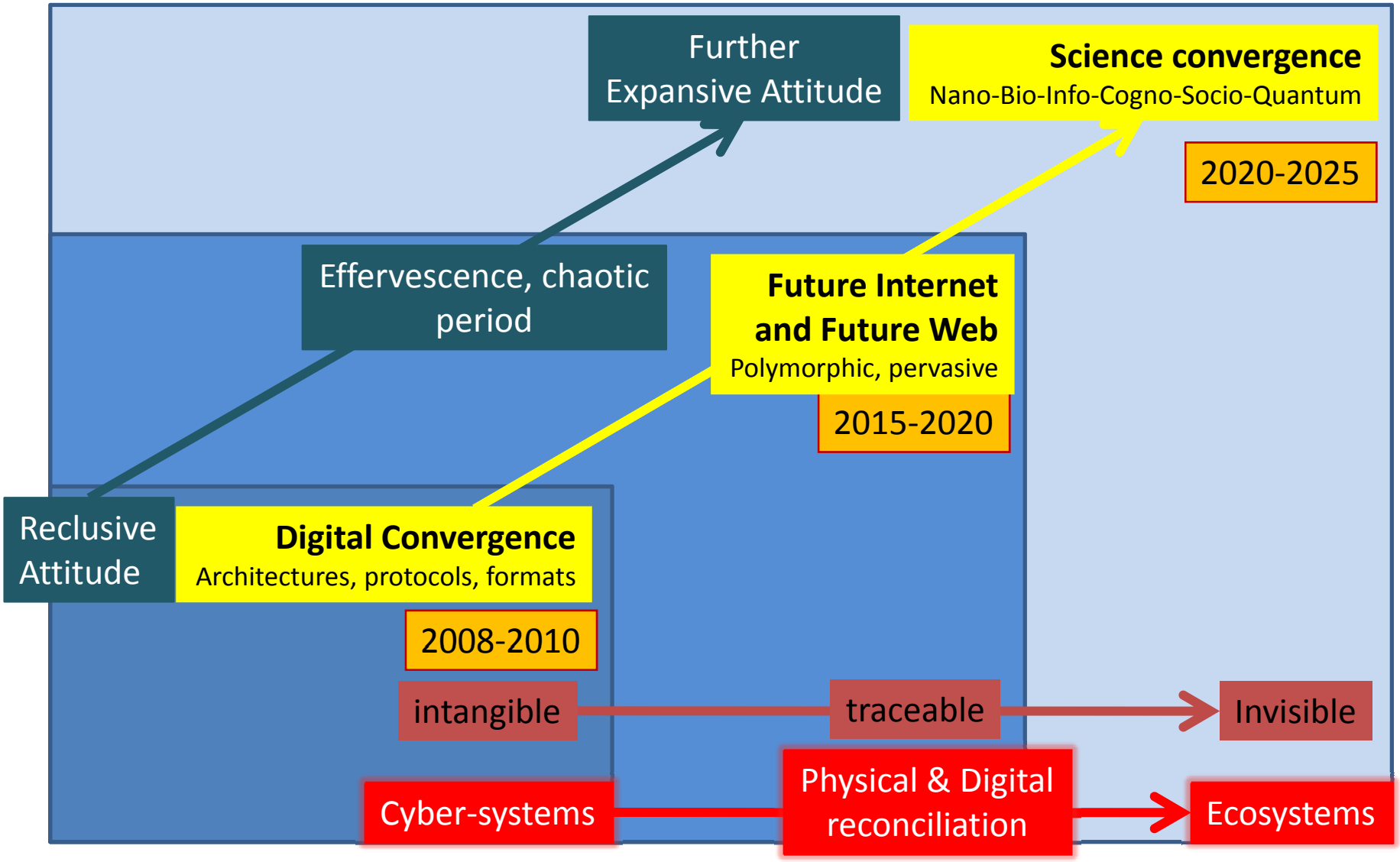
Clean slate
=> rethink & radically design

For security : radical redesign

Authentication with trusted clocks and position
Distribution of secrets using Quantum Crypto
Trust instrumentation (at the design level)

Digital world roadmap:

at a crossroads of intangible & invisible entities



Hidden Web, Deep services :

death of the 7 layer model

Old Internet :

flat architecture

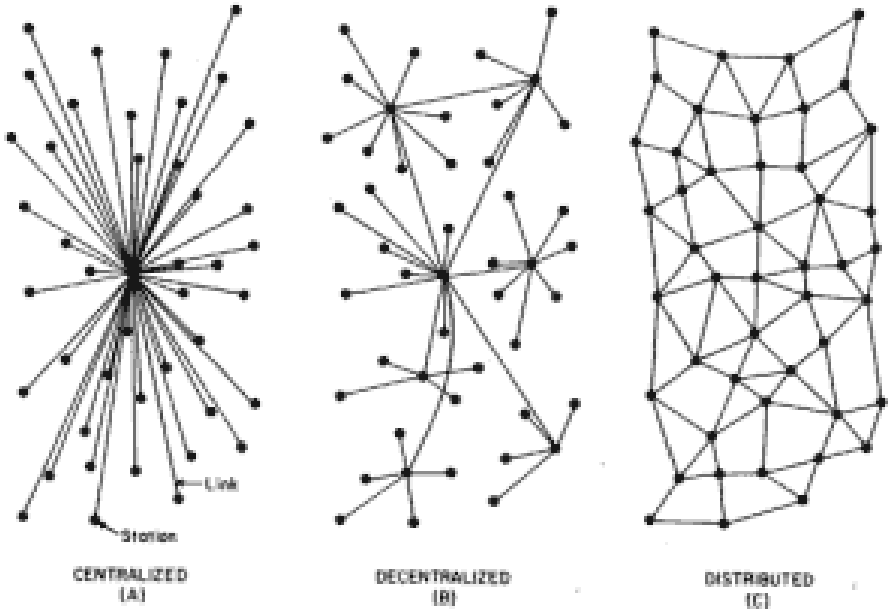
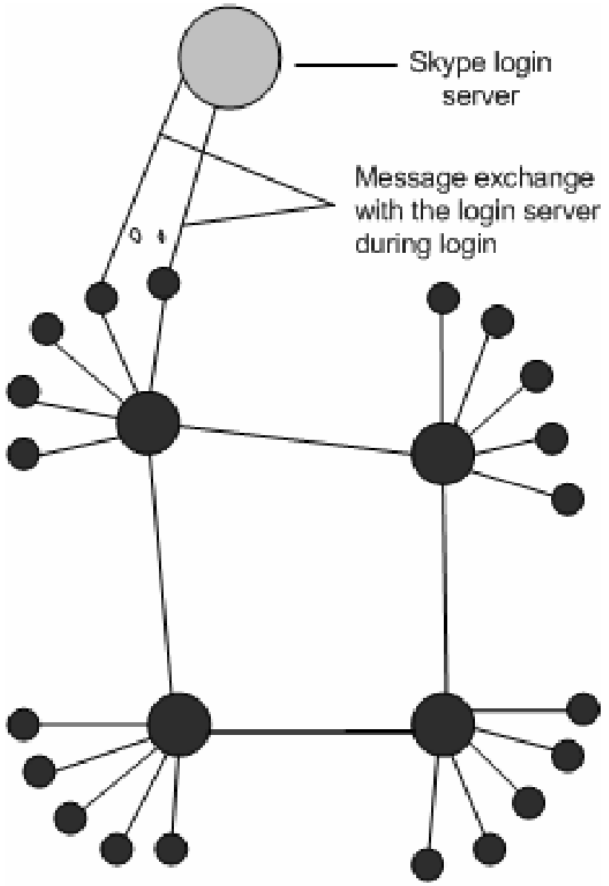


FIG. 1 — Centralized, Decentralized and Distributed Networks

First Drawing of Internet (1962)

Future Web :

distributed “aggressive” services

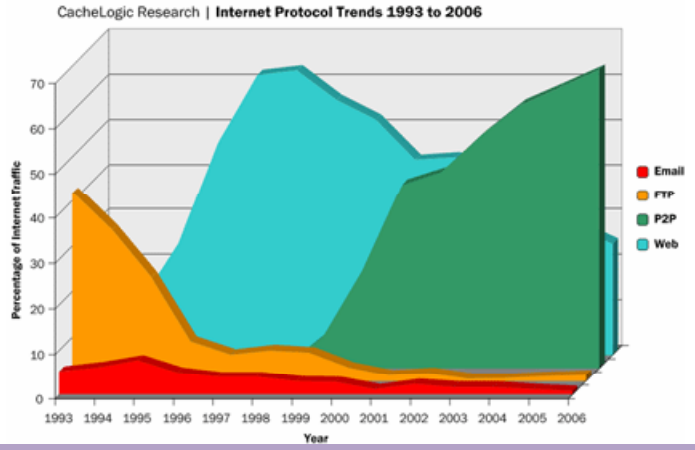


Example : Skype architecture

The Web evolution

- **Old Web : importance of the underlying protocols**

  Computers connected (Web pages, Web sites)
  - 1986 : ancient Web : (Wide Electronic Board)
  - 1991 : Web (Berners-Lee)
    - Web with text
    - 1995 : first success (Java encapsulated)
      - Bandwidth issue (wait-wait-wait)
  - 2000 : high data rate
    - Web with Multimedia
    - Web2 (Multiparties, Virtual), “Semantic” Web, …



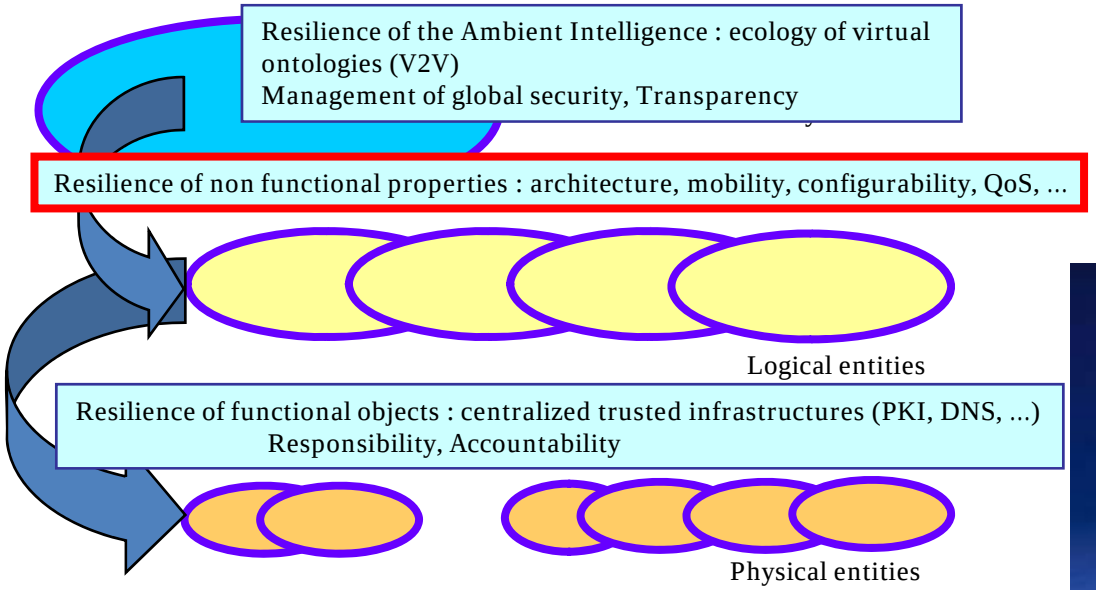
Catastrophic event in the protocol world in 2000 :
Web Http decreases, P2P protocols raises drastically

- **Future Web : importance of mobility, context and reinvestment of Humans & Reality**

  Computers (Mobile, Multimedia), networks at large, within physical world
  - profound evolution in parallel with Future Internet
    - Geography : Mobility, Ubiquity
      - Reconciliation with nomadicity (vocal Web)
      - Search engines with locality, smarter search engines : Post-Google engines
    - History : Memory of the web (Next Generation of the Deep Web, Hidden Web)
      - Stochastic XML (see P Senellart PhD Thesis December 2007, Paris)
    - Knowledge
      - Representation, Visualization
      - Search engines, Social computing, Natural language technology
  - Web of intentional Things
    - Things will display their public life cycle, will blog (for maintenance)

Virtualization – Incarnation dialectic

- **Virtualization of properties**
  - Heterogeneous infrastructures
  - Mobility, security …
- **Network concepts incarnation**
  - Situated services, context
  - Neighbors, Topology



Computational Cryptography

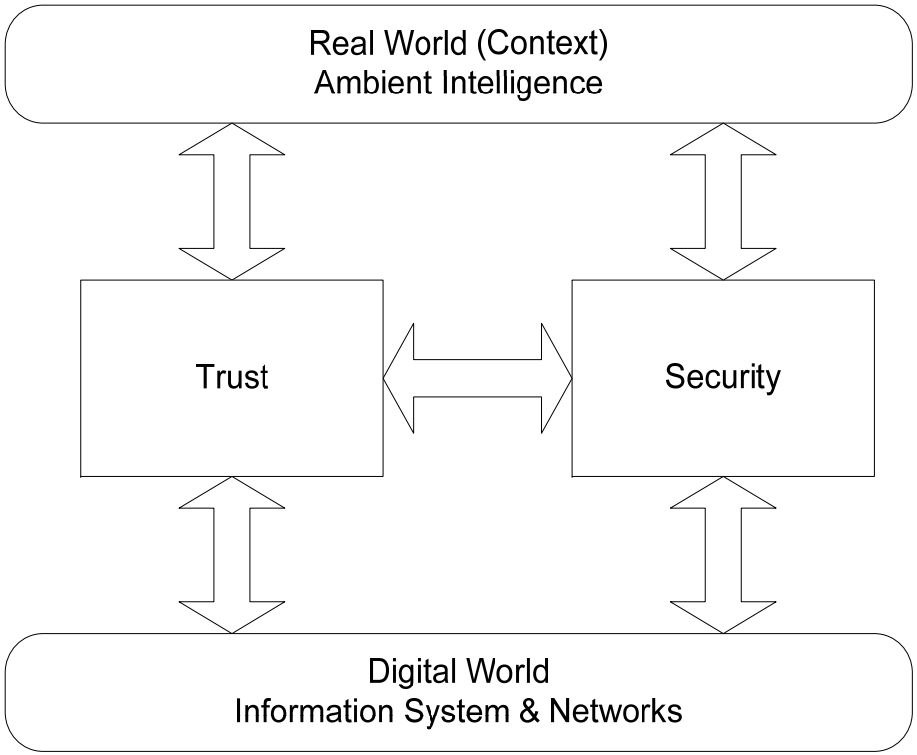
Traditional hierarchical ladder of the current internet

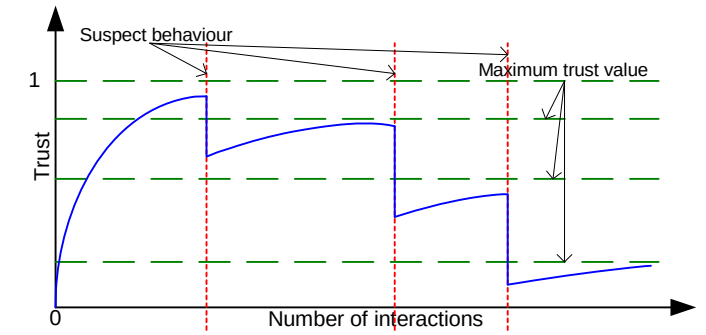
Re-equilibrium of forces within the future internet (attacks, cryptanalysis)

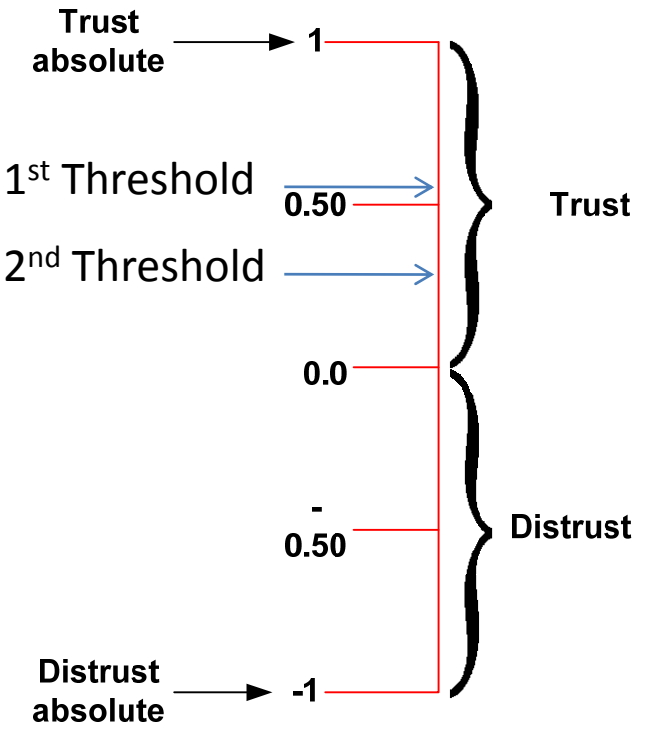
Massive externalized
furtive computer power
running within the
anonymous networks
confidential illicit computations

New Crypto with computation, history and geography ?
Alice and Bob are no more alone in this world:
They have witnesses, alibis, trajectories
They leave traces …

Security & Trust







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

Trust Continuum

1st Threshold to modify behavior

2nd Threshold to stop interacting

Regular:

artefacts for individuals & enterprises

Identification & Authentication

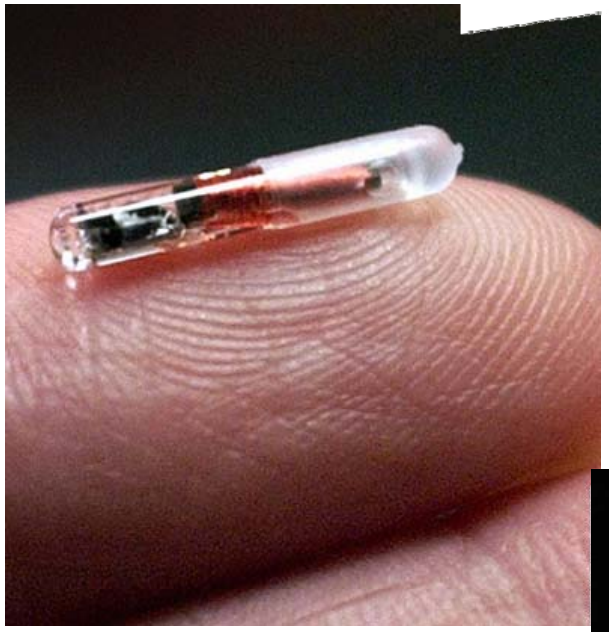
Accountability, Non repudiation

Traditional security to be improved and revisited (architecture & protocols):
Classical Cryptography
Engineering Security

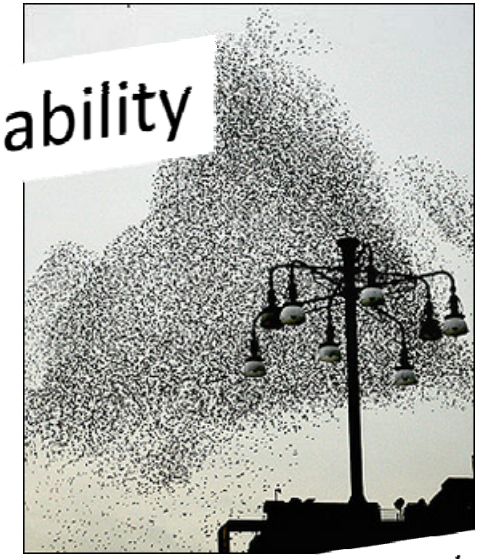
Dwarf :

tiny program, simple artifact, scarce resource

The digital world is
neither fractal
nor scalable …
For tiny objects,
Emergence of
self-* models
at the collection level



Traceability



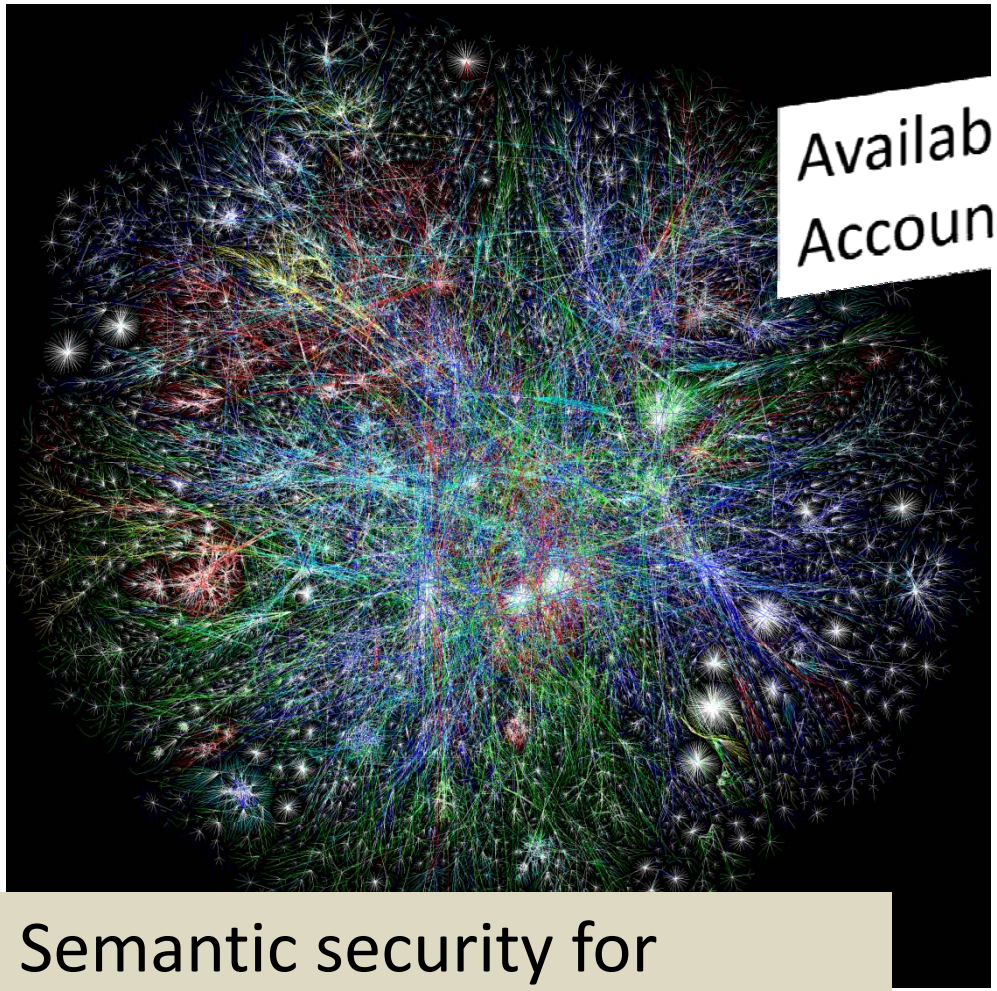
~~Identification & Authentication~~

Stochastic Security

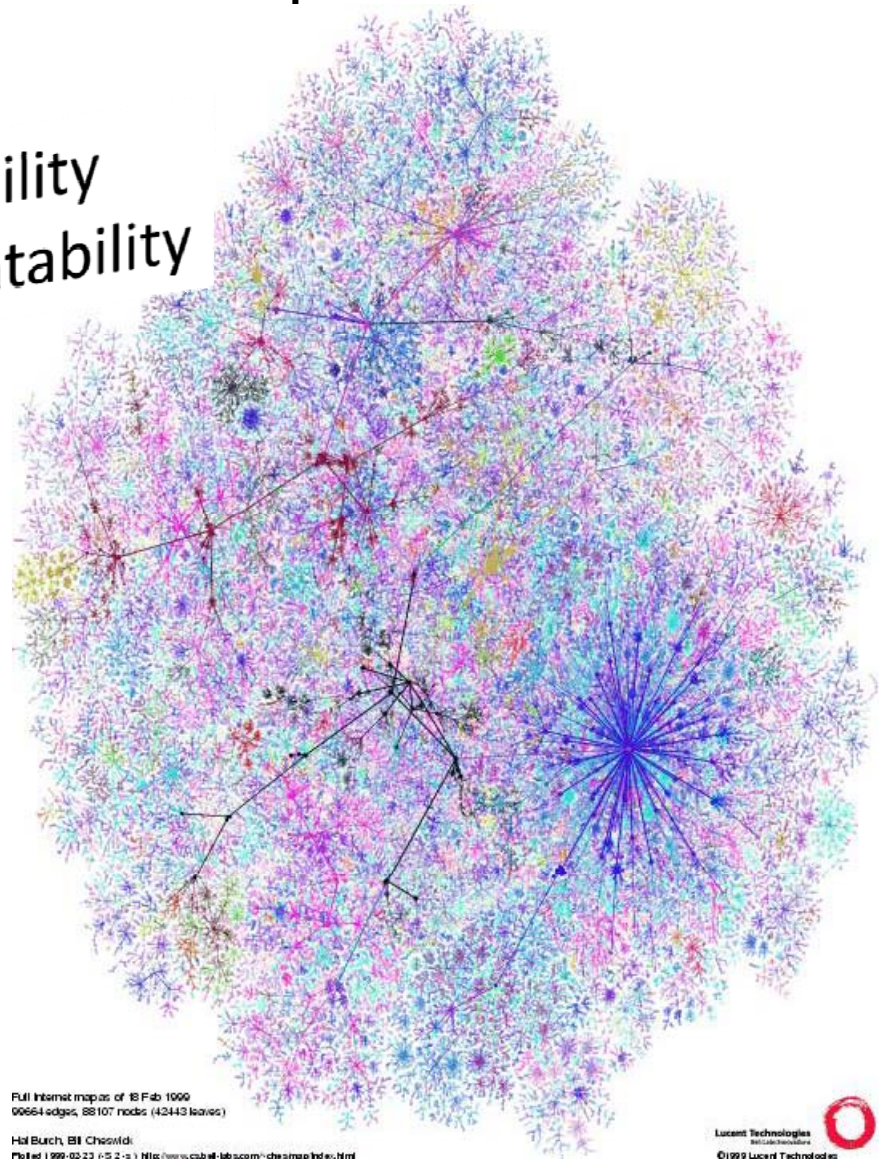
Strong security at the collection level (architecture)
Cheap weak security at the individual level
(massive & simple algorithms)

Huge, Giant :

Complex systems, inextricable problems



Availability
Accountability



Semantic security for
Complexity & human values
Trust

Virtual & Real world:

Proportional Responsibilities across the whole chain

Attacks swing between
virtual and reality, back and forth

avatar

What is biometry (voice, picture)
when digitized ? Just 1 and 0

On the future Internet, the audio video content
will be quite sensitive and highly valuable

Privacies :

Compartmented Multi-identities

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

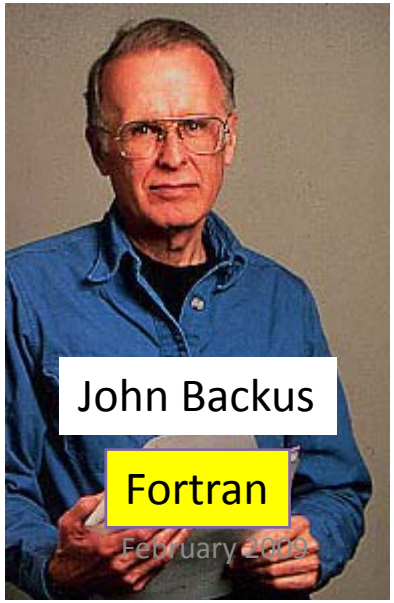
Physical identity(ies) & Cyber identity(ies) must be considered separately and as a whole

Evolution of languages :

complexification of abstract typing

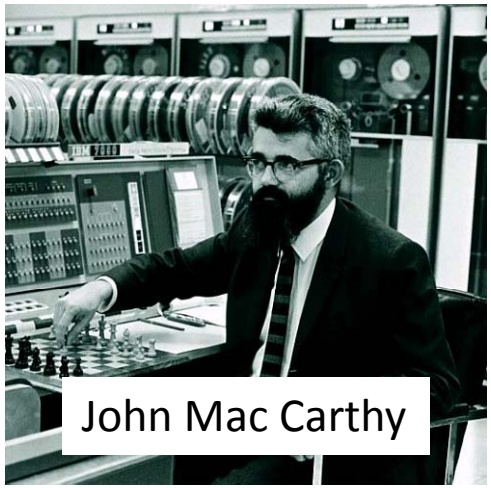
1955 — 1958 — 1965 — 1986 — 1992

1955	1958	1965	1986	1992
Flottants, Integers : Independent In memory	Lists : Organization of memory with strings	Pointers: Structures Statics heterogeneous	Pointers: Notion of objects Programs autonomous dynamic	



John Backus

Fortran

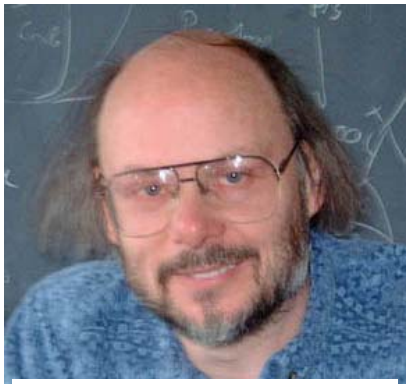


John Mac Carthy

Lisp

Dennis M. Ritchie

C



Bjarne Stroustrup

C++

Java

Evolution of Networks : Post-IP, Post-Google

complexification of abstract typing of links

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

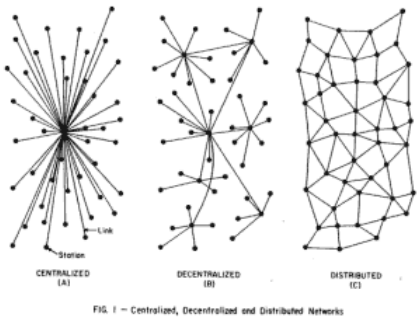
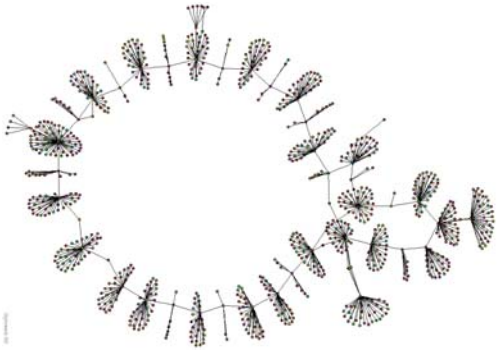
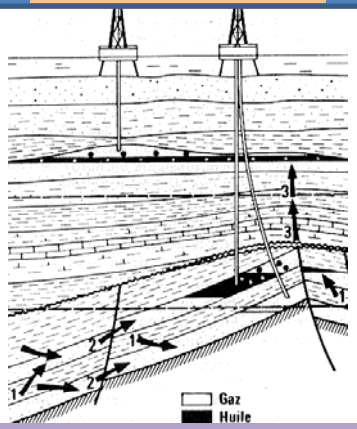


FIG. 1 — Centralized, Decentralized and Distributed Networks





Traditional Network
Graphs
Of nodes and links

Markov, Poisson

Ubiquitous computing
Plate 2D

Topology (P2P)
Flow of content
Geography

Ecosystem
3D Fluid, Plastic

Porous Media
History

A 3D space Programmable,
dynamic, semantic
Architecture
programmable

Intercontinental Thought : new models

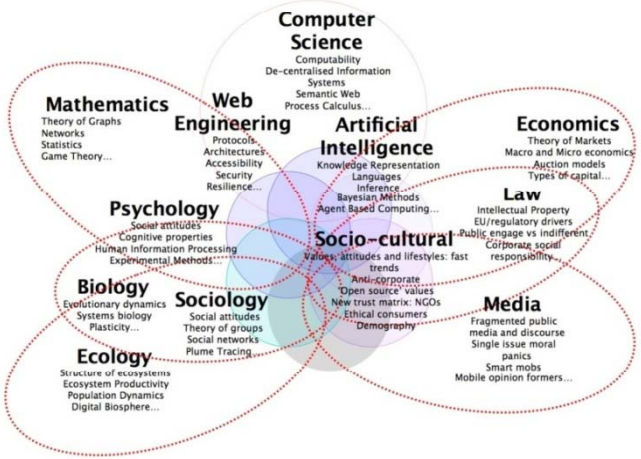
beyond an idyllic, pre-scripted vision of future networks

- Neither unique nor providential solution
  - Model, **counter-model, alter-model**
  - Arrival of China and India on the IT scene
    - change in concerns (demographic, development)
    - change in power
  - Alter-models
    - the pseudo-libertarians (“Naives of the Internet”)
    - repression pure players (some governments).
- Cyberspace & Cyber-governance (Κυβερ : rudder)
  - Technology free rein?
    - descriptive of order
      - no control and regulation becomes self-reflexive
    - normative of order
      - governing is defining order
  - In technologies, we talk about
    - often : what is
    - not often : what ought to be or what could be

- Multipolar Vision

Dictatorship of the single thought
In computer science

- Multidisciplinary Vision



Research at the international level

- Research, based on **progress & human values**
  - Awareness of
    - what is **achievable** (technical)
    - what is **acceptable** (civilized ethics, democratic values)
  - Countries: bearers of a **variously facetted humanism**
    - to be instantiated in the communications or protection tools
- Knowledge, partitioned for choice
  - **Users' awareness** to grasp the security & intimacy stakes
    - The choices: multiple, ephemeral and adapta
    - Defining the demarcation line: movable
  - **Users' behavior** to be taken into account
    - imagining and anticipating the effects on the behavior of both individuals and groups