eINDIA 2011
16th December 2011
Gandhinagar

BUILDING International Cooperation
for Trustworthy ICT

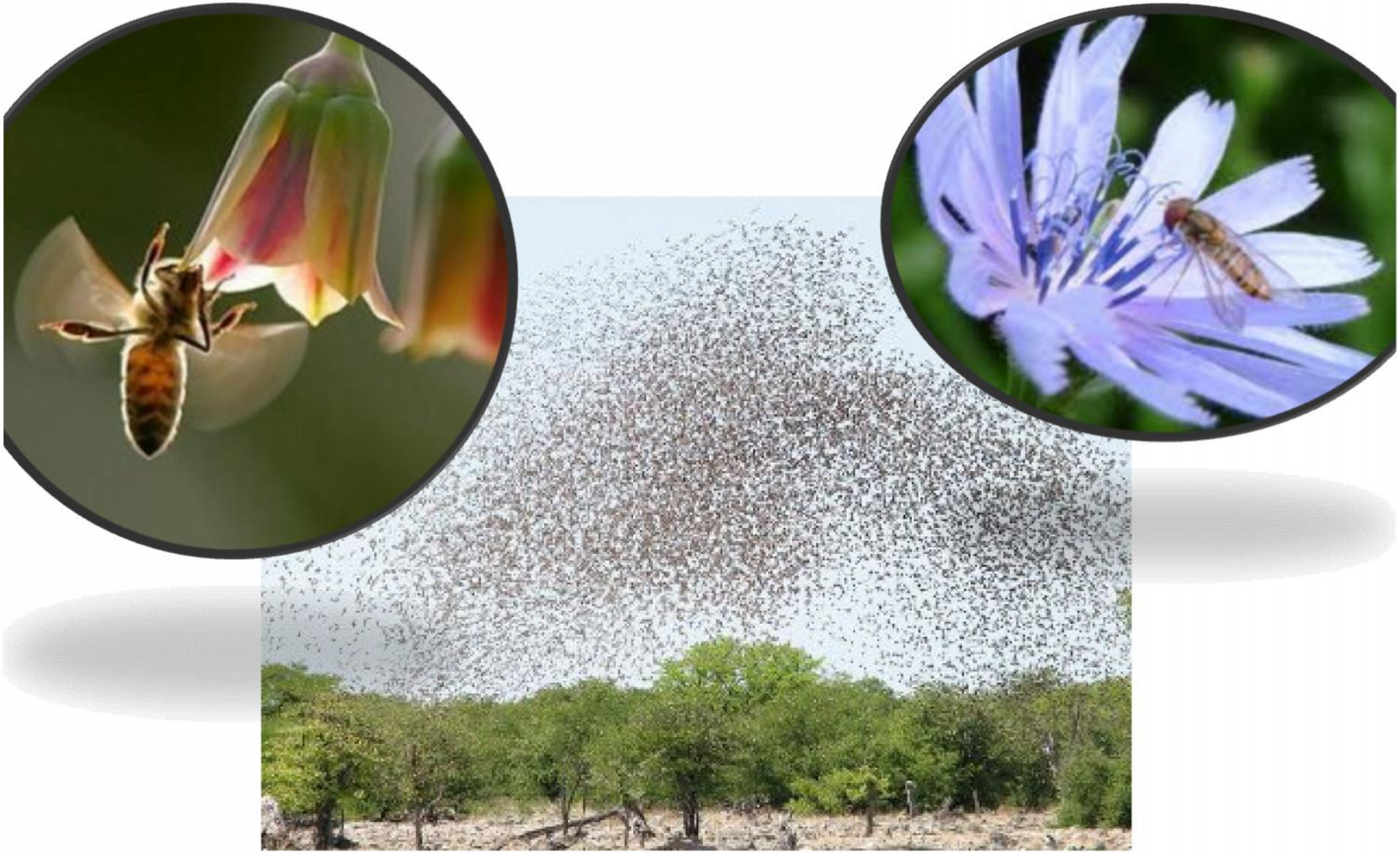
New models of communication & security for the Future Internet Trust and security technological challenges

Michel Riguidel

michel.riguidel@telecom-paristech.fr

TELECOM ParisTech

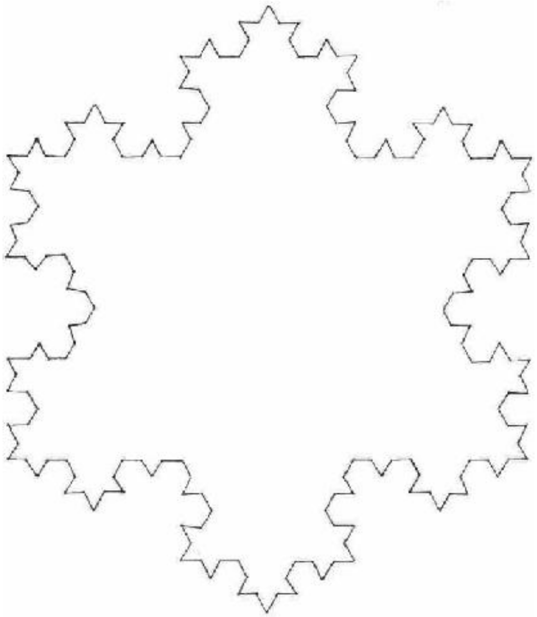
Security of the whole system & all the components

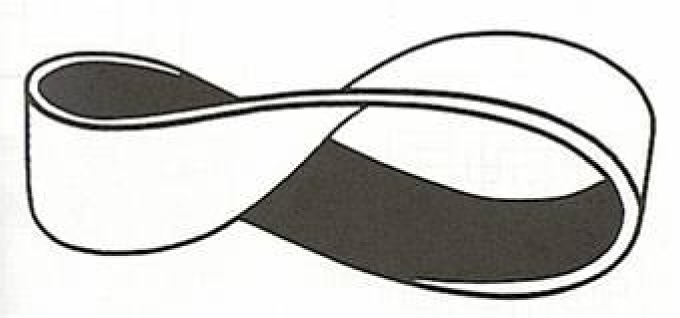


Complexity

Complexity is in

shape, size, etc





Complexity is in

motion, momentum, enthalpy

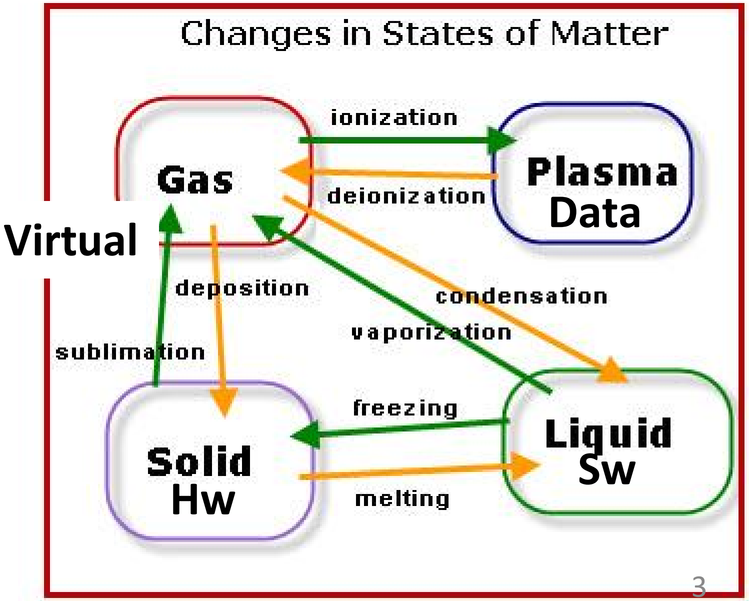
ΔH_x^θ

Δ = change in

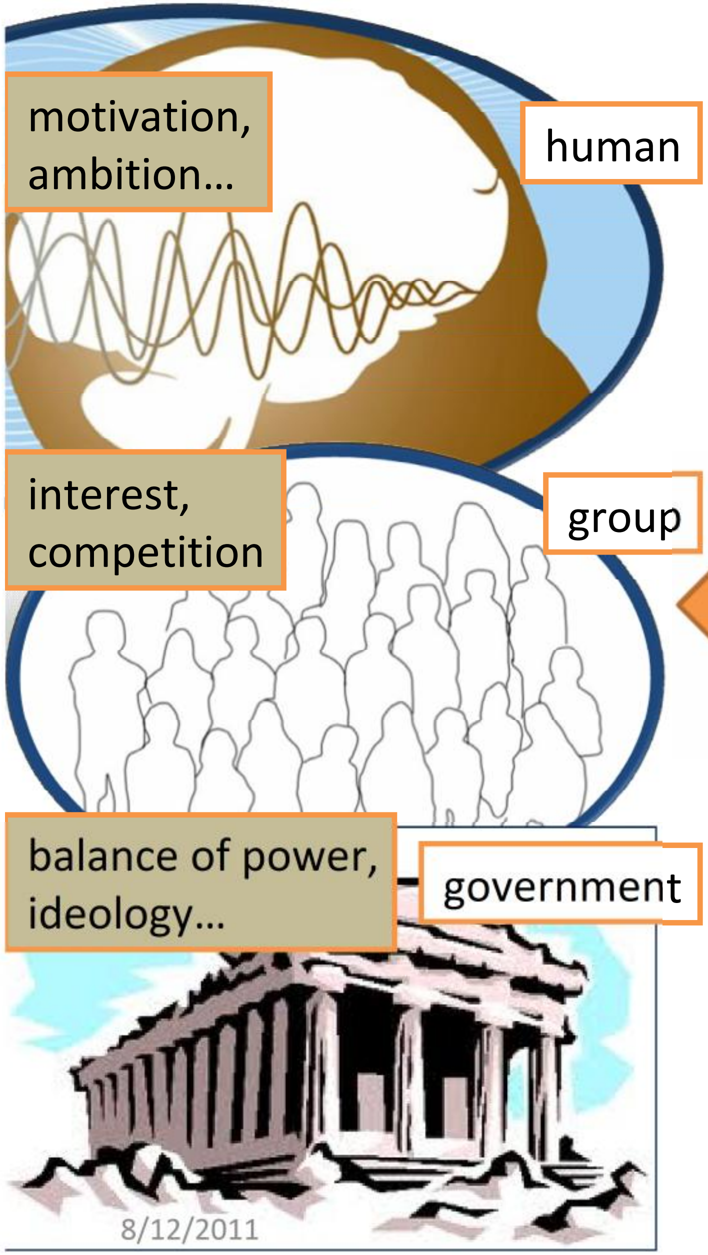
H = heat energy

θ = standard conditions

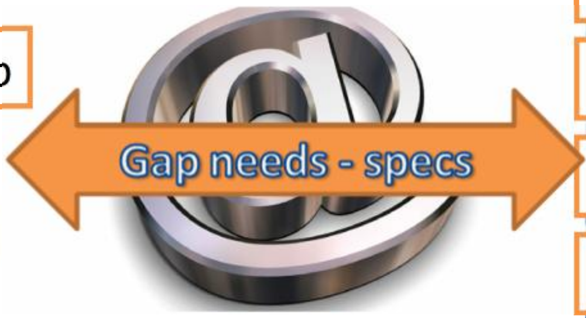
x = type of change



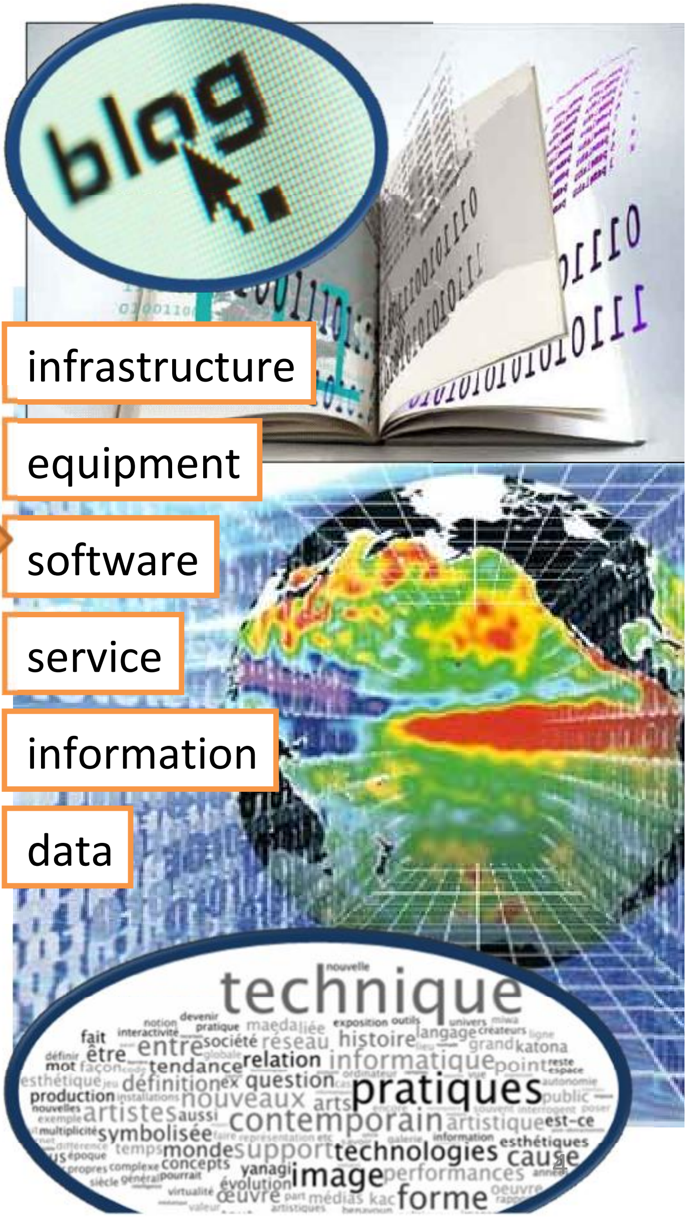
Digital Activity => cyber-social system



Digital world today: strong entanglement between Human & Machine



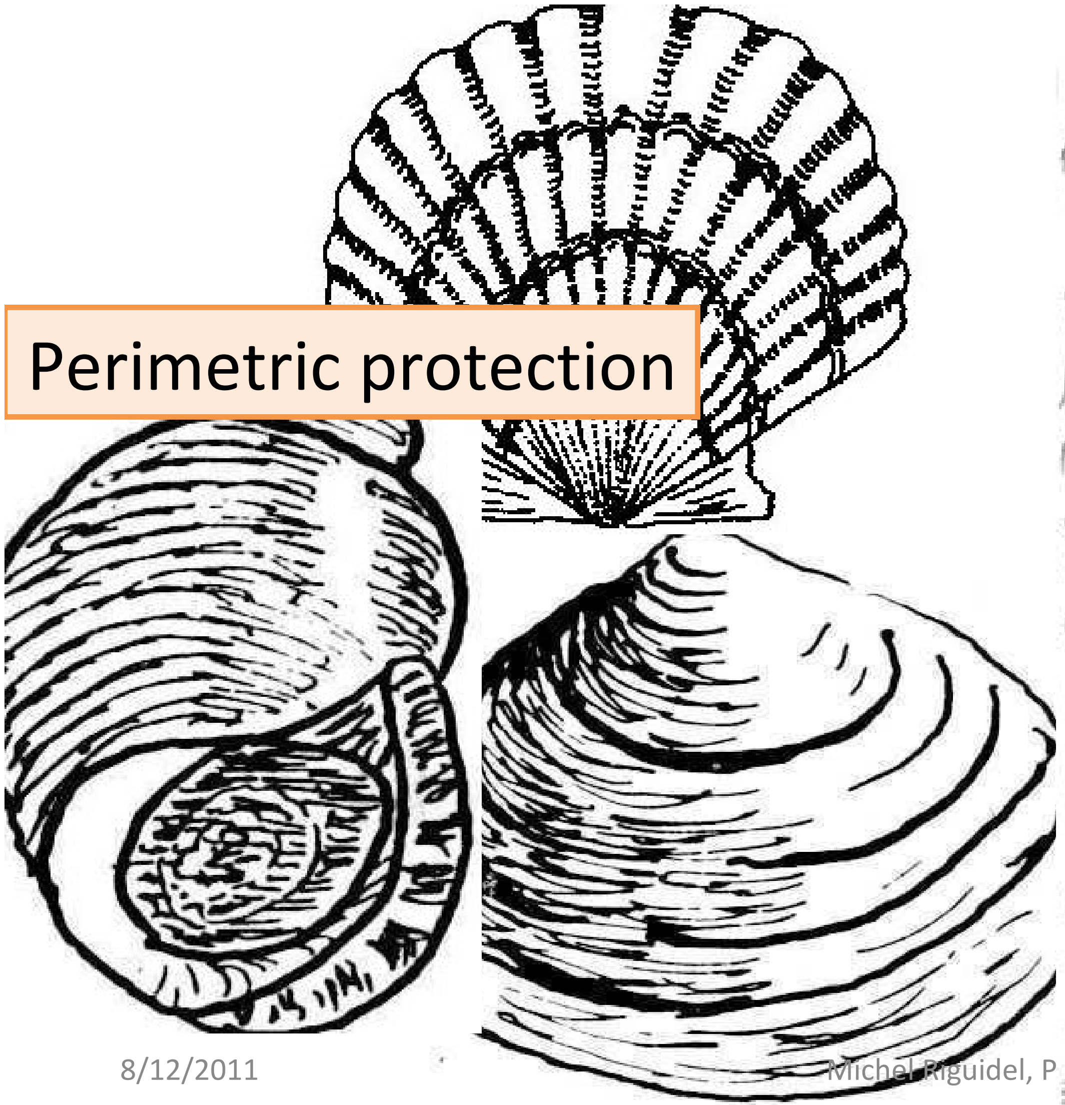
Security : strong entanglement between Culture (socio-economy-ethics) & Techniques



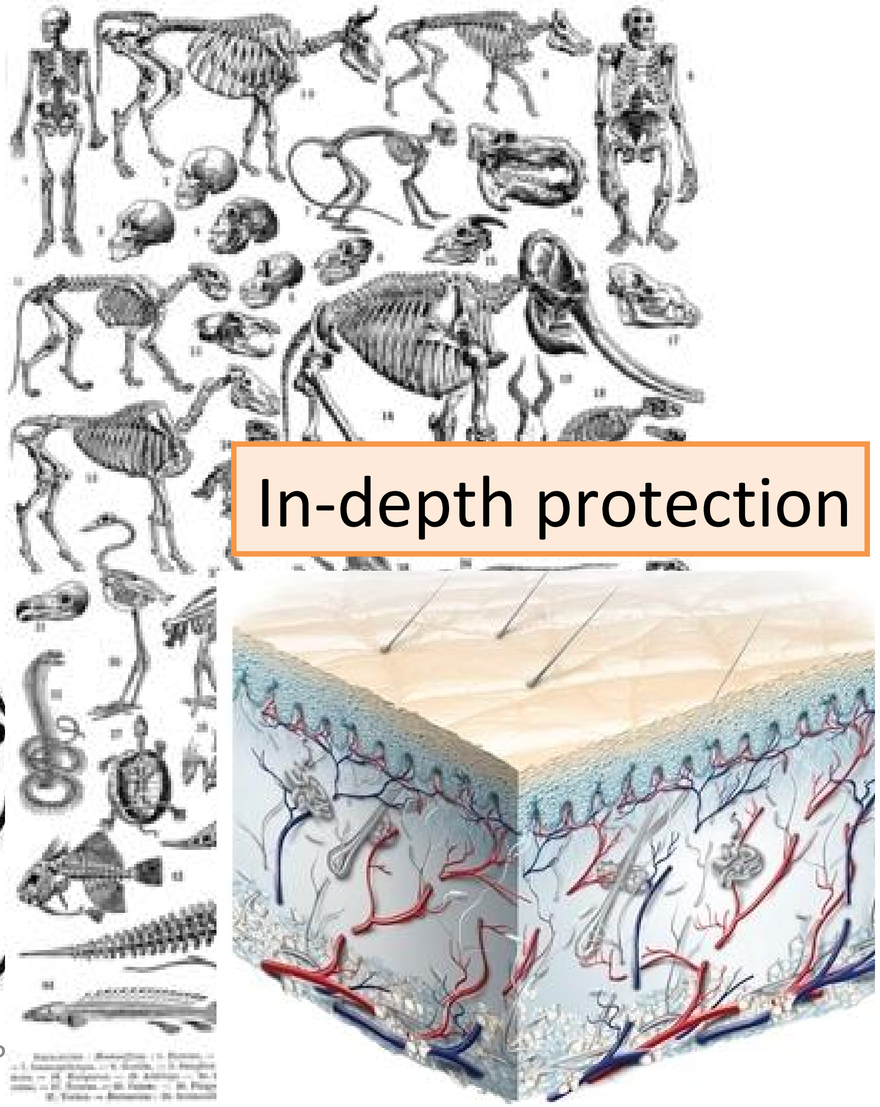
Crustaceans & Vertebrates' s Security

Harsh environment + Static

Mobility =>
skin + nervous system + backbone

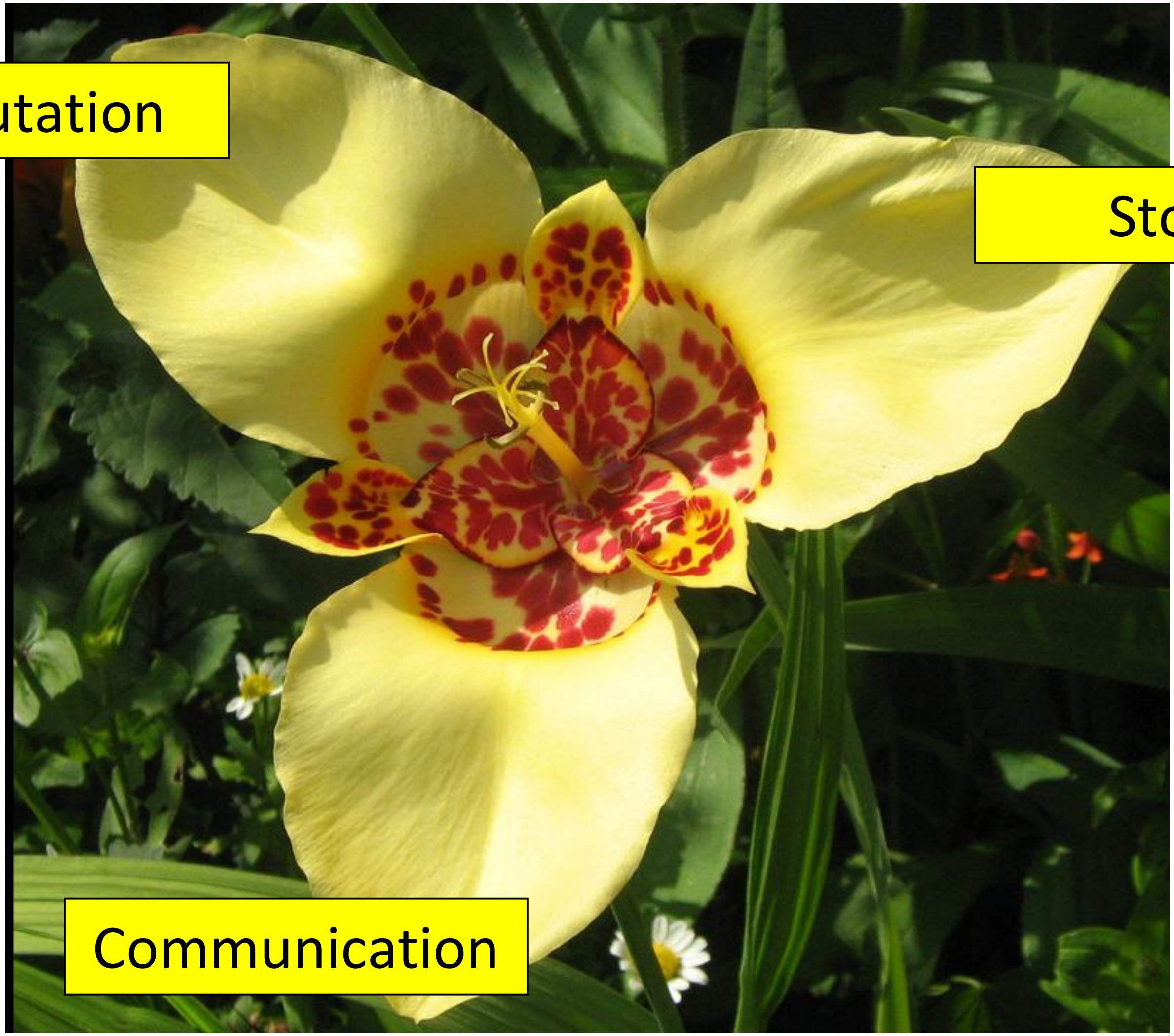


Perimetric protection



In-depth protection

Information & Communication Technology: a flower with 3 petals



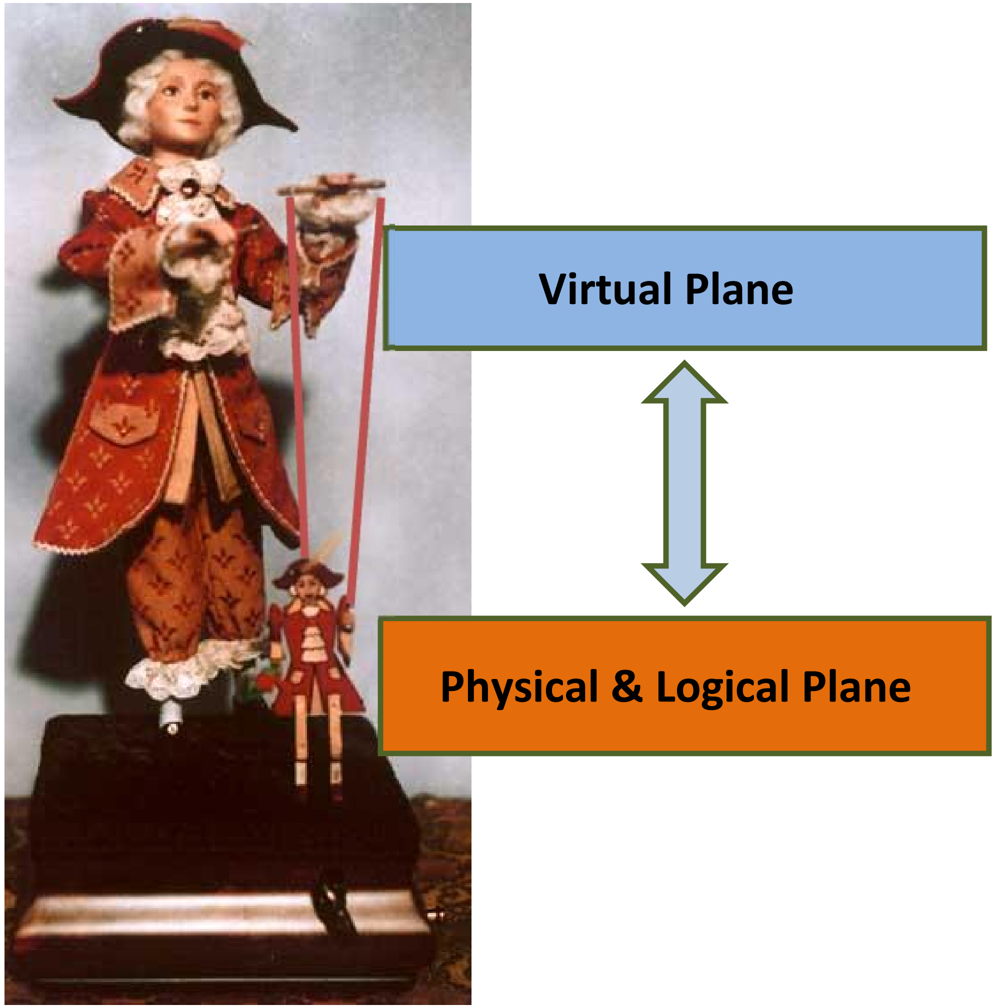
Computation

Storage

Communication

The invisible seams of the virtual world

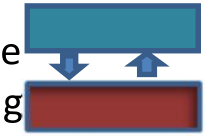
Management of abstractions in protocols and architectures



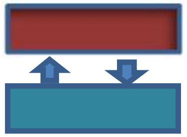
Engineering to override multi-technology complexity

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

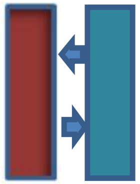
1. Above : **overlays**
   - Overlay Structures / architecture
   - Virtual wires sewed with hashing functions



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

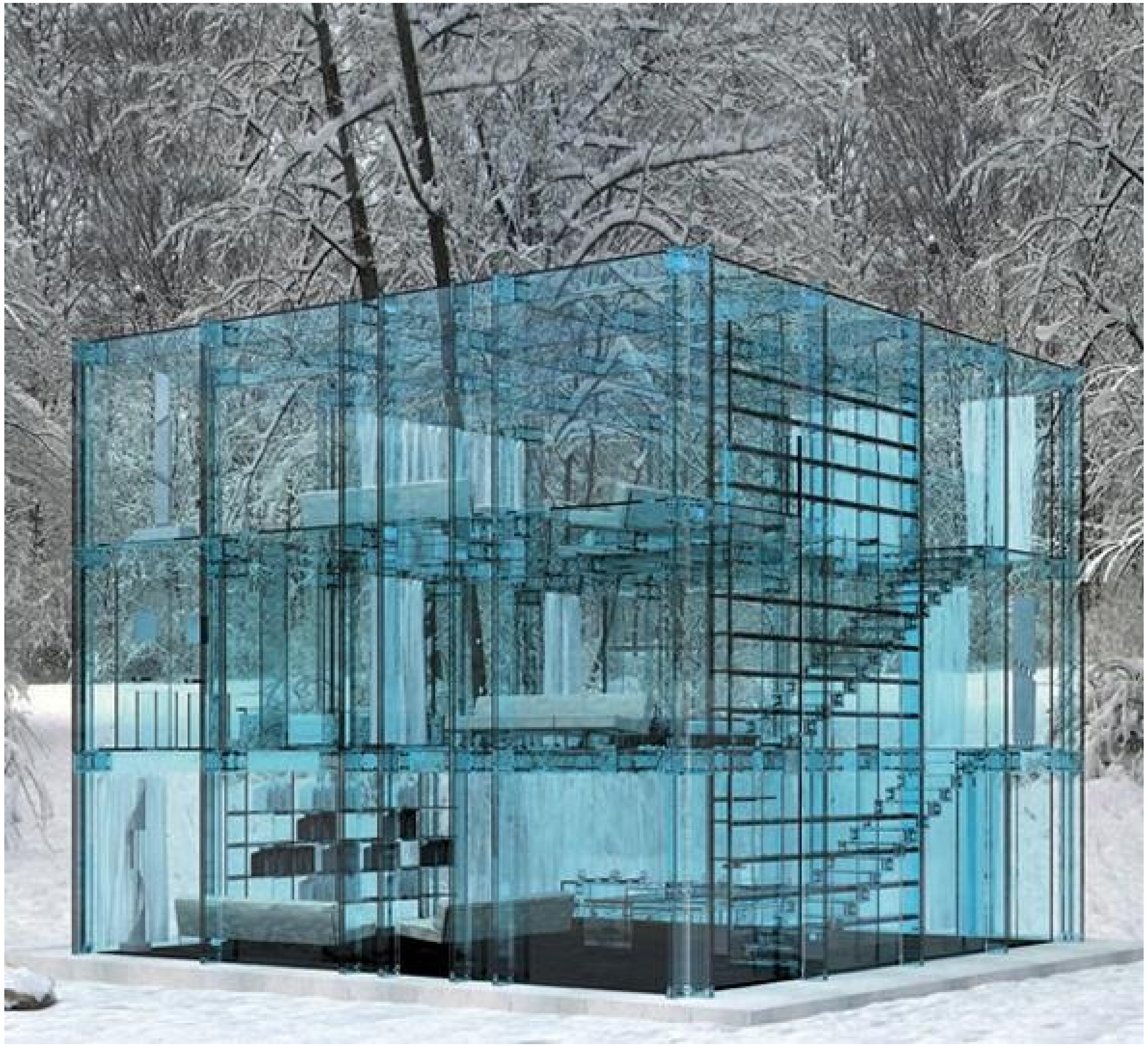


3. On the sides : **crosslayers**
   - Transgression of OSI layers to react faster
   - Triggers, logical wires to short-cut classical paths to perform rapidly

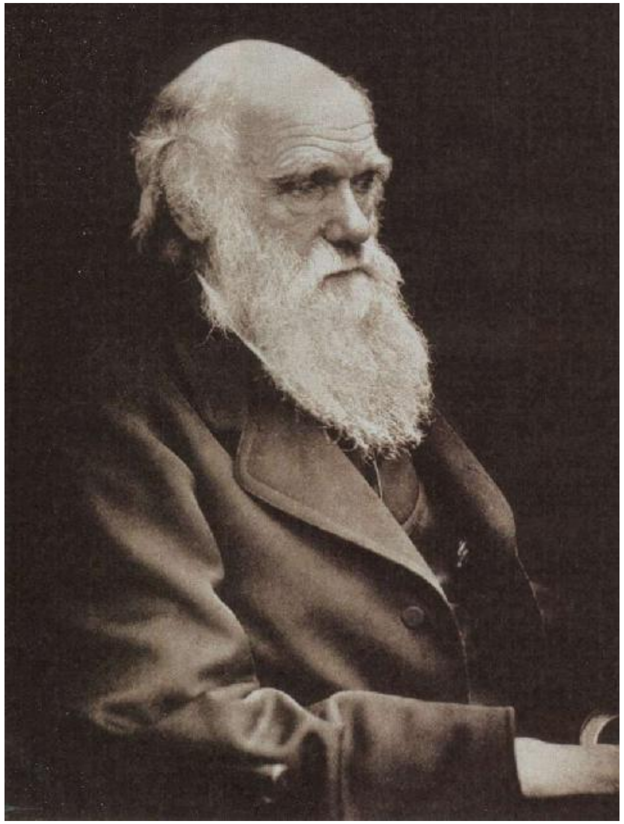


Openness & Proprietary component

Transparency & Trust



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

Evolution of computer languages:

complexification of abstract typing

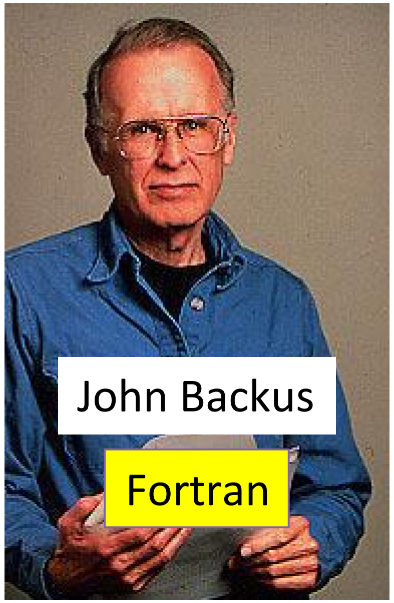
1955 1958 1965 1986 1992

Floatings, Integers:
Independent
in the memory

Lists :
Organization of the
memory in chains

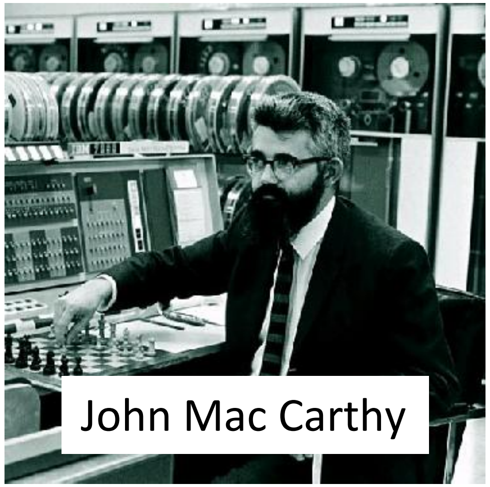
Pointers:
Static,
heterogeneous
Structures

Pointers:
Notions of objects
autonomous
dynamic
Programs



John Backus

Fortran

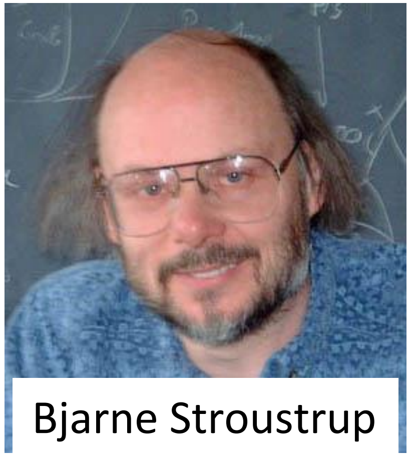


John Mac Carthy

Lisp

Dennis M. Ritchie

C



Bjarne Stroustrup

C++

JAVA

Java

Evolution of Networks: history repeats itself

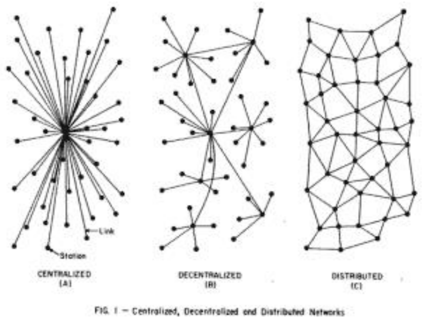
complexification of abstract typing links

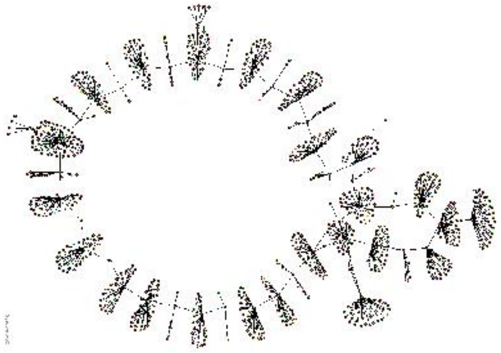
1960-2000

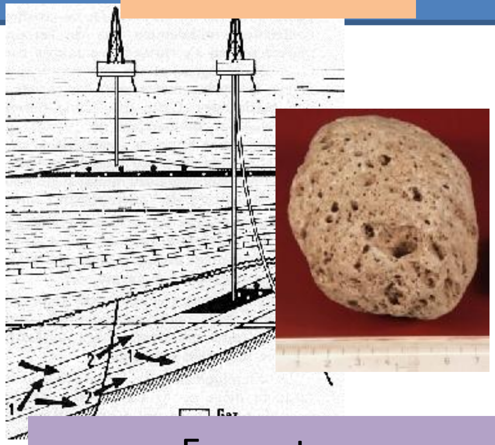
2000-2010

2010-2020

2020-2030


Link
Station
CENTRALIZED (A)
DECENTRALIZED (B)
DISTRIBUTED (C)
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

Security in 2011

Human oriented

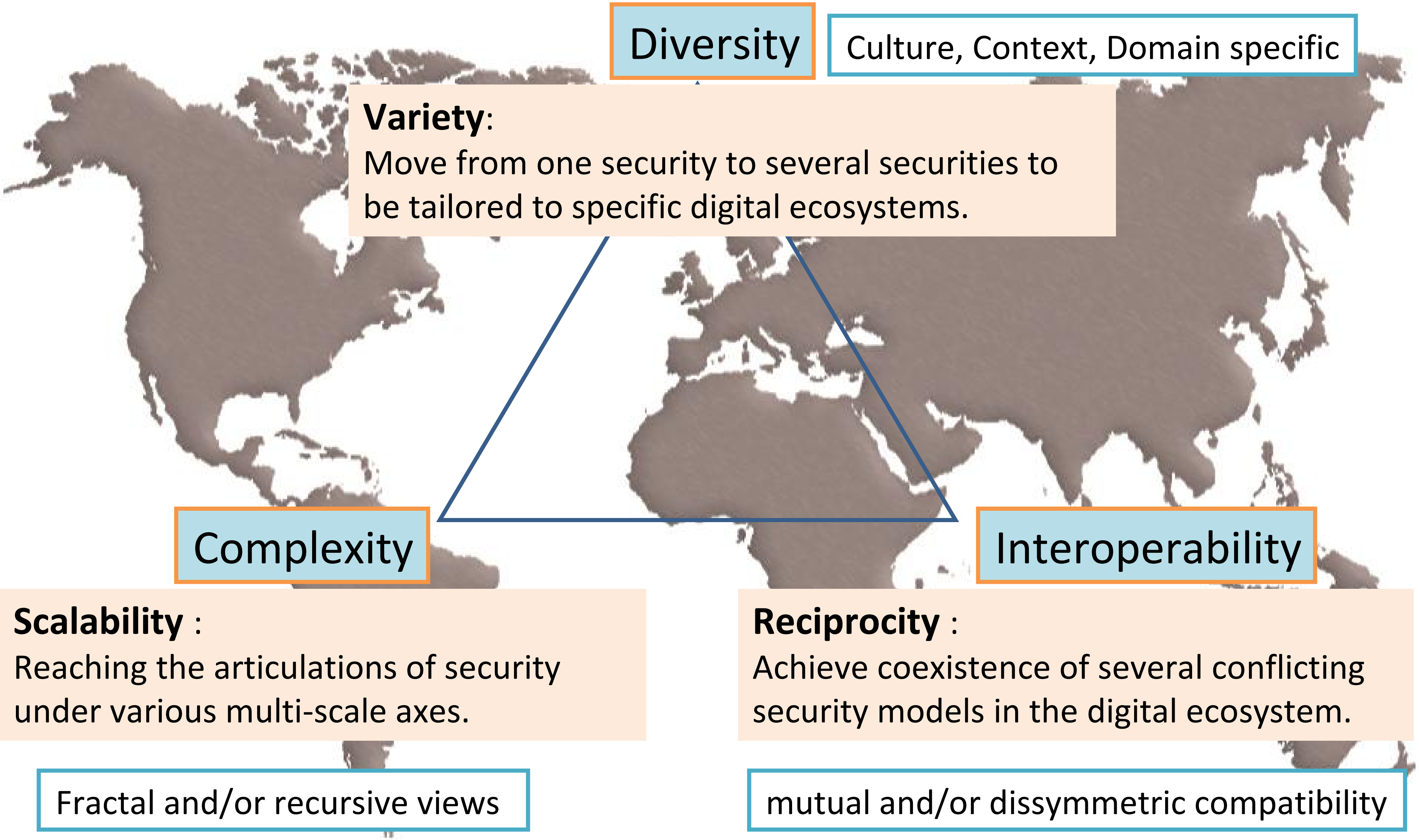
- To individuals, enterprises, institutions
- To struggle against
  - Terrorism, crime, spy, disinformation, hacktivism
- Security models
  - Diversity
    - cultures, contexts, domains: eHeath, e-commerce…
  - Usability

Digital ecosystem

- For personal data, services, infrastructures
- To circumvent failures and vulnerabilities
- Technology and Policy
  - Complexity
  - Fragility
  - Scalability

Not one single providential answer => interoperability of customized solutions

International Cooperation



Diversity

Culture, Context, Domain specific

Variety:
Move from one security to several securities to be tailored to specific digital ecosystems.

Complexity

Scalability :
Reaching the articulations of security under various multi-scale axes.

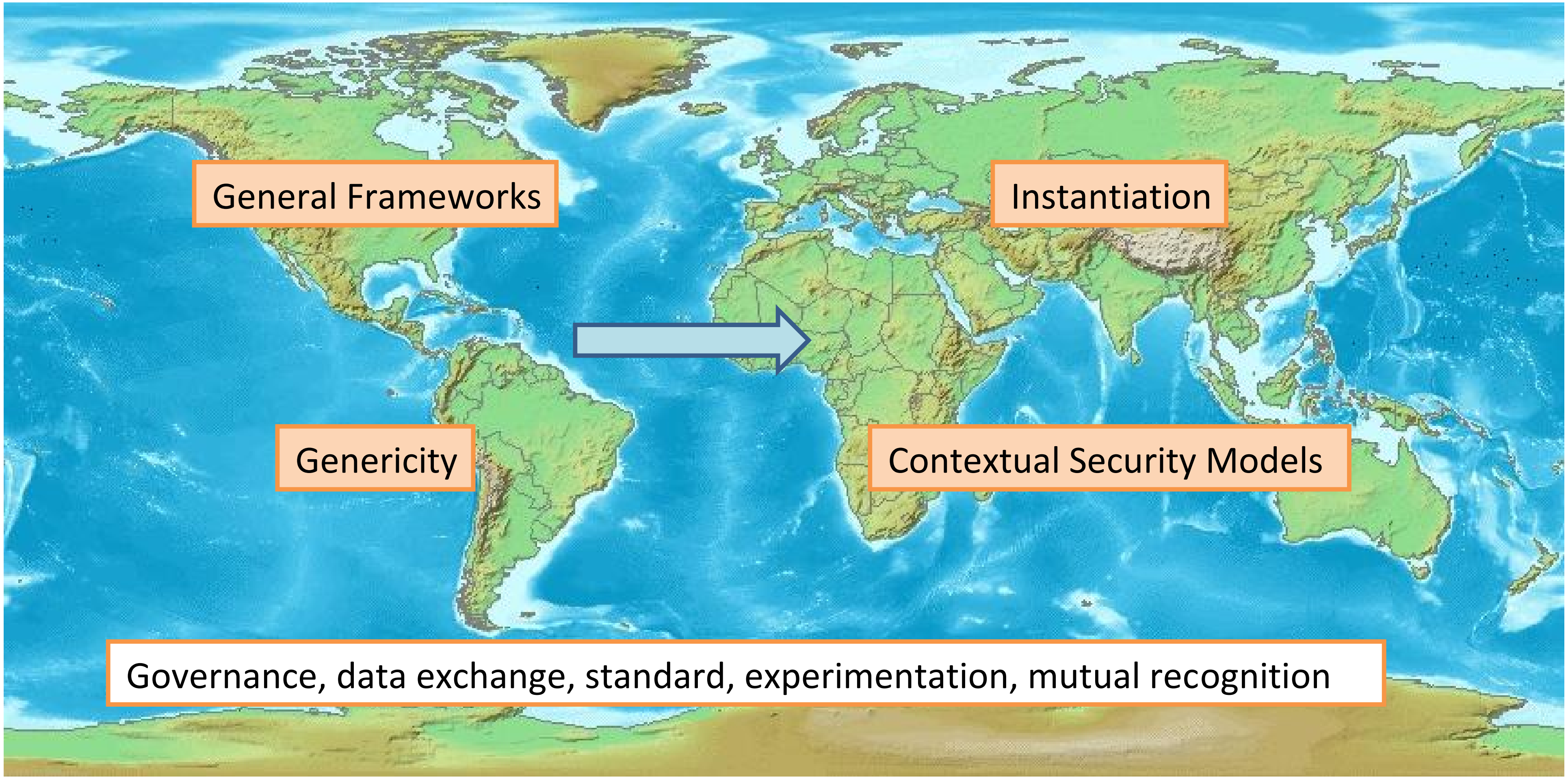
Fractal and/or recursive views

Interoperability

Reciprocity :
Achieve coexistence of several conflicting security models in the digital ecosystem.

mutual and/or dissymmetric compatibility

Go-between from global to local & local to global



General Frameworks

Instantiation

Genericity

Contextual Security Models

Governance, data exchange, standard, experimentation, mutual recognition

Transcontinental ⇔ Regional

International Cooperation to share mutual views

Human oriented security and trust

- Information and behavior
  - Privacy
  - Georeference
  - Dignity, Sovereignty
  - Ownership and authorship
- Identity Framework
  - Authentication, Accountability
  - Anonymity
  - Identity managements
- Trust models
  - Trust management
- Crisis management

Digital ecosystem trustworthiness

- Security of the current and the future internet
  - Openness
  - Transparency and secrecy
- Framework models
  - Generic
  - Flexible
  - Adaptive
  - Cognitive
- Instantiation to local context and needs
- Socio-economic vision

Expansion of a scrambled digital ecosystem

- Increase in the enthalpy of bits of data: informational chaos
  - Increasing volumes of data & informational waste
  - Accelerated movement of not validated (instantaneous) information
  - => The quality of "knowledge" and decision-making decrease
- Increase in cyber-violence
  - Interdependence with the physical and moral violence
  - Easier access to illicit activities: online software, people and data
  - Professionalization of the online black marketplace and parallel e-economy
    - Pointing of individuals (data, behavior) by opaque heuristic
    - Commodification of personal data (espionage), misappropriation
  - => Law of the Jungle ("FarWeb")
- Ideology of a world without constraints
  - Normalization of all values
    - The whole "right now", falsely Free
    - Race to the bottom of knowledge, culture, values
  - Rush of technology
    - The ultra-high speed, infinite bandwidth, infinite storage, unlimited computing resources
- Hypertrophy of anonymity: the mask of a hidden activity
  - Anonymity of individuals, groups, servers, locations, time
  - Virtualization technologies, encryption

Diluted Cybercrime & vertebrate Cyberspace

- Spray attack
  - Explosion of identity theft and slander (e-reputation)
  - Furtive, indirect, dispersed, networked, borderless attacks
    - Affect the fragile subjects, the information systems, fraud, financial crime, data collection
  - Commoditization and overthrow of the cryptography power
    - Cryptography: no more a tool for governments only
  - Dilution of attackers' profiles : hacker, predator, dealer
    - Isolated, sometimes networked individuals, Enterprise, or States, Internationalization
    - Professionalization of the specialized players' chain : identity captures, directory sales, manufacture of software for pirates or counterfeit credit cards, marketing attacks, ransoms…
    - From asymmetric warfare, cyber-war to illegal downloading
- Concentration and shift of the digital power
  - Primacy of the server farms to compute, to store and ultra-broadband highways
  - Shift to the private sector of the digital resource
  - Overvaluation of giant suppliers and hosts
    - (temporary) defeat of the communication function
      - devalued Peer-to-peer (since 2005)
      - Neutrality restrictive to the network, but no constraint to storage nor computing

Scope of International Cooperation

- Theme 1 : **Digital ecosystem trustworthiness**
  - Resilience of the current & the future internet
    - Infrastructure, services, data, etc.
  - Crisis Management
    - At all granularities (time & space) for enterprises and institutions
    - Asymmetric challenge: cyber-haktivism, frauds, cyber-terrorism
  - Security models : interoperability, subsidiarity, multidisciplinary
    - Security embedded within existing context, ambience and culture
- Theme 2 : **Trust & Privacy**
  - Human oriented security
  - Privacy
    - Identity & anonymity frameworks, accountability, e-reputation
  - Trust measurement & management
  - Dignity
    - e-reputation, rumors, non-sollicited information (pub + spams),
- Theme 3 : **Global Framework and international alignment**
  - Interoperability of the subsidiarity models
  - Policy, governance
  - Data exchange for cyber-security
  - Socio-economic area
- Theme 4 : **Engineering and Scientific domains**
  - Cryptography : inco works
  - Software : inco does not work currently, needs some efforts
  - Networks, Information Systems and Computer science : inco is difficult

International Cooperation in Security Research

- Theme 1 : Digital ecosystem security (**Network & Information security**)

  oriented to (What?) the System

  - Protection and Trustworthiness
    - Strengthening **infrastructure resilience** and control **crisis management**
      - Crisis management (CIP), Security and cyber-defence (incl. against the asymmetric challenge)
    - Securing the current and future internet, Network/system security, Securing cloud computing for enterprises, Mobile security, security for mobile connectivity
  - Policy properties: variety, **scalability** and reciprocity
    - Diversity, complexity and interoperability
- Theme 2 : Trust & Privacy (incl. **personal data protection**)

  oriented to (Who?) the Humans, Users

  - **Responsibility** (Identity versus Anonymity)
    - Designing identity and accountability management frameworks, international Privacy friendly authentication and reputation assurance
  - **Measurement** and Negotiation
    - Repositioning trust infrastructure at the same level as security infrastructure
    - Trust management
  - Secrecy, **Dignity**, Sovereignty
    - Designing digital sovereignty and dignity, and new privacy infrastructures, reconsidering privacy spaces, storage function areas
  - **Usability**
    - Human oriented and usable security

International Cooperation in Security Research

- Theme 3 : Global Framework & International alignment
  oriented to principles & governance
  - Properties
    - Interoperability, openness, transparency and secrecy
  - Policy
    - Preparation of policy frameworks to enable global collaboration and interoperability
  - Data
    - Knowledge and International Data exchange architecture for cybersecurity
  - Economy
    - Data policy, governance and socio-economic ecosystems area
- Theme 4 : Methodology, tools and technical challenges

  oriented to (how? when? where?) the tools
  - Expertise sharing
    - Science, technology & engineering
  - Methods
    - Support metrics and standardization issues.
  - Software
    - Software security: Enable the engineering of secure and trustworthy software and systems.
  - Data
    - Cryptology (digital signature, etc.)
  - Upstream
    - Initiate green security