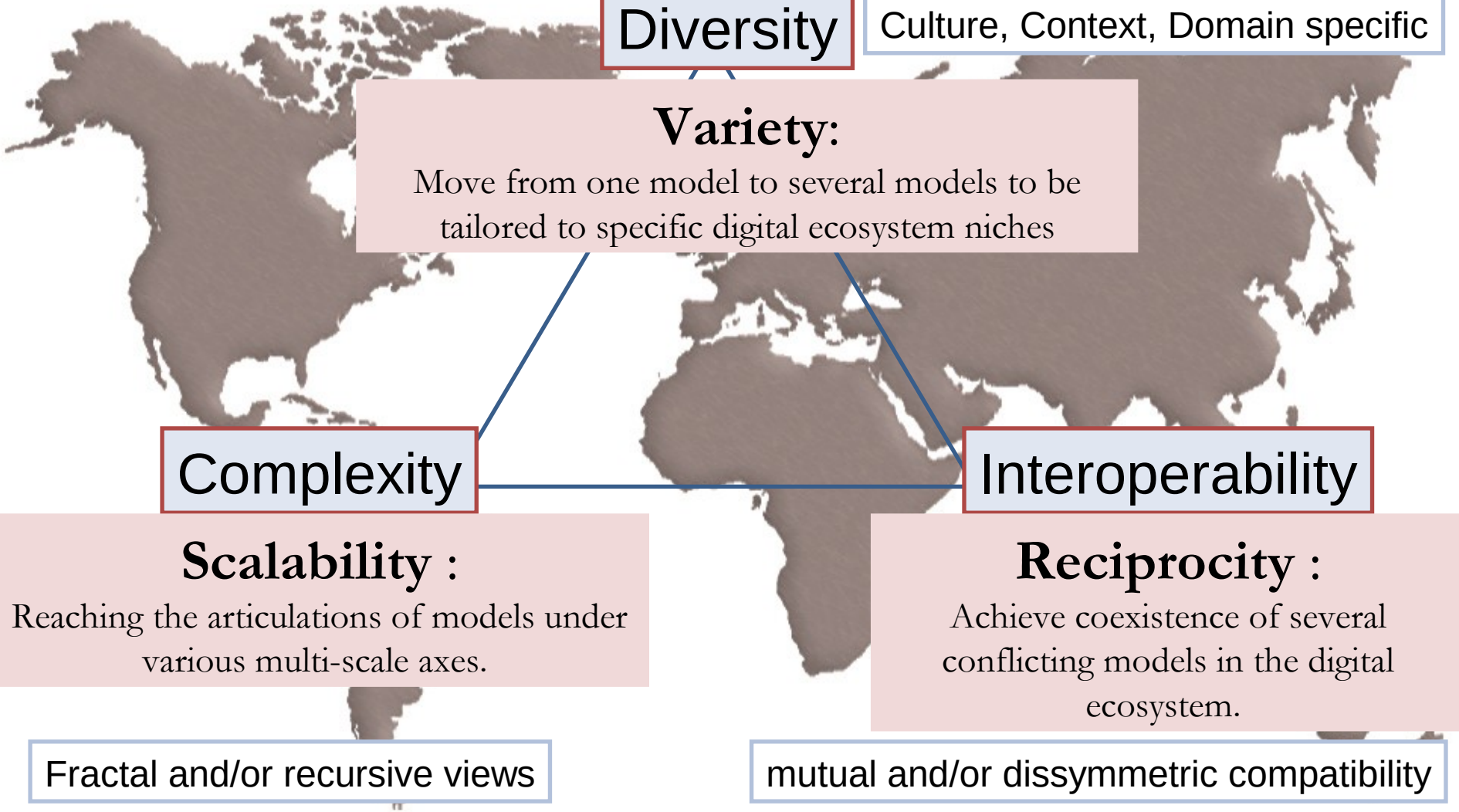

BUILDING International Cooperation
for Trustworthy ICT

Michel Riguidel, Institut Mines-Telecom, ENST

# Global vision of architecture

against a pre-written, idyllic vision of future networks => models, counter-models, alter-models



**Diversity** — Culture, Context, Domain specific

**Variety:**
Move from one model to several models to be tailored to specific digital ecosystem niches

**Complexity**

**Interoperability**

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

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

Fractal and/or recursive views

mutual and/or dissymmetric compatibility

**Transcontinental** ⟷ **Regional**

# Research topics identified at the BIC EU – South Africa cooperation workshop (extract)

Trust Management for techno-socio-business ecosystems for emerging economies

Need for collaborative on-line & real-time trading environment

- large enterprises such as suppliers and financial institutions transact with Very Small Enterprises
- lack of ICT infrastructure, VSEs dependent on mobile communications

International Cyber security research

Could Africa become the home of the world's largest botnet / cyber security pandemic?

Financial Infrastructure Protection

Need for providing secure eBanking in the face of a barrage of sophisticated, creative, efficient and persistent phishing attacks

Enhanced cooperation with Law Enforcement approaches to deal with cybercrime

To deal with a variety of cyber crimes with significant criminal intent (ransomware)

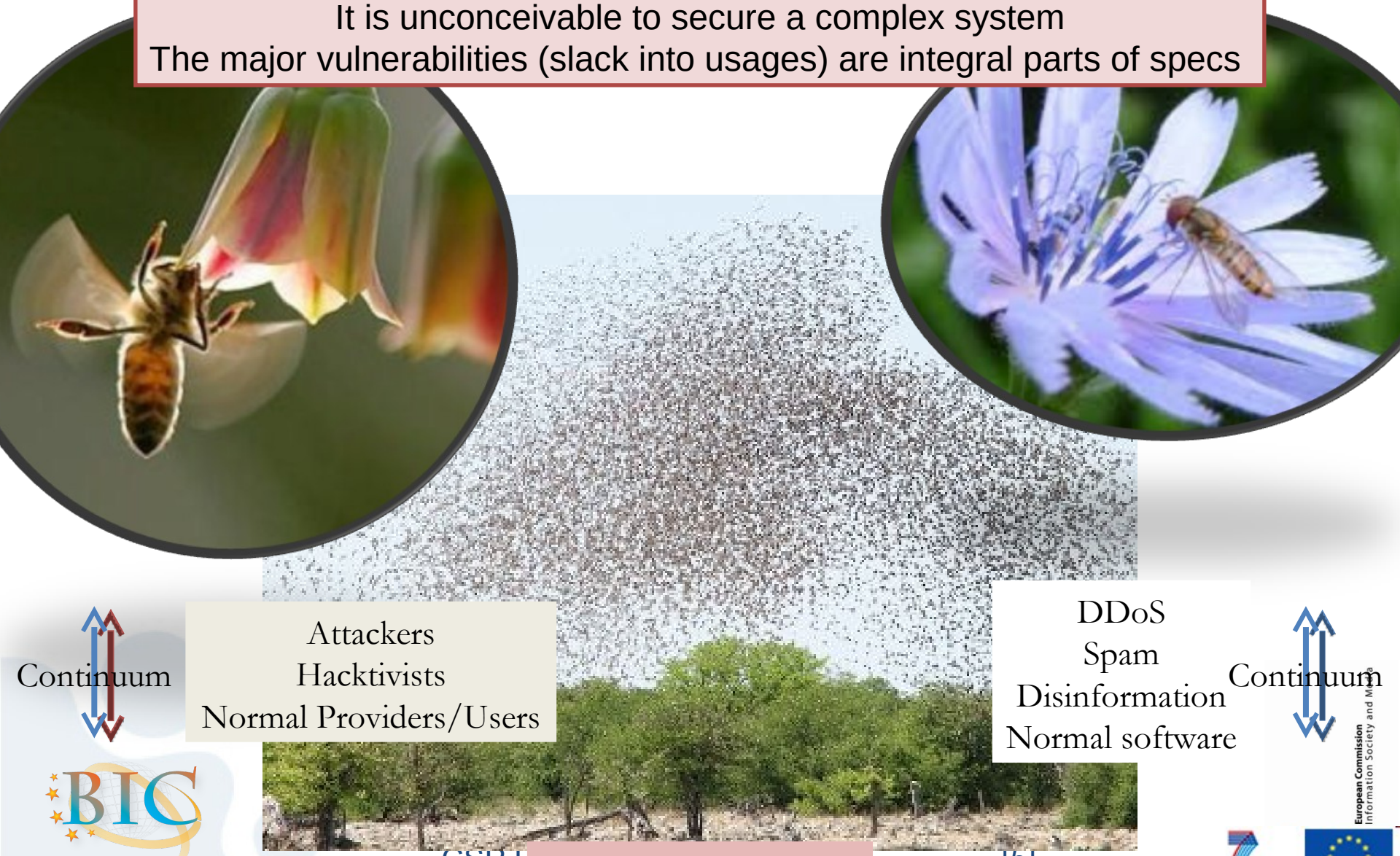
Coordinated approach to cross domain multi-disciplinary research in the "Future Internet"

# Research topics identified at the BIC EU –India cooperation workshop (extract)

| Indian approach to trust and security | EU approach to trust and security |
|---|---|
| The Indian approach to trust and security in ICT is functional, rather than conceptual. The main concentration is on the 'plumbing' or 'nuts and bolts'. | The EU approach is to examine the in depth concepts and horizontal aspects for trust, privacy and security e.g. empowering the users to gain control over trust, security and privacy issues. |
| Security, privacy and trust in are not sufficiently appreciated from the perspective of citizens' rights, benefits for business and society's entitlements | Enabling technologies for security and trustworthiness of ICT that guarantees rights, addresses security, trust and protect the privacy and personal data of the users and enables participative governance |
| How to guarantee protection of the citizen's rights, security, privacy in the context of the mammoth Unique Identification (UID) project | Concept of 'Privacy by Design' embedding privacy proactively into technology |
| The level of the Indian cryptography research is very high (e.g. the famous "Primes is in P" result showing that there is an elegant deterministic polynomial time algorithm for primality testing of integers); theoretical and practical aspects of cryptography, number theory, computational complexity. | Balancing between the right to anonymity (privacy) and the societal imperative of making personal data available |
| The level of the Indian mathematics research is recognized in applied mathematics: data mining and machine learning, formal approaches to security. | Addressing the international data exchange and sharing of information and intelligence on cyber-attacks for a free flow of the information in a secure and reliable manner. |
| Security of Mobile telecom; building trust for transactions. | Increasing the leadership of the European cryptography skill which is recognized at the international level. |
| Cryptographic protocols for micro-payment | |

# Security of the whole system & all the components

It is unconceivable to secure a complex system
The major vulnerabilities (slack into usages) are integral parts of specs



Continuum

Attackers
Hacktivists
Normal Providers/Users

DDoS
Spam
Disinformation
Normal software

Continuum

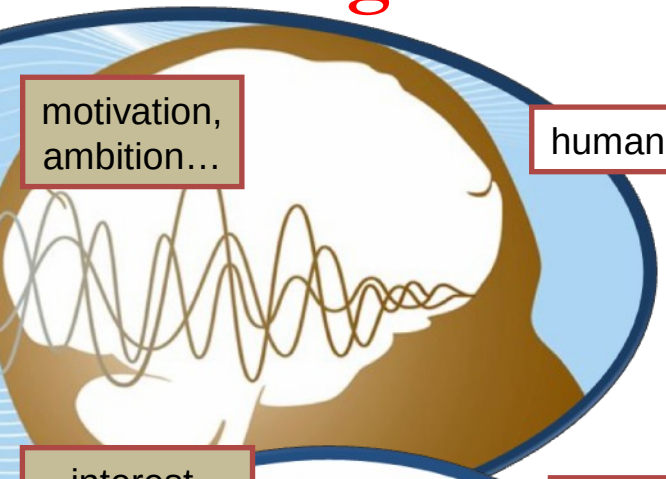
Digital ecosystem

[5]

BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

# Digital Activity => cyber-social system



motivation, ambition…

human

interest, competition

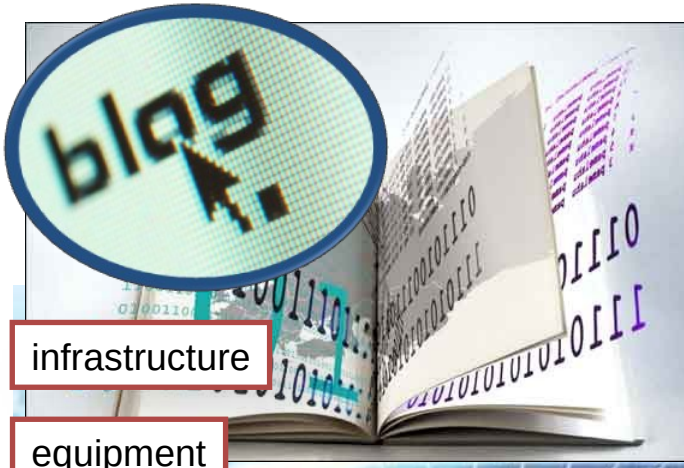
group

balance of power, ideology…

government

**Digital world today: strong entanglement between Human & Machine**


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




infrastructure

equipment

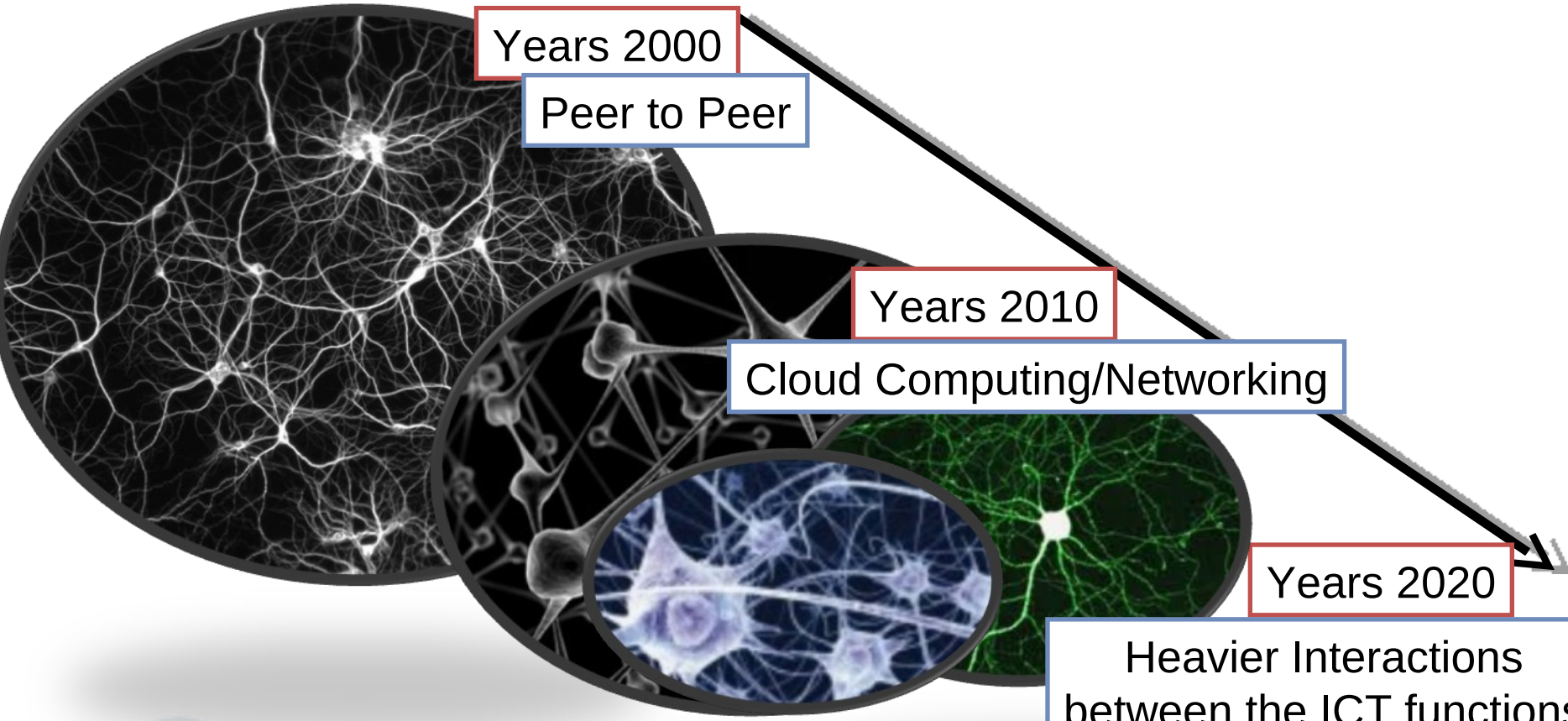
software

service

information

data

# The network is thickening and lumpy



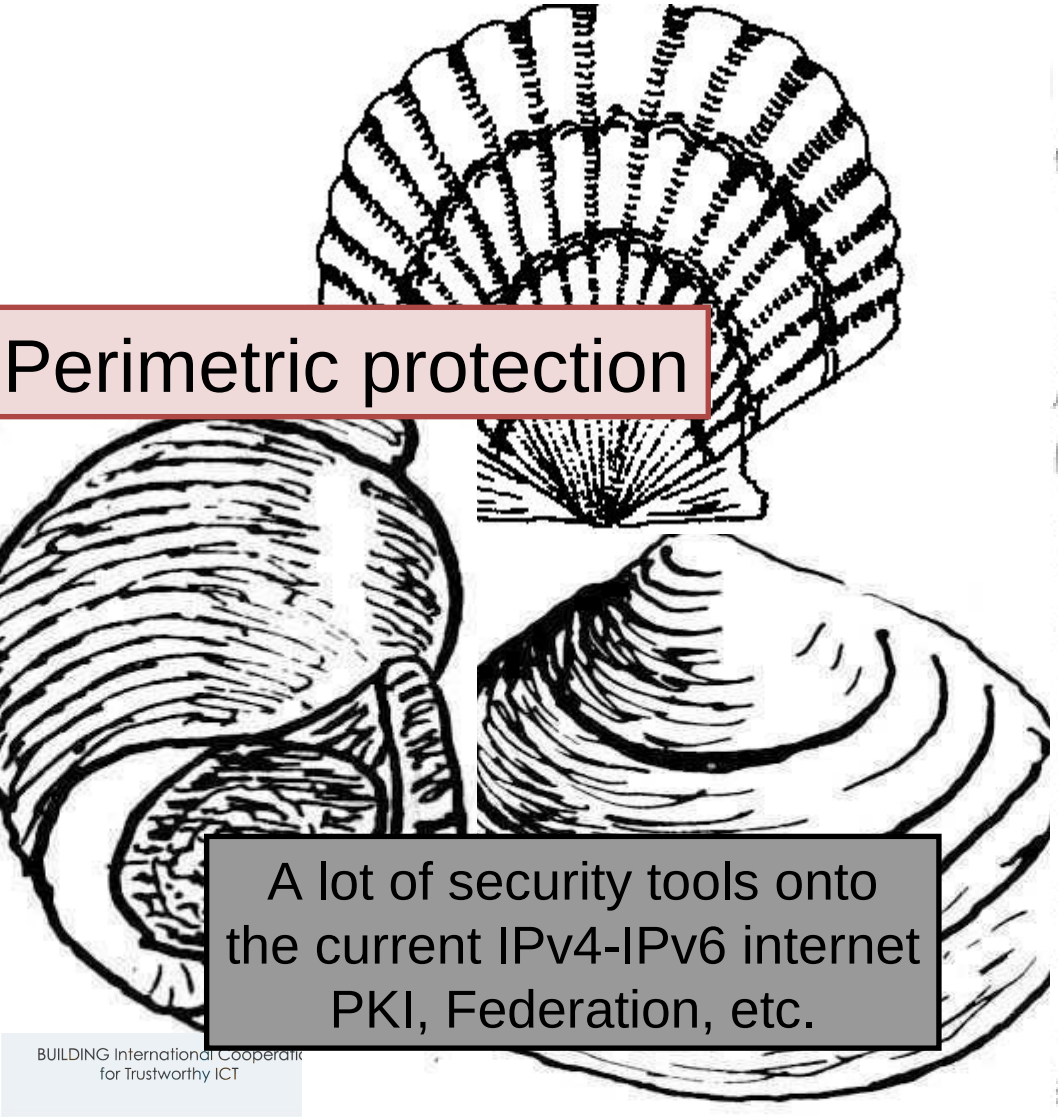

Strong interrelations between computation, storage and communication

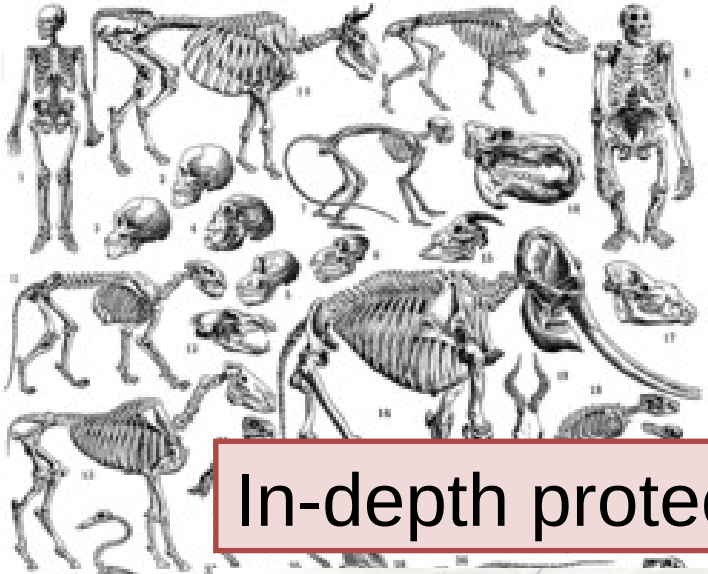
Burst clouds, massive structured distributed applications

# Crustaceans & Vertebrates' s Architecture

**Static & Harsh environment**

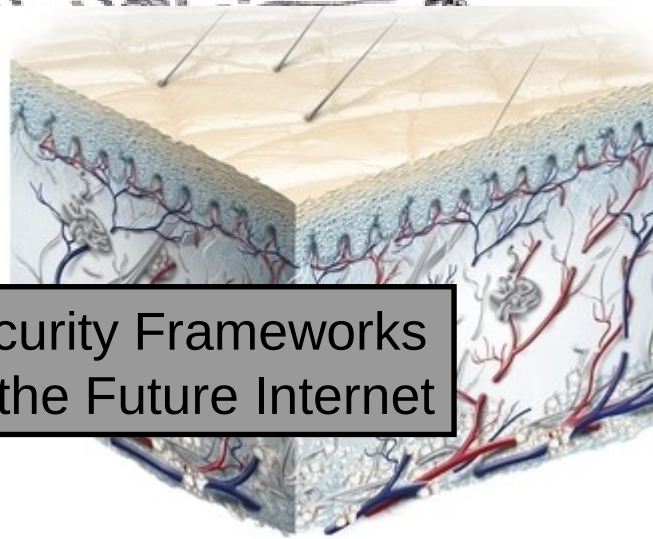
**Mobility =>**
**skin + nervous system + backbone**





Perimetric protection

In-depth protection

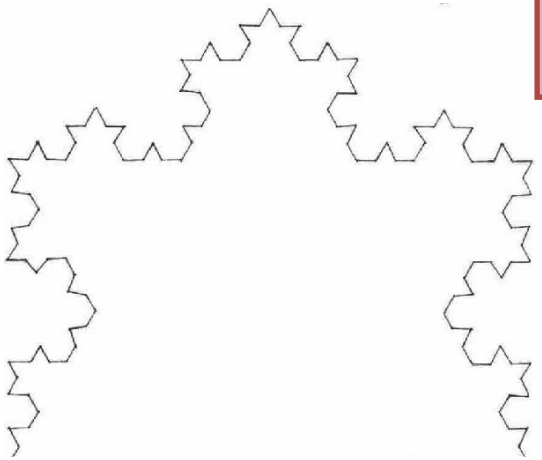


A lot of security tools onto the current IPv4-IPv6 internet PKI, Federation, etc.

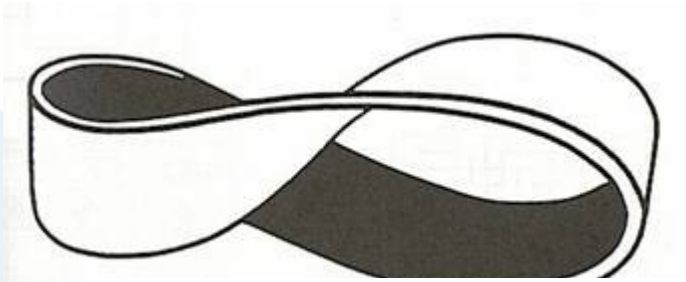
Security Frameworks for the Future Internet

# Which Complexity in security?

**Complexity is in shape, size => entropy**



Risk, Information theory, Cryptology
Shannon complexity? Kolmogorov complexity?
=> static meaningless information



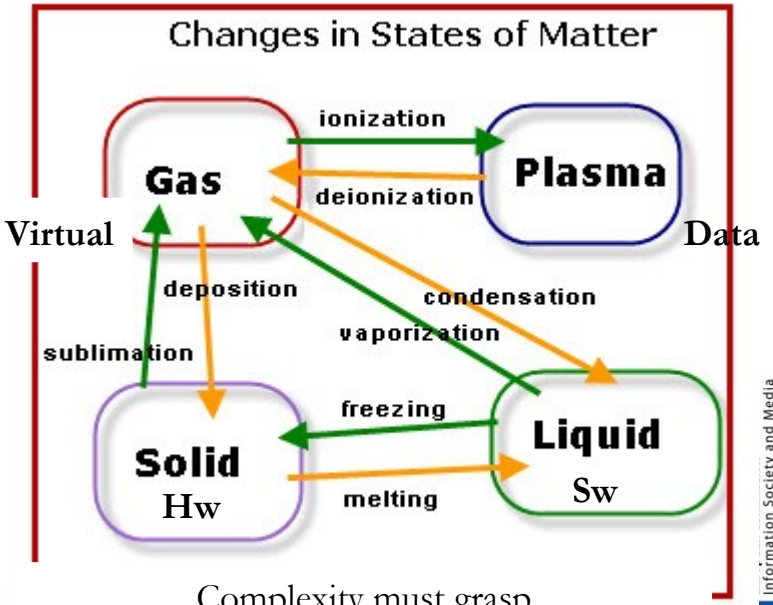
Scalability & Granularity : Threats are into macroscopic data displacements and into microscopic software variations

Gap
between both complexities

**Complexity is in motion, momentum, enthalpy**

$\Delta H_x^\theta$

Δ = change in
H = heat energy
θ = standard conditions
x = type of change



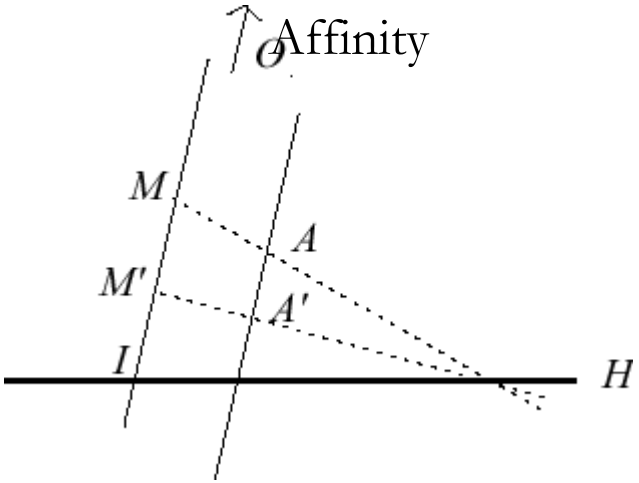

Complexity must grasp
{mobility + intentional message or program}

# Privacy

| Me | My Friends | Other |
|---|---|---|


End-users

Operators,
Service, Content,
Access, Identity …
Providers

# Privacy = {Security + Security Assurance + Trust}




Privacy # confidentiality

Privacy = { personal related data + digital behavior }

=> measures : technology + policy + procedure + organization

# Digital Identity (=> Authentication) vs Anonymity levels (=> Traceability)

Google+
Identity card
ID 117596712775912423303

Name : Stegancrypto
Nickname: Olga-Algo

Gender: Female
Location: Switzerland

Joined: 2012-03-28


**scalability**

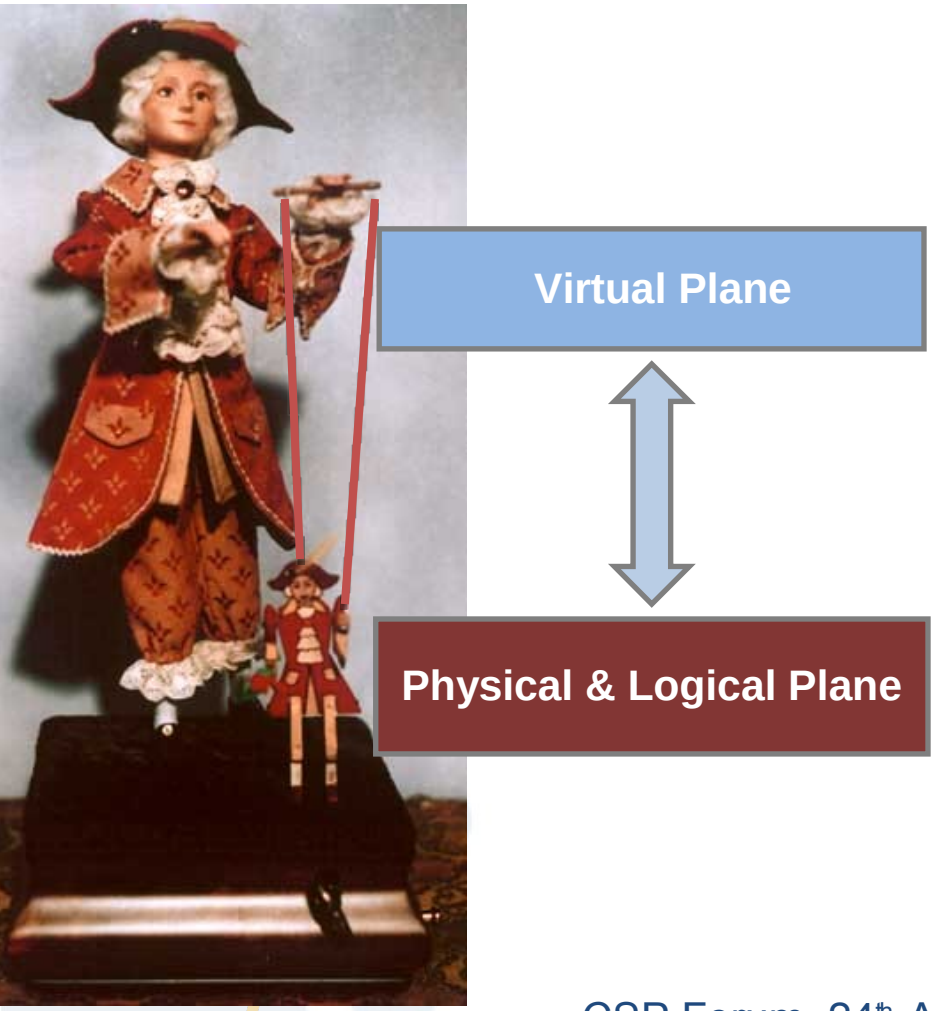
Security hardness ~ $O^{1.5}$

| $10$ | $10^3$ | $10^6$ | $10^7$ | $10^9$ | $10^{15}$ | $10^{21}$ |
|---|---|---|---|---|---|---|
| Personal Objects | Enterprise Prison | Estonia | Belgium Switzerland | China India | RFId | IP Packets |
| Kept in view leashed | Badge | Identity cards | | | Hash function | Host address |
| Direct | Specific Multimodal Biometry | | Ich bin ein Französisch Professor für Informatik | 我是一法国人名教师 wô shi fa-guo-ren lao-shi | | |

**interoperability**

# The invisible seams of the virtual world

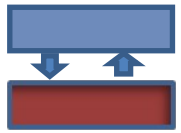
## Management of abstractions in protocols and architectures



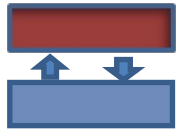

## Engineering to override multi-technology complexity

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

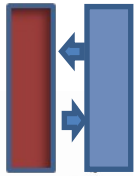
1. Above : **overlays**
   - Overlay Structures / architecture
   - Virtual wires sewed with hashing functions



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



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



# EU priorities driven challenges of trust and security research

- Advancing digital security culture worldwide
  - Increase knowledge and share best practices
    - Strengthen information exchange on incidents processing and threats
    - Cooperate in R & D on models of security and trust and of interfaces
    - Anticipate threats and crisis management: preparing international exercises
      - resistance test against attacks, players' ability to collaborate
    - Facilitating partnerships with multi-parties and multidisciplinary issues
      - Public/private sectors, governmental, institutional, economic
- Define a roadmap for a collective research
  - Technology
    - Advance the vision of threats and vulnerabilities, preparation of technical measures
      - early warning, crisis management, real-time analysis of global threats
    - Reduce geographic interdependencies
      - an attack on a system point can have impact on neighboring systems.
  - Policy
    - Awareness of the risks and sharing of information and experience
    - Taking responsibility for maintaining the security of the digital ecosystem
- Promote the benefits of Europe
  - Encourage other continents to share European values
  - Free flow of ideas, access to knowledge, protection of privacy

# EU priority driven global challenges of trust and security research

## Human Oriented Trust and Security

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

## Digital Ecosystem Trustworthiness

- Trust and security of the current and the Future Internet
  - Openness
  - Transparency and secrecy
- Framework models
  - Generic
  - Flexible
  - Adaptive
  - Cognitive
- Instantiation to local context and needs

| Country | Program Level | Research level | Priority research themes for INCO |
|---|---|---|---|
| **Brazil** | CNPq (National Research council), FUNTEL, State Research foundations<br>ITI (Instituto Nacional de Tecnologia da Informação) | Universidad de Brasilia,<br>Univ. of Sao Paulo,<br>CPqD<br>Serasa Experian, Others TBD | Future Internet, Wireless Technologies: Security, Privacy, Trust over ad-hoc networks, Quantum crypto, ID management. |
| **South Africa** | SA Dept. of Science and Technology SA Technological Innovation Agency | Council for Scientific and Industrial Research (CSIR) – The Meraka Institute;<br>Others | Wireless Technologies: Security<br>E-infrastructures, Botnets, Financial Infrastructures |
| **India** | Dept. of Information Technology, ERNET, EuroSpirit India Support action (FP7) | India Institutes of Technology (IITs), India Institute of Science (IISc), Universities - Hyderabad, Pune, Anna amongst others). | Broadband and WSN Security, Data Center Security, Data Privacy, ID card, ID management; Usable Security on low-cost, low-energy devices |
| **USA** | National Science Foundation<br>Department of Homeland Security | Rutgers University, University of California, San Diego, University of California, Davis, University of Illinois , Others | CyberSecurity/Privacy: Technology and Usage Issues Trustworthy International information exchange including data transfer and sharing, Security models for the Future Internet. |
| **Canada** | National Science & Eng. Res. Council | Univ. of New Brunswick, Ecole Polytechnique Montreal | Industry driven projects on trust, security and privacy. |
| **Korea** | Ministry of Knowledge Economy, KEIT | SoonChunHyang University, Seoul National Univ. Others | Internationalisation of data (identity management, privacy, end to end trust metrics, …); Countermeasures against Massive DDoS; Security of Cloud computing e.g. Security of Smart Grid; Security compliance management and information security assurance; Security for VoIP and Mobile communications; Future Internet. |
| **Japan** | Japan Science and Technology Agency, CREST programme | University of Tokyo, Tokyo Inst. of Tech, JAIST, Others | Dependability, Security, Privacy and Trust of embedded systems |
| **Australia** | Australian Research Council (ARC) | NICTA, CSIRO, Macquarie University, Univ. of Sydney, IIS Partners, many others | Communications Security, Trust and Privacy in the Future Internet; Formal approaches for trust and security.; Sensor networks. |

# Strategic* recommendations for International Cooperation

- International community collaboration recommendations:
  - SR1: **International Alignment**
    preparation of policy frameworks to enable global technical collaboration and interoperability
  - SR2: **variety** → diversity
  - SR3: **scalability** → complexity
  - SR4: **reciprocity** → interoperability
  - SR5: **secrecy** → the issues of digital sovereignty and dignity
  - SR6: **negotiation** → the theme of security and trust
  - SR7: **security** expertise → technological challenges of security
  - SR8: **protection** → cyber-defense

**Strategic refers to underlying and enabling actions to facilitate effective outcomes of INCO*

# Tactical* recommendations for International Cooperation

- The international ICT trust and security community should collaborate together on research to support the following tactical recommendations:
  - TR1: strengthening infrastructure resilience and control crisis management.
  - TR2: securing the current and future Internet related to diversity, complexity and interoperability.
  - TR3: securing cloud computing for enterprises.
  - TR4: designing identity and accountability management frameworks.
  - TR5: a new privacy infrastructure, reconsidering privacy spaces, storage function areas.
  - TR6: repositioning trust infrastructure at the same level as security infrastructure.
  - TR7: metrics and standardization issues.
  - TR8: to initiate green ICT security.
  - TR9: to support cooperation in cyber-defense against the asymmetric challenge
  - TR10: to enable the engineering of secure and trustworthy software and systems

***Tactical refers to specific research recommendations to develop building blocks and their relationships that will enable a globally trustworthy ICT ecosystem.**

# Requirements for the Future Internet 2015

- Support for new modes of communication
  - different needs => **different services, various securities**, QoS, by application / flow / packet / ontology
- Reconciliation of access and core network into a unified architecture
  - access links (dynamic, with mobility) & core network (static, high data rate)
  - mobility support at the network periphery
    - Geo-localization (Galileo, Beidu-2) and pervasiveness (sensor networks)
- Management : several views
  - **multi-polar management**; **self-adaptation**
- Security and dependability (robustness)
  - Intrinsic security of the infrastructure (beyond security of application / flow)
  - applications / critical needs such as emergency, defense, energy
- Green Networking
  - requires control more global than local
- Politico-socio-economical context
  - Ideological considerations and geostrategic context are crucial
  - economy (competition and innovation), sociology (balance security & privacy)
  - risk: **balkanization** of the universal digital ecosystem into **digital continental plates**