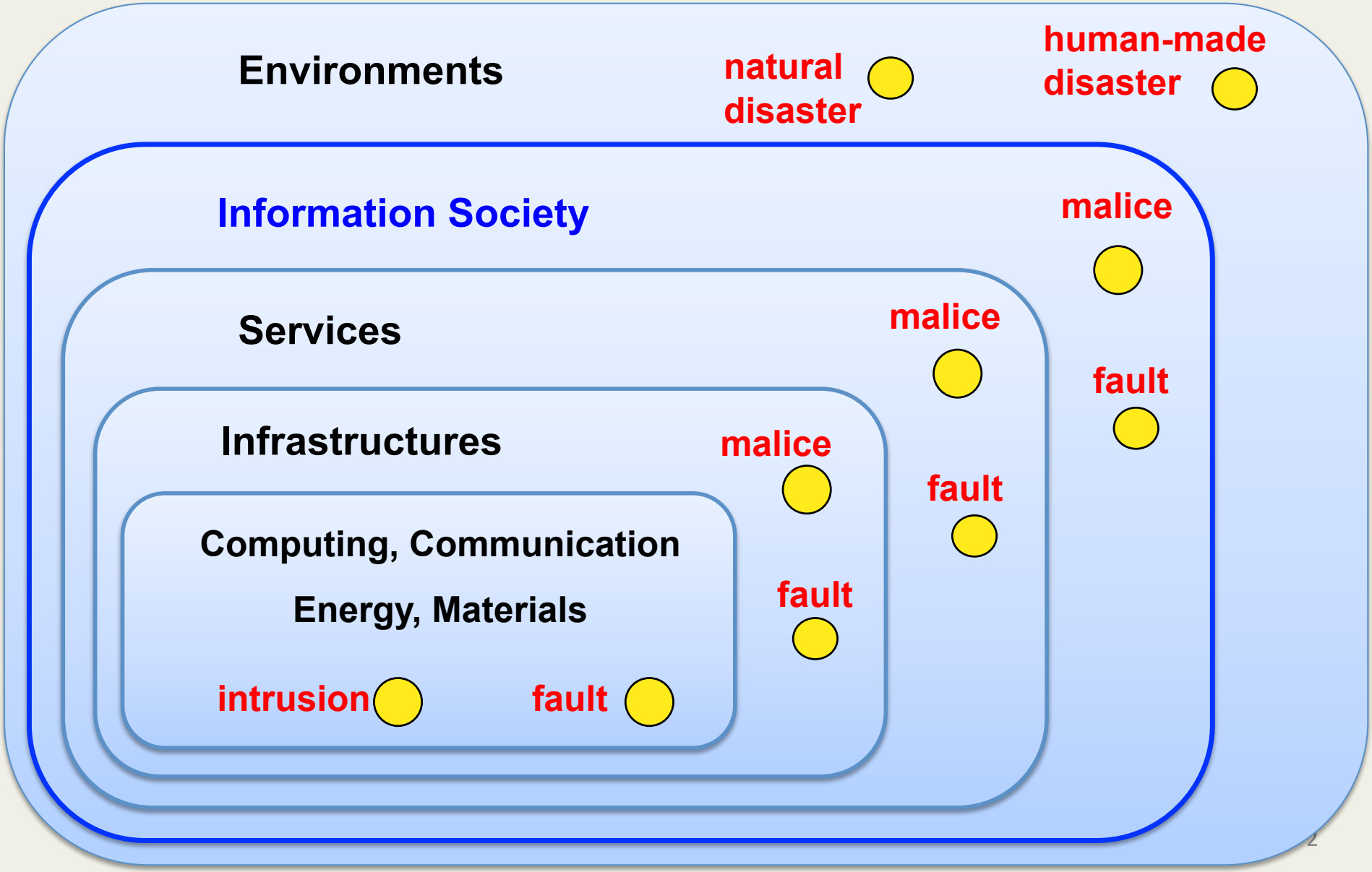
61st Meeting of the IFIP 10.4 Working Group
on Dependable Computing and Fault Tolerance
Martinique, France, January 26-30, 2012

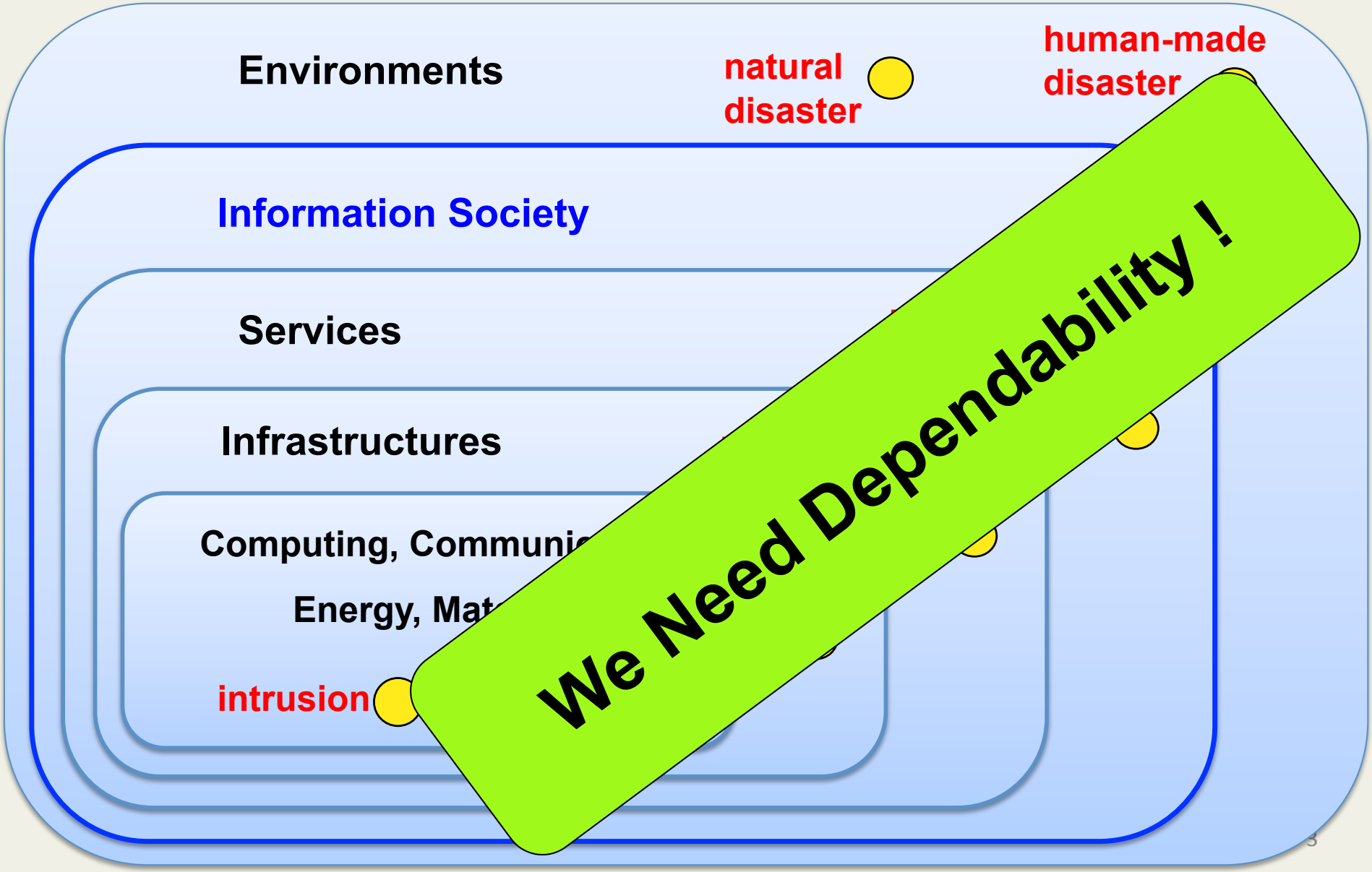
Toward Dependability for Information Society

Takashi Nanya
Canon Inc.

Information Society



Information Society



March 11, 2011: Summary

- 9.0-maginitude earthquake struck the east coast of Japan
- Accompanying “tsunami” waves with a maximum height of 23 meters swept off lives of more than 20K people in the coast
- Fukushima nuclear power station lost external power supplies and all in-house AC power supplies to lose cooling capabilities for reactors and spent-fuel pools, and a subsequent chain of mishaps led to meltdowns in three active reactors, releasing a large amount of radioactive materials and producing 116K refugees
- We still don’t know what’s actually happening inside the reactors
  - A week ago, on Jan.19, TEPCO peeked inside reactor 2 for the first time since March 11 by inserting an industrial endoscope into the containment vessel, but failed to detect any coolant water

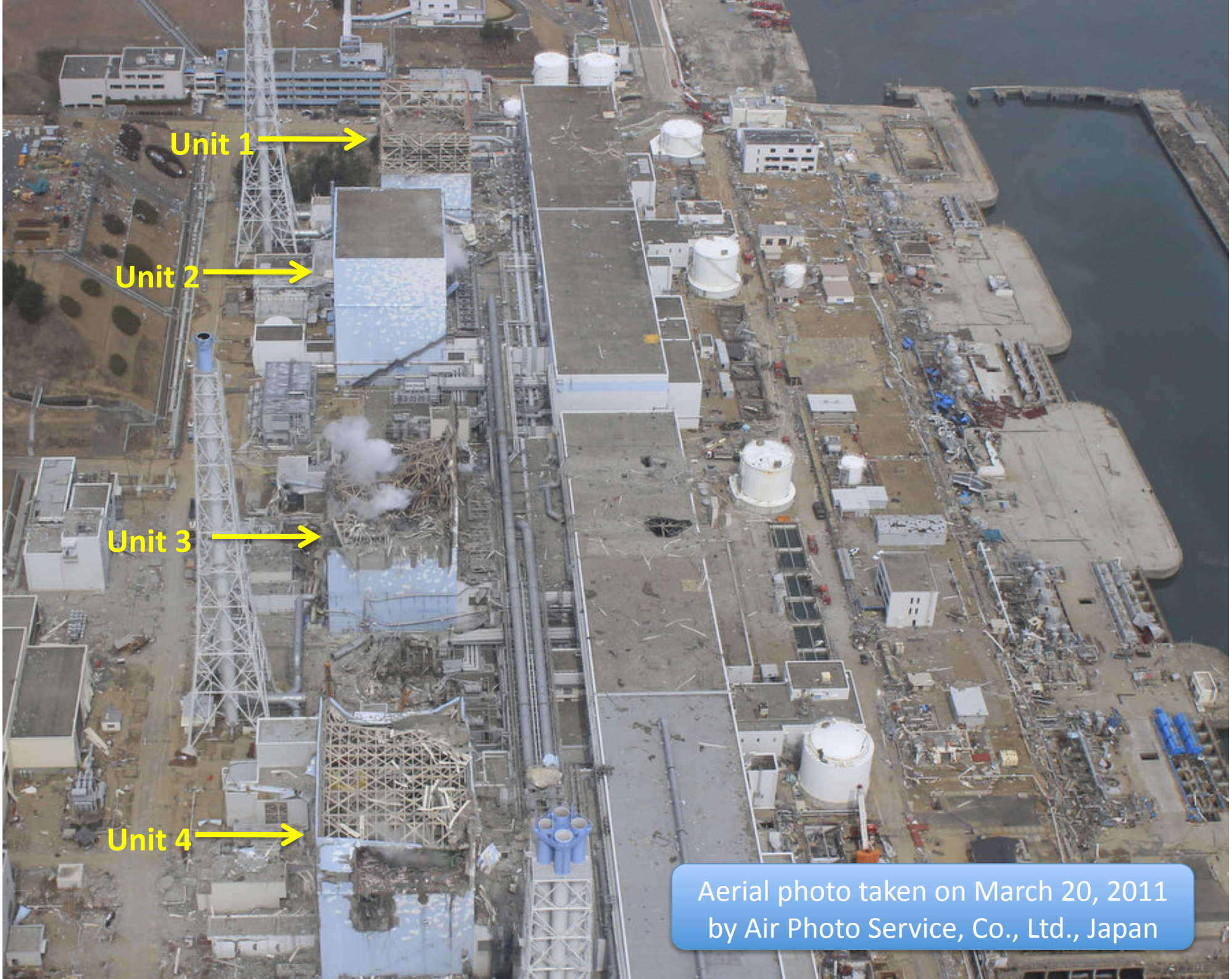
March 11, 2011: Chain of mishaps

- At 2:46 p.m., the earthquake struck east coast of Japan — Anticipated
- -> Nuclear reactors automatically shutdown => needs cooling — Flawless
- -> External power outage interrupted cooling systems — Anticipated
- => emergency power system (12 diesel generators) started up — Flawless
- -> Isolation Condenser (relying on convection and gravity) for Unit 1 automatically started => Just before tsunami, operators manually turned it off, and couldn't turn on again due to power outage — Flawless / design faults!
- At 3:35 p.m. A tsunami with height at 15 m rushed the plant whose site level is at 10 m above sea level — Inconceivable!
- -> Floodwater inundated 11 of 12 diesel generators to halt — Unanticipated!
- -> The entire station blacked out completely, with only one diesel generator kept working to have reactors 5 & 6 survive the crisis — Unanticipated!
- Backup-power-supply trucks racing toward Fukushima got stuck in traffic clogged with residents fleeing the disaster sites — Unanticipated!
- -> Operators had to respond to emergency without working instruments — Unanticipated!

Design faults !

March 11, 2011: Reported results

- At 9:00 p.m., nuclear core of reactor 1 began to melt down, producing high volatile Hydrogen gas
- At 11:00 p.m., pressure vessel began to damage, allowing highly radioactive water and gases to leak into the containment vessel
- **March 12:** At 2:00 p.m., containment vessel of reactor 1 began to vent, releasing radioactive gases into the air, and also causing hydrogen collected below the ceiling of reactor building 1.
- At 3:36 p.m., reactor building 1 exploded due to hydrogen gas.
- **March 13*:*** At 11:00 a.m., nuclear core of reactor 3 began to melt down
- **March 14:** Nuclear core of reactor 2 began to melt down before 8:00 p.m., and pressure vessel began to damage at 11:00 p.m.
- Reactor building 3 exploded at 11:00a.m., and pressure vessel began to damage at 10:00 a.m.
- **March 15:** At 6:00 a.m., reactor building 2 exploded
- Reactor building 4 also exploded on the same day due to unknown reason


Unit 1
Unit 2
Unit 3
Unit 4
Aerial photo taken on March 20, 2011
by Air Photo Service, Co., Ltd., Japan

March 11, 2011: Issues

- Poor management and responses by government organizations to the accidents
- Poor responses to the accidents at Fukushima nuclear power station operated by TEPCO
- Lack of timely disclosure of scientific and dependable information to prevent expansion of damage
- Lack of scientific imagination and systematic measures against complex disasters and severe accidents

March 11, 2011: Lessons learnt

- Murphy's Law is correct: "If anything can go wrong, it will"
- Perrow's hypothesis for "Normal Accidents" is validated, i.e. "interactive complexity" and "tight coupling"
- Design for dependability requires imagination of what is inconceivable
- The government and TEPCO have withheld critical information from public
  - Last Monday, on Jan 23, it was disclosed that there exist no official documents that recorded the decision-making process in the Nuclear Emergency Response Headquarters established on March 11, 2011 at the Prime Minister's Office to execute the emergency responses. Any "inconvenient truth"?

We, first of all, need dependability of Government !

“Normal Accidents” in Information Society

- Charles Perrow wrote “Normal Accidents” in 1984, describing the TMI accident that occurred in 1979
- The reactor unit 1 at Fukushima nuclear power station had been in operation for 40 years since 1971
- *Today’s information societies include “far more” interactive complexities and tightly coupled subsystems as components, making accidents more normal*

40 years ago…

- Our flag-ship symposium, FTCS, launched in 1971
- The first humans landed on the Moon by the Apollo 11 in 1969
- The world's first microprocessor, Intel 4004, emerged in 1971
- The UNIX originated at BTL on DEC PDP-7 in 1969
- C was developed at BTL with the UNIX during 1969 - 1972
- ARPANET started at UCLA, SRI, UCSB and U.Utah in 1969
- *Since then, many things changed !*

What changed

- Number of Transistors on a Chip:
  - 2300 “Intel4004”(1971) => 2.6 Billion “Intel Westmere-EX” (2011)
- Computing Performance:
  - 5 MFlops “CDC7600” (1969) => 8 PFlops “Fujitsu K” (2011)
- Internet Access:
  - 4 IMPs in ARPANET(1969) => 2B people on line in the world(2011)
- Software on a Car:
  - The first µP, M6802, was used for spark timing in GM Oldsmobile (1977)
    => 100M LOC running on 100 µP on a premium car (2011)

Information society changes

- Information systems are getting more complicated
- Services are getting more diversified
- Technological and societal environments change globally

But, human IQ remain unchanged!

Gaps between system complexity and human capability are the major sources of threats to the dependability for the information society !

And, the gaps are increasing !

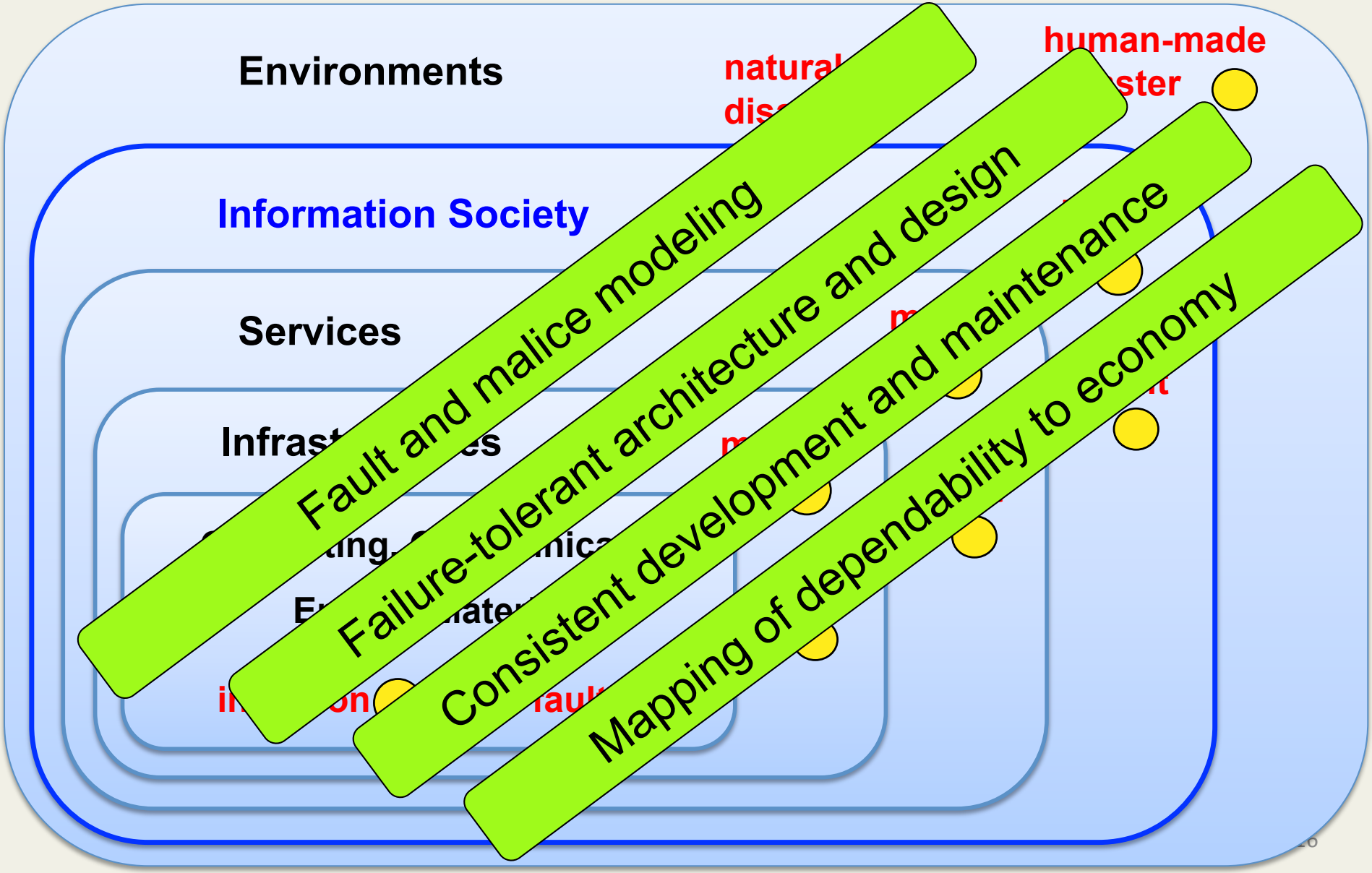
Threats to Dependability

- Open systems : Systems can interact unintentionally with unknown systems
- Black-box components: Systems can include components whose mechanism and internal behavior are unknown
- System complexity: Systems are increasing in complexity and interdependency with huge scaling gaps between hierarchical layers
- VLSI miniaturization: Nanometer devices can be highly sensitive to process variation and environmental interferences
- System deterioration: Systems can deteriorate due to aging and environmental changes

Threats --- continued

- Data explosion: The amount of data produced and distributed everyday on the network grows explosively.
- Human behavior: Psychological behavior of human beings is uncertain and error-prone
- Service diversity: Services provided by networked systems are unpredictably diversified
- User diversity: A variety of people, even malicious or naïve users, can equally have access to networked systems.
- Ambiguous responsibility: It is somewhat ambiguous who is responsible for what happens in globally networked systems

What we need


Environments
human-made
Information Society
Services
Fault and malice modeling
Failure-tolerant architecture and design
Consistent development and maintenance
Mapping of dependability to economy

Difficult problems for dependability

1. Effect estimation and action planning for global environmental changes
2. Forecast, protection and recovery strategy for natural disasters
3. Prevention and recovery strategy for epidemic diseases
4. Understanding life processes and prevention of incurable diseases
5. Understanding mental phenomena and healing of mental disorder
6. Global security for energy, food and water
7. Sustainability and risk management of critical infrastructure
8. Understanding economic phenomena and prevention of financial crisis
9. Dependability and security in networked systems and services

Research Gaps

- Extreme events in modern societies include
  - System failures (internally caused)
    - social systems, services, critical infrastructures, information systems
  - Disasters (externally caused)
    - natural disasters, human-made disasters

- Most difficult problems encountered in modern societies are attributed to "complex systems"
  - *Can the traditional "complexity science" solve these difficult problems ?*

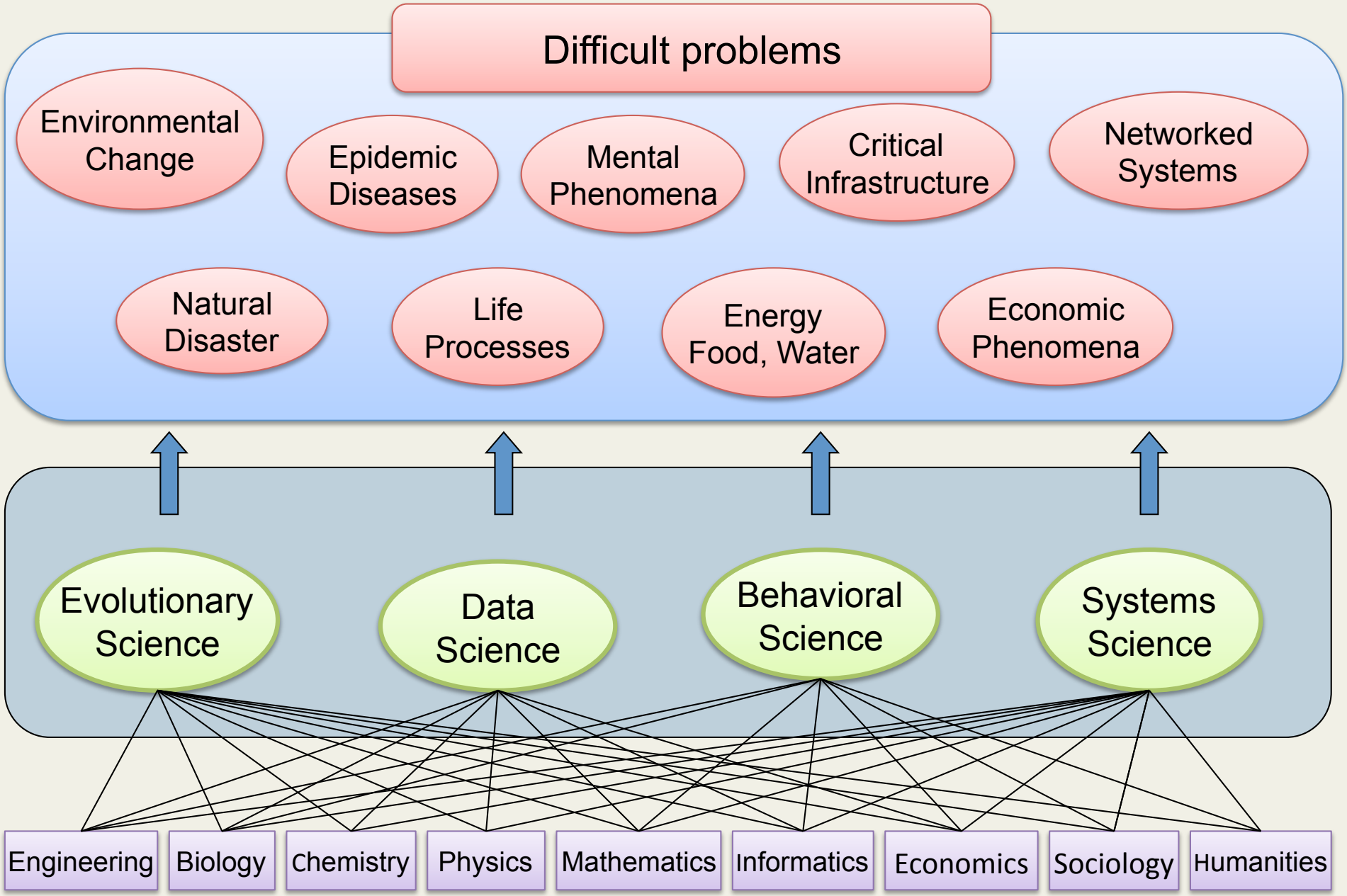
Issues of complex systems

- Scientific points of view
  - Can the systems (including interdependency) be modeled ?
  - Can all the necessary parameters be measured ?
  - Can the modeling be validated ?
  - Can the model be computed for analyses and simulations ?
  - Can the results be evaluated ?

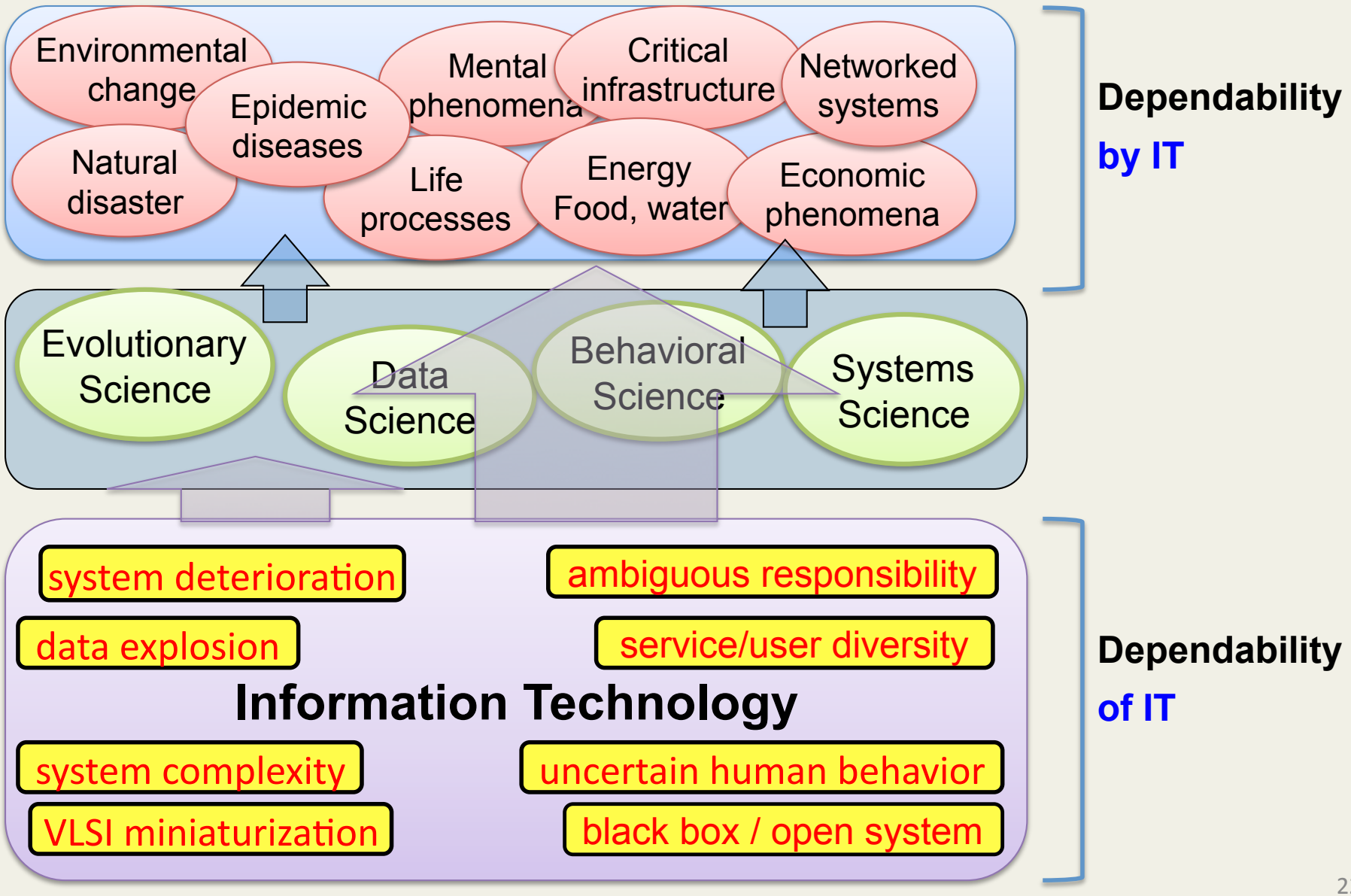
- Engineering/policy points of view
  - Can value metrics that are internationally agreeable be defined ?
  - Can the value metrics be measured and quantitatively evaluated ?
  - Can systems adaptable to changes be designed, implemented and maintained both technologically and economically ?

Converging Disciplines

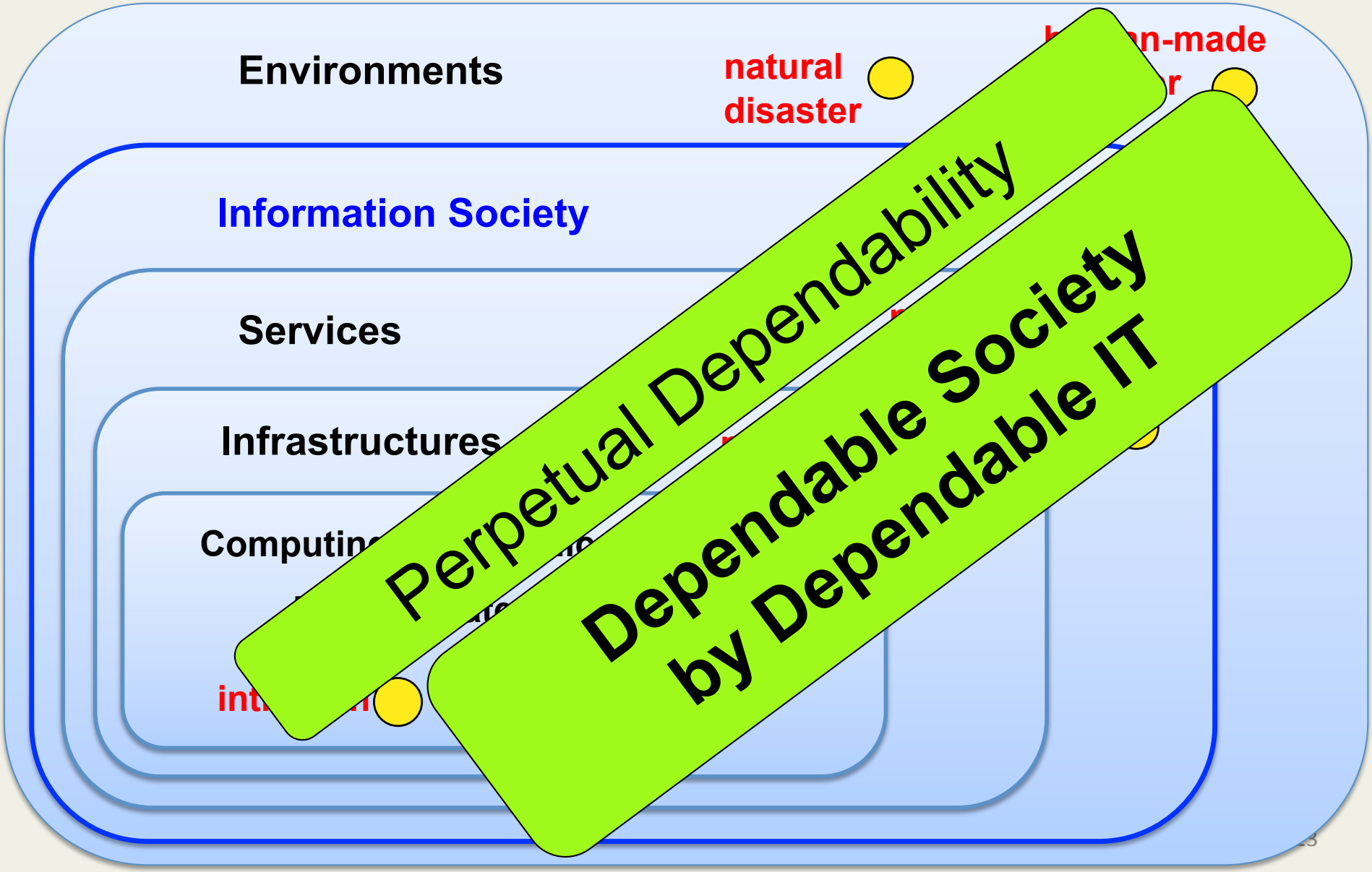
- **Data Science** : *Understanding management of a huge amount of data*
- **Behavioral Science** : *Understanding psychological behavior of human beings*
- **Evolutionary Science** : *Understanding change and evolutionary processes of nature, human and society*
- **Systems Science** : *Understanding complexity of systems with interdependencies and uncertainties*


Difficult problems
Environmental Change
Epidemic Diseases
Mental Phenomena
Critical Infrastructure
Networked Systems
Natural Disaster
Life Processes
Energy Food, Water
Economic Phenomena
Evolutionary Science
Data Science
Behavioral Science
Systems Science
Engineering
Biology
Chemistry
Physics
Mathematics
Informatics
Economics
Sociology
Humanities

Goal for Information Technology



Changing Information Society



Conclusion & Question

- Dependable Systems and Networks can imply a broad area including : “Government” systems, “Euro” system, “Biological” systems, “Social Network” systems, etc.

- DSN has traditionally addressed “dependability of IT”, excluding “dependability by IT”

- *Should DSN continue to concentrate itself on the former, or should it expand to explicitly address both ?*