# Towards a Trust Infrastructure with the Bright Internet

WSIS Forum

May 28, 2015

**Jae Kyu Lee**
**President (2015-6),**
**Association for Information Systems**
**Chair Professor at KAIST, Seoul**

## Side Effects of ICT

- **ICT has changed our life in good ways**
- **But seriously venerable to Cybercrimes, Terrors, and Privacy Infringement**

### Cybercrimes

- **378m Users (41%) per year**
- **38% of mobile users**
- **US$ 400 billion**

  - Verizon 2015

- 56 Billion Spam Mails per day (68%)
- 90% from Zombie (Kohavi, 2014)
- 71% of Web sites exist less than 24 hours

### Terrors

- DDoS Attack : 60% of US Companies (Neustar, 2014)
- Potential Attack to Energy, Telco, Financial, Transportation Infrastructure and IoT critical

### Privacy Infringement

- **552Mil Data Leakages**

  - Symantec, 2013

- Cyber Bulling,
- Harsh Reply

# AIS Grand Vision of the ICT-enabled Bright Society

## Task Force of Bright ICT Initiative

- ☐ **Jae Kyu Lee (AIS President-Elect): Chair**
- ☐ **Helmut Krcmar (AIS President,** Technische Universität München**)**
- ☐ **Nils Bjorn-Anderson (AIS Past President)**
- ☐ **Jane Fedorowicz (AIS Immediate Past President,** Bentley University**)**
- ☐ **Ramayya Krishnan (Dean, Heinz,** Carnegie Mellon university **)**
- ☐ **Joey George (Past President)**
- ☐ **Allen Lee (AMCIS EC, Chair)**

# GUEST EDITORIAL

## Research Framework for AIS Grand Vision of the Bright ICT Initiative

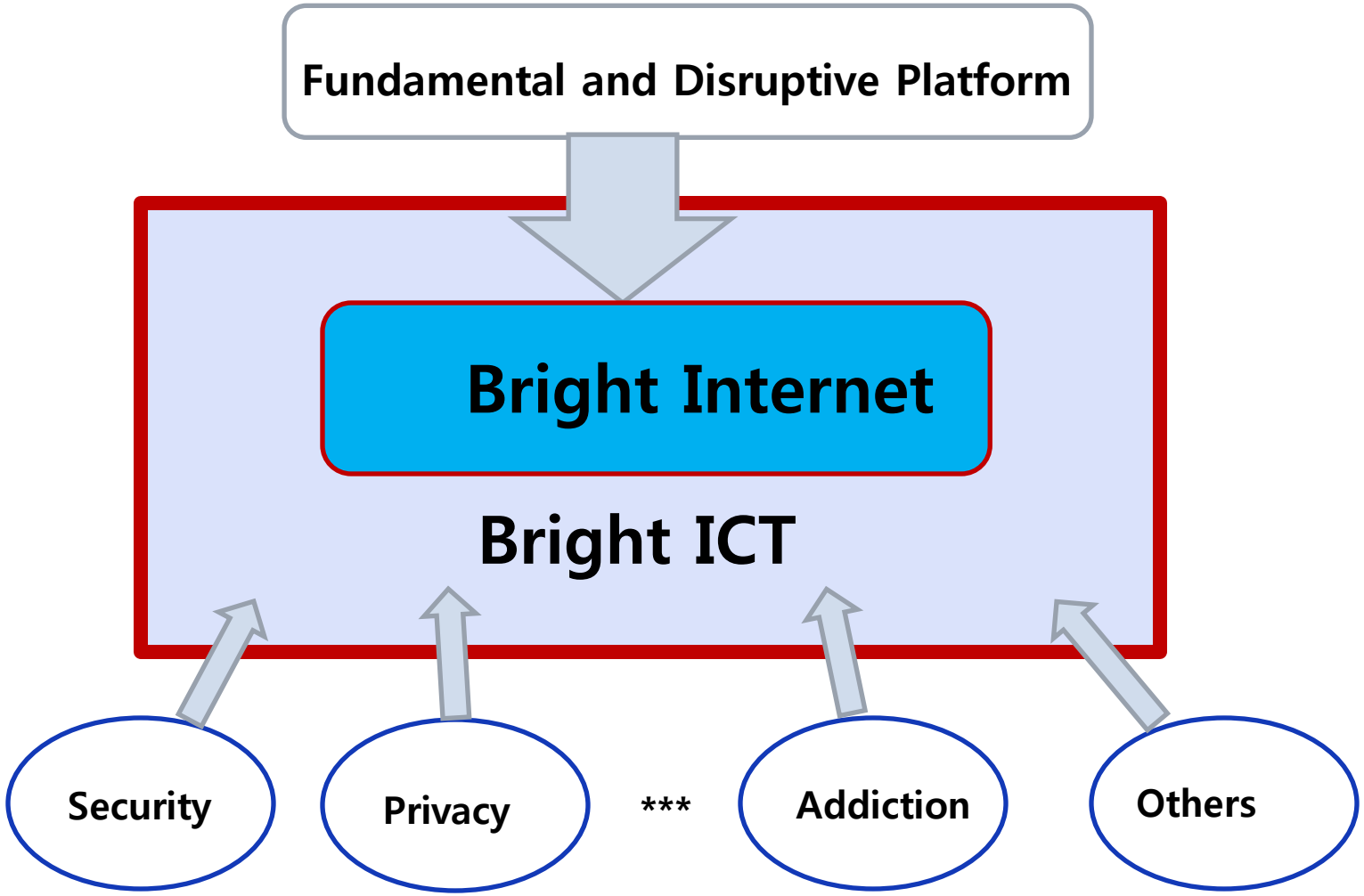
By: **Jae Kyu Lee**
**President, Association for Information Systems (2015–2016)**
**Korea Advanced Institute of Science and Technology**
**Seoul, Korea**
**jklee@business.kaist.ac.kr**

The Internet has become a minefield of crime, fakes, and terror perpetuated by anonymous users on a global scale. The security burden of protecting organizations is becoming increasingly difficult and costly, and this burden cannot be lessened under the current Internet protocol. In order to fundamentally solve these side effects, the Council of the Association for Information Systems (AIS) has adopted a grand vision of an ICT-Enabled Bright Society (in short, the *Bright ICT Initiative*). With the goal of preventing undesirable activities on the Internet, diverse issues can be investigated using a bottom-up perspective. Scholars are beginning to examine the concept and various approaches with the support of the AIS conferences and the information system journals. However, a unique approach and fundamental solution must be identified in order to drastically eliminate the negative side effects of these adverse online activities. In order to achieve this, four principles are proposed that will provide the foundation of the framework for a new and safer Internet platform, the *Bright Internet*, while protecting users' privacy at an appropriate level. The proposed principles are *origin responsibility, deliverer responsibility, rule-based digital search warrants,* and *traceable anonymity*. This endeavor requires the investigation of technologies, policies, and international agreements on which new business models can be created.

### *Introduction: Negative Side Effects Caused by the Internet*

The proliferation of the Internet worldwide has resulted in over 929 million websites and 3.1 billion users as of April 15, 2015 (Internet Live Stats 2015). Smart phones have pushed the expansion of the mobile Internet to 1.64 billion users with a 25 percent increase in 2014 (eMarketer 2014). Internet-based commerce has become part of daily life and more personalized services have become possible due to ubiquitous data collection and big data analysis (Craig and Ludloff 2011). The future of the "Internet of Things" (IoT) will further expand the penetration of the Internet in unimaginable ways. As such, Internet-based information and communication technologies (ICTs) have become an inevitable tool in daily life around the world.

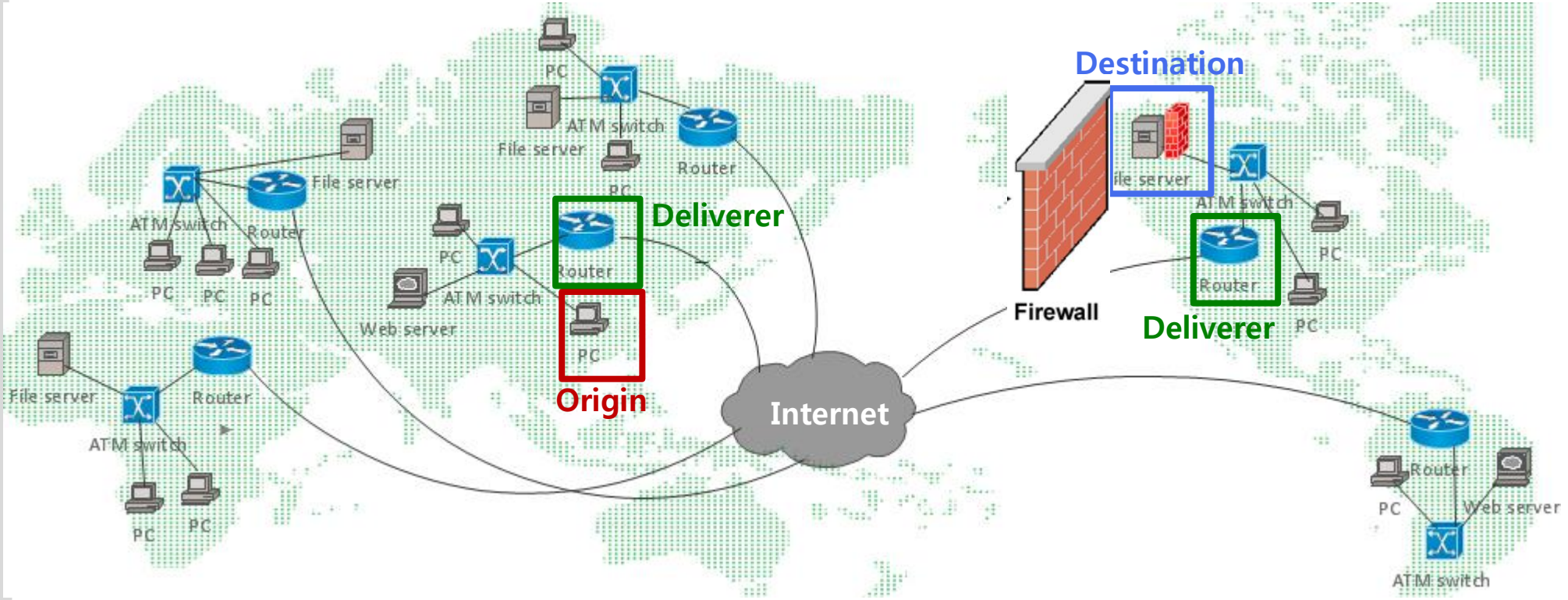
# Bright Internet as a core of Bright ICT



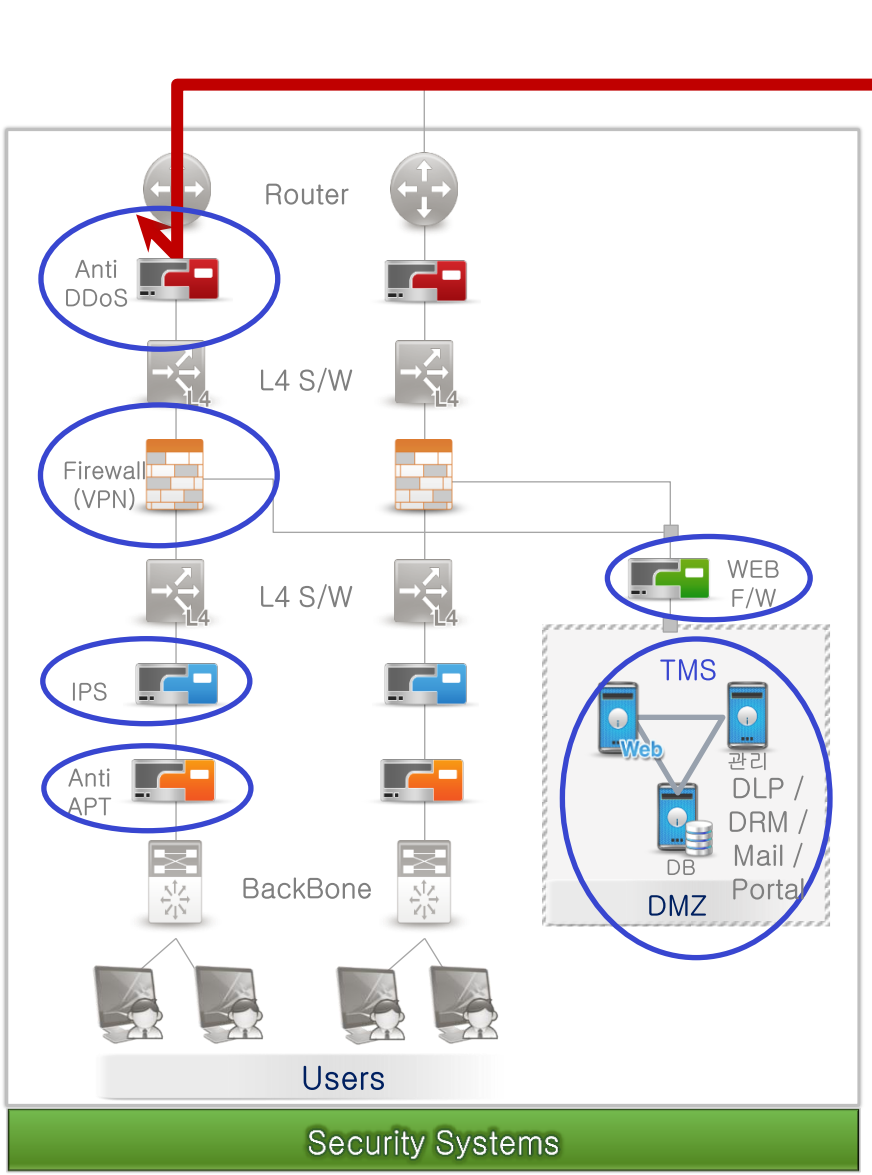
# Current Internet: Who should prevent the attacks?

## Principle of Destination Responsibility

- **Current Status**:
  The responsibility of security risk is born by the users and destination server



# Corporate Security Systems: High Cost and Vulnerable




**IPS : Intrusion Prevention System**

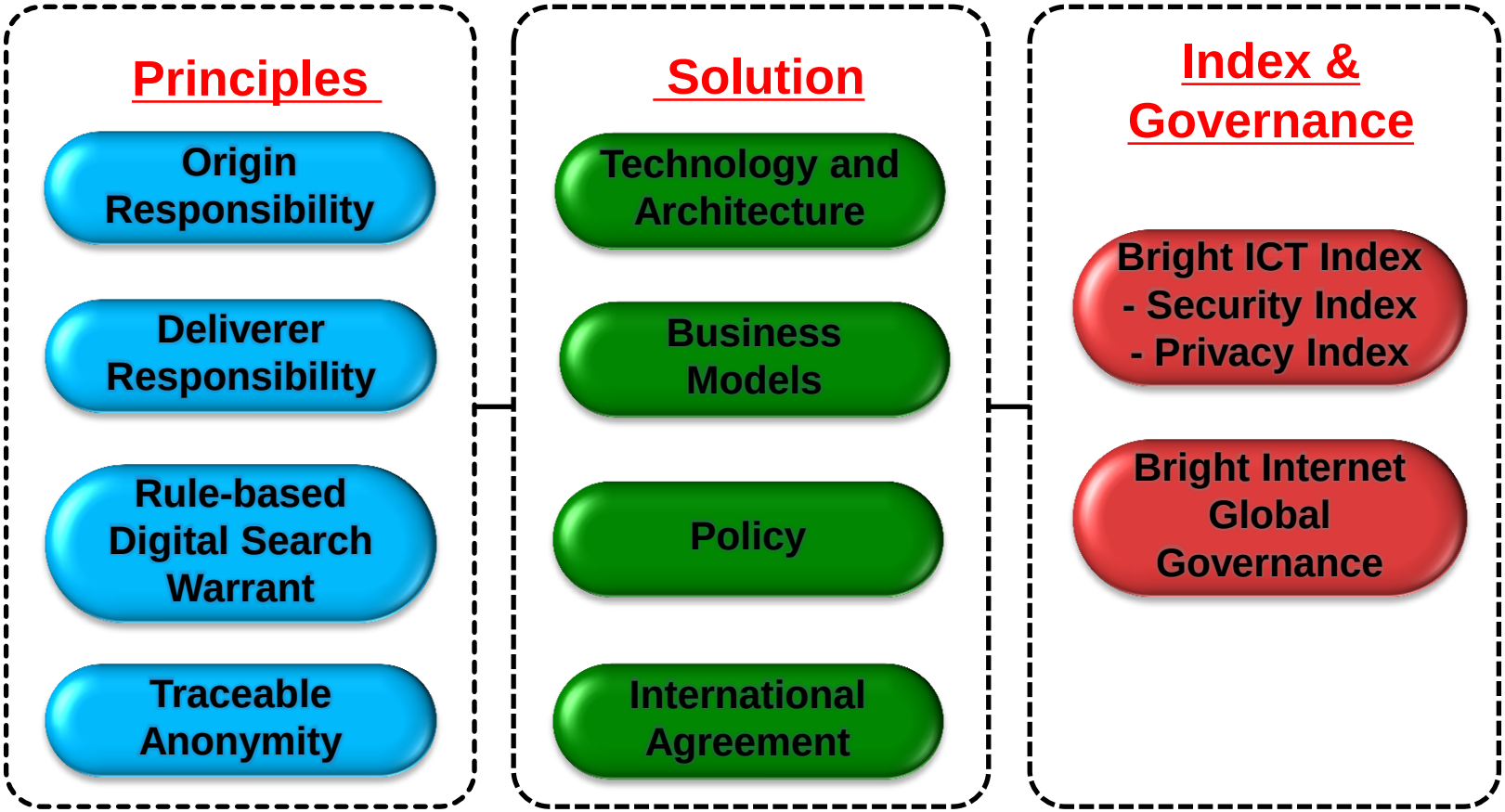
**APT : Advanced Persistent Threat**

**DLP : Data Loss Prevention**

**DRM : Digital Rights Management**

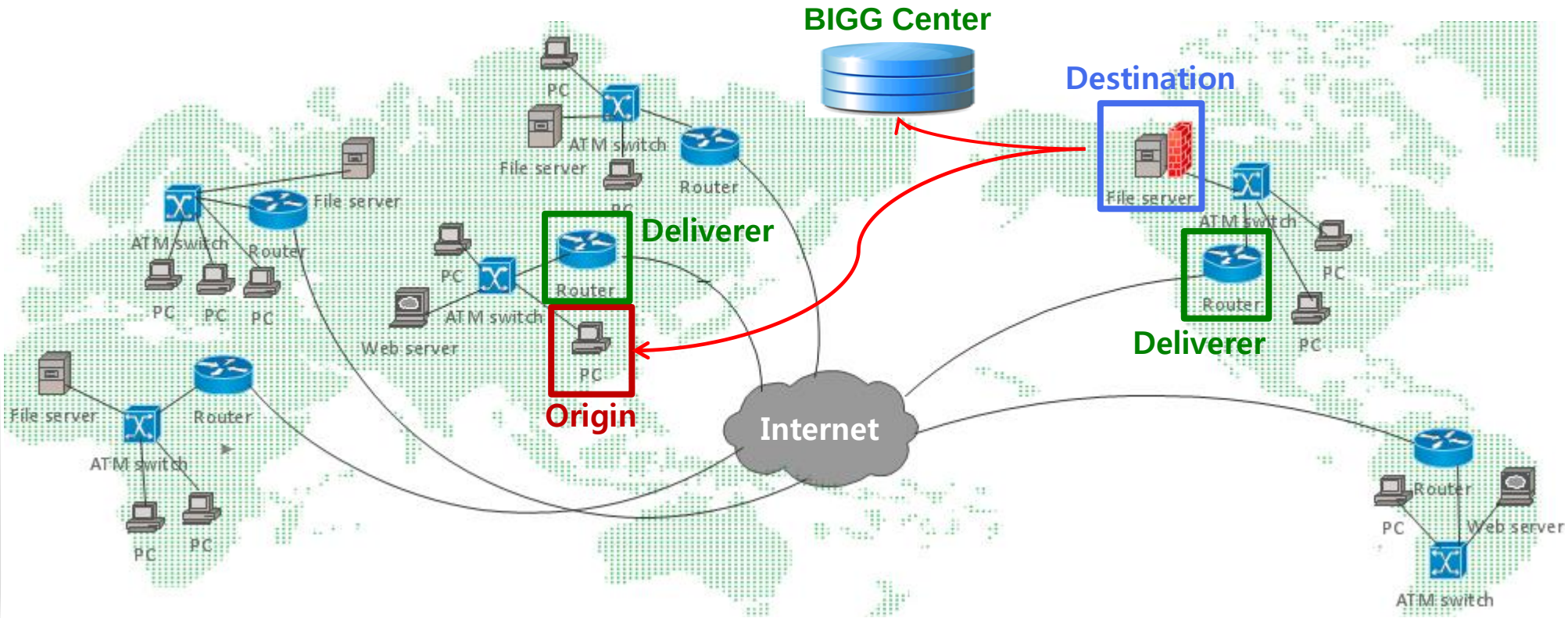
**TMS : Threat Management System**

# Framework of Bright Internet



## Principle 1: Origin Responsibility

- **Current Status**: The responsibility of security risk is born by the users at destination server
- **Approach**: Refer to the principle of individual producer's responsibility that is adopted for the management of electronic and electric equipment waste
- **Benchmark**: Extended producer responsibility

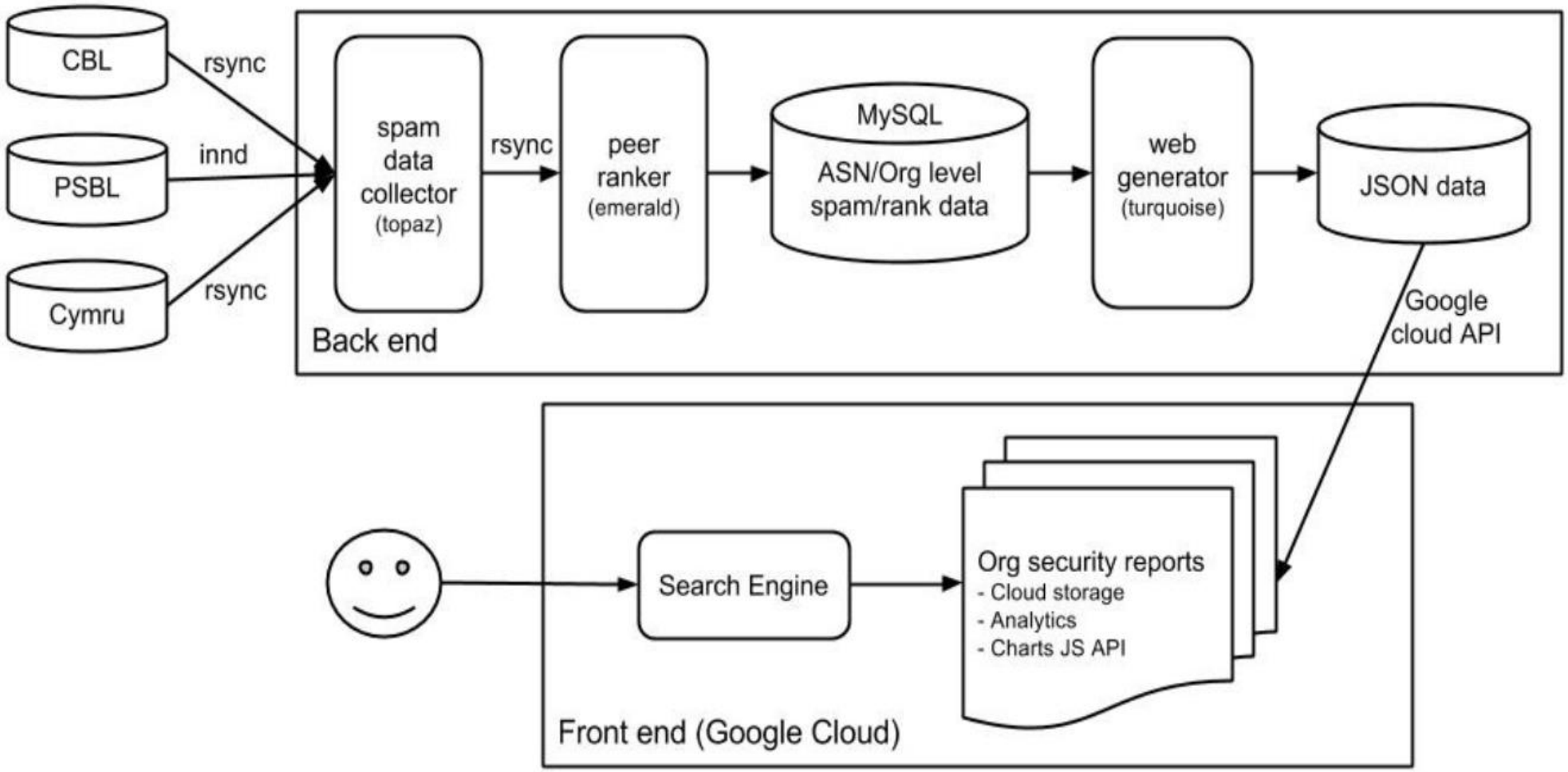


# Principle of Individual Producers Responsibility:
# Model for e-Waste Take-back:

- **The pan-Europe recycling organization created in response to the WEEE Directive to promote e-waste collection and recycling.**
- **Business model of the company" for ERP**
  - **Cost effective implementation of WEEE for IPR**
  - **In 2007 (2009)**
    - **1100 (1300) members in 8 countries**
  - **In 2014**
    - **Collected 2 Million tons across 17 countries**

# SPAM Mail Origin and Destination Analysis

## U Texas Research (Whinston & Gene Moo Lee, U Texas, Austin)



# Ranking Information ➔ Bright ICT Index

THE UNIVERSITY OF TEXAS AT AUSTIN
McCOMBS SCHOOL OF BUSINESS

## Outbound spam may be leaving your organization

This advisory indicates the level of spam sent from computers at T-Mobile USA Inc., compared t
information may be useful in determining network security improvements.

December 2013 Rankings for T-Mobile USA Inc.:

| Rank | Top % | Among | Type | Code | Description |
|---|---|---|---|---|---|
| 57 | 2.0% | 2,888 | NAICS | 517210 | Wireless Telecommunications Carriers (except Satellite) |

For graphics and more information about spam volume originating from your organization, please vis
information provided on this web page is publicly searchable on cloud.spamrankings.net.

## About this project

The cloud.Sp@mRankings.net project operates out of the Center for Research on Electronic Commerce
project compares relative spam amounts by correlating outbound spam blocklist data to Autonomo
data from several blocklists into a Composite Borda count. Our goal for publishing the rankings is to
for dealing with outbound spam. For more information about the project, please visit our About the pr

For a list of terms we use in this email and in our organizational analysis page, please visit our Glossa

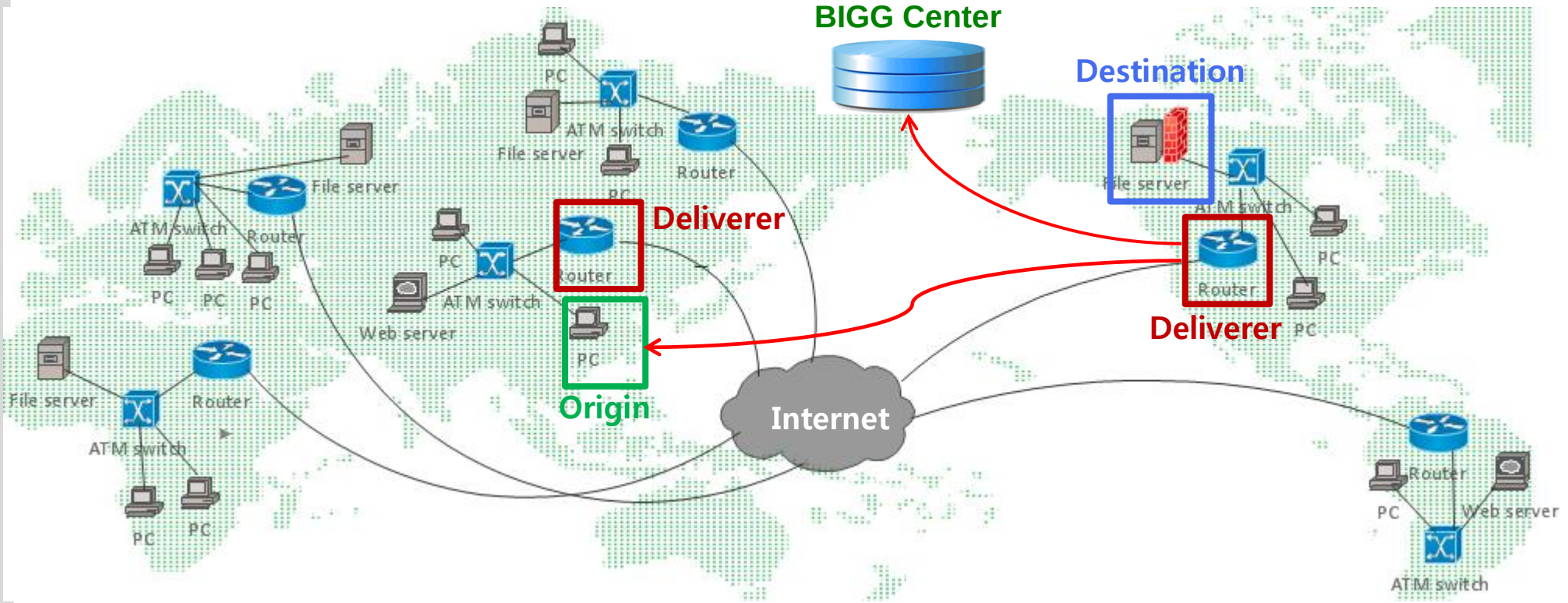
## Data source details

Borda Count rank 70 score 38,363 composed from:

| Source | IP Addresses | | Spam Messages | |
|---|---|---|---|---|
| | Rank | Hosts | Rank | Volume |
| CBL | 39 | 8,162 | 124 | 61,198 |
| PSBL | 62 | 95 | 184 | 300 |

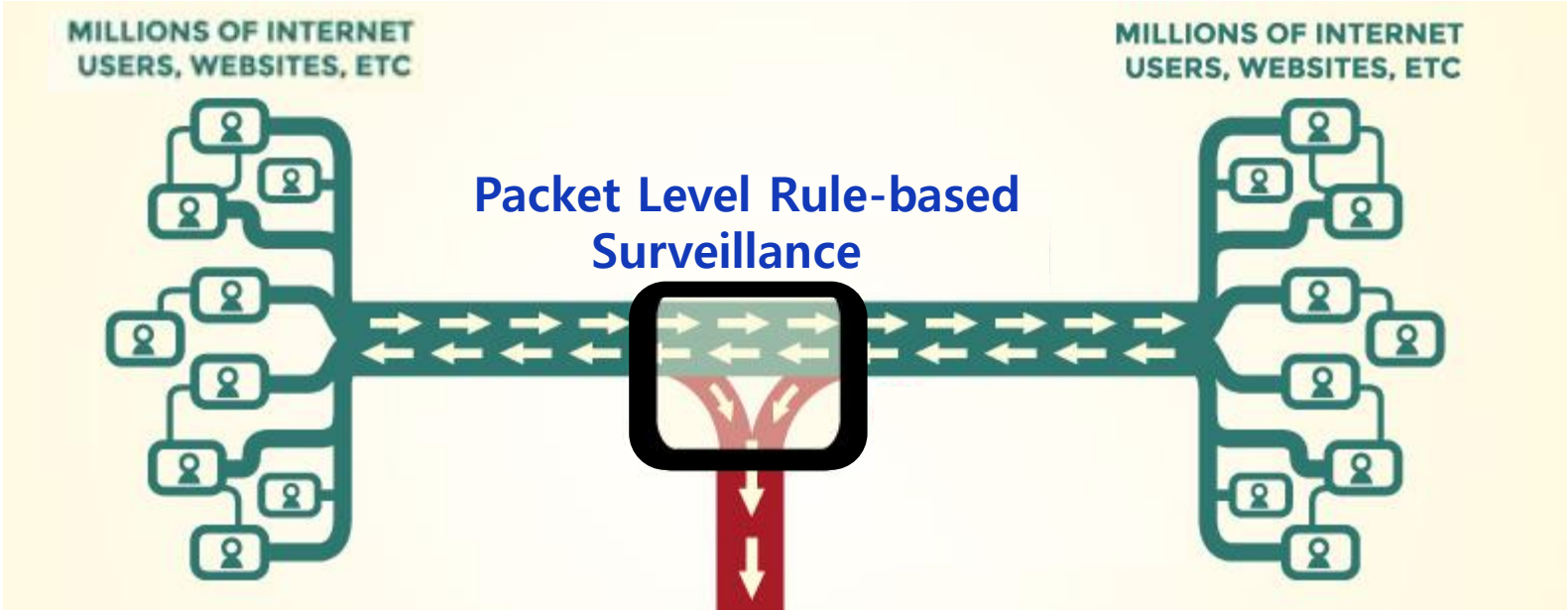
## 2) Principle 2: Deliverer Responsibility

- **Current Status**: 90 % of mail from Compromised Servers; Router and Carriers Responsibility
- **Approach**: Delivers have the responsibility of willful negligence of delivering wicked contents
- **Benchmark**: Drug runner who delivered strangers' bags



## 3) Principle 3: Real-time Rule-based Digital Search Warrant

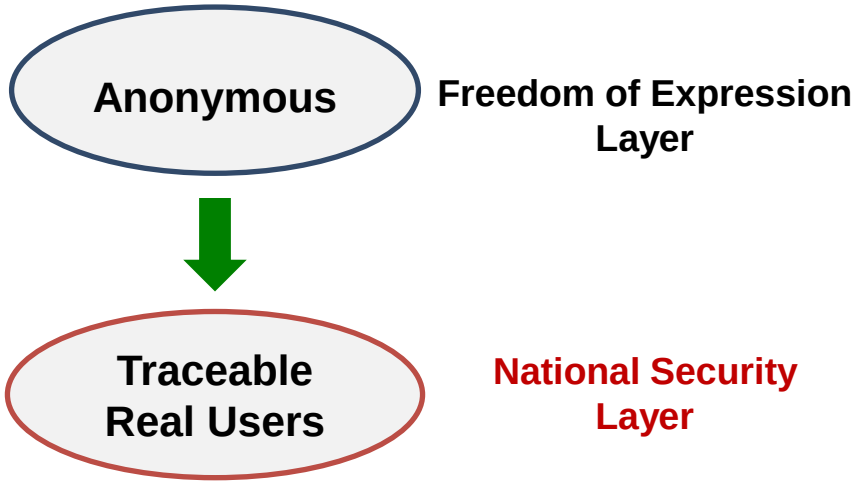
- **Current Status**: The execution of current search warrant collects more bundled information system than the authorized relevant information
- **Approach**: Rule-based software agents issued by judge identifies whether a packet is suitable to execute the warrant or not




**Issue a search warrant only if illegal statement detected**

## 4) Principle 4: Traceable Anonymity

- **Current Status**: Anonymous criminals are abusing the internet Protocol
- **Approach**: Protect anonymity when the privacy should be protected. If the anonymous user turned out to be a criminal or has a potential to commit crime, the traceability of real name should be guaranteed

# Solutions for the Bright Internet

## Holistic Solution of Architecture, Technology, and Policy

- **Current Status**: Current security research are dealing with fragment issues of technology development or regulation
- **Approach**: To implement the principles, we need holistic solution of architecture, technologies, policy, and business models

## Mechanism of International agreement

- **Current Status**: There is no agreement and dedicated mechanism for the countries to reduce the cross border side effects and conflicts
- **Approach**: The Global Bright ICT Summit in cooperation with ITU will be an appropriate mechanism

# Bright Internet – Index & Governance

## Corporate and National Indices of Bright ICT

- **Current Status**: At the moment, there is no measurement about the ICT brightness
- **Approach**: National measurement of ICT Brightness and its comparison with other countries will motivate the country to recognize its status of ICT Brightness and to seek solutions to reduce side effects

## Bright Internet Global Governance

- ⦿ Define the Bright ICT Index
- ⦿ Measure the Origin & Deliverer Responsibilities, Protection of Privacy and Security Potential
- ⦿ Compensate the Responsibility
- ⦿ Establish the Governance Structure for Global Agreement and Clearance

# ITU Trust Infrastructure and AIS Bright Internet

## Trust Infrastructure

- Technical Standards
- International Agreement
- Industry Relations

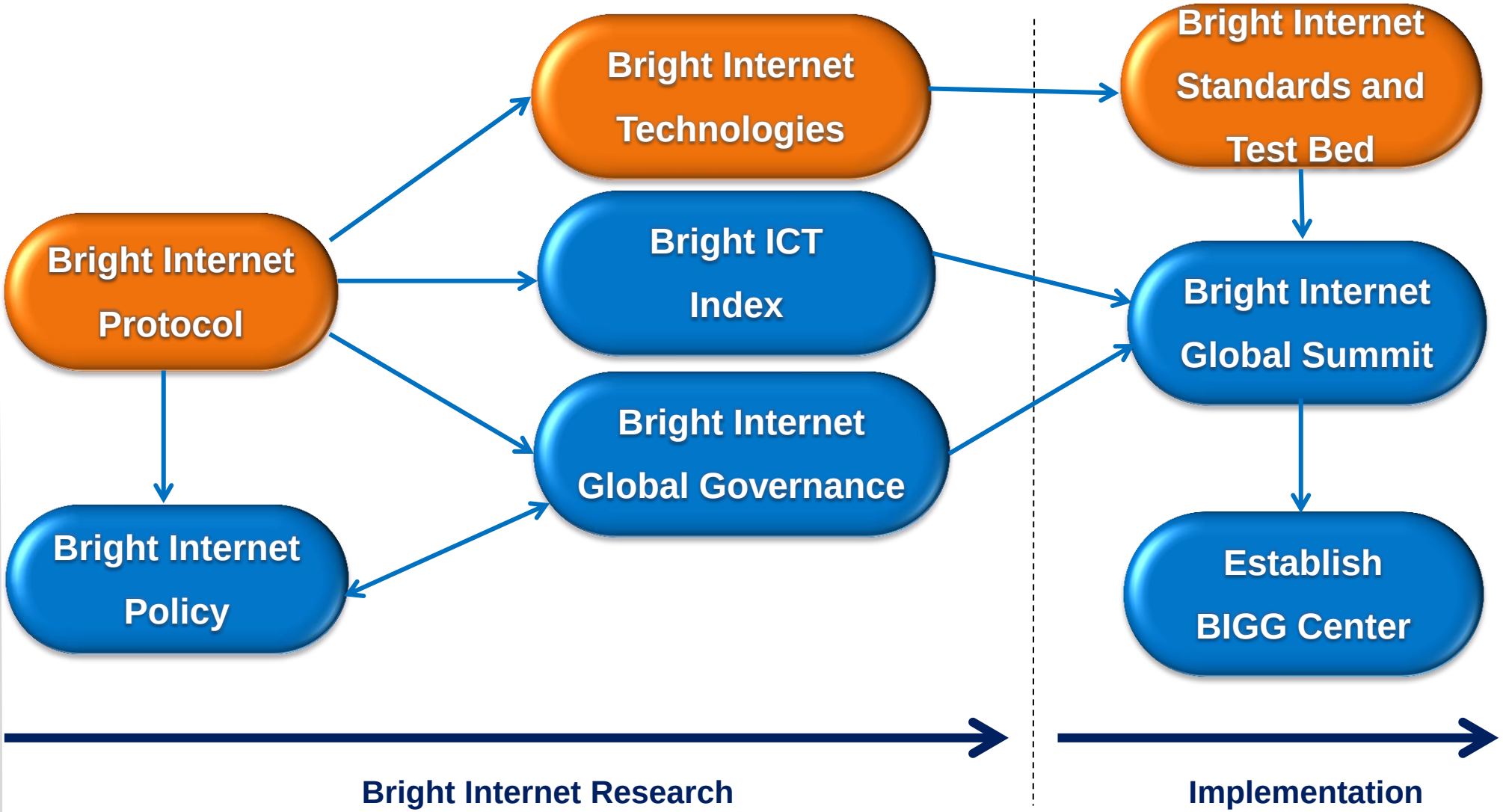
## Bright Internet

- Technology and Architecture
- Business and Economic Models
- Policy and Global Governance

International Telecommunication Union

ASSOCIATION FOR INFORMATION SYSTEMS

# Bright Internet Road Map



# Conclusion

- The Bright Internet will drastically reengineer the security and privacy issues on the Internet
- The Bright Internet will open the next generation of Internet
- Collaboration of the Bright Internet Initiative with ITU Trust Infrastructure Project are complementary with the same goal
- Collaboration of ITU and AIS will create the trustful society with bright future.