The Bright Internet
Principles and Research Progress:

APRU Business Off Site at Stanford University
May 25-26, 2017

Jae Kyu Lee (이재규, 李在奎)

- Chair Professor, Yonsei University & KAIST, Seoul, Korea;
- YL Fellow Professor, Xi’an Jiaotong University, China
- Distinguished Visiting Professor, Carnegie Mellon University, USA
Issues to Discuss (1/2)

- What should be the Principles of Next Generation Internet?
  - Are the Bright Internet Principles appropriate alternative?
  - Are the Internet Peace Principles appropriate alternative?

- What should be the Global Governance Structure for the Next G. Internet?
  - Can the Bright Internet Global Summit a channel of communication?
  - Can the Bright Internet Global Governance an Alternative Body?

- Can we develop the Market Driven Business Models for the deployment of Bright Internet?
  - Bright Cloud and Extend Networks
  - Block Chain Technology for the Blacklist Sharing

- Can the Bright Internet Framework be the foundation for the Secure 4th Industrial Revolution?
  - With AI, IoT, Robot, and Self-driving Cars and Drones?
Issues to Discuss (2/2)

Can we conduct a Holistic Research toward the Bright Internet?
- Technologies
- Business Models
- National Regulation and Support
- Global Governance Body

Who should lead the Bright Internet Initiative?
- Academic Society: Association for Information Systems, Others
- University’s Bright Internet Research Center Network
- National Research Group: Country Specific Issues
- Basic Research: Academic + Industry + Government Policy + International Policy
- Test Bed Research: Industry + Academic + Policy Test
Background Information: Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
- Road Map Ahead
AIS Grand Vision Project of the ICT-enabled Bright Society:

Bright ICT Initiative

- Adopted by AIS Council in Dec 2014

- Objectives
  - Pursuit of High Impact IS Research
  - Eliminate Dark Side of ICT, particularly on the Internet

- Academic Activities
  - Panels and Workshop in AIS Conferences
  - Special Issues of Leading IS Journals

- Global Research Network and Research Opportunity
  - Bright ICT
  - Bright Internet
Bright Internet as a core of Bright ICT

Fundamental and Disruptive Platform

Bright Internet

Bright ICT

Security  Privacy  ***  Addiction  Others

Focus  Diversity
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 perpetrated 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.
Invited Commentary—Reflections on ICT-enabled Bright Society Research

Jae Kyu Lee
College of Business, Korea Advanced Institute of Science and Technology, Seoul 130-722, Korea

Permalink: http://dx.doi.org/10.1287/isre.2016.0827
Published Online: March 7, 2016
Page Range: 1 - 5

Abstract

Since the advent of the AIS Grand Vision Project of ICT-enabled Bright Society (in short, Bright ICT), there has been significant excitement as well as confusion about the concept. To resolve ambiguities about the types of research that are consistent with this vision, the notions of Restorative Bright ICT Research and Enriching Bright ICT Research are defined. In addition, we propose three perspectives that can differentiate Bright ICT research from traditional research approaches to create a disruptive impact on society. To address societal problems that are often global in scope, Bright ICT research recommends taking a holistic design of future society encompassing technologies and policies as well as business models driven by visionary principles. This paradigm can be an extension of design science for the scope of a Macro Information Society.
A DESIGN THEORY OF THE BRIGHT INTERNET

Jae Kyu Lee
KAIST, Carnegie Mellon University, Xi’an Jiaotong University;
jklee@kaist.ac.kr

Daegon Cho
College of Business, KAIST; daegon.cho@kaist.ac.kr

Gyoo Gun Lim
School of Business, Hanyang University; gglim@hanyang.ac.kr

ABSTRACT
Anonymous cybercrimes and cyber terror have proliferated on an uncontrollable scale, but the sources of such malicious attacks are not easy to identify. Thus, current cybersecurity defensively protect their own systems, without any control on the sources of these threats. In this research, our intention is to design a safer Internet platform that can significantly mitigate the sources of such security threats by enabling the identification of originators who commit malicious behaviors. However, the endeavor of upgrading preventive security may increase the risk of breaching the privacy and freedom of anonymous expression. As a result, we aim to prescriptively design the so-called Bright Internet, which can achieve the goal of preventive security, balanced with privacy protections and freedom of expression for innocent netizens. Note that innocent netizens are distinguished from criminal individuals so as to fulfill these conflicting goals simultaneously. To realize the intended goals of the Bright Internet, five cohesive principles are derived: Origin Responsibility, Deliverer Responsibility, Identifiable Anonymity, Global Collaborative Search, and Privacy Protection. These principles are justified based on the seriousness of the social needs and social norms of analogical reference practices. To design solutions according to these principles, the necessary technologies, policies and global collaborations are prescribed holistically, and interactions among them are analyzed. The framework of designing the Bright Internet is demonstrated with the pioneering project Bright Internet 1.0 from the design theory perspective.

Keywords: Bright Internet, Cybersecurity, Preventive Security, Privacy, Freedom of Expression, Origin Responsibility, Deliverer Responsibility, Identifiable Anonymity
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society

- Background of the Bright Internet

- Research Framework

- Design Principles for the Bright Internet

- Road Map Ahead
Security Problems on the Internet

- Information systems is seriously vulnerable 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
- 552 Mil Data Leakages
  - Symantec, 2013
- Cyber Bullying,
- Harsh Reply

Internet: A lawless world of anonymous attackers; What is the status in Japan, USA, Korea, and China?
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

Self Defense Principle; Protective Security

Should we regard the external attacks from the unidentifiable origins as a given condition?
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
- Road Map Ahead
Purpose of The Bright Internet

- Who govern the current Internet
  - ICANN; Anonymous criminals
  - No responsibility about the consequence of malicious behavior
  - **Protective Security**: Assumption (External Attacks Given)

- Safe Internet
  - Criminal sources should be traceable and identifiable
  - Eliminate the sources of cyber threats: **Preventive Security**

- But Keep the Freedom of Speech
  - Allow the **Anonymity of Innocent Netizens**
  - Also protect the **Privacy of Innocent Netizens**
UN’s Spirit of Internet Governance

The United Nations World Summit on the Information Society (WSIS) declared in the paragraph 40 and 42 of Tunis agenda (2005) under the Chapter of Internet Governance.

“57. The security and stability of the Internet must be maintained.”

“42. … We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.
Goal Driven Principles & Prescriptive Design

Goals
- Preventive Security
- Freedom of Expression
- Privacy

Principles
- Origin Responsibility
- Deliverer Responsibility
- Identifiable Anonymity
- Global Collaborative Search
- Privacy Protection

Solutions
- Technology (Protocol and Standards)
- Policies (Legislation)
- Global Collaboration (Governance)

Applications
- Bright Internet Solutions
- Bright Cloud
- Bright E-mail
- Bright E-Commerce
- Bright IoT
- Prevent Cyberbullying
- National Security
Bright Internet Research Approach

Design Activities of Global Societal Information Infrastructure

- Technologies
- National Policies
- Global Collaboration

Design Principles of The Bright Internet

Design Goals

Social Needs

Analogical Social Norms
Prescriptive & Consistent Design

**Origin Responsibility**:
- TO1: Design the Origin based Surveillance System
  - TO1a: Design the Target of Surveillance
- TO2: Virtual Blacklist Management at Global Scale
  - TO2a: Evaluation Model of Attackers
- TO3: Victim Initiated Surveillance
- TO4: Architecture Standards and Management of Origin Responsibility
- TO5: Technology for the traceability and Spoof Proof

**Deliverer Responsibility**
- TD1: Design the Zombie based Surveillance System
- TD2: Design the Intermediator based Surveillance System
- TD2a: Design the Target of Surveillance by Intermediator

**Identifiable Anonymity**
- TI1: Architecture for Identifiable Anonymity
- TI2: Methods for Real Name Identification
- TI3: Digital search warrant management systems

**Technologies for Privacy Protection**
- TP1: Privacy Protection by the Security Principles of Bright Internet

**Technologies for Global Collaboration**
- TG1: Multilateral Collaboration Models for All Principles
ITU Trust Infrastructure and AIS Bright Internet

Signed MOU in ICIS 2015

Trust Infrastructure
- Technical Standards
- International Agreement
- Industry Relations

Bright Internet
- Technology and Architecture
- Business and Economic Models
- Policy and Global

International Telecommunication Union

Association for Information Systems
Activities in 2016

- **Research Project Grants in Korea**
  - Planning Project conducted in 2017 by IITP in Korea
  - Grants in Progress: Bright Cloud (IITP-USAF)
  - Planning in Progress: Multi-ministries Joint Project

- **Bright Internet Research Centers**
  - KAIST, Yonsei University, Xi’an Jiaotong University

- **AIS Bright Internet Global Summit, Dec 2017, Seoul**
  - Bright Internet Research Group: National Initiatives (Korea, China, USA, Australia, …)
  - Bright Internet China Symposium. June 5-6, 2017, Xi’an

- **Keynote speeches in the International Community**
  - AIS Conferences, PACIS, ICEC, Brazil Chapter, EuroSymposium
  - IEEE/ACM, “Can the Bright Cloud be a Business Model?”, Dec 6, Shanghai

- **China and Xi’an Jiaotong University**
  - Bright Internet Global Governance, China Research Center at XJTU
  - Bright Cloud Project: Yovole Network
Planning Project in Korea in 2016

Partner Institutions

<table>
<thead>
<tr>
<th>Academic/Global Organizations</th>
<th>Universities</th>
<th>Government Agencies</th>
<th>Research Institutes</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>- AIS</td>
<td>- KAIST</td>
<td>- Korea Internet and Security Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ITU</td>
<td>- Yonsei U</td>
<td>- Korea Police Bureau</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- KMIS Bright ICT SIG</td>
<td>- Korea U</td>
<td>- National Information Society Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- TII Forum</td>
<td></td>
<td></td>
<td>- ETRI Connectivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- ETRI Standardization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- National Security RI</td>
<td></td>
</tr>
</tbody>
</table>

Bright Internet Research Center
Jae Kyu Lee (KAIST)

Office
SH Park, JO Lee

Team 1
Social Needs and Social Norm
DG Cho (KAIST)
JY Park (KAIST)
JY Kim (KISA)
YW Lee (KT)
MW Sun (Police)

Team 2
Technology, Solution and Test
MC Kim (KAIST)
GG Lim (HY U)
SH Maeng (KAIST)
SG Whang (ETRI)
SG Park (MarkAny)
WT Kim (KT)
JG Yun (Certificate)

Team 3
Policy and Global Governance
DM Lee (KAIST)
YS Kwon (KAIST)
CH Lee (KAIST)
HY Kwon (Korea U)
NH Park, MH Jung (KU)
JI Lim (KU)
YW Shin (KAIST)

Team 4
Applications
KJ Lee (KH U)
JH Ahn (KAIST)
JH Ju (KAIST)
JW Lee (Yonsei U)
HW Kim (Yonsei U)
JH Kim (Daekyo)
KD Lee, EH Song(KIA)
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
  - Origin Responsibility
- Road Map Ahead
Goal Driven Principles & Prescriptive Design

Goals
- Preventive Security
- Freedom of Expression
- Privacy

Principles
- Origin Responsibility
- Deliverer Responsibility
- Identifiable Anonymity
- Global Collaborative Search
- Privacy Protection

Solutions
- Technology (Protocol and Standards)
- Policies (Legislation)
- Global Collaboration (Governance)

Applications
- Bright Internet Solutions
- Bright Cloud
- Bright E-mail
- Bright E-Commerce
- Bright IoT
- Prevent Cyberbullying
- National Security
How to implement the Origin Responsibility?

- Destination Driven Protective Solution: 68% are spam mails

- Bright Internet Approach
  - Origin Driven Preventive Solution: Reverse Engineering

How to motivate? How to measure the effectiveness of Bright Internet Approach?
Bright Internet – Origin Responsibility Principle
System Architecture

Victim’s reports

Traceability
Identifiability

Inbound Filtering
MDS

Outbound Filtering
Reverse MDS

Bright Cloud A
Technology Module Design for Origin Responsibility

TO1: Design the Origin based Surveillance System
   TO1a: Design the Target of Surveillance

TO2: Virtual Blacklist Management at Global Scale
   TO2a: Evaluation Model of Attacks (Origin-Destination)

TO3: Victim Initiated Surveillance

TO4: Architecture Standards and Management of Origin Responsibility

TO5: Technology for the Traceability and Spoof Proof
How to measure the Bright Internet Index of Origins

SPAM Mail Origin and Destination Analysis

✓ U Texas Research (Whinston & Gene Moo Lee, U Texas, Austin)
How to use the measured Indices?

Example: Disclosure of Ranking Information and its Effect

Outbound spam may be leaving your organization

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

December 2013 Rankings for T-Mobile USA Inc.:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Top %</th>
<th>Among</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>2.0%</td>
<td>2,888</td>
<td>NAICS</td>
<td>517210</td>
<td>Wireless Telecommunications Carriers (except Satellite)</td>
</tr>
</tbody>
</table>

For graphics and more information about spam volume originating from your organization, please visit the information provided on this webpage or search publicly on cloud.spamrankings.net.

About this project

The cloud.SpamRankings.net project operates out of the Center for Research on Electronic Commerce and compares relative spam amounts by correlating outbound spam blacklist data to Autonomous System data from several blocklists into a Composite Borda count. Our goal for publishing the rankings is to help organizations deal with outbound spam. For more information about the project, please visit our About the project page.

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

Data source details

Borda Count rank 70 score 38,363 composed from:

<table>
<thead>
<tr>
<th>Source</th>
<th>IP Addresses</th>
<th>Spam Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rank</td>
<td>Hosts</td>
</tr>
<tr>
<td>CBL</td>
<td>39</td>
<td>8,162</td>
</tr>
<tr>
<td>PSBL</td>
<td>62</td>
<td>96</td>
</tr>
</tbody>
</table>
Typical Cases of State-led Cyber Attacks

<table>
<thead>
<tr>
<th>Cases</th>
<th>Duration</th>
<th>Targets</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Korea Hydro &amp; Nuclear Power Co. Ltd. Hacking</td>
<td>● Dec. 9, 2014~ Mar. 12, 2015</td>
<td>● KHNP, which operates 23 nuclear reactors in South Korea</td>
<td>● Overall social infrastructure in Estonia (Government, national assembly, newspaper companies,</td>
</tr>
<tr>
<td>(2) Sony Pictures Entertainment Hacking (The FBI, 2014; Musil, 2014; Peterson, 2014)</td>
<td>● Nov. 24, 2014</td>
<td>● SPE in the USA</td>
<td></td>
</tr>
<tr>
<td>(3) 3/20 APT Attack (Ministry of Science, ICT &amp; Future Planning, 2013; Shin et al., 2013)</td>
<td>● Mar. 20~26, 2013</td>
<td>● 6 Orgs. (3 broadcasters, 3 banks) in South Korea</td>
<td></td>
</tr>
<tr>
<td>(4) Iran Stuxnet Attack (Zetter, 2011)</td>
<td>● Around Sep.~ June 24th, 2012 (Auto-destruction)</td>
<td>● Natanz Nuclear Facility in Iran (Germany Siemens’ SCADA system)</td>
<td></td>
</tr>
<tr>
<td>(5) 7/7 DDoS Attack (National Police Agency, 2009)</td>
<td>● Jul. 7 (18:00)~10 (18:00), 2009</td>
<td>● 14 US government organizations</td>
<td></td>
</tr>
<tr>
<td>(7) Estonia DDoS Attack (Tikk et al., 2010, pp.14-34)</td>
<td>● Apr. 27~May.19, 2007</td>
<td>● Homepage of government organizations including the presidential office and others in Georgia</td>
<td></td>
</tr>
</tbody>
</table>
Layers of Origin

A Process of Victim Initiated Reporting Procedure about Responsible Origins

- **Individual Layer**
  - [Identify who attacked me. Let the Innocent Origin Server prevent the attacks]

- **Server Layer**
  - [Identify which server attacked me. Let the innocent Owing Company prevent the attacks]

- **Company Layer**
  - [Identify which company attacked me. Let Government prevent the attacks]

- **Country Layer**
  - [Identify which country attacked me. Let BIGG (Global Governance) prevent the attacks]
Internet Peace Principles
against State-led Cyberattacks

Bright Internet

(1) Origin Responsibility
(2) Deliverer Responsibility
(3) Identifiable Anonymity
(4) Global Collaborative Search
(5) Privacy Protection
(6) Internet Peace

National Policies and Global Governance
Bright Internet Protocols and Technologies

Extension to Cyberspace
- UN Charter
- Responsibility of States
- Geneva IV Convention

Specialization

Expansion to Global Members
- UN GGE
- Tallinn Manual
- CECC

Generalization

Analogical International Norms
- Outer Space Treaty
- Non-Proliferation Treaty of Nuclear Weapons

Similarity
Analogical Reasoning
Internet Peace Principles and Justifications

- All states should maintain international peace and security in cyber space.
  - UN Charter: Specialization to Cyber Space
  - UN Group of Governmental Experts: Generalize to all countries

- States should not knowingly allow their territory to be used for internationally wrongful act using ICTs including the breaching of Principles of Origin Responsibility, Deliverer Responsibility, and Privacy Protection.
  - Responsibility of States: Specialization to Cyber Space with the Bright Internet Principles

- Prohibit preemptive cyberattacks against critical infrastructure including nuclear power plants, innocent civilians and their facilities in cyberspace
  - Geneva Convention: Specialization to Cyber Space
Internet Peace Principles

- All states should maintain international peace and security in cyber space.

- States should not knowingly allow their territory to be used for internationally wrongful act using ICTs including the breaching of Principles of Origin Responsibility, Deliverer Responsibility, and Privacy Protection.

- Prohibit preemptive cyberattacks against critical infrastructure including nuclear power plants, innocent civilians and their facilities in cyberspace.

- Prohibit the use of State-led Cyberattacks except for legitimate self-defence and countermeasure purposes.

- States should cooperate to exchange information to assist each other and to prosecute terrorist and criminal use of Internet including the identification of real name upon the issuance of valid search warrant.

- Offending state should be held responsible for the consequence of its cyberattacks.

- Attacked state is entitled to request compensation and take legitimate self-defence and countermeasures.

- An international governance body like Bright Internet Global Governance is necessary to conduct research and verification of Bright Internet and Internet Peace Principles.

- UN may take effective collective measures for the prevention and removal of cyber security threat and for the suppression of cyberattacks considering cyber blockade.
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
  - Origin Responsibility
  - Bright Cloud: Bright Internet Based Cloud Services
- Road Map Ahead
Applications of the Bright Internet: Example of the Bright Cloud

Goals
- Preventive Security
- Freedom of Expression
- Privacy

Principles
- Origin Responsibility
- Deliverer Responsibility
- Identifiable Anonymity
- Global Collaborative Search
- Privacy Protection

Solutions
- Technology (Protocol and Standards)
- Policies (Legislation)
- Global Collaboration (Governance)

Applications
- Bright Internet Solutions
- Bright Cloud
- Bright E-mail
- Bright E-Commerce
- Bright IoT
- Prevent Cyberbullying
- National Security
- Cyber Addiction
Can the Bright Cloud be a Business Model?

Professor Jae Kyu Lee (KAIST, Carnegie Mellon University and Xian Jiaotong University)

Abstract: The Bright Internet aims a safer Internet platform where the origination of malicious behaviors can be deterred because their origins can be identified. As such, the primary goal of the Bright Internet is the establishment of Preventive Security paradigm in contrast with the current paradigm of protective security of its own system. The current cloud computing service providers have no choice but to adopt the protective security paradigm. In this talk, the benefit of adopting the Bright Internet platform will be presented in the cloud service provisioning. A question is how to motivate the individual Cloud Service Providers (CSPs) to adopt the Bright Internet platform. For this purposes, we analyze the benefits of adopting the Bright Internet platform in terms of marketing, economy, and compliance to regulation.
Number of PSBL IP Address in Cloud

Absolute Numbers

<table>
<thead>
<tr>
<th>Provider</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>77.4</td>
<td>13.9</td>
</tr>
<tr>
<td>Google</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Microsoft</td>
<td>106.4</td>
<td>36.5</td>
</tr>
</tbody>
</table>

Percentage

<table>
<thead>
<tr>
<th>Provider</th>
<th>Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>0.033%</td>
<td>0.012%</td>
</tr>
<tr>
<td>Google</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>0.047%</td>
<td>0.023%</td>
</tr>
</tbody>
</table>
Lifetime of IP Addresses of PSBL

◆ PSBL IP Address Lifetime:
  - Average 1 Week
  - Maximum 2 weeks

◆ One Day Wonders:
  - 71% of Web sites exist less than 24 hours

=> What is happening in Cloud Services Providers?
Risk of Outbound Spam to CSPs

- Do sending spam mails means revenue?

- What if stolen cards are used (MailChannels)

Legal responsibility of CSP as unwitting or willfully negligent accomplice

- Importance of fraud detection for sustainability (Scrpati)
Business Models of Bright Cloud

**Market Advantage**
- Cost\_i (Filtering) < Benefit\_i (Marketing)
- Enablers
  - Disclosure of Origin information
  - Certification of origin responsibility (Bright Internet)
  - Collective Damage Claims on behalf of clients

**Compliance Advantage: Ready to regulation**
- Not satisfied for most \( i \), Cost\_i (Filtering) < Benefit\_i (Marketing)
- But \( \Sigma \) Cost\_i (Filtering) < \( \Sigma \) Social Benefit\_j (Marketing)

**Economic Advantage: Demarketing**
- Eliminate harmful and criminal customers: Reduce risk
Bright Cloud: Business Model

A Cloud Service Provider Perspective

Bright Cloud Service Platform

Server A

Internal Incoming (Origin)

Internal Outgoing (Destination)

External Outgoing (Destination)

External Incoming (Origin)

Type II: Reduced Risk from Trustful Origins
Type IO: Business Creation with Higher Trust
Type EI: Higher Protective Model due to Black List Management
Type EO: Business Creation with Higher Trust
Bright Cloud – Origin Responsibility Principle
System Architecture

Victim’s reports

Traceability
Identifiability

Bright Cloud A

Inbound Filtering MDS

Outbound Filtering

Reverse MDS
Bright Cloud Extended Network Model

- **Bright Cloud Service A**
  - Server A
  - **II**: Internal Incoming (Origin)
  - **IO**: Internal Outgoing (Destination)

- **Bright Cloud Service B**
  - **EI**: Virtually Internal Incoming (Origin)
  - **EO**: External Outgoing (Destination)

- **External**
  - **EI**: External Incoming (Origin)
  - **EO**: External Outgoing (Destination)

- **VPN**
Bright Cloud Extended Network: System Architecture

- Bright Cloud A
  - Inbound Filtering MDS
  - Reverse MDS
- Bright Cloud B
  - B
- Bright Cloud C
  - C
- Bright Cloud D
  - D

Victim’s reports

Traceability
Identifiability
Bright Cloud Extended Network: Shared Blacklist via Block Chain Technology

- Inbound Filtering MDS
- Outbound Filtering
- Reverse MDS
- Victim’s reports
- Traceability
- Identifiability

Bright Cloud A

Bright Cloud B

Bright Cloud B

Bright Cloud D
Bright Cloud Extended Network with Shared Blacklist in Block Chain

- Inbound Filtering MDS
- Outbound Filtering
- Reverse MDS

VPNs

Block Chain

Bright Cloud A

Bright Cloud B

Bright Cloud B

Bright Cloud D

Victim’s reports

Traceability
Identifiability
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
  - Origin Responsibility
    - Bright Cloud: Bright Internet Based Cloud Services
  - Deliverer Responsibility
- Road Map Ahead
Goal Driven Principles & Prescriptive Design

Goals
- Preventive Security
- Freedom of Expression
- Privacy

Principles
- Origin Responsibility
- Deliverer Responsibility
- Identifiable Anonymity
- Global Collaborative Search
- Privacy Protection

Solutions
- Technology (Protocol and Standards)
- Policies (Legislation)
- Global Collaboration (Governance)

Applications
- Bright Internet Solutions
- Bright Cloud
- Bright E-mail
- Bright E-Commerce
- Bright IoT
- Prevent Cyberbullying
- National Security
<table>
<thead>
<tr>
<th>Cases</th>
<th>Origins</th>
<th>Paths*</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Korea Hydro &amp; Nuclear Power Co., Ltd.</td>
<td>25 North Korean IPs →</td>
<td>North Korean ISP(SJV**) → South Korean ISP → South Korean VPN (use other’s name) →</td>
<td>Nuclear Power Plant (Log record was confirmed)</td>
</tr>
<tr>
<td>(2014~5)</td>
<td>Five IPs of North Korean Post and Telco (KPTC) located in Beijing China</td>
<td>Chinese ISP → South Korean ISP → South Korea VPN (North Korean IP was found on a South Korean VPN) →</td>
<td>Nuclear Power Plant (Log record was confirmed)</td>
</tr>
<tr>
<td></td>
<td>IP(s) from Shenyang, China (175.167.xxx.xxx) →</td>
<td>Chinese ISP → ISPs in US, China, Japan, Thailand, The Netherlands → South Korean ISP → South Korean VPN →</td>
<td>Collected information from a retiree community</td>
</tr>
<tr>
<td></td>
<td>Russian IP (Vladivostok) →</td>
<td>Russian ISP → South Korean ISP →</td>
<td>→ Sent phishing emails to retired employees</td>
</tr>
<tr>
<td></td>
<td>North Korean IP →</td>
<td>→ North Korean ISP (SJV) → US ISP → US VPN (Peters, 2014) →</td>
<td>→ Collected and leaked information from the affiliated companies</td>
</tr>
<tr>
<td>(2) Sony Pictures Entertainment Hacking</td>
<td>North Korean IP →</td>
<td>→ North Korean ISP (SJV) → US ISP →</td>
<td>→ Threatened five times by blackmail to ask for the money and to reveal the leaked information to the public through Naver, Twitter, and other routes.</td>
</tr>
<tr>
<td>(2014)</td>
<td></td>
<td>US VPN (Peters, 2014) →</td>
<td>→ Leaked the blue prints of nuclear power plant and exposed through the Twitter that was used by North Korean Hacker, and asked for the money</td>
</tr>
</tbody>
</table>

Table 2: Origins, Paths, and Targets of State-led Cyber Attacks
Principle 2a: Deliverer Responsibility

- Should the OS providers of compromised computers and network make effort to prevent not being abused?
  - Yes
  - No

Principle of Deliverer Responsibility (Zombie Perspective)

The Principle of Deliverer Responsibility means that the individuals or service providers who are involved in the delivery of cyber-attacks intentionally or unintentionally in the routing process of Internet should do their best to prevent the delivery of damages to the users at destination.

TD1: Design of Zombie Based Prevention System

  ** Qihoo 360, Microsoft
Principle 2b: Deliverer Responsibility (ISP)

- Top 10 ISP delivers 85% of spam mails
- Should the security agent filter obvious criminal codes on ISP?
  - Yes
  - No

**Principle of Deliverer Responsibility (ISP Perspective)**

**TD2:** Design the Intermediator based Surveillance System

**TD2a:** Design the Target of Surveillance by Intermediator

- MDS-ISP Version ; Telco Version
- Blacklist Management Extended Version

AIS Grand Vision Project of ICT-enabled Bright Society

Background of the Bright Internet

Research Framework

Design Principles for the Bright Internet
- Origin Responsibility
  - Bright Cloud: Bright Internet Based Cloud Services
- Deliverer Responsibility
- Identifiable Anonymity

Road Map Ahead
Goal Driven Principles & Prescriptive Design

Goals
- Preventive Security
- Freedom of Expression
- Privacy

Principles
- Origin Responsibility
- Deliverer Responsibility
- Identifiable Anonymity
- Global Collaborative Search
- Privacy Protection

Solutions
- Technology (Protocol and Standards)
- Policies (Legislation)
- Global Collaboration (Governance)

Applications
- Bright Internet Solutions
- Bright Cloud
- Bright E-mail
- Bright E-Commerce
- Bright IoT
- Prevent Cyberbullying
- National Security
Deployment Model I: Overlaid Approach

Bright Internet

Traditional Internet

Time
Deployment Model II: Two Accounts Approach

- Bright Internet
- Traditional Internet
- Anonymous Freedom of Expression Space

Time
Architecture of Identifiable Anonymity

Freedom of Expression Layer

Preventive Security Layer

- Real Name Request only by Search Warrant

a Priori (Direct) vs. a Posteriori Identification (Indirect)
Technologies for Identifiable Anonymity

**TI1: Architecture for Identifiable Anonymity**
- Two Layered Architecture
- Two Accounts Approach

**TI2: Methods for Real Name Identification**
- Pure Real Name
- A Priori Registration of Real Names
- A Posteriori Registration of Real Names

**TI3: Digital Search Warrant Management System: Real Time**
- Application, issuance, execution, and reporting
Two Principles Skipped Here

Goals

Preventive Security
Freedom of Expression
Privacy

Principles

Origin Responsibility
Deliverer Responsibility
Identifiable Anonymity
Global Collaborative Search
Privacy Protection

Solutions

Technology (Protocol and Standards)

Policies (Legislation)

Global Collaboration (Governance)

Applications

Bright Internet Solutions
Bright Cloud
Bright E-mail
Bright E-Commerce
Bright IoT
Prevent Cyberbullying
National Security
Agenda

- AIS Grand Vision Project of ICT-enabled Bright Society
- Background of the Bright Internet
- Research Framework
- Design Principles for the Bright Internet
  - Origin Responsibility
    - Bright Cloud: Bright Internet Based Cloud Services
  - Deliverer Responsibility
  - Identifiable Anonymity
- Road Map Ahead
The Bright Internet Road Map

1. Social Needs
   - Social Norm
2. Bright Internet Principles
3. Bright Internet Policy
4. Bright Internet Technologies
5. Bright Internet Business Models
6. Global Collaboration Models
7. Bright Internet Standards and Test Bed
8. Bright Internet Global Summit
9. Bright Internet Global Governance

Research → Implementation
AIS Initiated Global Summit on the Bright Internet

- Global Research Partnership: KAIST, Xi’an Jiaotong U., CMU

Constituents

- Internet related global organizations: UN ITU, ICANN, IETF, IGF, UN GGE
- Research Groups: Universities, Research Institutes
- Governments Agencies
- Private Companies

Meeting Schedule as a Pre-Conference of ICIS

- ICIS 2017 in Seoul (December 2017)
- ICIS 2018 in San Francisco; ICIS 2019 in Munchen
Planning the Bright Internet Research Project with Global Research Partnership

- Social Needs and Social Norm of the Bright Internet
  - Survey on Netizens’ Perception, Responsibility Index

- Technology and Protocol of the Bright Internet
  - Prototype, Standardization, Simulation, and Test Bed

- Policy and Global Governance
  - Act of Preventive Cyber Crime; Act of Preventive Cyber Terrorism
  - Global organizations: IGF, UN ITU, ICANN, IETF, etc.

- Applications by Business Models
  - Bright Cloud Computing, Bright IoT, Bright eCommerce,
  - Transition to Next Generation Internet Platform