Security FIRST

- International Cooperation in Cyber Security -

2015.06.13. FIRST

School of Information Security, Korea University
former Special Adviser to the President for National Security

Lim, Jong In

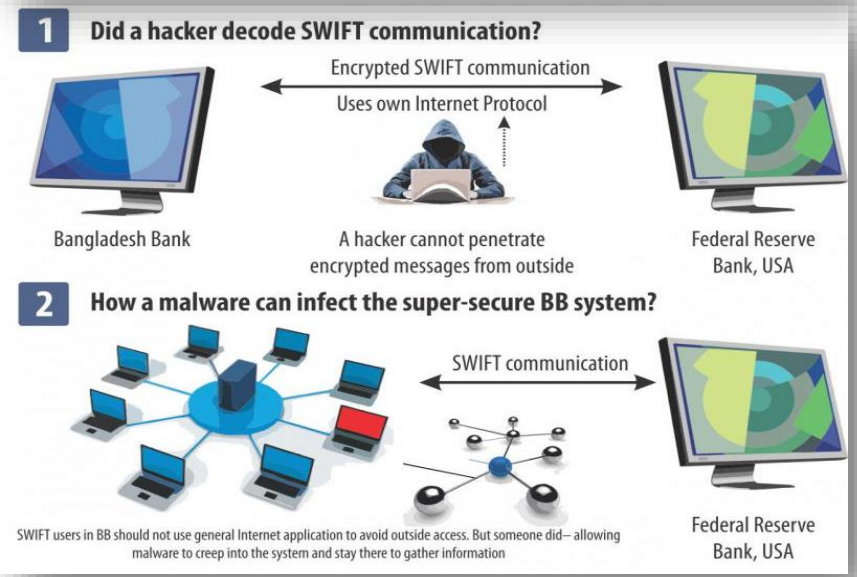
Recent Issues – SWIFT Hacking

- $81 million dollar deposit was stolen via a forged message instructing that some of the Bangladesh Central Bank's deposit in the Federal Reserve Bank of New York should be transferred

The New York Times

Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million

By RICK GLADSTONE MARCH 15, 2016



Bangladesh Cyber Theft

- Feb. 2016. Hackers stole $81 million from the Bangladesh Central Bank's official account at the Federal Reserve Bank of New York
- New York Fed announced that the transfer of the money had been "fully authenticated" by SWIFT(international financial messaging system)
- Bangladesh's central bank was vulnerable to hackers because it did not have a firewall and used second-hand, $10 switches for network computers connected to SWIFT

Source : NYT, Reuter

Recent Issues – SWIFT Hacking

- There were SWIFT hacking attempts against 8 banks besides Bangladesh Central Bank. The incident is believed to be the work of North Korean hackers, judging from the similarity of the malicious code to that in the Sony Pictures hacking incident.


The New York Times

North Korea Linked to Digital Attacks on Global Banks

By NICOLE PERLROTH and MICHAEL CORKERY MAY 26, 2016

2013.06. Journals in Korea | 2014.11. Sony Pictures | 2015.12. Vietnam Bank | 2016.02. Bangladesh Bank

Similarities in File Deletion Function

Continuous hacking attempts against SWIFT and assumed mastermind

- According to the malicious code analysis by IssueMakersLab in Korea, the file deletion function codes of the following malicious codes are similar, making us assume that the attacks were launched by the same group:
  - February 2016 :Bangladesh Central Bank
  - December 2015 : Vietnam's Commercial Bank
  - November 2014 : Sony Pictures
  - June 2013: Press in Korea
- Since the analysis results of Symantec also show high similarity to the Sony Pictures malicious code, North Korea is assumed to be the mastermind

Recent Issues - Ransomware

- **Korea is experiencing a social problem due to the spread of ransomware that exploits the vulnerability of major online community advertising banners**

SimilarWeb

Website Ranking

Top 50 sites in Korea, Republic Of for all categories

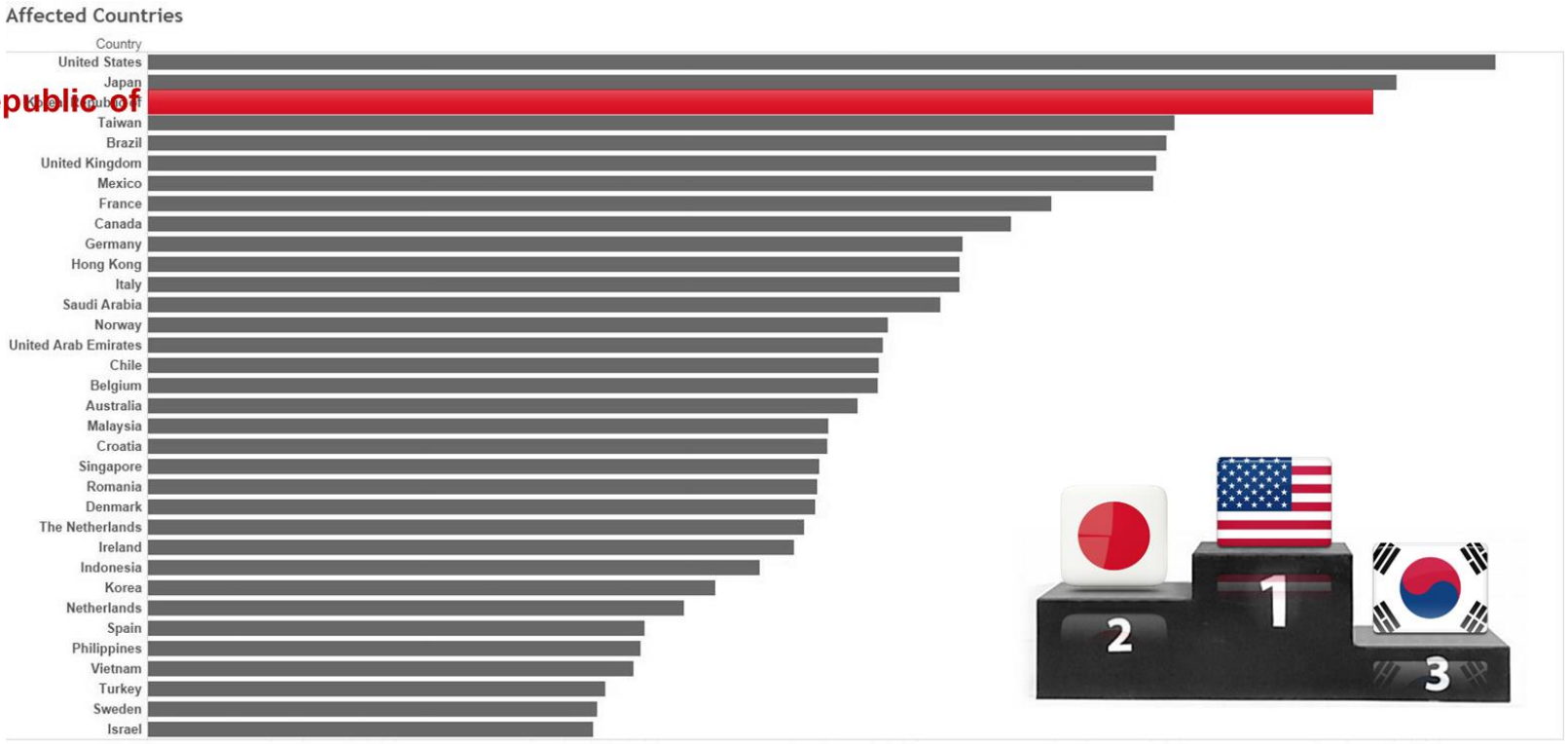
Rank	Website	Category
1	naver.com	News and Media
2	google.co.kr	Internet and Telecom > Search Engine
3	daum.net	Internet and Telecom
4	youtube.com	Arts and Entertainment > TV and Video
5	google.com	Internet and Telecom > Search Engine
6	facebook.com	Internet and Telecom > Social Network
7	news.naver.com	News and Media
8	tistory.com	Internet and Telecom
9	donga.com	News and Media
10	dcinside.com	News and Media > Magazines and E Zines
11	twitter.com	Internet and Telecom > Social Network
12	ppomppu.co.kr	Internet and Telecom
13	clien.net	Computer and Electronics
14	instagram.com	Internet and Telecom > Social Network

Spread of ransomware targeting online communities in Korea

- **Distributing ransomware among major online communities in Korea**
  - **Crypt0L0cker randomware was distributed on Clien.net in April 2015**
  - **UltraCrypter randomware was distributed on PPOMPPU.co.kr in June 2016**
- **Both sites are representative online communities in Korea (ranked 12th and 13th in web traffic volume), and several hundred million worth of damages were reported**
- **Both malicious codes require BitCoin deposit, and it is difficult to respond due to difficulty in tracing back**
- **Since BitCoin deposit is not confirmed for UltraCrypter, recovery is expected to be impossible**

Recent Issues - Ransomware

- Korea is the third affected countries of the LOCKY ransomware



Source : FireEye

Recent Issues – Sony Pictures

- **Sony Pictures Entertainment was hacked before its release of 'The Interview', a movie that plans to assassinate North Korea's leader**

Overview of the Sony Pictures Hacking

- Sony Pictures Entertainment's internal system was breached and some of its data was leaked in November, 2014.
- Leaked data includes, among others:
  - personal information of employees
  - e-mails among employees
  - information on executive salaries
  - copies of unreleased Sony films
- The hackers called themselves the "Guardians of Peace" and demanded the planned release of the film 'The Interview', a comedy on a plot to assassinate North Korean leader Kim Jong-un, be cancelled

Recent Issues – Sony Pictures

- The U.S. attributed the Sony Picture hack to North Korea, calling it 'Cyber Vandalism,' and took a series of actions in response

U.S. Government's Reaction

- On December 19th, 2014, F.B.I. published an investigative report on the hack, in which it identified North Korea as the perpetrator
- President Obama called the hack 'Cyber Vandalism' and claimed that the U.S. weighed proportionate response to the attack
- North Korean websites were shut down, allegedly by cyber attacks orchestrated by the U.S.
- President Obama sanctioned North Korea's Directorate of Reconnaissance

THE WALL STREET JOURNAL.

U.S. NEWS

Updated Dec. 19, 2014 1:03 p.m. ET

FBI Says North Korea Behind Sony Hack

U.S. Considering Steps to Take in Response, But 'There Are Few Good Options'

The Washington Post

Post Politics

Obama: North Korea hack 'cyber-vandalism,' not 'act of war'

By Sean Sullivan December 21, 2014 Follow @WaPoSean

abcNEWS HOME | VIDEO | U.S. | WORLD | POLITICS | ENTERTAINMENT

President Obama Sanctions North Korea After Sony Cyberattack

HONOLULU — Jan 2, 2015, 4:11 PM ET

DEVIN DWYER

The Washington Post

Asia & Pacific

North Korea slams U.S. over Internet shutdown, calls Obama a 'monkey'

By Simon Denyer December 27, 2014 Follow @simondenyer

Recent Issues – KHNP

- Korea Hydro & Nuclear Power(KHNP) was threatened to be destroyed by a hacker who claimed to have hacked its control system

KHNP Hacking Overview

- In December 2014, a hacker who claimed to be against nuclear power development posted some of KHNP's confidential data on his internet blog
- The hacker claimed that he had breached into KHNP's internal control system and threatened that he would destroy KHNP's nuclear power plants unless it shut them down itself
- Investigation by South Korean government and KHNP found no evidence of intrusion into KHNP's control system. There has not been any cyber attack on the Nuclear Power plant thereafter

theguardian

South Korean nuclear operator hacked amid cyber-attack fears

Operator begins two-day exercise after suspected hacker tweets information on KHNP plants and its staff

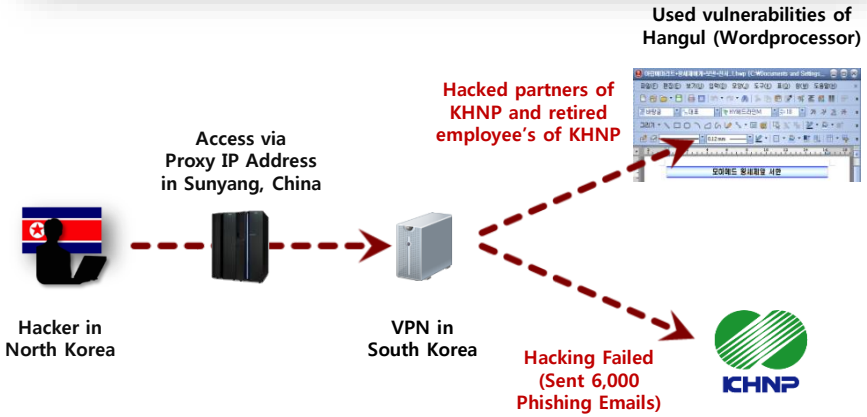
Justin McCurry in Tokyo and agencies Tuesday 23 December 2014 05.14 GMT

Recent Issues – KHNP

- South Korean government's investigation unit alleged North Korea of having perpetrated the hack with a Chinese IP address

South Korean Government's Reaction

- On December 20th, 2014, a government team was assembled to probe into the hack
- The team found that the hacker had accessed VPN in South Korea via proxy IP address in Shenyang, China. Having failed to hack KHNP directly, the hacker sent phishing emails to partners of KHNP and retired employees
- On December 24th, 2014, the investigation team requested cooperation from the Chinese Police
- On March 17th, 2015, the government team presented an interim probe result, which suggested that North Korea had orchestrated the hack



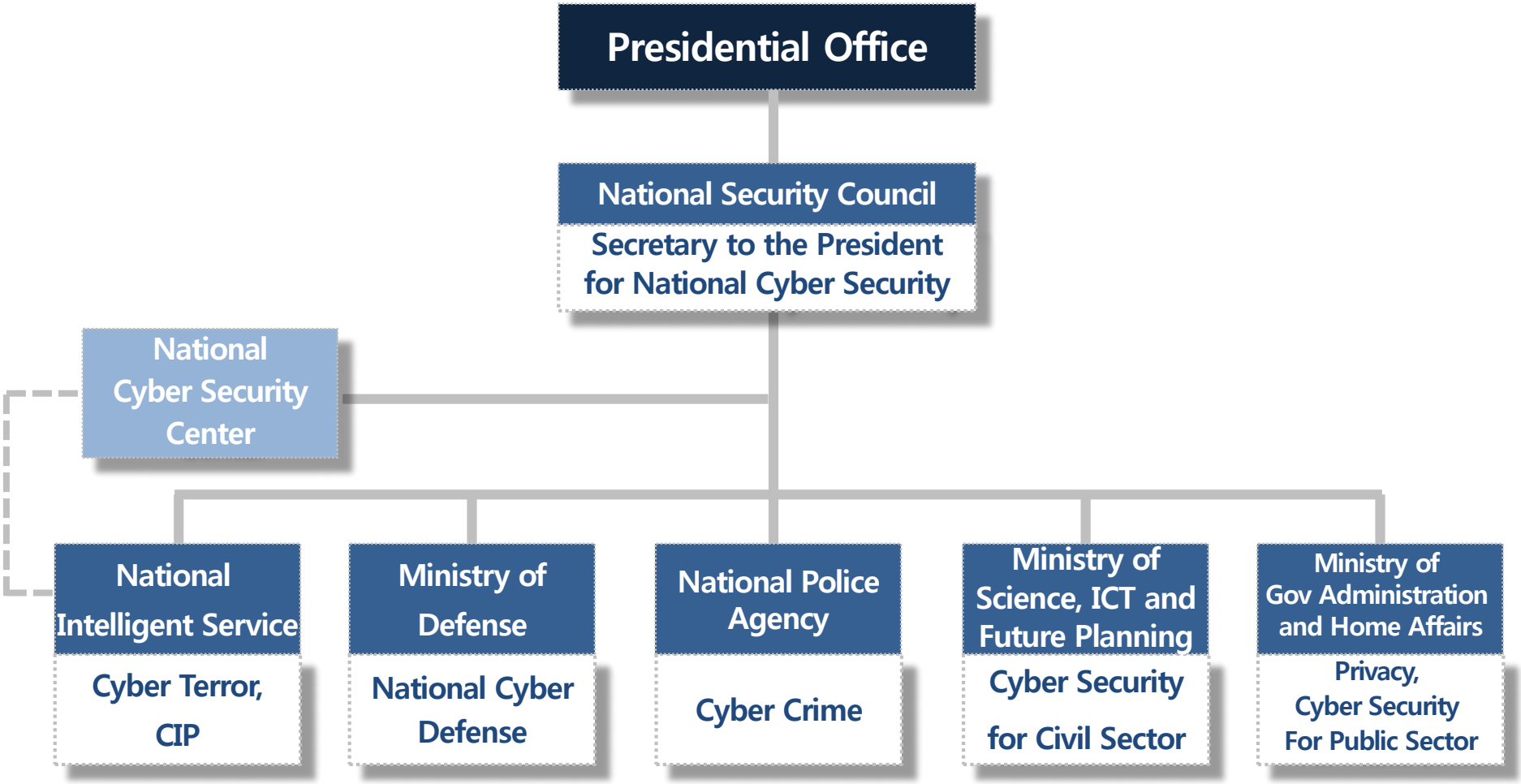
Case of South Korea - Cyber Threats that S.Korea faces

South Korea has had numerous cyber attacks since 2009, but failed to identify and prosecute suspects for any of the attacks

Year	Cyber attacks on S.Korea
2003	• 1.25 Internet Intrusion : Korea's major internet networks went down due to the Slammer Worm taking advantage of vulnerabilities of Microsoft's SQL servers
2009	• 7.7 DDoS Attack : Three DDoS attacks from July 7th to 10th paralyzed the major government sites including website of the Presidential Office
2010 ~ 2012	• GPS Disturbance : From 2010 to 2012, GPS disturbance occurred annually, causing signal interference and damage to GPS receivers in private and military sectors, including those in Korea Telecom's base stations
2011	• 3.4 DDoS Attack : DDoS attacks on 40 local websites, including those of major portals, government offices, the Ministry of National Defense and financial institutions
2011	• NH Bank's Cyber Terror : NH Bank's internal data and server system were damaged. Service access paralyzed entirely or partially
2013	• 3.20 Cyber Terror : Major local broadcasters' and six financial institutions' computer networks went down
2013	• 6.25 Cyber Terror : The Presidential Office website, major government websites, media and political parties' websites were under cyber attacks
2014	• Hacking on KHNP : KHNP's blueprints and operating methods for nuclear power stations were leaked on the internet

Case of South Korea – Countering Cyber Threats

- South Korea established a comprehensive national system to counter cyber threats, controlled and coordinated by the Presidential Office



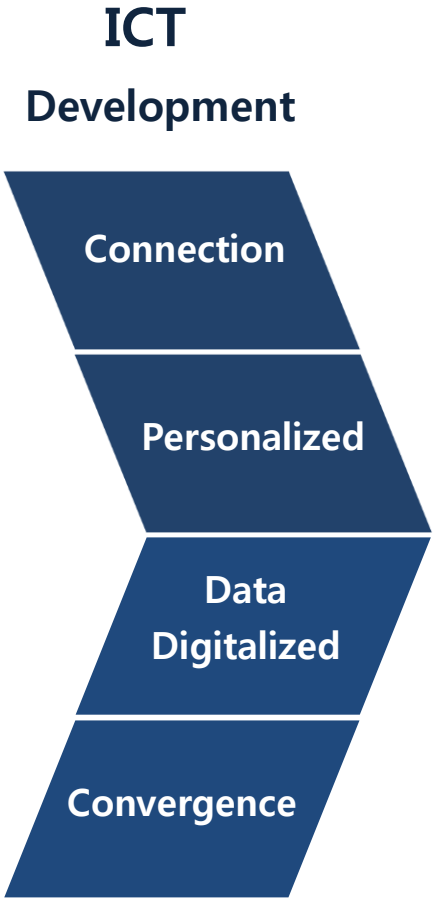
Case of South Korea – Countering Cyber Threats

- **While receiving cyber attacks continuously, the Korean government is endeavoring to strengthen national cyber security continuously by setting up strategies and plans to respond to such cyber attacks**

Mid-term comprehensive information security plan (2008)	• Recognized the necessity of responding to information security issues including personal information protection due to the Auction hacking incident in 2008 • Aimed to establish a social safety network by improving policies and building infrastructure by 2010
Comprehensive measures against the national cyber crisis (2009)	• It was recognized that a cyber attack can threaten national security due to the 7.7 DDoS attack in 2009 • Obtained good results, such as establishment of the cyber security government system and definition of roles and responsibilities by department
National cyber security master plan (2011)	• Recognized the necessity of an effective response method due to the 3.4 DDoS Incident and Nonghyup Computer Problems in 2011 • Obtained good results, such as awareness improvement, outsourcing company management, and implementation of the S/W security vulnerability diagnosis system
Comprehensive national cyber security measures (2013)	• Recognized the necessity of integrating cyber capabilities distributed among government departments due to the 3.20 and 6.25 Cyber Terror • Established the organizational structure (the Blue House plays the role of control tower, and the National Intelligence Service supervises hands-on work) and prepared personnel fostering plans
National cyber security posture and capability strengthening plan (2015)	• Recognized the necessity of protecting cyberspace safely following the Korea Hydro & Nuclear Power hacking incident • Strengthened the cyber security control tower function of the National Security Office, newly established a dedicated pan-government cyber security organization

ICT Development and Evolving Cyber Threats

- As ICT development begets new technologies such as IoT, Big Data, and Cloud Computing



IoT

- Network of physical objects or "things" embedded in electronics, software, sensors and connectivity
- 26 billion devices on the IoT by 2020 (Gartner)
- Wearable Devices, Smart Car, etc.

Cloud Computing

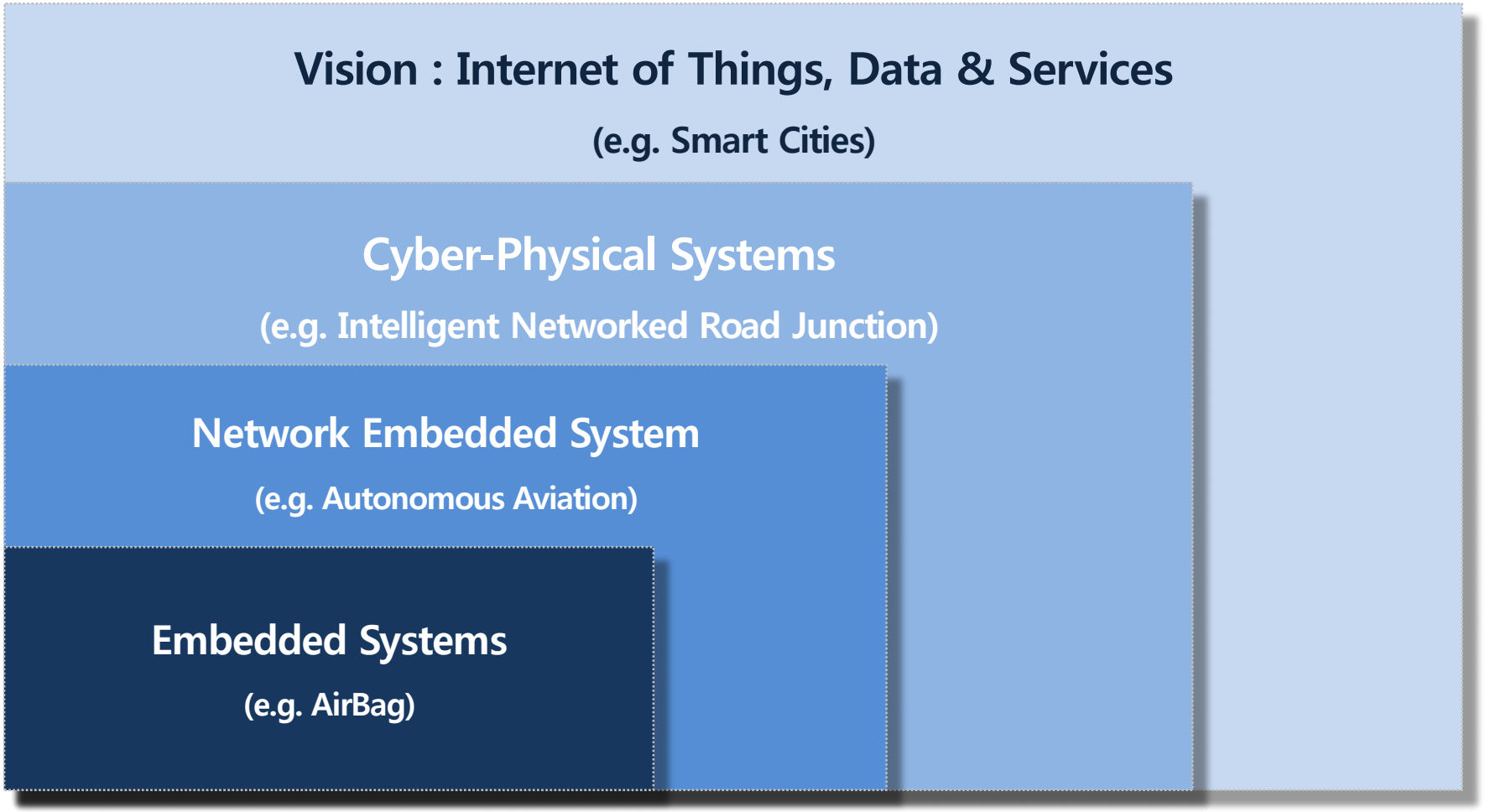
- Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources
- IaaS(Infra), PaaS(Platform), SaaS(Service)

Big Data

- High volume, high velocity, high variety information assets that require new forms of processing to make more meaningful information
- Data Volume : 2.7 ZB (2012) → 7.9 ZB (2015)

ICT Development and Evolving Cyber Threats

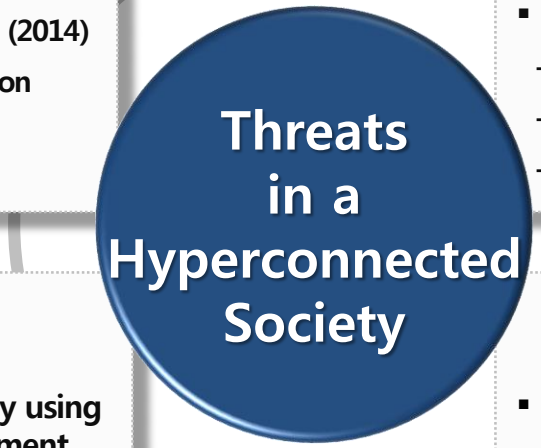
- European Commission's Next Generation Computing predicts that ICT will evolve to IoT Environment through Embedded system and CPS



Source : NGC Study, 2013, EUTEMA

ICT Development and Evolving Cyber Threats

- **In a hyperconnected society where various new ICT applications are adopted, threats to the new applications are anticipated**



Smart Home Appliance

- ICT added home appliances for remote control and efficiency, and convenience
- Hacked or Demonstrated Cases
  - Refrigerator hacked to send spam emails (2014)
  - Philips LED Lighting hacking demonstration (Dhanjani, 2013)
  - Web Camera Exposed (BBC, 2014)

Smart Car

- IT component and services are integrated into automobiles for information gathering and remote control
- Hacked or Demonstrated Cases
  - U.S. Embedded Security Center Demonstration (2010)
  - Korea University Demonstration (2012)
  - BlackHat USA Demonstration (2014)

Smart Healthcare

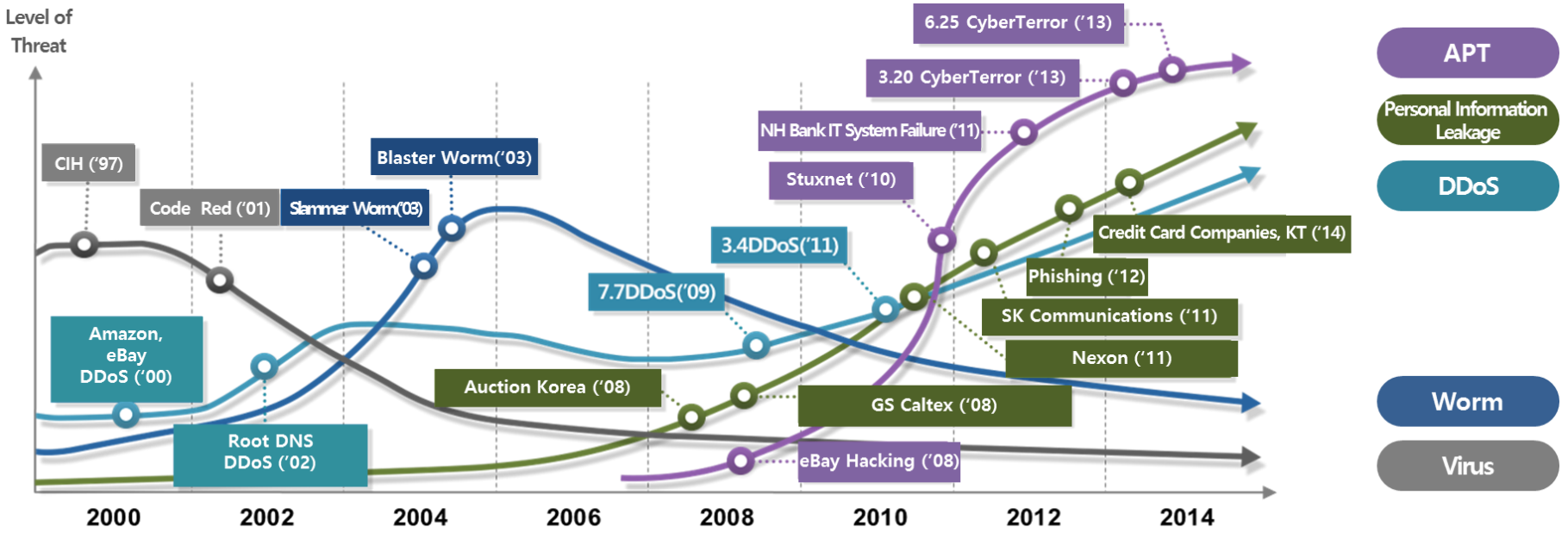
- Using body-measured information by using wearable devices and medical equipment
- Hacked or Demonstrated Cases
  - Breakpoint Security Conference, Pacemaker Hacking Demonstration (2012)
  - BlackHat USA, Insulin Pump Hacking Demonstration (2013)

Smart Energy

- Increasing energy efficiency by managing information such as SmartGrid, Smart Buildings
- Hacked or Demonstrated Cases
  - Puerto Rico SmartMeter Tempering (2009)
  - 'Dragonfly' Backdoors in U.S. and Europe Power Grid Control Systems (2014)

Cyber Threat Trends

- Cyber threat is becoming more intentional, destructive, targeted, and external in origin



Accidental	⟷	Intentional
Failure	⟷	Attack
Random	⟷	Targeted
Internal Origin	⟷	External Origin
Technical	⟷	Human

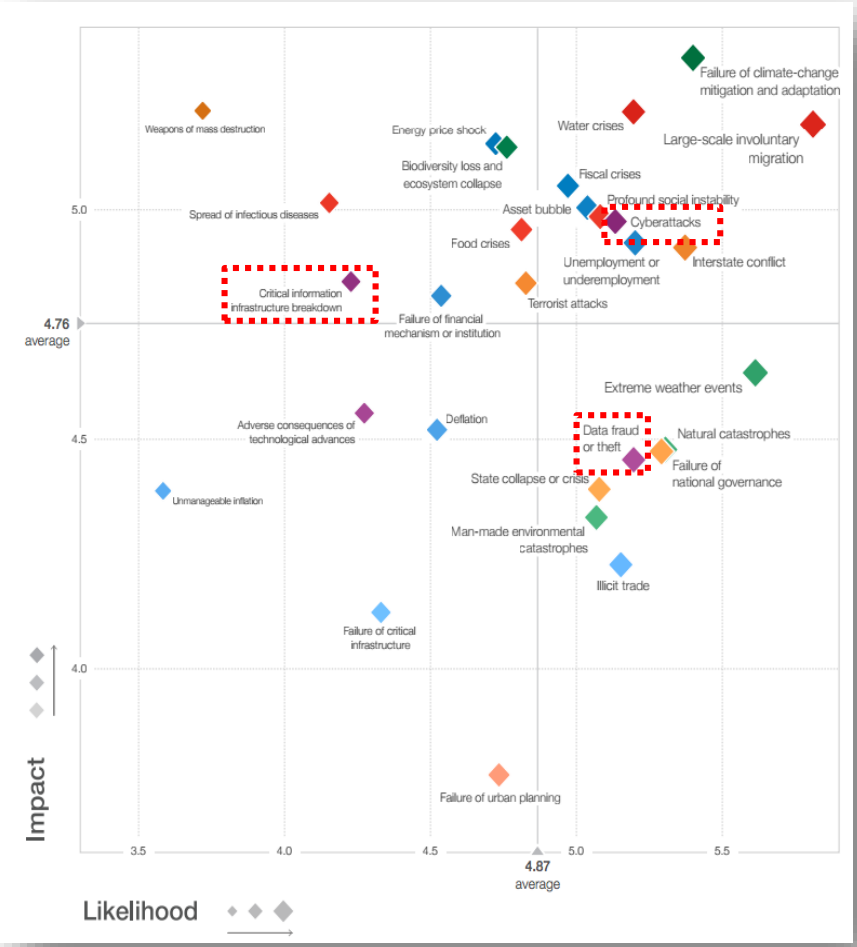
Source : Korea Internet & Security Agency

Cyber Threat Trends

- Cyber-related threats are selected as a high-priority risk factor in the “Global Risks Report 2016” published by the World Economic Forum (World Risk) in Jan., 2016

Global Risk Report 2016

- About 750 experts in each area selected global risks that can affect the world economy based on likelihood and impact
- Among the 29 global risks presented, technological threats include adverse consequences of technological advancement, breakdown of critical information infrastructure, cyber attacks, and data fraud and theft
- As dependency on cyber increases, the likelihood and impact of risk related to cyber were rated significantly high; risk connectivity and mutual impact with other major threats were rated highly as well
- The evaluation suggests that cyber attacks can affect the economy considerably, and that the financial industry is required to have the response capability and level matching the risk level



Source : World Economic Forum

International Cooperation

- International cooperation ha are being developed, yet the outcome of cooperation is insufficient to countering cyber threats

Bilateral Cooperation

- Cooperation between two States that have common interests
  e.g.) US – China Cyber Working Group

Regional Cooperation

- Cooperation among States in the region
  e.g.) ASEAN Regional Forum

International Cooperation

- Cooperation through International Organizations e.g.) UN GGE
- Conventions, Treaties or Laws e.g.) Convention on Cybercrime

Military Aspect Cooperation

- Cooperation in Military or National Defense Aspects
  e.g.) NATO Cooperative Cyber Defense Centre of Excellence
  EU Cyber Defence Policy Framework
  ANZUS Treaty applies to Cyber attacks
  China - Russia Non Aggression Pact for Cyberspace

International Cooperation

- **Budapest Convention on Cybercrime came into force in 2001, which includes substantial/procedural articles of cybercrime regulation and international cooperation procedure**

< Major Implications>

- **The First legally-binding international instrument to comprehensively address the cybercrime issues**
- **Scope of the Convention**

- Criminalising Conduct

: Illegal Activities / Fraud / Interference / Child Pornography / etc.

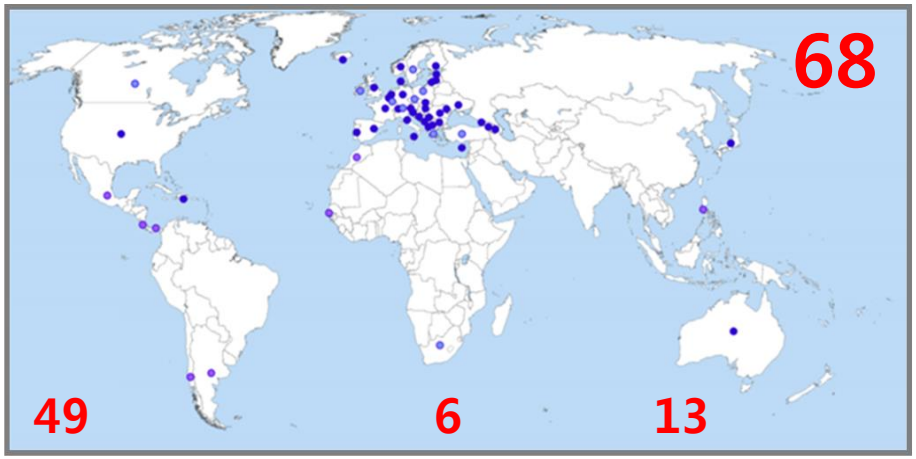
- Procedural tools

: Preservation / Search and Seizure / Interception of Data

- International Cooperation

: Mutual Legal Assistance Treaties, Point of Contact

< Status as of May, 2016 >



Ratified / Acceded		Signed	Invited to Accede	
- 20 European	- 19 European	- Andora	- Russia	- Morocco
- Australia	- Domician Rep.	- Greece	- San Marino	- Paraguay
- Canada	- Mauritius	- Ireland	- Argentina	- Peru
- Japan	- Panama	- Monaco	- Chile	- Philippines
- Sri Lanka	- Liechtenstein	- Sweden	- Costa Rica	- Senegal
- United States		- South Africa	- Mexico	- Tongo
- Israel			- Colombia	

International Cooperation

- Seoul Framework on 'Seoul Conference on Cyberspace 2013', UN GGE Recommendations & Reports can be the base of international cooperation

< Seoul Framework >

- **Cyberspace**
  - Economic Growth, Social and Cultural Benefits
- **International Security**
  - Promote voluntary confidence-building and transparency measures
- **Cybercrime**
  - Law enforcement cooperation in the investigation and prosecution of international cases
- **Capacity Building**
  - Enhance efforts to close the digital divide

< UN GGE Report A/70/174 >

- **Responsible behaviour of States**
  - Voluntary, non-binding norms of responsible State behaviour
- **Confidence-building measures**
  - Adopt existing Guidelines for CBM
- **ICT Security Capacity-Building**
  - International community to work together for assistance
- **International Law applies to Cyberspace**
  - The adherence by States to international law is an essential framework

Capacity Building

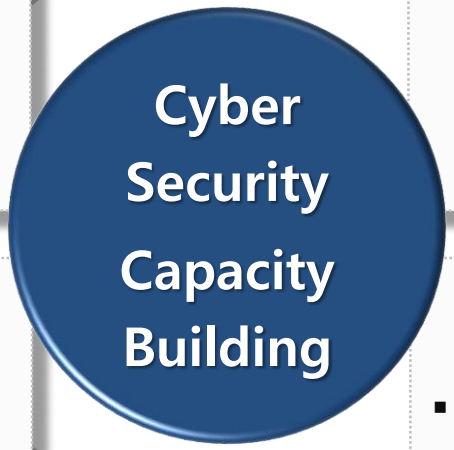
- Effort to build capacity to defend one's own cyberspace

Governance, Role & Responsibility

- Setting a national cyber security governance framework
- Identify the role and jurisdiction of each agency within the cyber security governance structure

Research & Development

- Acquisition of various cyber security technologies
  - Digital forensic and cyber investigation tools
  - Cyber genome or cyber map
  - Count cyber threat technologies



Education

- Cultivating and securing cyber security experts is key to promoting national cyber security
  - Cyber education for teens
  - Cyber security department in university
  - Training course for employees

Cooperation

- State-level cooperation
  - Inter-agency cooperation
  - Public-private partnership
- International-level cooperation
  - International organizations, Conventions or cooperation between States

Conclusion

- To deter the rapid growth of cyber threats, it is important for each State to build its own capacities and yet cooperate internationally

Evolving Cyber Threats

- Cyber threats are getting more sophisticated and targeted
- Cyber threats are one of the most serious threats that most States face

Increasing Dependence on ICT

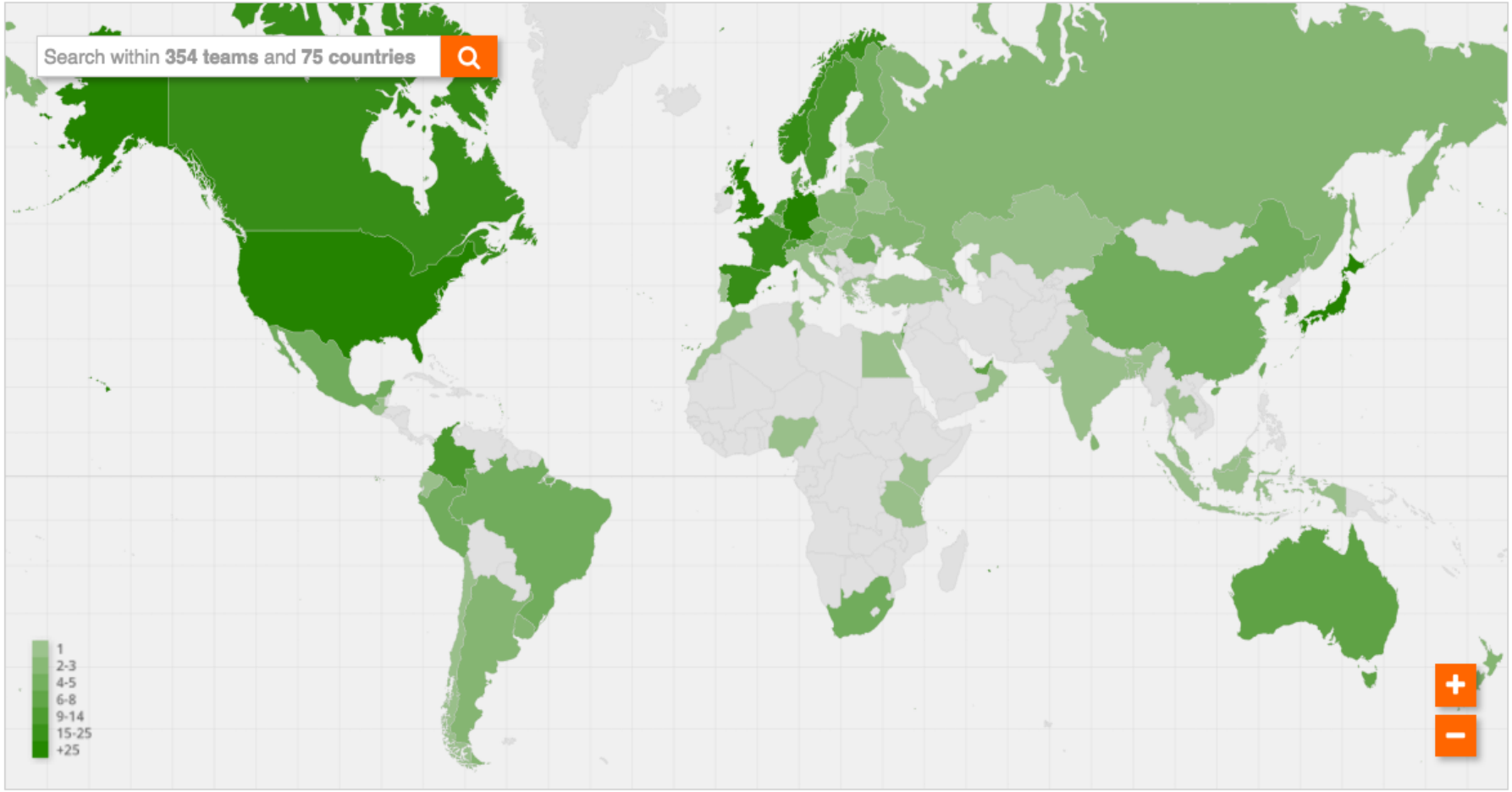
- New technologies such as IoT, Big Data and Cloud computing are being used
- States' increasing dependence on ICT

Each State's Effort to Deter Cyber Threats

- International Cooperation
- Capacity Building

Conclusion - Possibility of FIRST

- FIRST is a multi-stakeholder network participated in by more than 350 CERT teams in 75 countries, and it can play a key role in global cyber security cooperation.



Conclusion - Possibility of FIRST

- The achievement and role of FIRST in cyber security and the developmental direction as a major subject of global cyber security need to be sought

Cooperation in responding to cyber threats

Possibility of joint response based on voluntary cooperation, if cyber threats occur

Infringement/Threat information sharing

Information sharing such as infringement status and exemplary cases related to cyber infringement and threat

Support capacity building

Strengthening the overall cyber security level by training and providing technical support to the less capable CERTs

Basis of private/public cooperation system

Laying the basis for the private/public cooperation system as a cooperation organization of the multi-stakeholder CERT

Thank you

jilim@korea.ac.kr