Introduction of the GCCD
(Global Cybersecurity Center for Development)

미래창조과학부
Ministry of Science, ICT & Future Planning

KISA

Contents

I. Background

- **What's happening on the Internet in 60 seconds?**

e-mail: 240 mill. are transmitted

Flickr: 20 mill. photos are viewed

Amazon: 47,000 app are downloaded

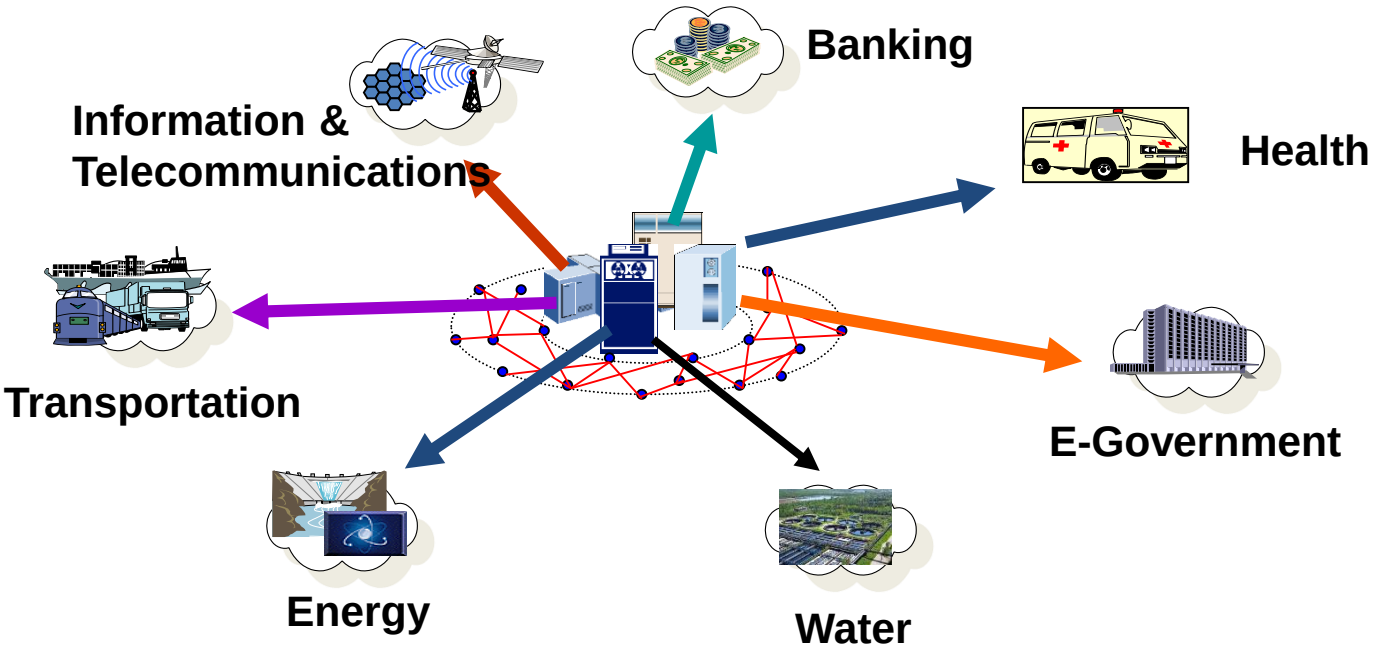
Facebook: 6 mill. page views

YouTube: 1.3 mill. videos are played

※ Source: March 20, 2013 Daily of the UK

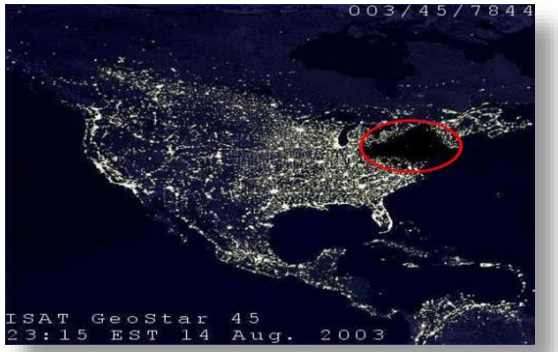
I. Background

Cyberspace is becoming increasingly crucial for the creation of broader societal benefits. However these economic and social benefits might be put at risk by poor security, such as the growth in **cyber crime** or **cyber attack** against **ICT network and system as a whole.**



I. Background

- **Target : Expanded to national and social infrastructures**



A blaster worm caused the New York blackout (August 2003)

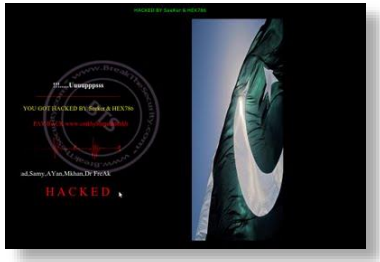
A closed network isolated from the outside

Stuxnet infected through USB (July 201

Cyber war between Russia-Estonia (2007) /Georgia cyber (2008)

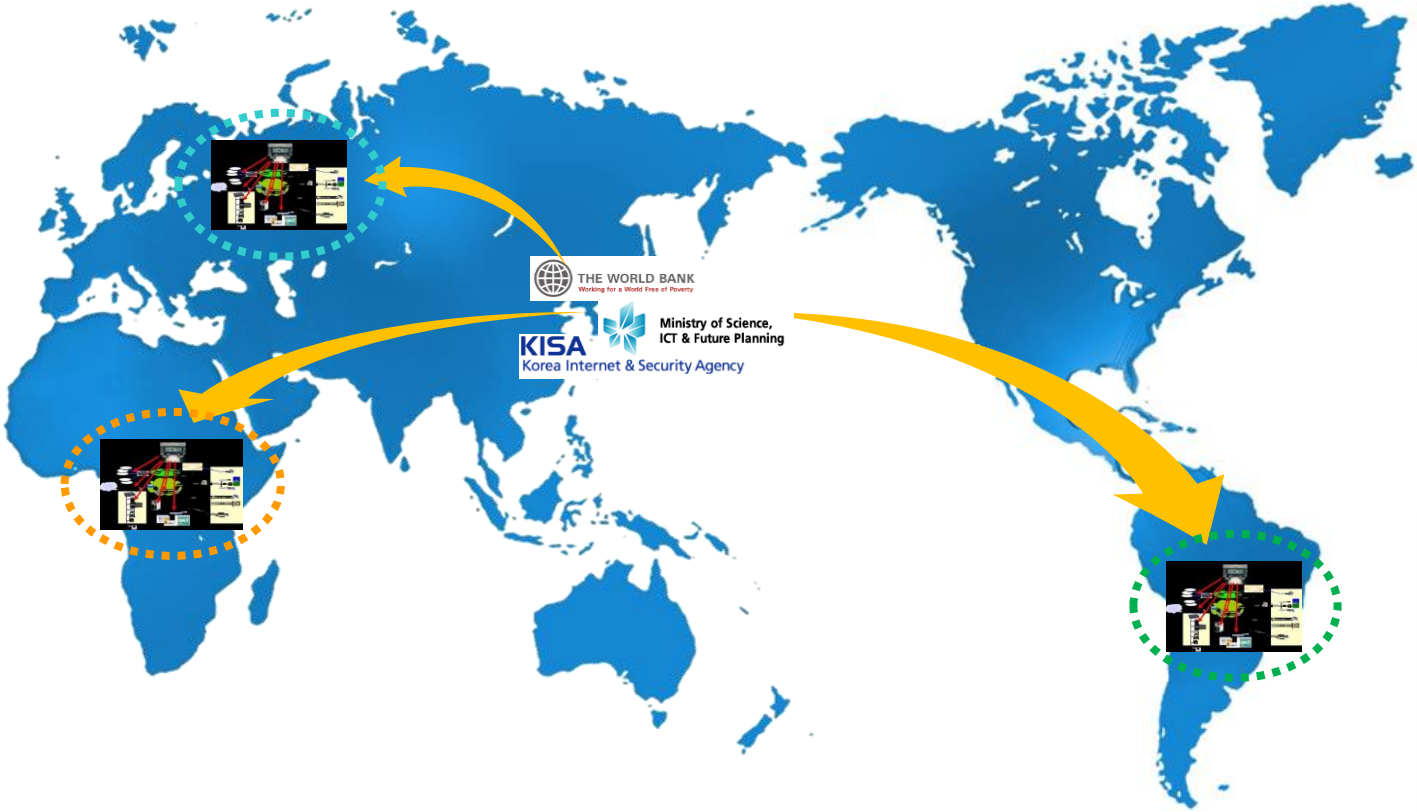
Iran manipulated GPS signals to capture an American drone reconnaissance plane (December 2011)

India hacked the intelligence bureau of Pakistan (March 2013)



II. Vision

GCCD will bring together the knowledge and experience of Korea in cyber-security, and its application in government and business services, with the WBG related expertise in development and poverty reduction, and its global reach and contacts in order to help developing countries build a trusted and secure environment.



III. Roles and Responsibilities (1)

Capacity Building for securing cyber space is becoming crucial as security incidents are increasing all around the world.

Roles and functions	Key contents
Capacity Building through Human Resource Development	It will provide training courses for experts and policy-makers of WB member states, especially developing countries, in the field of cybersecurity.
Providing the standard guideline for Information Security	It will jointly review the information security guideline (information security management system, CERT building/operation, wireless LAN security, cloud service information security, standards for technical and administrative measures to protect personal information, etc.), published by KISA, and translate the standard guideline into English and disseminate it to developing countries.
Free dissemination of security S/W in developing countries	It will translate the security software (vaccines, firewall, self-inspection tools, etc.) developed by KISA and the private sector into English for developing countries and prevent the global dissemination of malicious codes and DDoS by disseminating it free of charge in developing countries

III. Roles and Responsibilities (2)

It needs measures for Critical Information Infrastructure to provide secure protection against advanced hacking technologies.

Roles and functions	Key contents
Providing information security measures for Critical Information Infrastructure	It will disseminate the maturity check system for Critical Information Infrastructure (CII) Protection in developing countries to evaluate the protection level of the Critical Information Infrastructure in developing countries and provide response plans.
Mobile Information Security	It will develop the mobile information security check system for mobile apps so that a virtual machine is utilized to check for unauthorized data access or malicious code insertion.
Establishing the Early Warning System	It will monitor the Internet networks of Worldbank member states without Computer Security Incident Response Team (CSIRT) in real time, and if any sign of abnormality is detected, it will notify the country and neighboring countries so that the dissemination of malicious codes and traffic can be blocked in early stage.
Hacking simulation and vulnerability consulting	It will simulate the internal systems of the governments and public institutions of member states with professional equipment, and develop the simulation system for assessing vulnerability through simulation attacks and performing defense training.

IV. Organizational Structure and Facilities

Organization is consists of Steering Committee, Director, Cooperation Team, Outreach Team, Academy Team, R&D Team and Management.

(Total (at least) 19 Staffs until 2017)

- **Cooperation Team : 3 staffs(CSIRT, External Partnership, etc.)**
- **Outreach Team : 3 staffs(CIIP, F/S, etc.)**
- **Capacity Building Team : 3 staffs(Development, Operation, etc.)**
- **R&D Team : 3 staffs(Mobile security, Standardization, etc.)**
- **Management Team : 5 staffs(Planning, Accounting, Administration, etc.)**
- **Co-Directors : 2 staffs**

• The function and organization of the center will be established in three years time frame by stages.

Minimum requirements for the center to start business and operate educational programs are as below.

- **Office, Lecture, Laboratory, Conference rooms should be equipped**

• A variety of N/W equipments, Hacking simulation equipments, and Briefing and Monitoring facilities for CSIRT should be added to the Center for future activities.

V. Partnership Plan

GCCD is going to be set up with close cooperation between Korean government and World Bank

Korean Gov. (MSIP, KISA)

- **Korea-Worldbank Co-Workshop**
- **Cybersecurity Experts**
- **F/S on Cybersecurity**
- **ICT Expert Training Course**

International Organization

- **World Bank ICT Project**
  → Analyze cybersecurity component and apply it
- **Other Organizations**
  (EBRD, AfDB, WEF, IDB, ADB, ASEAN, APEC, OAS, OECD, ITU IMPACT, ENISA, etc.)

WB GCCD

Member States

- **Developing Countries**

External Partner

- **Global ICT Companies**
- **Academy**
  (Univ. of Oxford - Global Cyber Security Capacity Centre, a couple of Korean Universities)

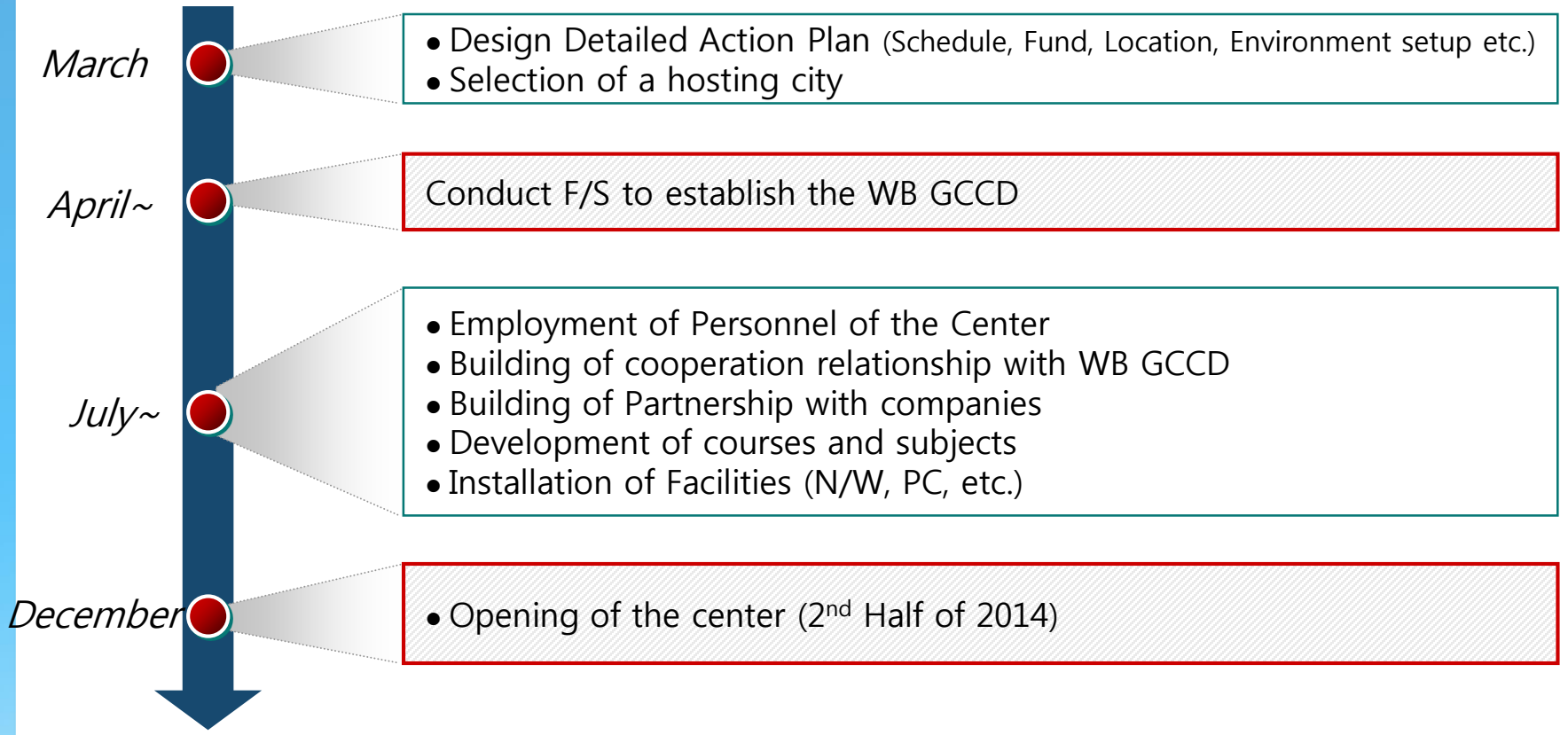
VI. GCCD's Service for Developing Countries

Countries hoping to enlist help from the GCCD in establishing information security system can benefit from the center's professional support as the following.

- **Information Security Expert Training Course**
- **Consultation for CIIP (Critical Information Infrastructure Protection)**
- **Local advisory to help build information security system**
- **Educate public officials from developing countries by dispatching them to the GCCD (In-Kind Contribution)**

Ⅶ. Implementation Schedule

Aim to open the center in 2nd Half of 2014



Thank you