



Internet, Cybersecurity & KISA in Korea



Contents

I Internet, KISA & Cybersecurity Trend

II Cyber Attack Incidents

III National Cybersecurity Plan



Frontier..



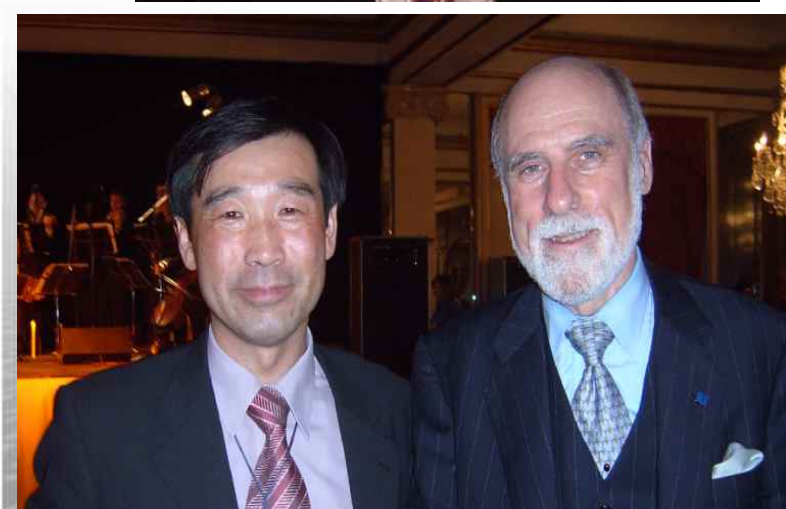
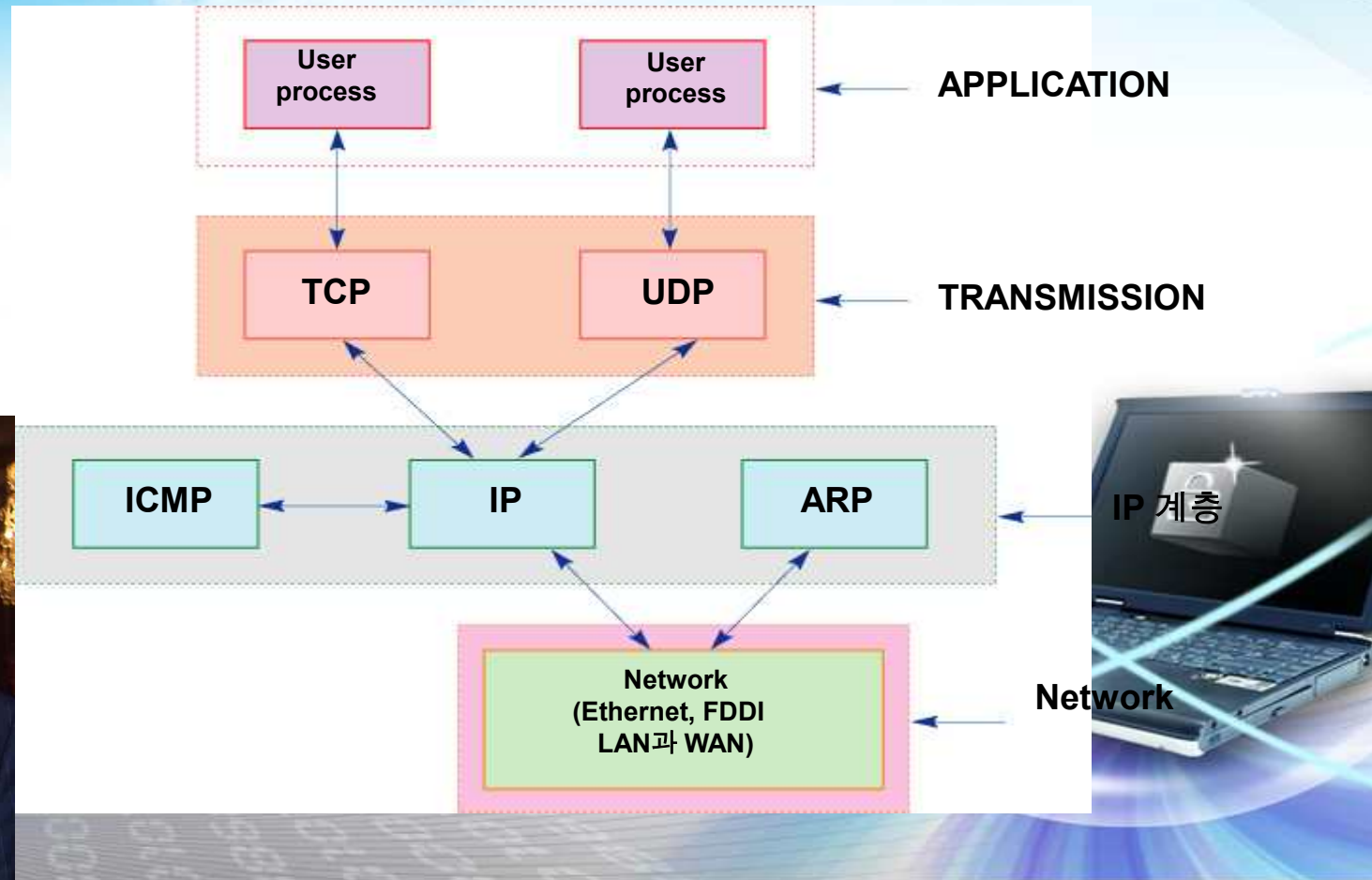
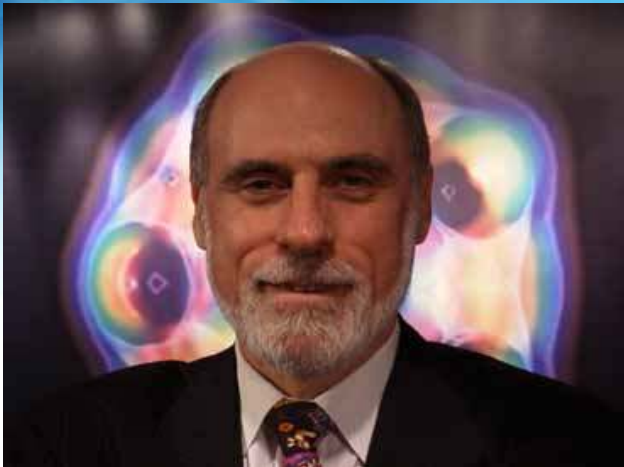
Jon Postel
(1943.8–1998.10)

- * OPENNESS
- * AT LARGE
- * BOTTOM UP
- * OUT REACH
- * SHARENESS



Father of Internet

- Vint Cerf (The father of the Internet, ICANN Former Chairman, Google Vice Chairman)



RFC NO.1 Father of Korea Internet



Dr. Steve Crocker

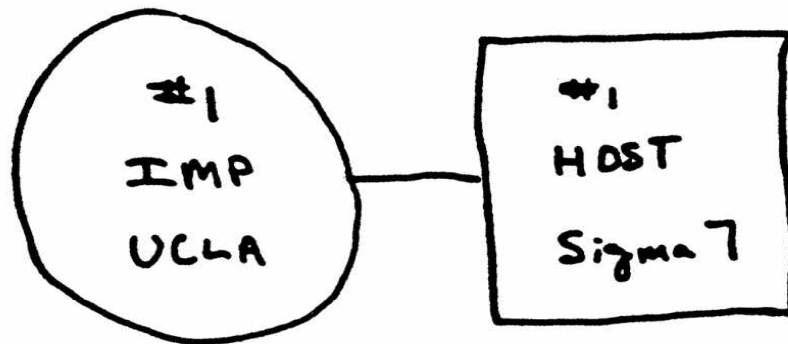
Stephen D. Crocker (born October 15, 1944 in [Pasadena, California](#)) is the inventor of the [Request for Comments](#) series^[1], authoring the very first RFC and many more. He received his [bachelor's degree](#) (1968) and [PhD](#) (1977) from the [University of California, Los Angeles](#).^[2]

Dr. CHUN, Kilnam(1943~)

- He is a professor of Korea Advanced Institute of Science and Technology (KAIST).
- The start of Internet and the introduction of www in Korea was done by him



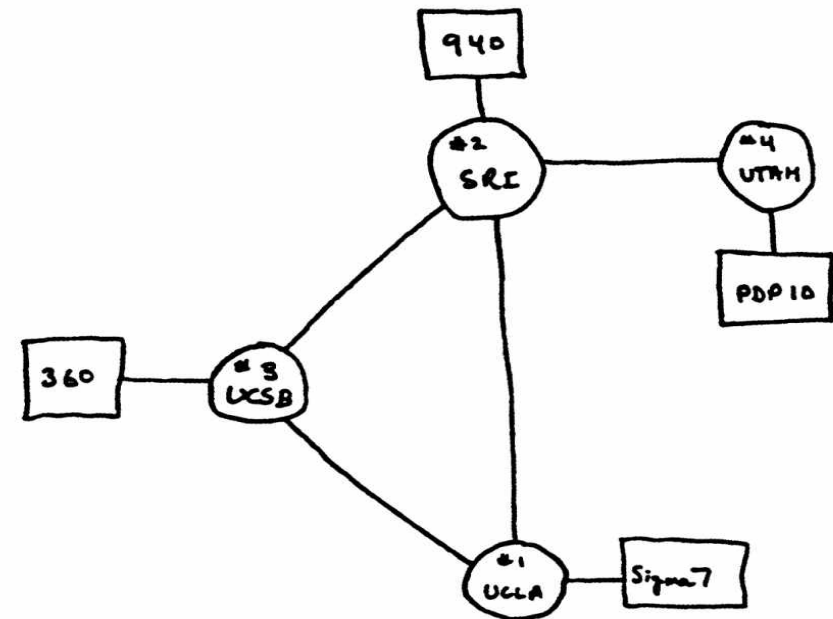
Very Small but NOW?



THE ARPA NETWORK

SEPT 1969

1 NODE

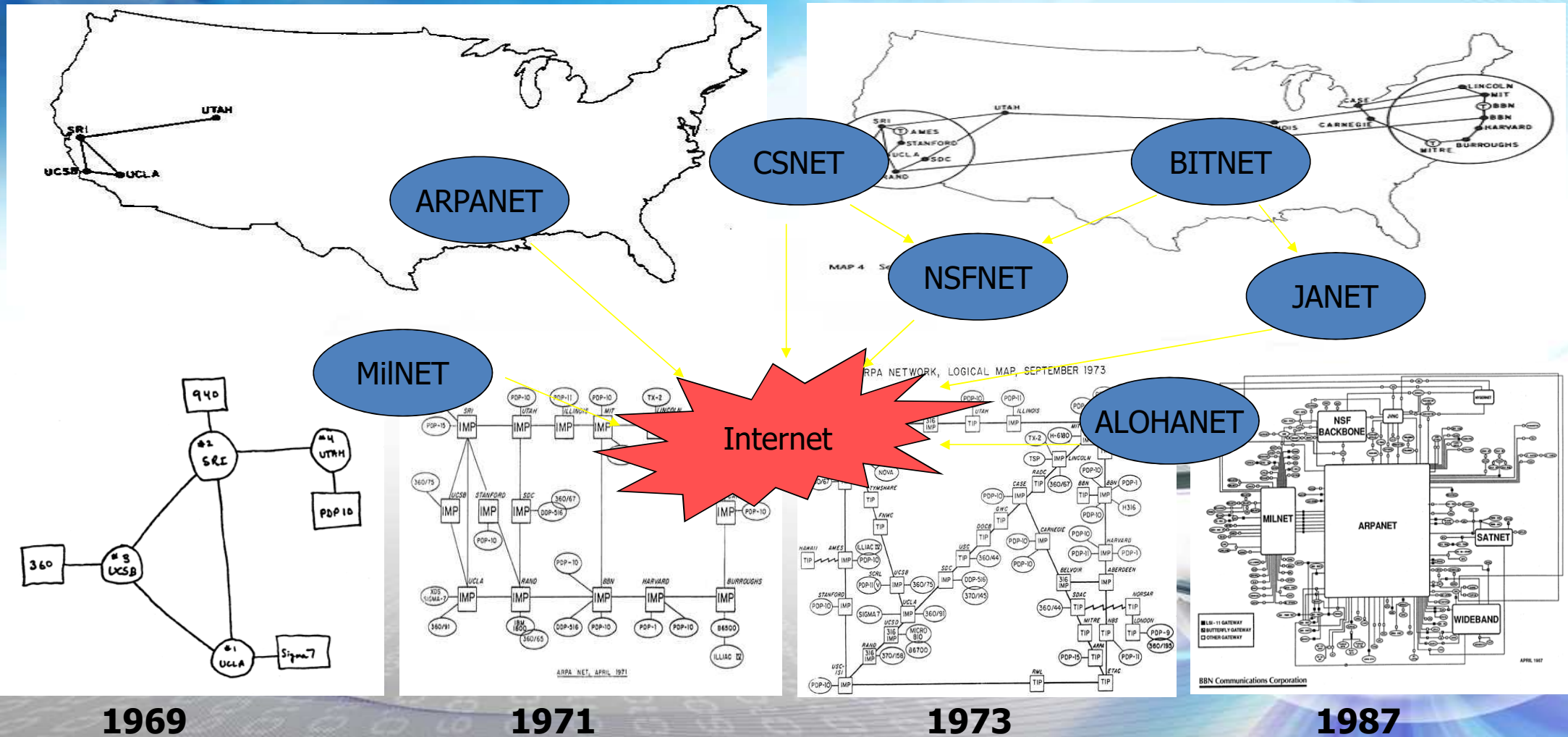


THE ARPA NETWORK

DEC 1969

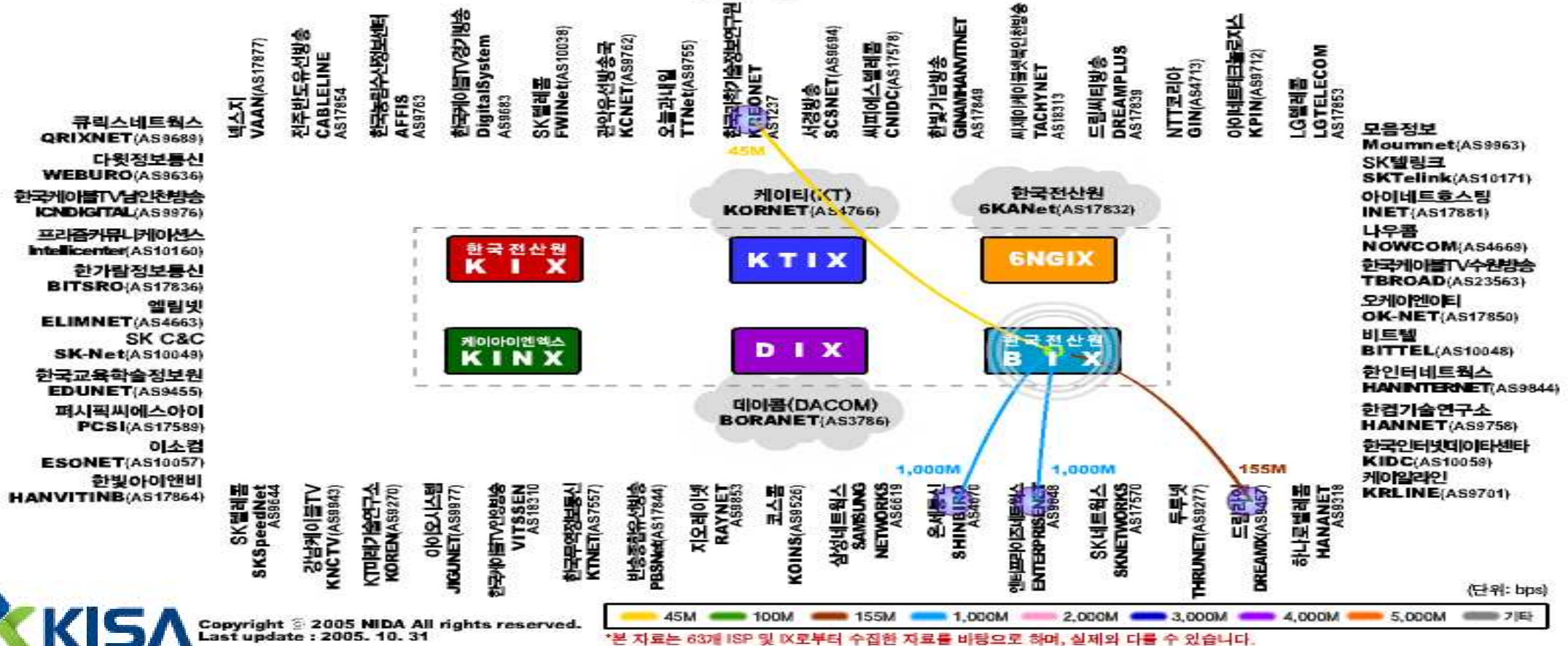
4 NODES

Development of Internet



Status : Internet Connectivity Map

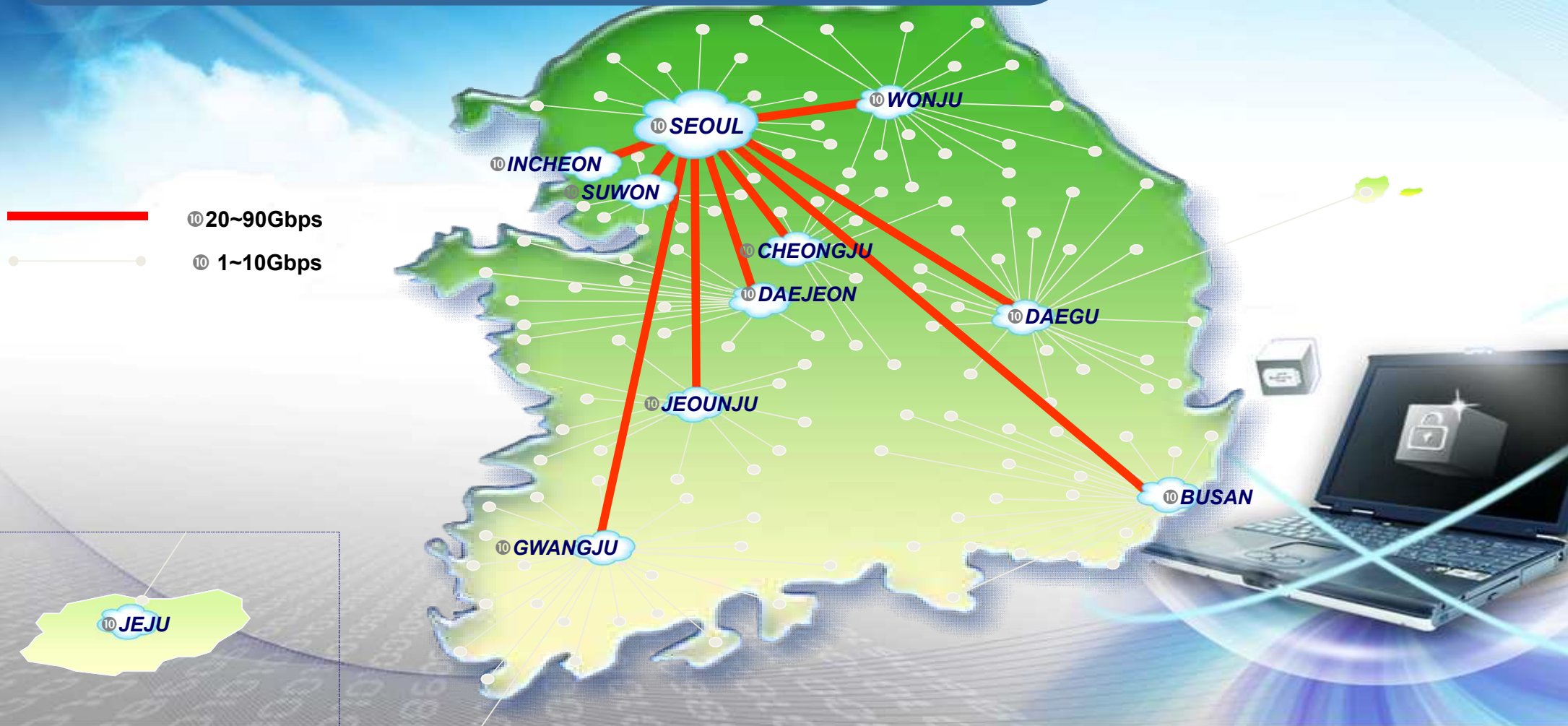
Internet Connectivity Map Between ISP & IX



*본 자료는 63개 ISP 및 IX로부터 수집한 자료를 바탕으로 하며, 실제와 다를 수 있습니다.

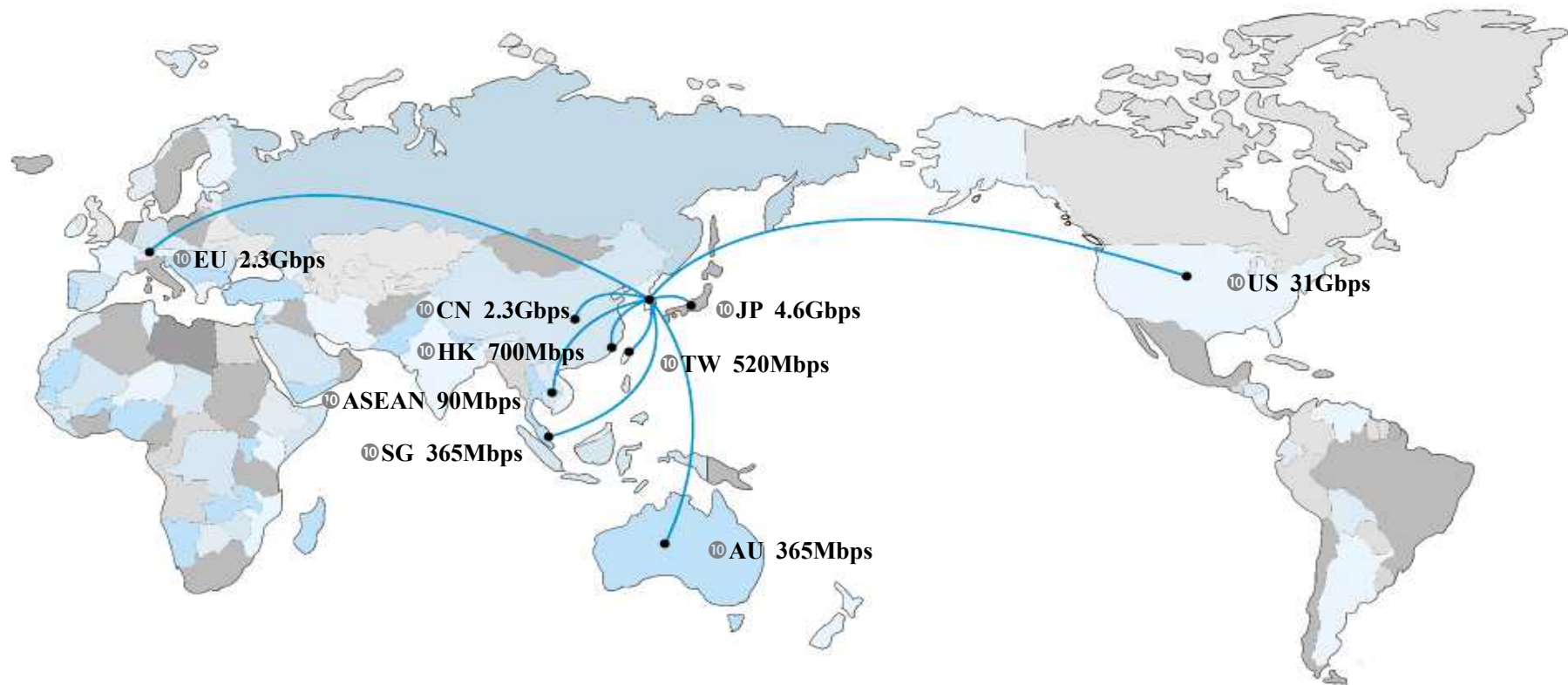
Status of IT : Infrastructure

Broadband Network in Korea



Status : Infrastructure

Broadband Network abroad

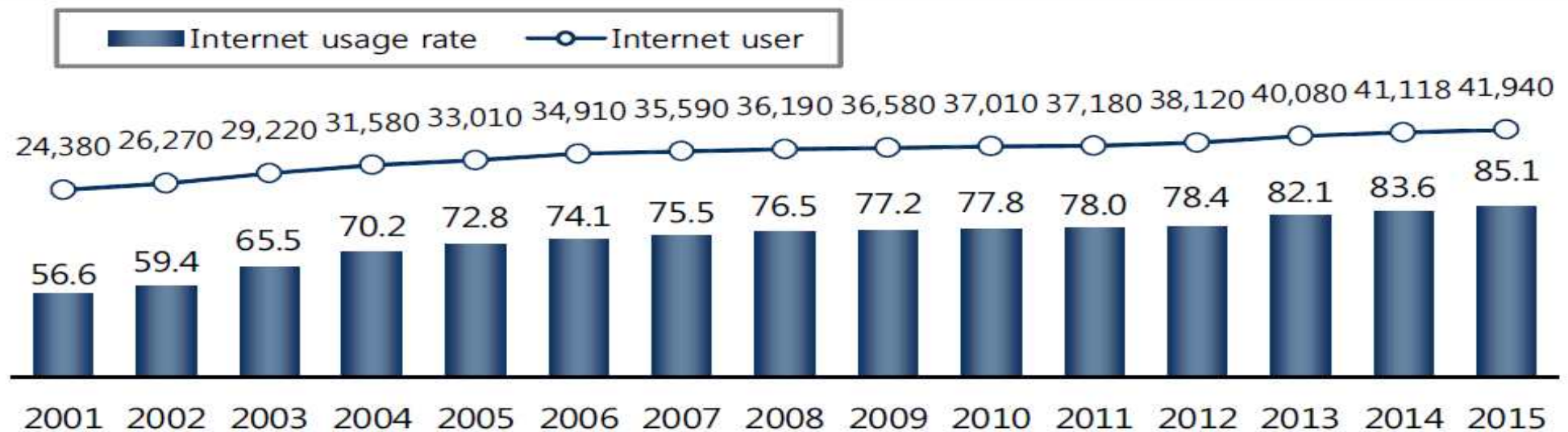


Status of Internet – Ratio of User

3 Broadband Penetration

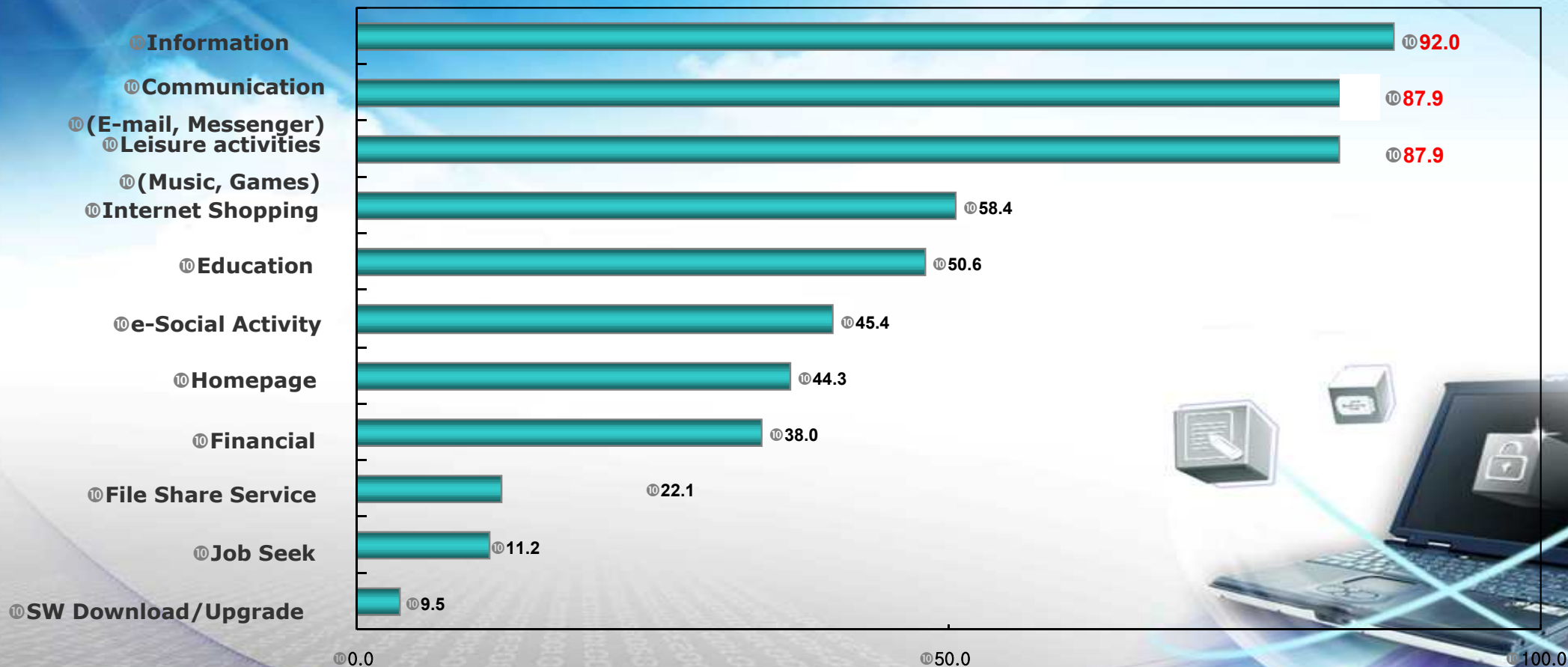
<Figure2-1> Trends in Internet Usage Rate and Internet Users

(unit: %, thou)



- 1) Since 2004, wireless Internet through mobile communication network has been included in the scope of Internet. Also the definition of Internet users has been changed from 'those who use the Internet at least once a month on average' to 'those who have used the Internet at least once in the last 1 month'
- 2) Since 2006, the sample eligibility has been expanded to the population ages 3+ (2000-2001 : population ages 7+, 2002-2005 : population ages 6+)

Purpose of Internet use

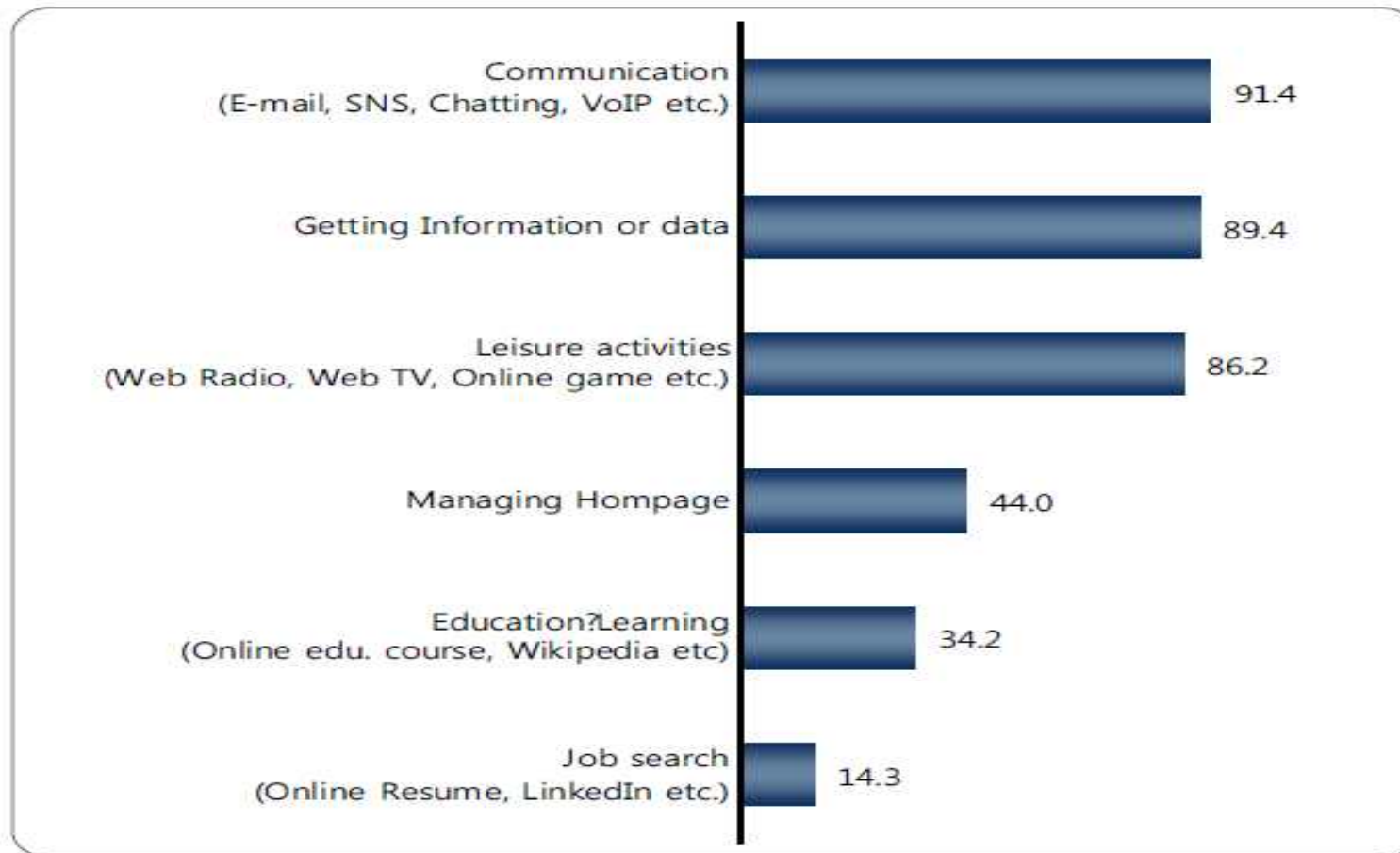


[Source : KISA, 2011 Korea Internet White Paper]

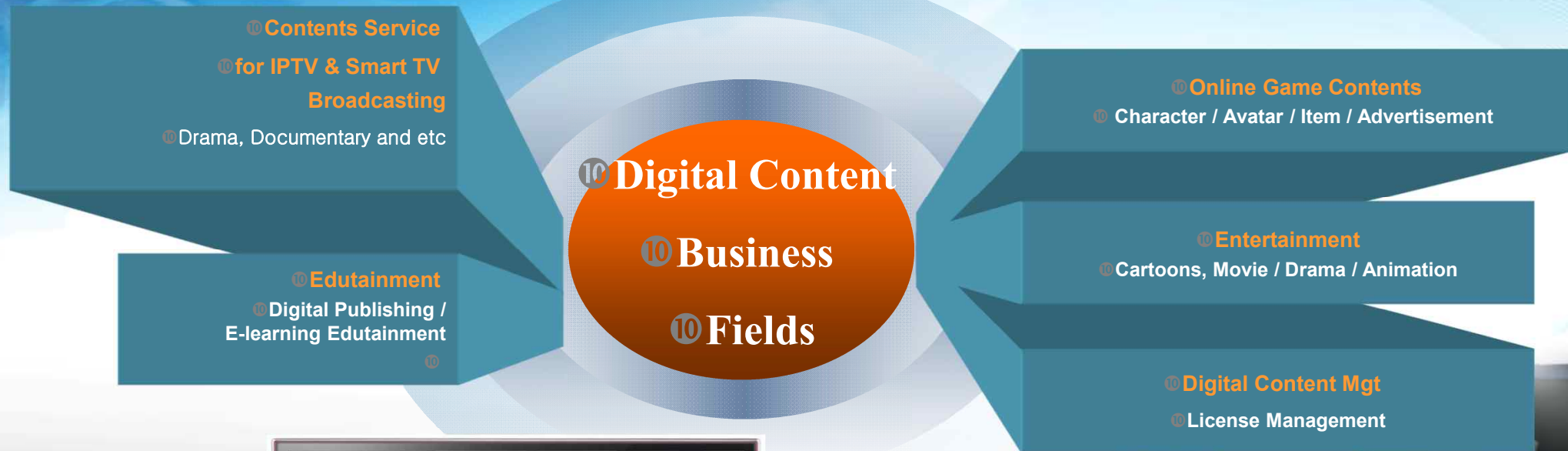
Purpose of Internet use

<Figure2-21> Purpose of Using the Internet (multiple responses)
- Internet Users ages 3+

(unit : %)



New Trends On Internet



ROOT DNS (A~M, 13개)

전세계 루트DNS 배치 현황

원본
(13개)



복제본
(470여개)
*국내 (47개)



.KR DNS in World

krDNS 구축현황

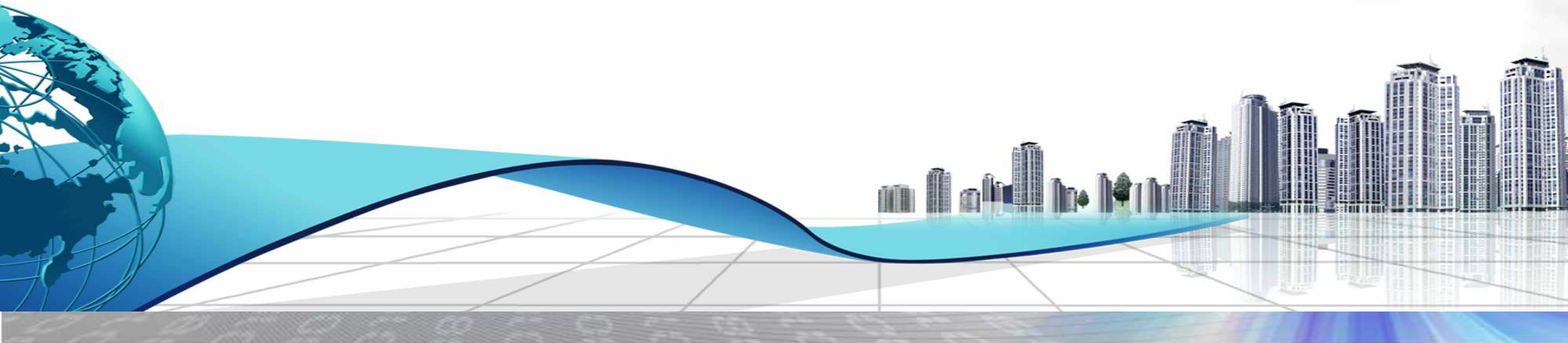
DDoS 대응 (4개)



IDN (Internationalized Domain Name)



Introduction to Korea Internet & Security Agency



Foundation

Legislation

Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

- Article 52 (Korea Internet and Security Agency)
 - to upgrade the information and communications network, encourage the safe use thereof, and promote the international cooperation and advancement into the overseas market in relation to broadcasting and communications.

Main

Information Security

- Internet Incidents Prevention and Response
- Protection of Personal Information
- Policy Development and Law

Internet Development

- Create a better and safer Internet Environment
- Encourage new Internet related services
- Management of Korea Network Information Center

International Cooperation

- International Cooperation on Broadcasting & Communication
- Expansion of Exchanges with Various International Organizations

Policy Development

- Studying Legal system related with Internet and Supporting Govn't enactment
- Studies and Improvement of Legal System in Compliance with IT Convergence

History

1996. 4	Korea Information Security Agency(KISA)	2010. 1	Launching the ☎118 Call Center
1999. 6	National Internet Development Agency of Korea(NIDA)	2011. 5	Launched the service of Hangeul dot Hanguk(한글. 한국) domain Add
2002. 1	National IT International Cooperation Agency(KIICA)	2012. 5	Internet Personal Information Clean Center
2009. 7	Korea Internet & Security Agency (merger of KISA, NIDA and KIICA, 23 rd Jul)	2013. 1	Phishing Response Center



Key Facts

- Budget : ₩176 billion (in 2014) about 174 million US dollar



<Annual Budget>

- Staff : 613 (2015. 1.)

Post-Graduated and above : 308

(Ph.D : 59, MA degree: 249)

Average Age : 34.6 years old

ratio of 20-30th : 76%

Gender : male 67%



female 33%

What we do

Information Security

[Public Sector Information Security]

- Establishing Critical Information Infrastructure(CII) Protection measures & supporting for incident recovery
- G-ISMS, Information Security Consulting for e-Government services
- SW assurance service & IT security product(smartcard, firewall, etc.) evaluation
- Operation of RootCA for National PKI & Promoting PKI usages

[Personal Information Protection]

- Operating the Privacy Incident Response System(PIRST) 24/7
- Operating 118 call center 24/7
- Providing Consultation & Alternative Dispute Resolution(ADR) for personal information dispute



What we do

Korea Internet Security Center

[Reliable and secure Internet environment]

- Korea Internet Security Center(KrCERT/CC)
[※ CERT : Computer Emergency Response Team]
- Early detection and response to prevent damages from Internet incident
- Strengthening domestic and international cooperation for incident response
- Operating Spam Response Center
- Strengthen collaboration with specialized institution(agency)
- Support developing countries to establish CERT



What we do

Policy Development and International Cooperation

[Policy Development]

- Providing the Issue Report on Global IT, ICT Policy Trends etc
- Studying **legal system** related with Internet and Supporting Govn't enactment
- Analysis of Internet & Security Policy and Statistical Research on Main Business
- Studies and Improvement of Legal System in Compliance with IT Convergence

[International Cooperation]

- Strengthening ICT SMEs capabilities for global market
- Hosting ICT training programs and creating human networks
- Promoting cooperation in ICT areas with International Organization such as OECD ,ITU, WB and many others
- Developing and sharing best practices for cyber security policy and practices



What we do

Internet Development

[Better and healthier Internet environment]

- Raise the awareness of youth about the importance of Internet
- Take the leading role in global issues on Internet ethics
- Run national campaign for beautiful Internet world

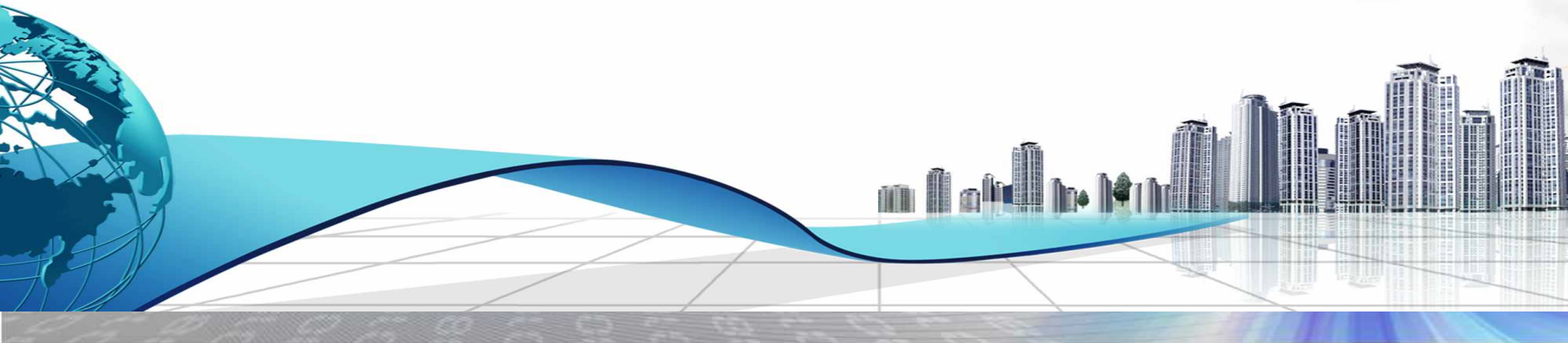
[Industry Development]

- HTML5(Alternative technology of active X) consulting
- Testing and certifying service for domestic biometric system [K-NBTC]
- Development of new services for Near-Field Communication(NFC)
- Promotion for domestic Cloud service and cooperation of global relationship



Introduction to Korea Internet Security Center (KrCERT/CC)

 **KrCERT/CC** 인터넷침해대응센터



CONTENTS

1

Cyber Security Framework of Korea

2

Primary Response Activity of KrCERT/CC

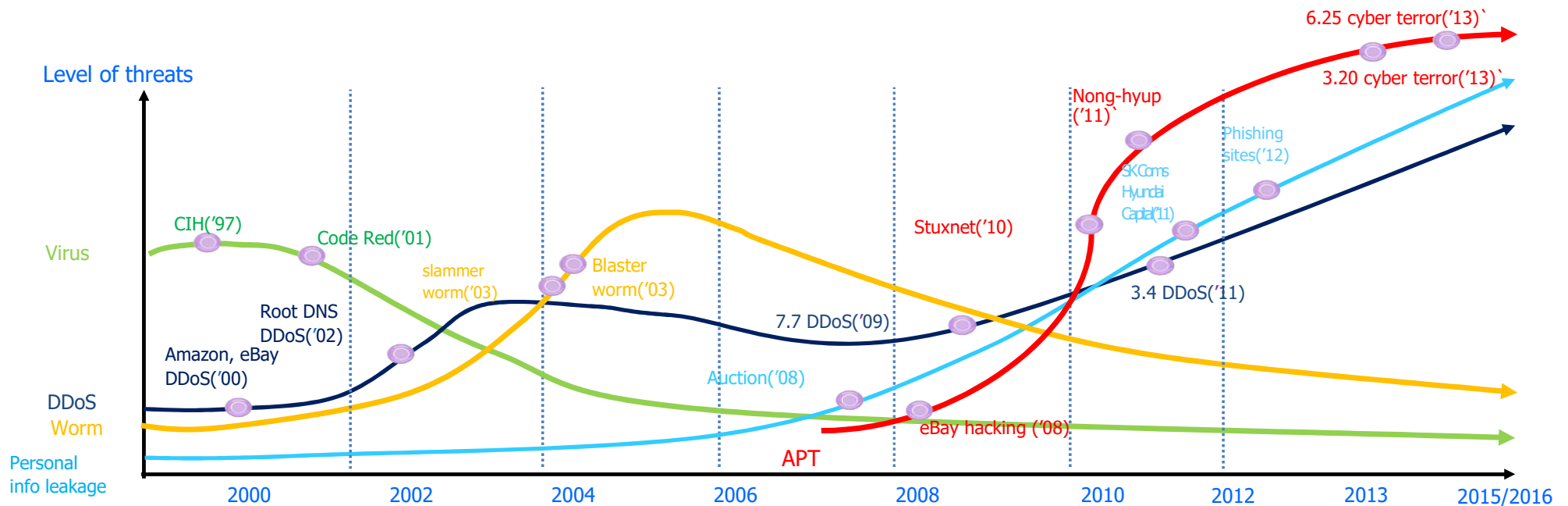


Cyber Security Framework of Korea



Cyber security trends

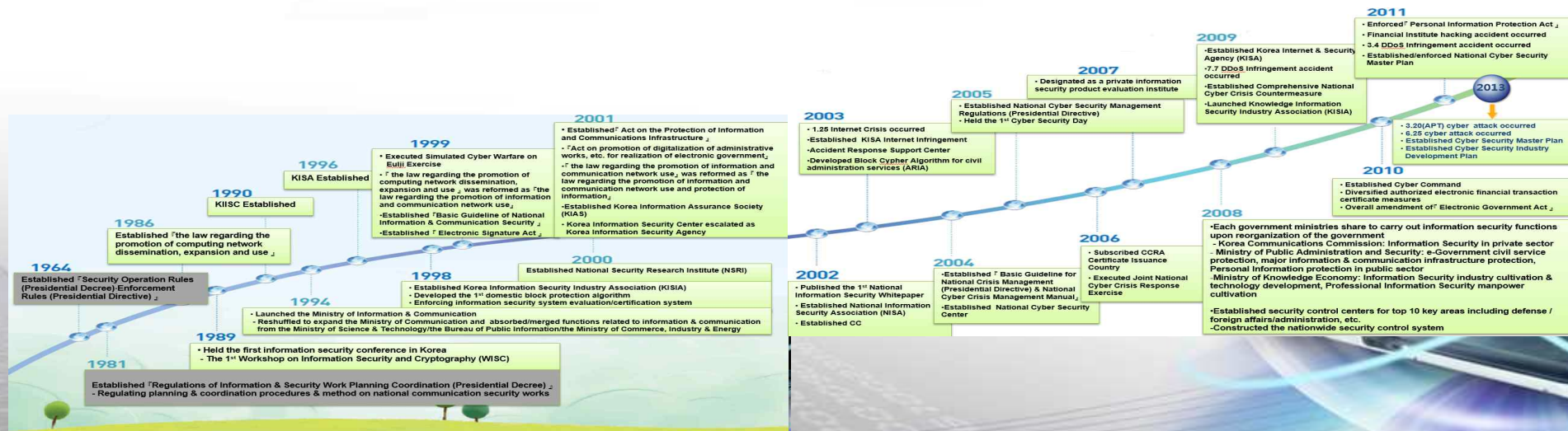
- ◆ Purpose : show-off → financial → cyber terrorism (social unrest)
- ◆ Technique : manual → stealth, automatic → organized and intelligent
- ◆ Target : individual system → large-scale, network → social infrastructure, state



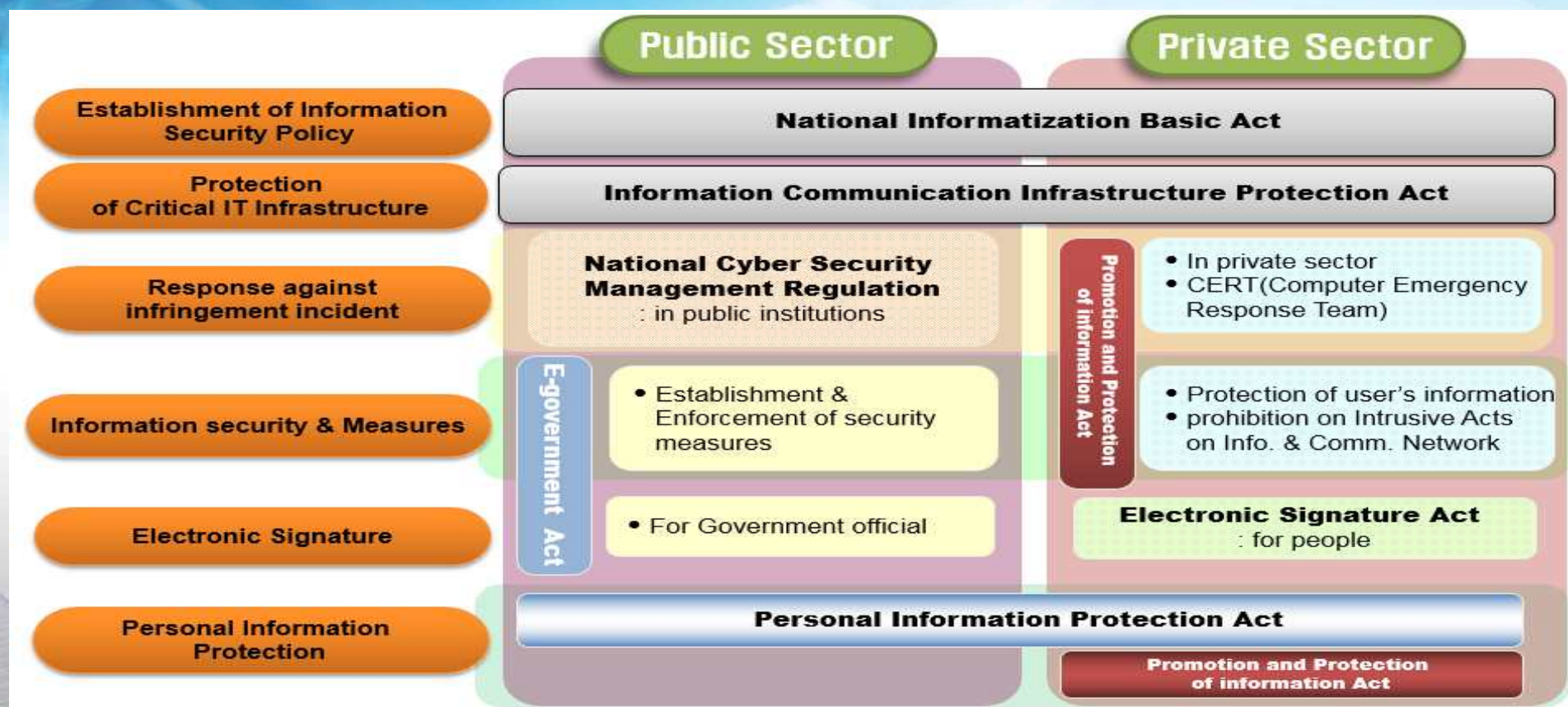
Backgrounds

- We have long history about information security.
- Before 1980's, the 'Security' term is about national security or military security
- Late 1980's, eventually made a regulation about information security
- In 2003, we meet the turning point due to the 'Slammer worm'

『 the law regarding the promotion of information and communication network use and protection of information 』



In a nutshell, related laws



* Promotion and Protection of information Act : the law regarding the promotion of information and communication network use and protection of information

1-1. KISC(KrCERT/CC) Mission and Organization

Mission

- 7days/24hours Monitoring, Early Detection/Response on Cyber Attacks in Private sector
- Rapid Response for Nation-wide Major Internet Incidents to Prevent and Minimize damages
- Cooperation with Domestic(ISPs, Anti Virus Companies), and Foreign Partners (FIRST, APCERT, Microsoft, Symantec, etc)

Organization

Korea Internet Security Center

Internet Incident Response Division

Internet Incidents Analysis Division

Infrastructure Protection Division

Internet Incidents Response Planning Team

Internet Security Response Team

Internet Incidents Analysis Planning Team

Internet Incident Investigation Team

Critical Infrastructure Protection & Planning Team

e-Government Security Team

Internet Incident Detection Team

Internet Incidents Response Technology Team

Code Analysis Team

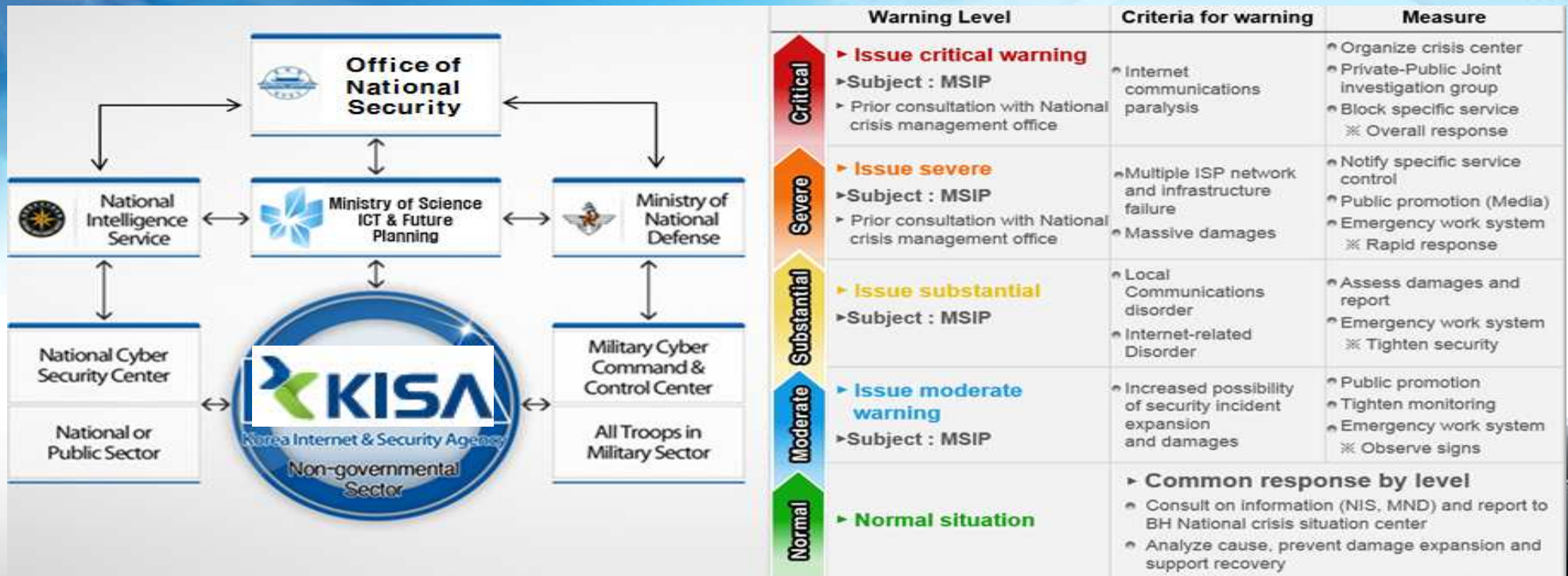
Vulnerability Analysis Team

IT Security Evaluation Team

Information Security Management Team

Cyber Fraud Response Team

1-2. National Cyber Security Framework



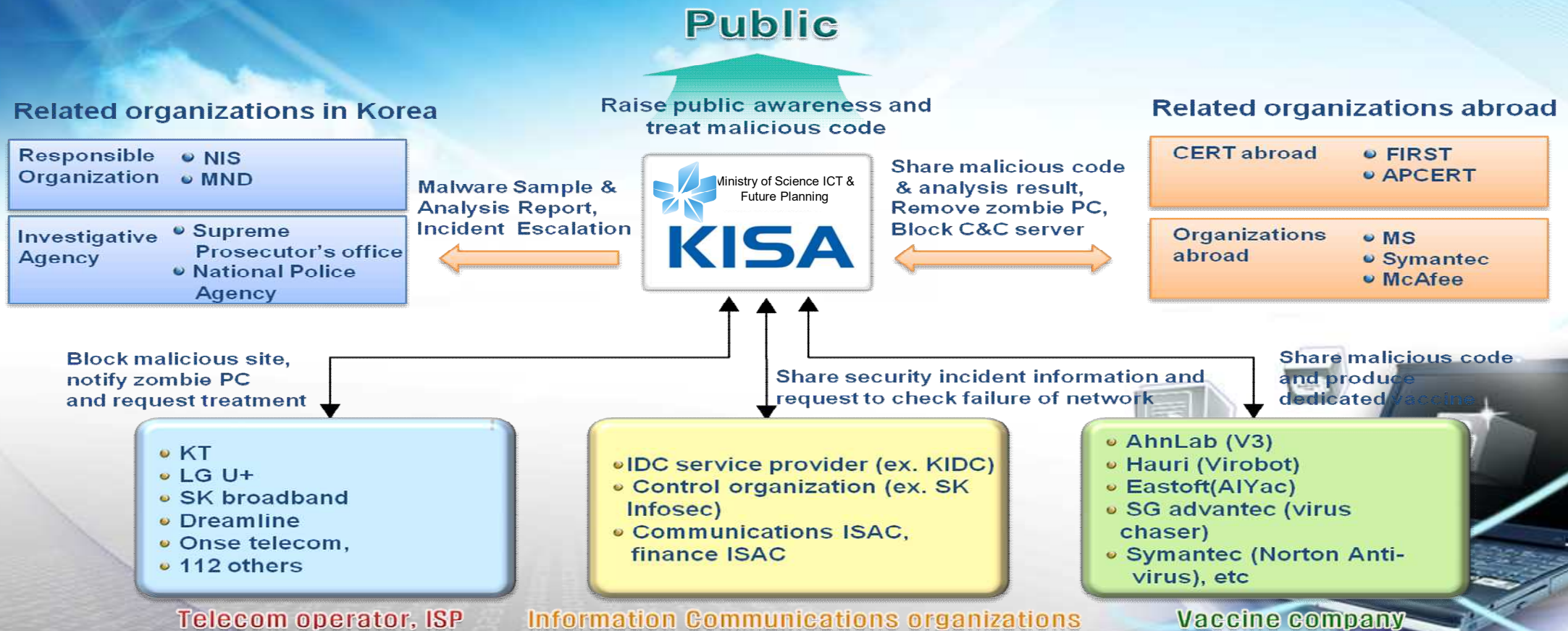
- **KISA under MSIP in charge of Cyber Security of Private sector**

✓ Most security incidents including zombie PC occur in private sector and KISA is responsible for that incidents

- **Cyber Threat Warning System (Normal, Moderate, Substantial, Severe, Critical)**

✓ MSIP/KISA is in charge of issuing cyber security alarm(Composed of 5 threat levels) for the private sector

1-3. Cyber Threat Response Cooperation System



Primary Response Activity of KRCERT/CC



2-1. Security Monitoring Room

Security Monitoring Detail

- Traffic : 158 Domestic ISP/IDC/MSO/MSSP Traffic, Ports, Protocols, Attacks
- Web Servers : 600+ Major Domestic Web servers
- DNS : 13 Root DNS, 6 KR DNS, 12 Major Domestic ISP DNS
- Security Information : Major Anti-Virus, System/Software/Security Company sites
- Honey-net / Honey-pot
- Monitor web-embedded malicious code : 2.3 Mil Domestic Websites
- Hotline (ISPs, Anti-Virus Companies, NCSC, etc)

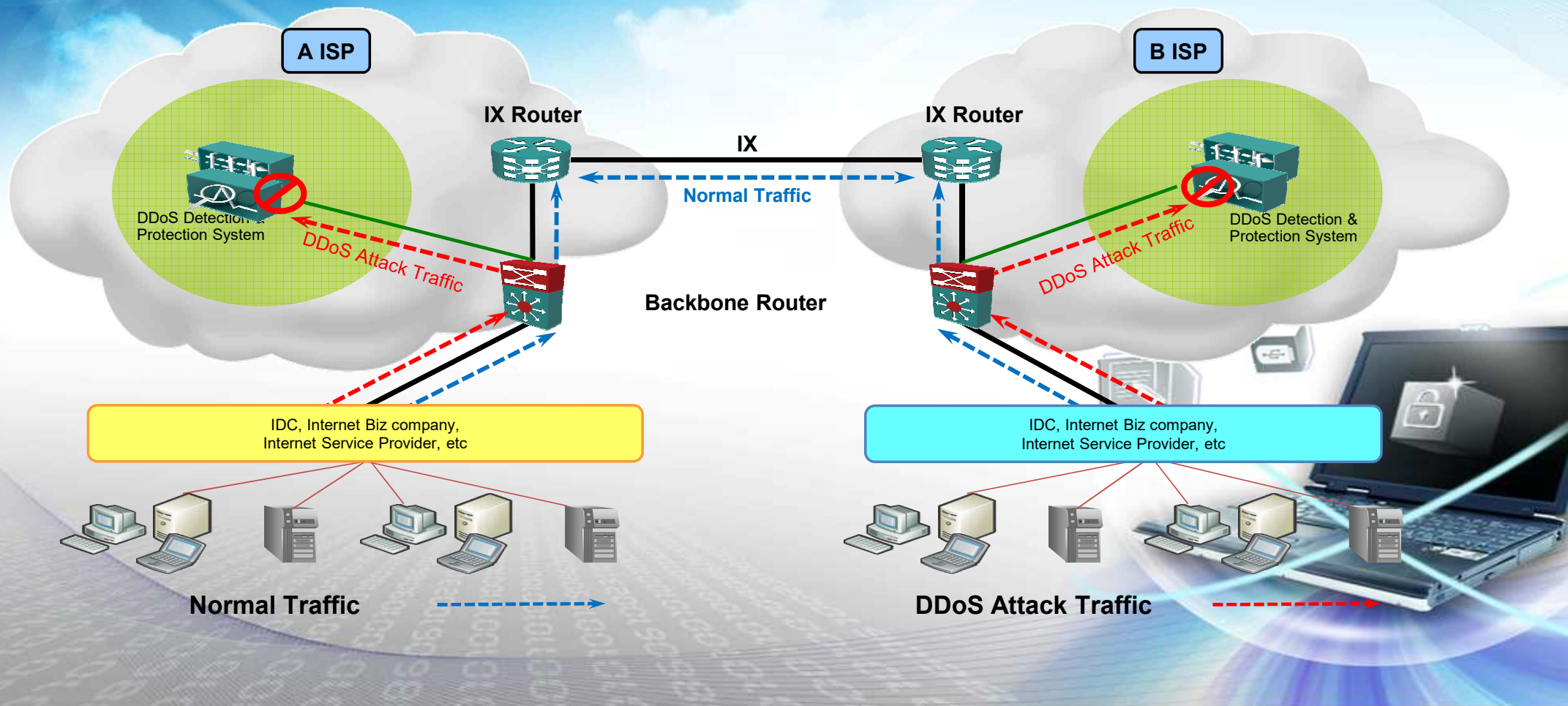
Incident Call Center Services

- Call Center for Incidents Response & Private Outreach : +82-118 (free)



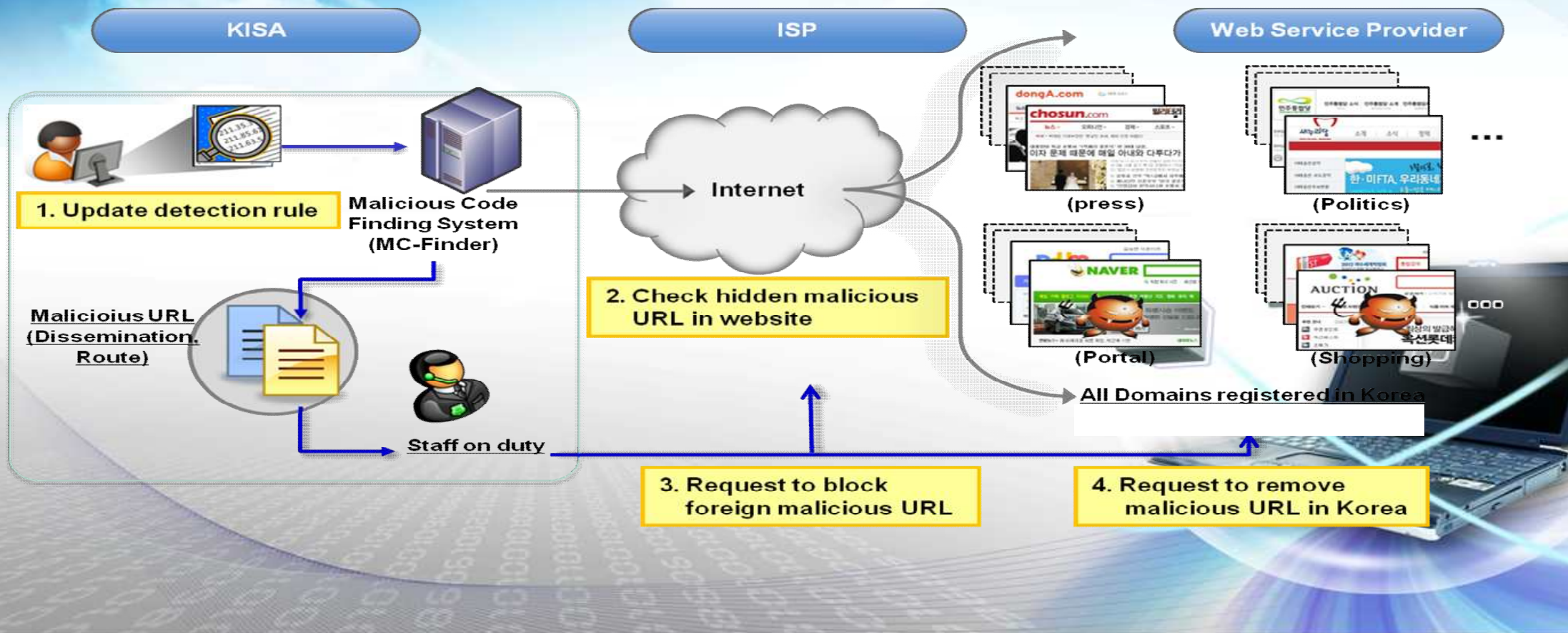
2-2. DDoS Defense System

- Early DDoS attack detection at Internet Exchange (IX) node



2-3. Malicious Code Detection System

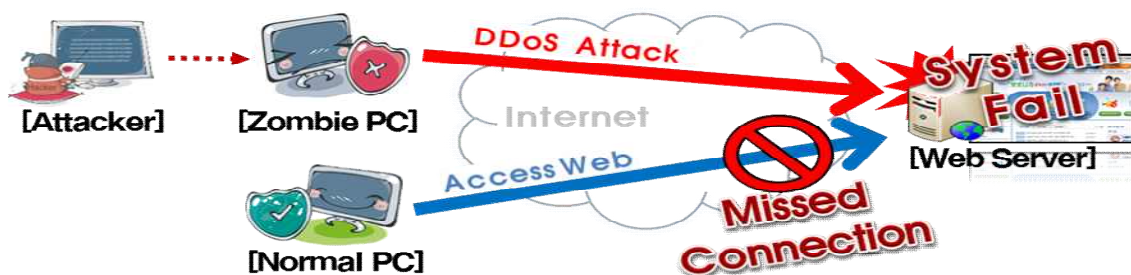
- ❑ Monitor web-embedded malicious code (2.3 Mil Domestic Websites)
- ❑ Enhance the security of domestic websites and Internet users



2-4. DDoS Shelter System

☐ DDoS defense service at the government level for SMEs

- It's blocking DDoS attack and supporting normal web service of SMEs



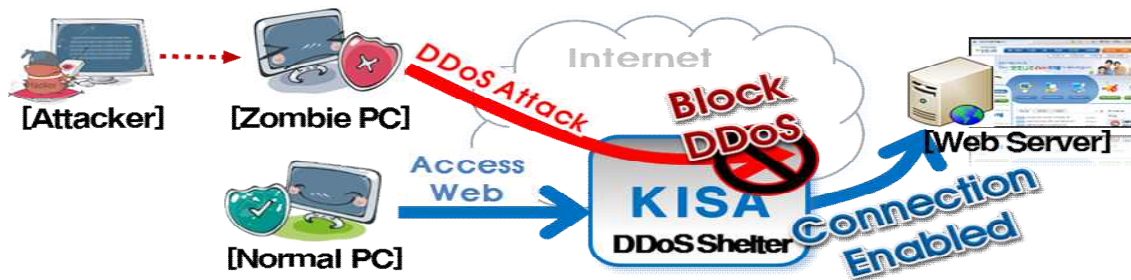
● System is failed by DDoS Attack

- Normal web server is failed by DDoS Attack

● Applying DDoS Shelter

- Replace the Web Server IP in DNS with IP provided by the DDoS Shelter

After applying DDoS Shelter



● DDoS Traffic detoured from Web Server to DDoS Shelter

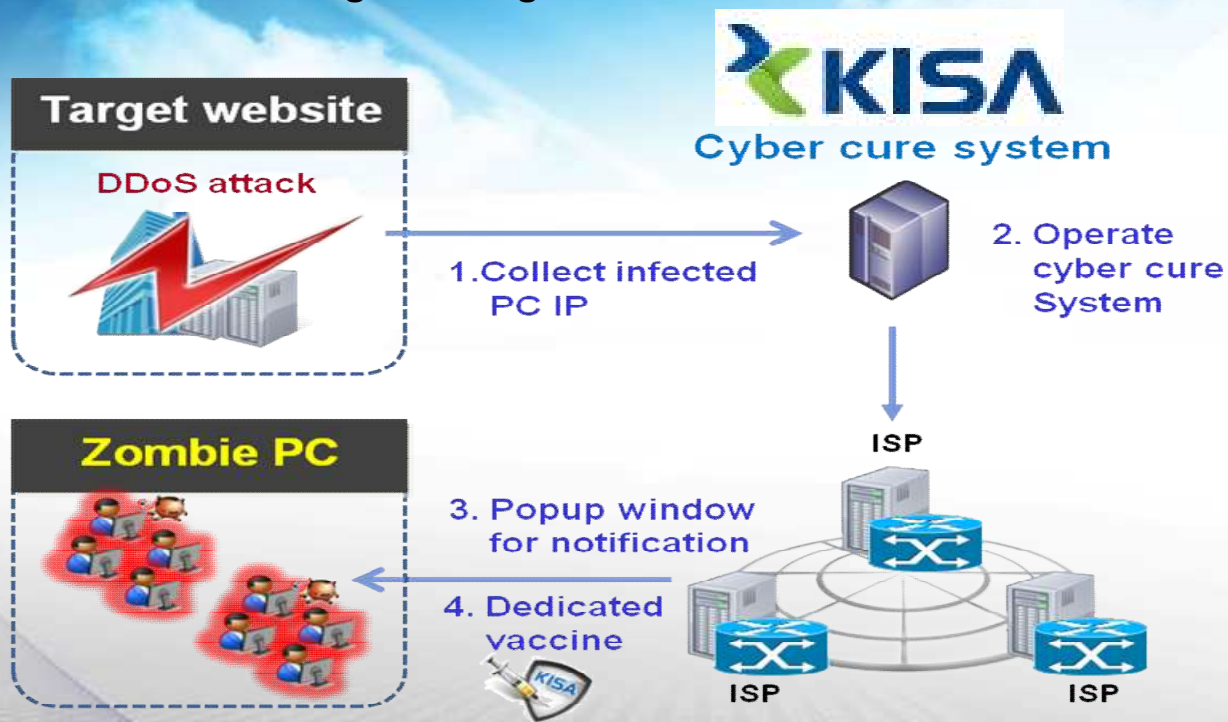
- Normal & DDoS traffic flows to the DDoS Shelter

● DDoS traffic blocked and Normal traffic allowed

- The DDoS Shelter filters DDoS traffic and normal traffic flows into the web server

2-5. Cyber Curing System

- Provide a notification of malware infection and removal method using popup window
- Effective measure against large-scale DDoS attack



2-6. International Cooperation

Security Training Course



- Training course for AP countries on CERT establishment and cooperation
- 203 trainees from 40 countries since 2005

Bilateral Cooperation



- Signed MoU with leading organizations to enhance cyber security cooperation
- Joint response to incident handling
- Information sharing on infected computers

Internet Security Framework



	Warning Level	Criteria for warning	Measure
Critical	▶ Issue critical warning ▶ Subject : MSIP ▶ Prior consultation with National crisis management office	● Internet communications paralysis	● Organize crisis center ● Private-Public Joint investigation group ● Block specific service ※ Overall response
Severe	▶ Issue severe ▶ Subject : MSIP ▶ Prior consultation with National crisis management office	● Multiple ISP network and infrastructure failure ● Massive damages	● Notify specific service control ● Public promotion (Media) ● Emergency work system ※ Rapid response
Substantial	▶ Issue substantial ▶ Subject : MSIP	● Local Communications disorder ● Internet-related Disorder	● Assess damages and report ● Emergency work system ※ Tighten security
Moderate	▶ Issue moderate warning ▶ Subject : MSIP	● Increased possibility of security incident expansion and damages	● Public promotion ● Tighten monitoring ● Emergency work system ※ Observe signs
Normal	▶ Normal situation	▶ Common response by level ● Consult on information (NIS, MND) and report to BH National crisis situation center ● Analyze cause, prevent damage expansion and support recovery	

- KISA under MSIP in charge of Cyber Security of Private sector

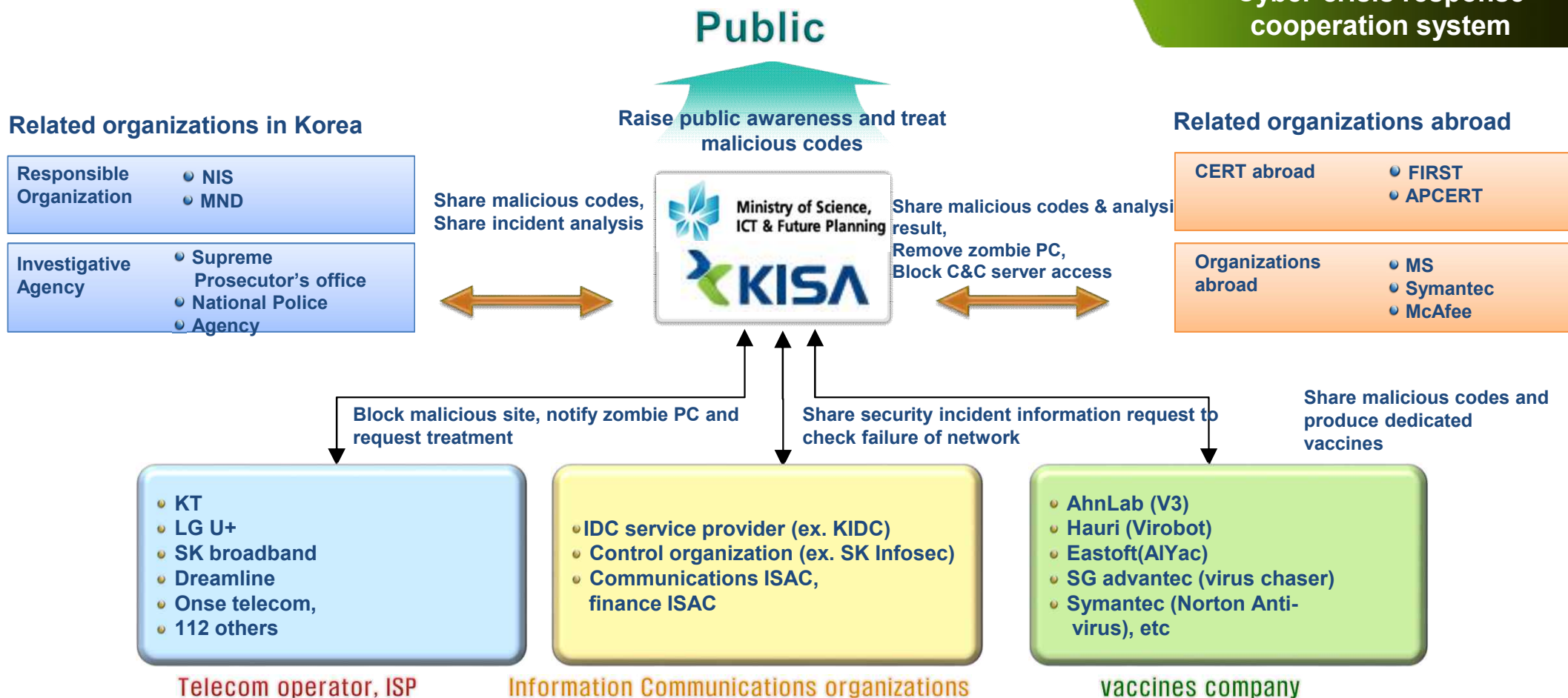
✓ Most security incidents including zombie PC occur in private sector and KISA is responsible for that incidents

- Cyber Threat Warning System (Normal, Moderate, Substantial, Severe, Critical)

✓ MSIP/KISA is in charge of issuing cyber security alarm (Composed of 5 threat levels) for the private sector

Security Incident Prevention and Response

Cyber crisis response cooperation system



Major Policies (CIIP, ISMS)

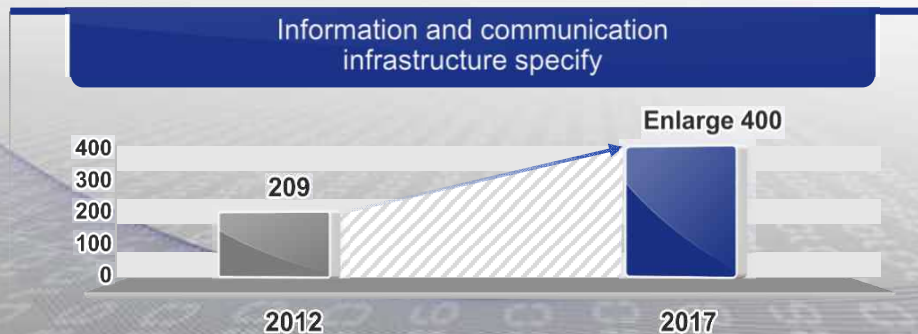


◆ CIIP - Critical Information Infrastructures Protection

- ✓ Operates in the sectors such as telecommunications, finance, administration, and energy from cyber attacks

◆ ISMS – Information Security Management System

- ✓ Providing certification after checking whether an organization systematically established appropriate security management procedures and continuously managed and operated them to protect major information assets



Major Policies (Industry)

◆ Promoting Cyber Security Industry

Construction of Open
Innovation Lab for Incubating
Cyber Security Start-up



Construction of Test Bed for
R&D of Cyber Security New
Products and Test Certification



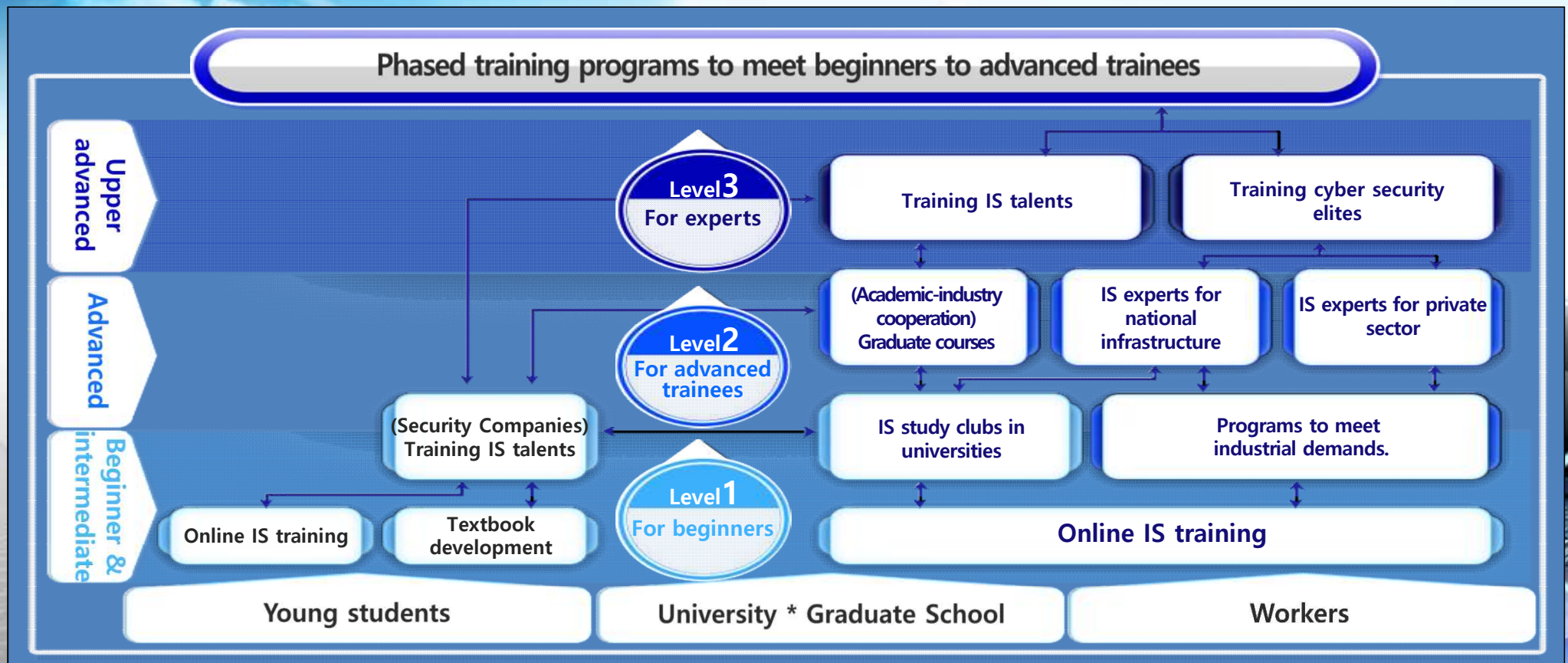
Construction of
One-stop Service Center
for Cyber Security
Company Promotion



Preparing of Enactment of the
「Cyber Security Industry
Promotion Act」



Major Policies (Expert Training)



Major Policies (Awareness)

- ◆ Street campaign to distribute music videos and songs designed to advertise information security



Security Incident Prevention and Response

Security incident prevention activity

- **Monitor internet network in Korea for abnormal signs 24/7**
 - Check 2.3 million Korean websites for malicious codes
- **Inspect information security vulnerability and take measures for protection**
 - Information protection inspection on ICT service providers
 - Make remote inspection on website vulnerability and take protection measure
- **Operate KrCERT for rapid response of cyber security incident and cooperate at home and abroad**
 - Cyber exercise for security incident response with AP regional CERT and related agencies in Korea twice a year



Personal information protection

- Educate PI protection and Distribute *i*-PIN
 - Delete PI disclosure on websites 24/7
 - Expand targets (520 thousand→ 3.5 million) under PI protection act (Sep 30, 2011)
 - Technical support center of PI protection for SMEs (Oct. 19, 2011)
 - Promote Personal Information Management System(PIMS) (22 companies, May 2013)
- √ PIMS: Comprehensive system for management for technical measure (ex. firewall, encryption), responsible agency and compliance (adopted in Nov. 2010)



Healthy cyber culture

● Run national campaign for healthy cyber culture

➤ Set up national association

- √ Established in August, 2010
- √ With 65 organizations including the government, internet companies and private organizations
- √ Initiated campaign and signed a MOU for good replies for 100 days

➤ Korea Internet Star(KIS)

- √ Comprised of elementary and middle school students to lead healthy cyber culture

● Internet ethics education

➤ Educate teenagers, parents, teachers and children on internet ethics

● Produce and distribute Internet ethics B.I.(Brand Identity)

- ### ➤ Develop and utilize character and logo song for Internet ethics to give impression on people



Promote ICT service abroad

- **Support ICT business to advance into the global market**

- **Global Market for Digital Convergence**

- √ Roadshow, showcase, government consulting service

- **Support ICT strategic items**

- √ Items: Smart 4G, media contents, broadband, information protection, mobile TV, IPTV, etc

- **ICT Expert Training Program**

- (K-LINK: Korea-Global ICT Leaders Information Network)

- **12 courses, 330 trainees**

- √ Provide education for overseas experts (about 4,300 officials, 145 countries) since 1998

- **International conference and international organization activities**

- WICS

- ITU-PP 14, Telecom World

- OECD

- World Bank



118 call center

● Run center to provide consulting service related to the Internet

- Receive complaints and provide consulting service related to the Internet (hacking, virus, spam, PI disclosure)
- Q&A and counseling service for PI protection act

● Easy to remember, anytime/anywhere

- Call : free consulting service 24/7
√ the average number of call per day : 1,300
- Website : www.118.or.kr
- Twitter & Facebook ID : kisa118



Cyber Security Incident

I. What is Cybersecurity ?

① DDoS Attack (3.4, 7.7)

② Information Stealing

(NH Bank, SK Comms)

③ Spam Mail Relay

Global Mail Server

Server Located On Overseas

DB

Results

- System Shut Down
- Sabotage
- Criminal Exploit

Results

- Sold on black market
- Abuse 2nd attack

Results

- Advertising message
- Annoying message
- Malicious code attached

8. Execute Command

Bot PCs

7. Forward Command

C&C (command & control) Server

Exploit Server

Bot

1. Hack and Procure C&C Servers
6. Command attack

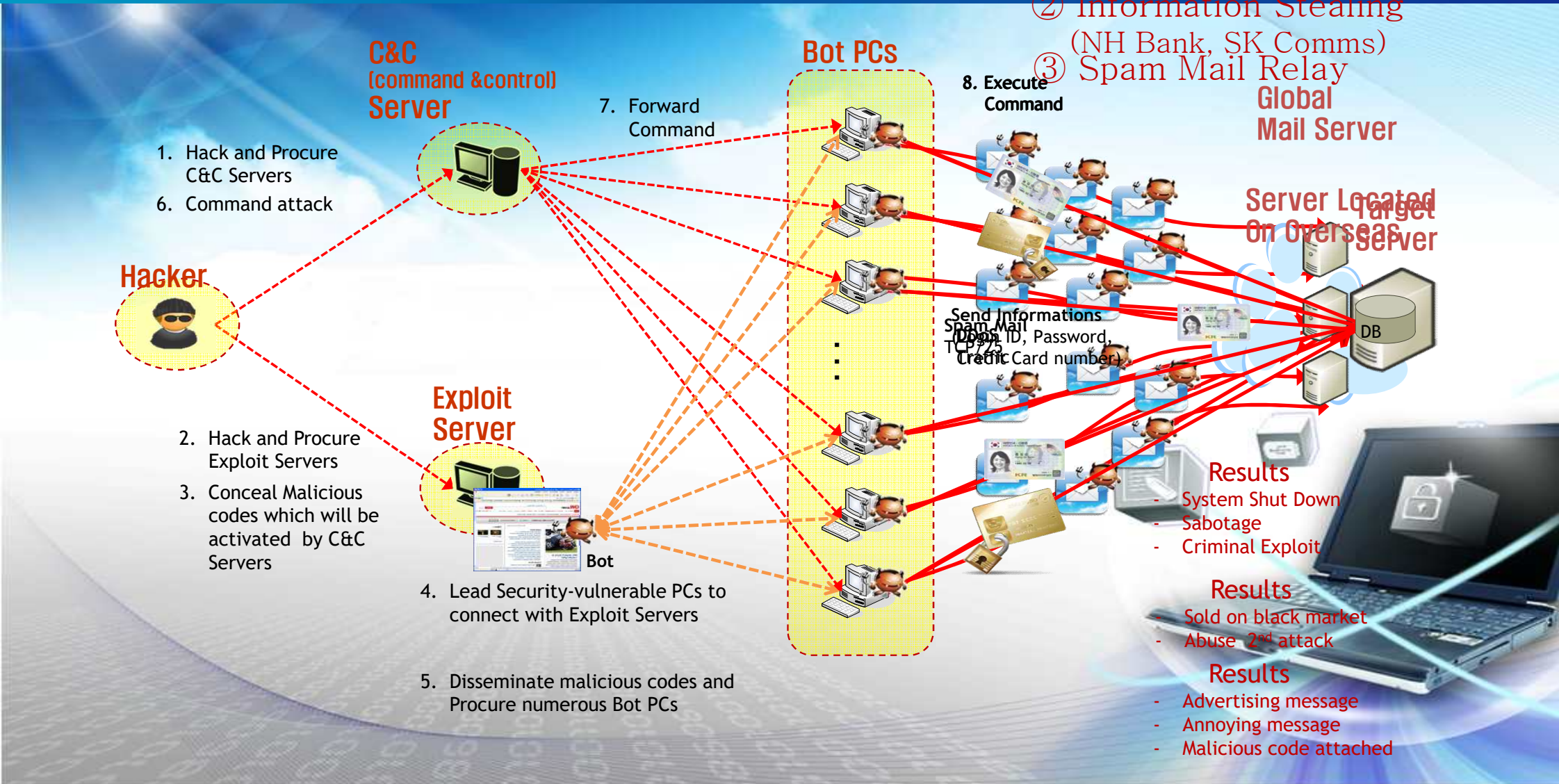
2. Hack and Procure Exploit Servers
3. Conceal Malicious codes which will be activated by C&C Servers

4. Lead Security-vulnerable PCs to connect with Exploit Servers

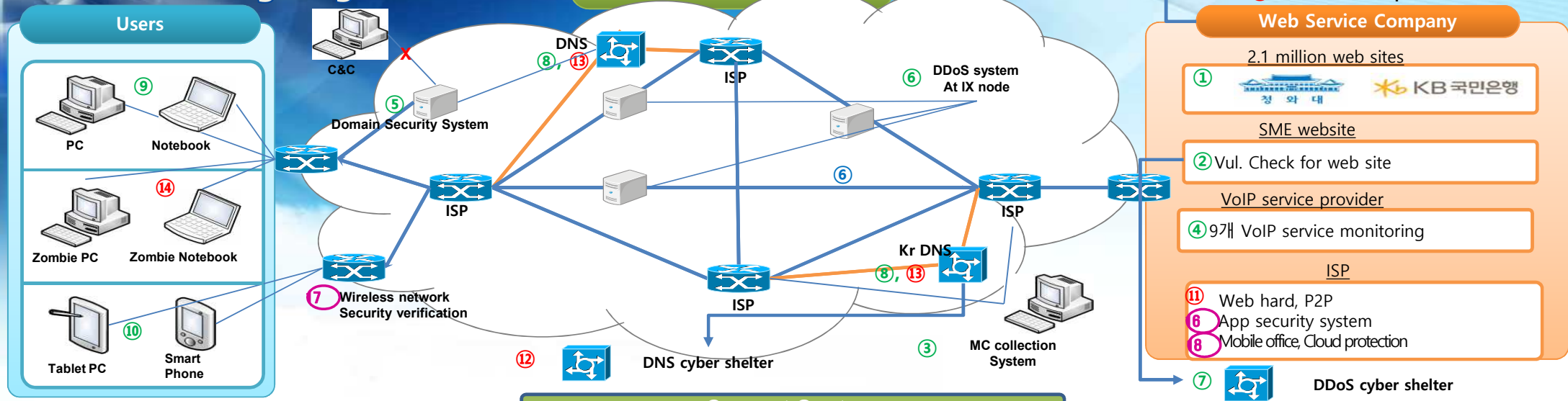
5. Disseminate malicious codes and Procure numerous Bot PCs

Hacker

Send Informations
ID, Password,
TCP/IP,
Credit Card number



IT Security Systems



Current System

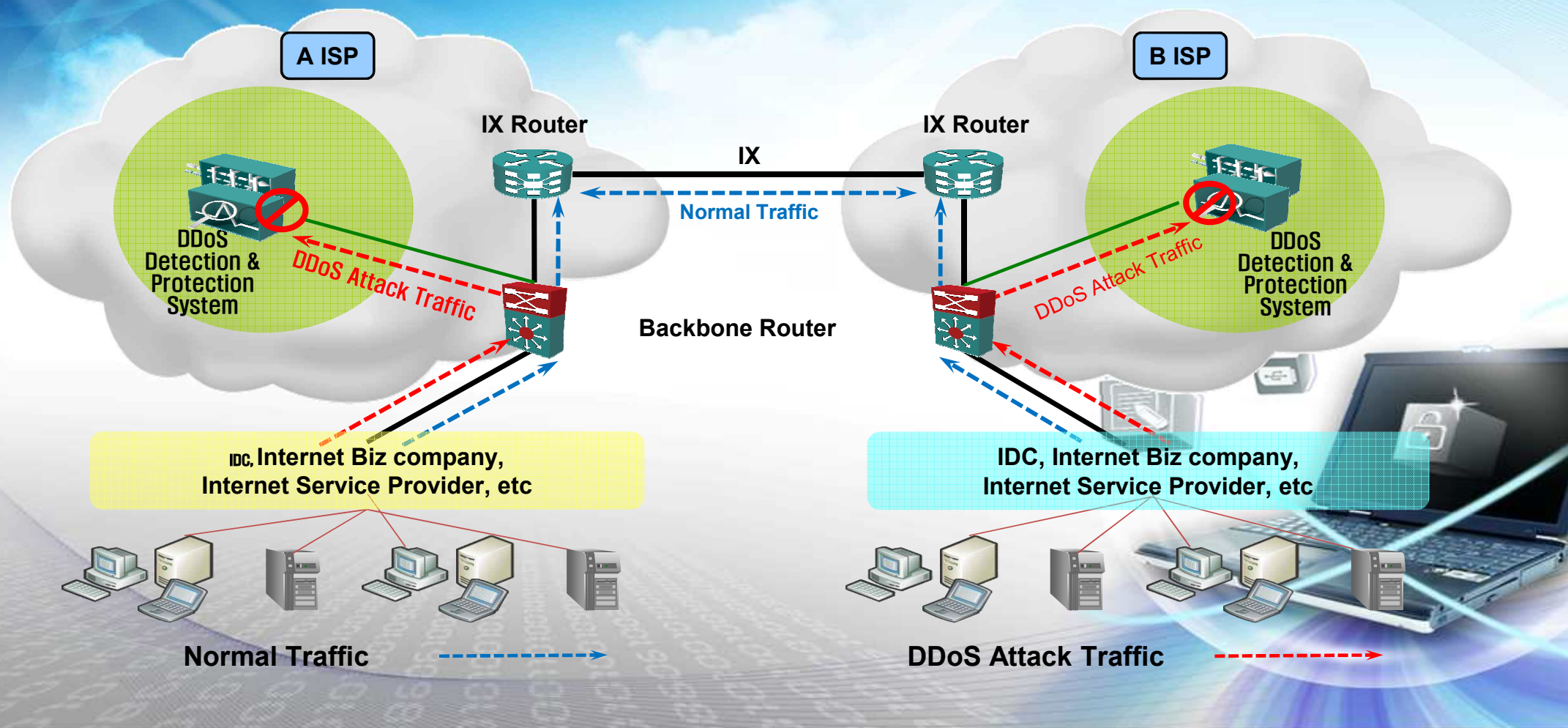
①	MC Finder	Checks 2.1 million websites to fine MC	⑥	DDoS System	DDoS detection system at Internet Exchange node
②	Whistle, Castle	Check vulnerabilities for SME websites	⑦	DDoS Cyber Shelter	Reroute DDoS packets to Shelter
③	MC collection System	Collecting MC using virtual PC	⑧	Kr DNS DDoS System	DDoS defense system for Kr DNS
④	VoIP Monitoring System	Monitoring system for VoIP	⑨	Cyber Curing System	Pop-up window for zombie PC users and provide vaccines
⑤	Domain Security system	Block C&C from sending command to zombie PC	⑩	Convergence Security System	Security system for smart phone, wireless communication

New System

⑪	Webhard service protection	Monitor web hard service, P2P's update or download S/W	⑮	Active X replacement tech.	R&D Active X replacement technology
⑫	DNS protection	DDoS system for SME's hosting co. DNS server	⑯	Device Security	App security review
⑬	Kr DNS DDoS system	DDoS protection for all Kr DNS servers	⑰	Wireless network security	3G, 4G, WiFi security
⑭	Forensic Tool	Automatically collect evidence, analyze Infected PCs	⑱	Mobile service protection	Protection for new IT services such as mobile office, mobile cloud, smart screen

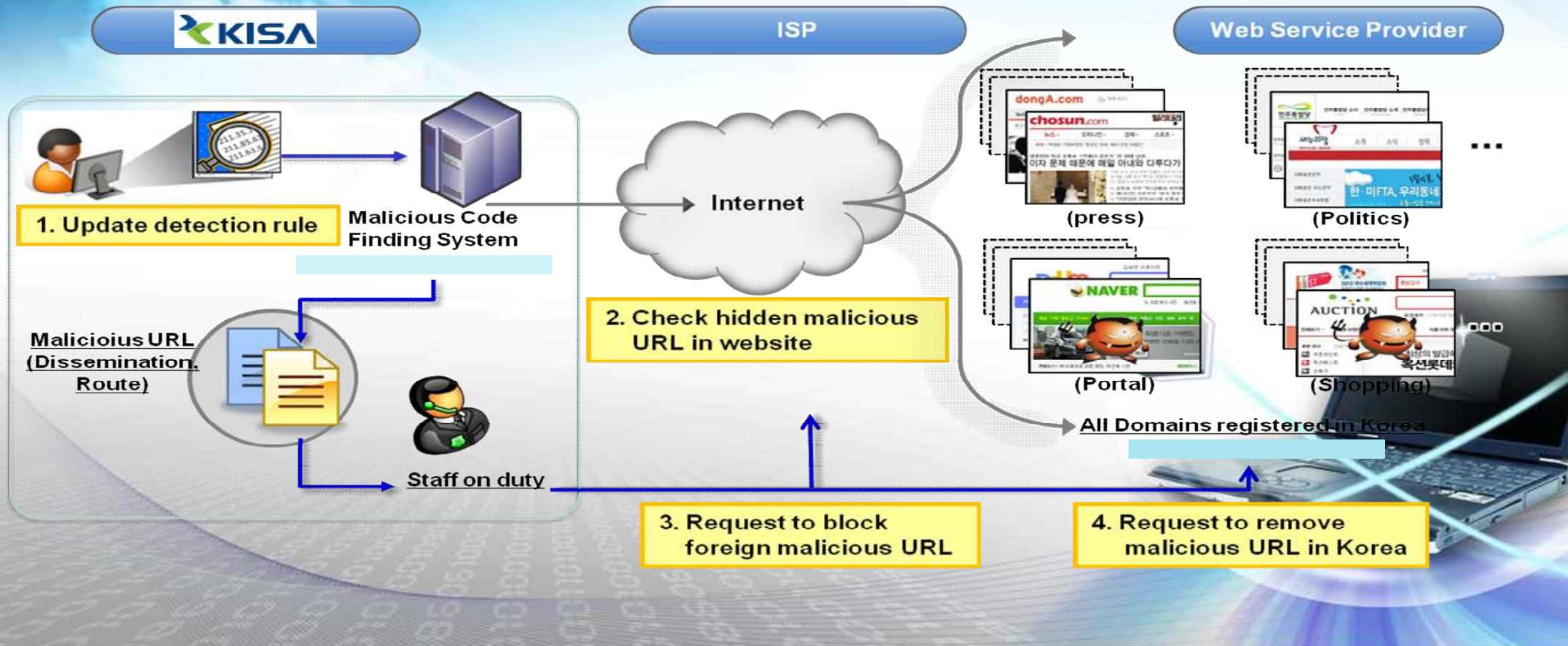
DDoS Defense System

- Early DDoS attack detection at Internet Exchange (IX) node



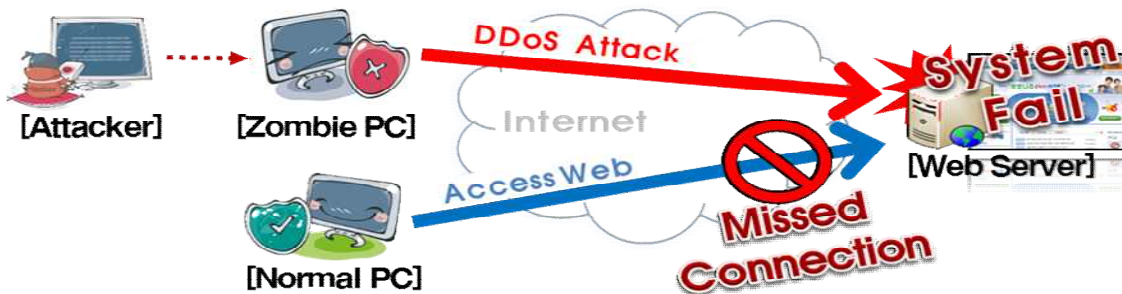
Malicious Code Detection System

- ❑ Monitor web-embedded malicious code (2.3 Mil Domestic Websites)
- ❑ Enhance the security of domestic websites and Internet users



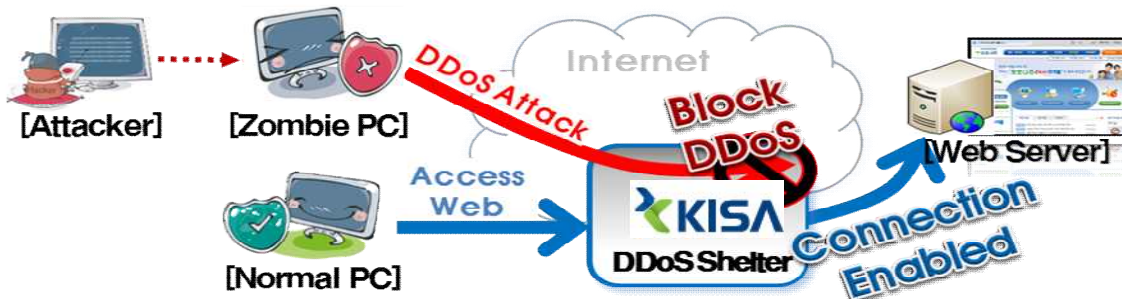
DDoS Shelter System

- DDoS defense service at the government level for SMEs
 - It's blocking DDoS attack and supporting normal web service of SMEs



- **System is failed by DDoS Attack**
 - Normal web server is failed by DDoS Attack
- **Applying DDoS Shelter**
 - Replace the Web Server IP in DNS with IP provided by the DDoS Shelter

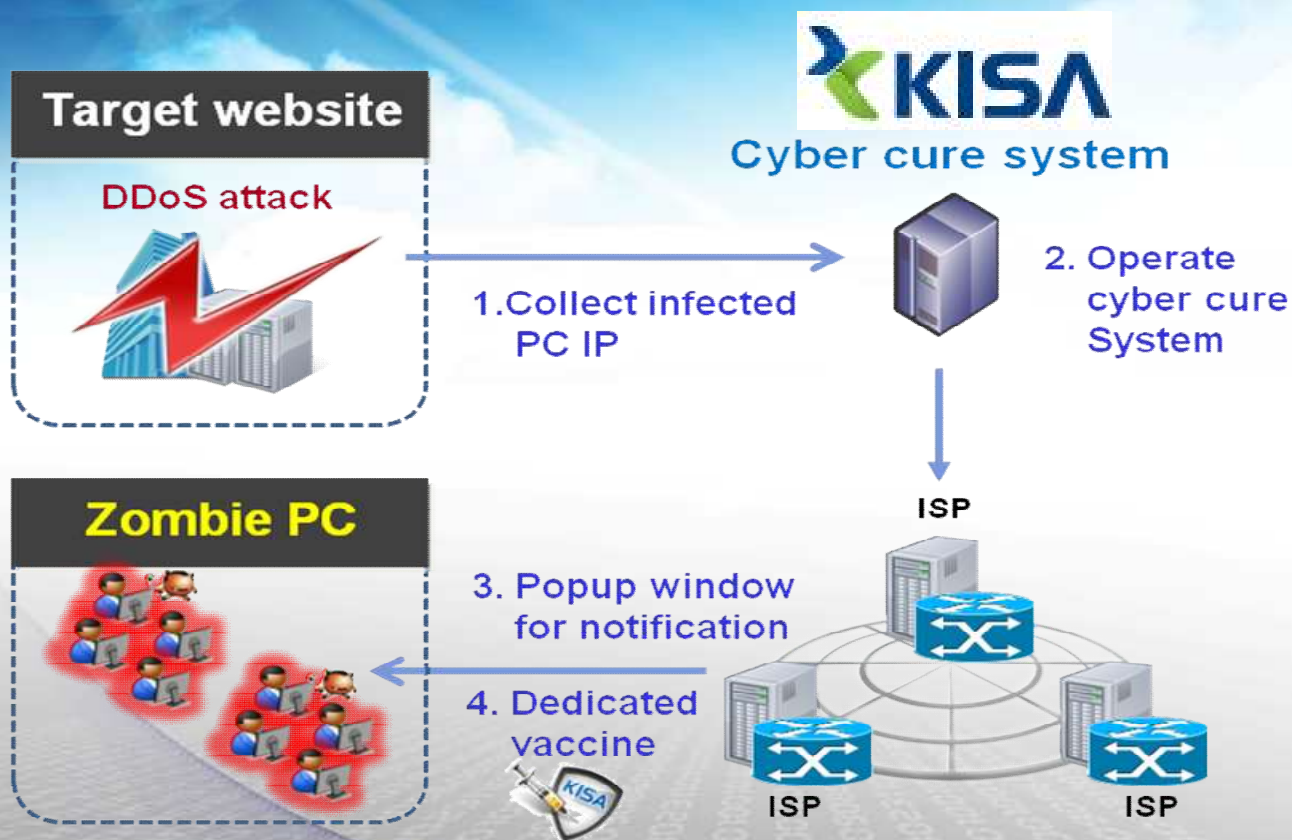
After applying DDoS Shelter



- **DDoS Traffic detoured from Web Server to DDoS Shelter**
 - Normal & DDoS traffic flows to the DDoS Shelter
- **DDoS traffic blocked and Normal traffic allowed**
 - The DDoS Shelter filters DDoS traffic and normal traffic flows into the web server

Cyber Curing System

- Provide a notification of malware infection and removal method using popup window
- Effective measure against large-scale DDoS attack



감염PC 사이버 치료서비스

Stop!
Cure zombie PC

현재 사용하신 PC가 악성코드에 감염되어, 한국인터넷진흥원에 신고되었습니다.

이 PC는 해커의 조종을 받아, 귀하의 개인정보 유출 또는 특정사이트 DDoS 공격에 악용될 수 있으니, 반드시 아래 맞춤형 전용백신으로 점검 및 치료하신 후, 인터넷을 사용하시기 바랍니다.

Download dedicated vaccine

※ 관련법률 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의3
※ 문의사항 : 전국 어디서나 국번 없이 ☎118(한국인터넷진흥원 상담센터)
[본 서비스 상세소개 페이지 가기](#) / [FAQ보러가기](#)

Ministry of Science, ICT & Future Planning

KISA

Rapid and continuous increase of Cyber threat

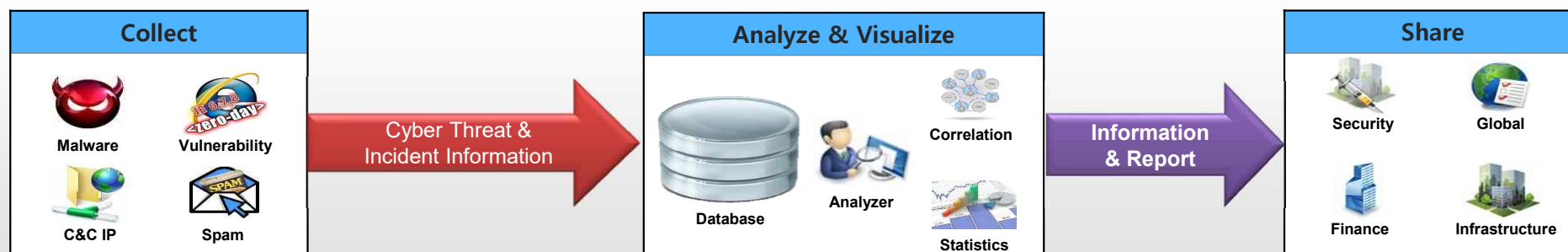
- Cyber attacks such as DDoS, APT, EMP are becoming more sophisticated
- Cybersecurity vulnerability increases from expansion of application services and growing number of IT devices such as smart phones, etc



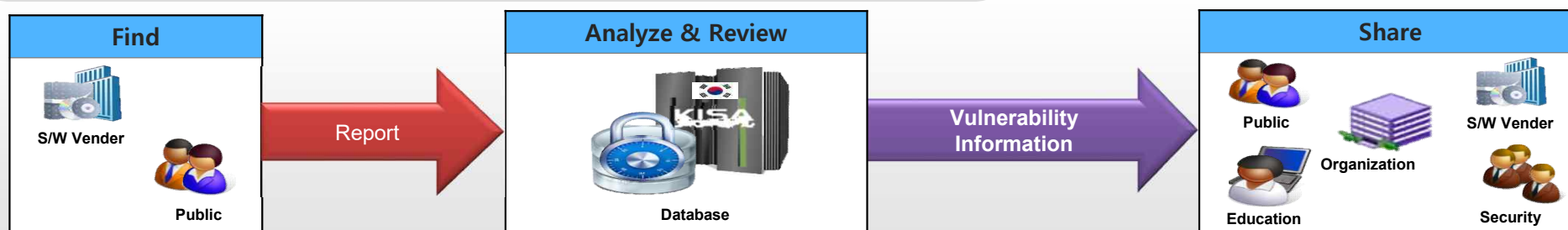
- Stuxnet : a computer worm that targets industrial control systems that are used to monitor and control large scale industrial facilities like power plants, dams, waste processing systems and similar operations
- APT(Advanced Persistent Threat) : APT uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term
- EMP(Electromagnetic Pulse) : EMP is a short burst of electromagnetic energy and is generally damaging to electronic equipment.

Reinforcement of Cyber Incident Analysis

Cyber Threat & Incident Information Analysis · Sharing System

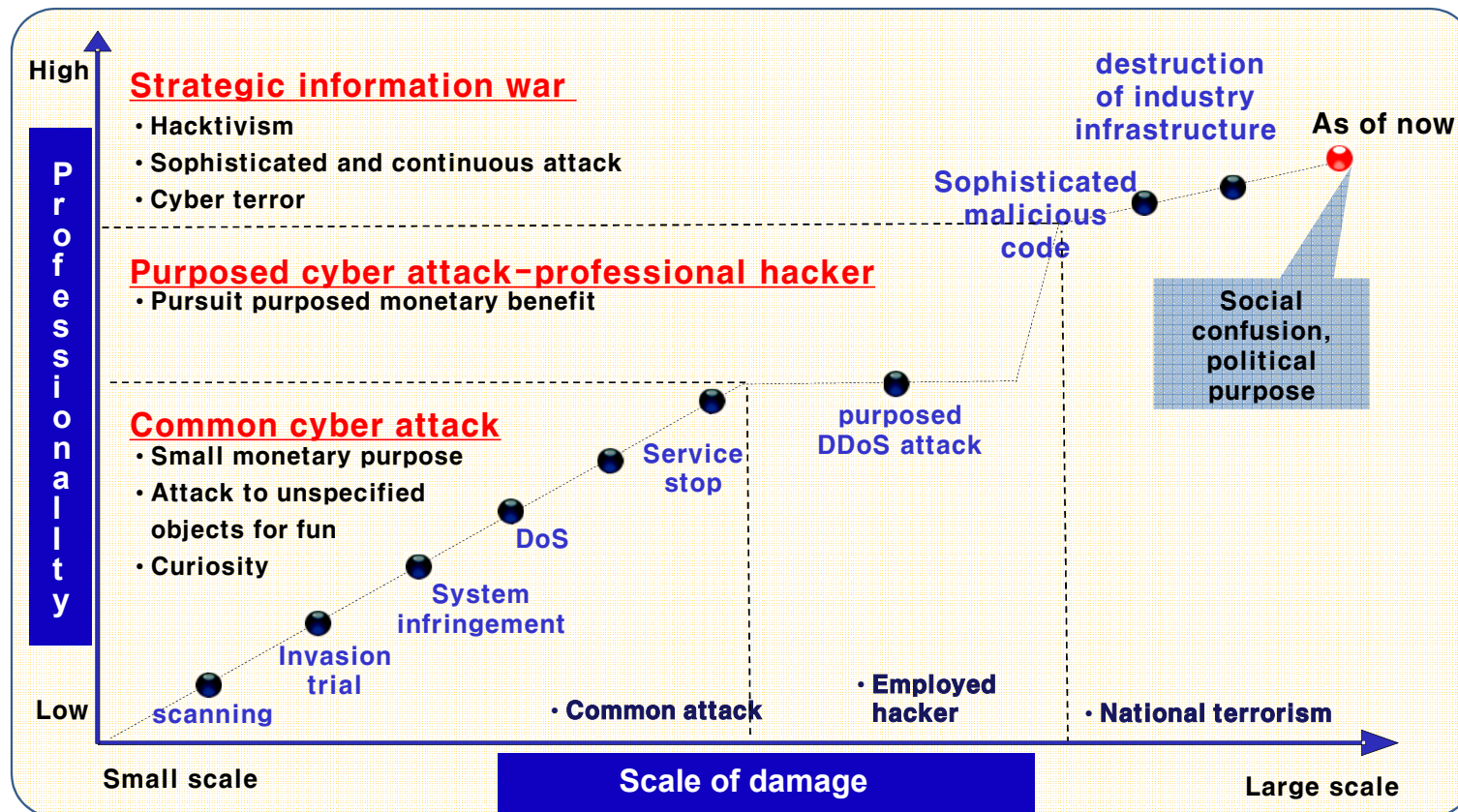


National Security Vulnerability Database



Changes in trend of cyber attack

- (Professionality) Beginner → Professional → strategic information war
- (Scale of damage) small scale of individual, group → massive information disclosure → interrupt system management(large scale)



Cyber Attack Incidents



Cyberwarefare



Cyberwarfare in South Korea[\[edit\]](#)

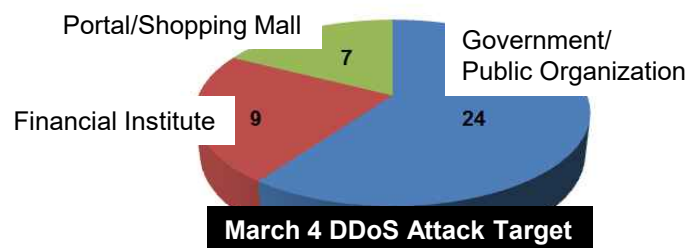
Main article: [2013 South Korea cyberattack](#)

With ongoing tensions on the Korean Peninsula, [South Korea's defense ministry](#) stated that South Korea was going to improve cyber-defense strategies in hopes of preparing itself from possible cyber attacks. In March 2013, South Korea's major banks – Shinhan Bank, Woori Bank and NongHyup Bank – as well as many broadcasting stations – KBS, YTN and MBC – were hacked and more than 30,000 computers were affected; it is one of the biggest attacks South Korea has faced in years.^[52] Although it remains uncertain as to who was involved in this incident, there has been immediate assertions that North Korea is connected, as it threatened to attack South Korea's government institutions, major national banks and traditional newspapers numerous times – in reaction to the sanctions it received from nuclear testing and to the continuation of [Foal Eagle](#), South Korea's annual joint military exercise with the United States. North Korea's cyber warfare capabilities raise the alarm for South Korea, as North Korea is increasing its manpower through military academies specializing in hacking. Current figures state that South Korea only has 400 units of specialized personnel, while North Korea has more than 3,000 highly trained hackers; this portrays a huge gap in cyber warfare capabilities and sends a message to South Korea that it has to step up and strengthen its Cyber Warfare Command forces. Therefore, in order to be prepared from future attacks, South Korea and the United States will discuss further about deterrence plans at the Security Consultative Meeting (SCM). At SCM, they plan on developing strategies that focuses on accelerating the deployment of ballistic missiles as well as fostering its defense shield program, known as the Korean Air and Missile Defense.^[53]

March 4th 2011 DDoS Attack

□ March 4th DDoS attack in 2011, evolved from July 7th DDoS in 2009

Overview – DDoS attack targeting 40 major Korean websites



Classification	Mar 4	Jul 7
# of Zombie PCs	116,299	115,044
target websites	40	36
# of Blocked C&C servers	748	538
# of destroyed HDDs	756	1,466

March and July DDoS attacks are similar in used no. of exploited zombie PCs and infection method however **March DDoS attack Method is more Intelligent and destructive than July DDoS**

Implications

Attack method continually changes with the response to the attack

KISA Response		Change in Attack Method
Vaccine distribution via www.boho.or.kr	⇒	Block zombie PC's access to www.boho.or.kr
Effective defense against DDoS Attack	⇒	Destroy HDD just after the infection
Hard disk damage prevention guideline	⇒	HDD is destroyed even at safe mode booting

March 20th 2013 Cyber Attack

- **Attack on 6 broadcasting and financial companies which destroyed 48,700 PC, Server, ATM(March 20th)**
 - Distributed Malicious Code through “nalsee.com(Weather Forecast)” and infected 800 PCs (March 25th)
 - Destroyed 58 Digital YTN website servers (March 26th)
 - Deleted data from 14 conservative groups’ website (March 26th)
- **Recovered to normal operation (March 29th)**
 - Recovery of 58 Digital YTN web servers (April 12th)



Jun 25th 2013 Cyber Attack

- Hacking and DDos attack happened against 24 government offices, news outlets/broadcasting company(6.25)
- Disclosure of personal information of 200,000 registered users of the government office' s website

※ disclosed personal information : name, date of birth, ID, address, IP





북한 인터넷 다운... '사자 코털' 건드려서?

23일 새벽 1시~오전 11시, 북한 인터넷망 다운
 "'라우터'가 디도스 공격 받았을 때와 같은 모습"

최진욱 기자·심희영 기자·김정현 기자



Truth of BotNet???



1977. 12. 31. PSY



1987. 3. 25. RYU.H.J



1983. 1. KIM, JUNG EUN.

Major responses

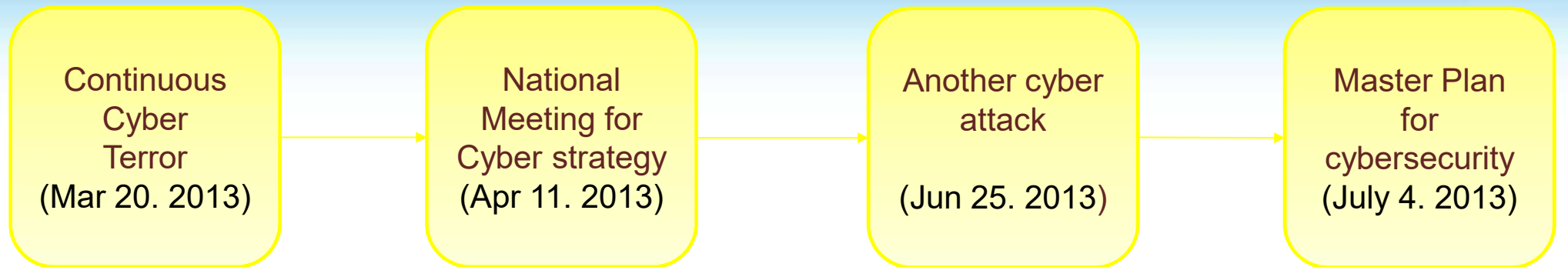
- ① **Raised the alert level on cyber risk to level three on a five-ties scale(June 25)**
- ② **Blocked relevant malicious websites through mutual assistance with domestic and international ISPs and CERTs**
- ③ **Detected and deleted the websites where DDoS attack script was being distributed**
- ④ **Developed and distributed the specialized vaccine programs for the malicious codes**
- ⑤ **Shared information and cooperated with relevant national organizations including NIS and Korea National Police Agency(KNPA)**
- ⑥ **Provided assistance for those affected by the government personal information disclosure incident through personal information incident report center**

National Cybersecurity Plan



Background of establishment of Master plan for cyber security

- Continuous Cyber terror such as March 4, July 7(2011), March 20 urged Korean government to develop master plan for cyber security for Korea to respond systematically to those attempts

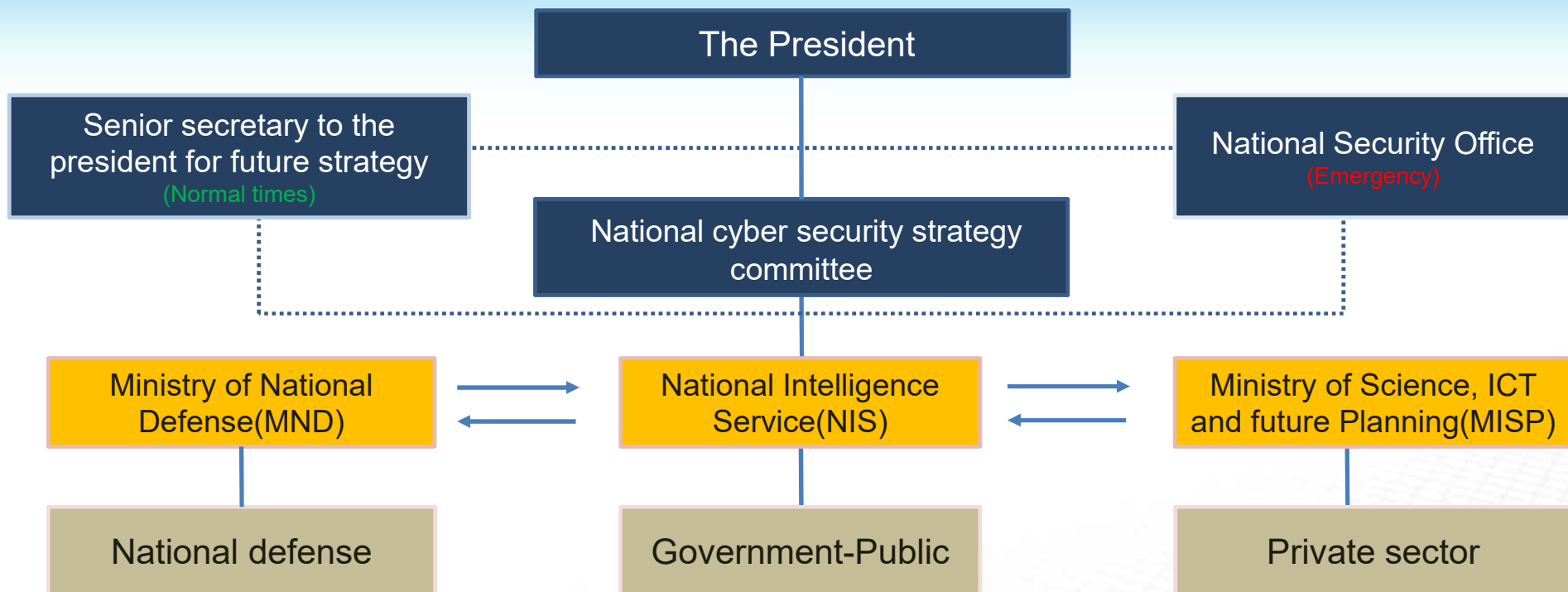


Establishing Master plan for cyber security for Korea by 16 relevant government agencies including Blue house, NIS, MISIP, MND, MOI, etc

To add regularly close inspection on major government homepages, Expansion of DDoS shelter, Introduction of safety evaluation on IC objectives such as communications company

Previous Risk management system for national cyber security

- Based on 'Rule for managing national cyber security' (Presidential instruction no.267, 2010.4.16 partial amendment), separate response system for each government- public sector, private sector and national defense sector is operated



Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

- 1 Enhance the prompt response system against cyber threats (Prompt)
- 2 Build the smart cooperation system between the relevant authorities (Cooperative)
- 3 Enhance the robustness of protection of cyber space (Robust)
- 4 Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower

Full-out enhancement and complementation of the situation propagation system

Establishment of the cooperation system for response against cyber threats

Activation of sharing of threat information among private sector, government and military

Enhancement of security of computer networks of the national Critical infrastructure

Removal of cyber security blind spots in public sector

Enhancement of security level and awareness in private sector

Recruitment, fostering and systematic management of cyber security experts

Fostering of the information security industry and reinforcement of technology competitiveness

Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

1 Enhance the prompt response system against cyber threats (Prompt)

Build the smart cooperation system between the relevant authorities (Cooperative)

Enhance the robustness of protection of cyber space (Robust)

Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower

Activation of sharing of threat information among private sector, government and military

Enhancement of security level and awareness in private sector

Full-out enhancement and complementation of the situation propagation system

Enhancement of security of computer networks of the national Critical infrastructure

Recruitment, fostering and systematic management of cyber security experts

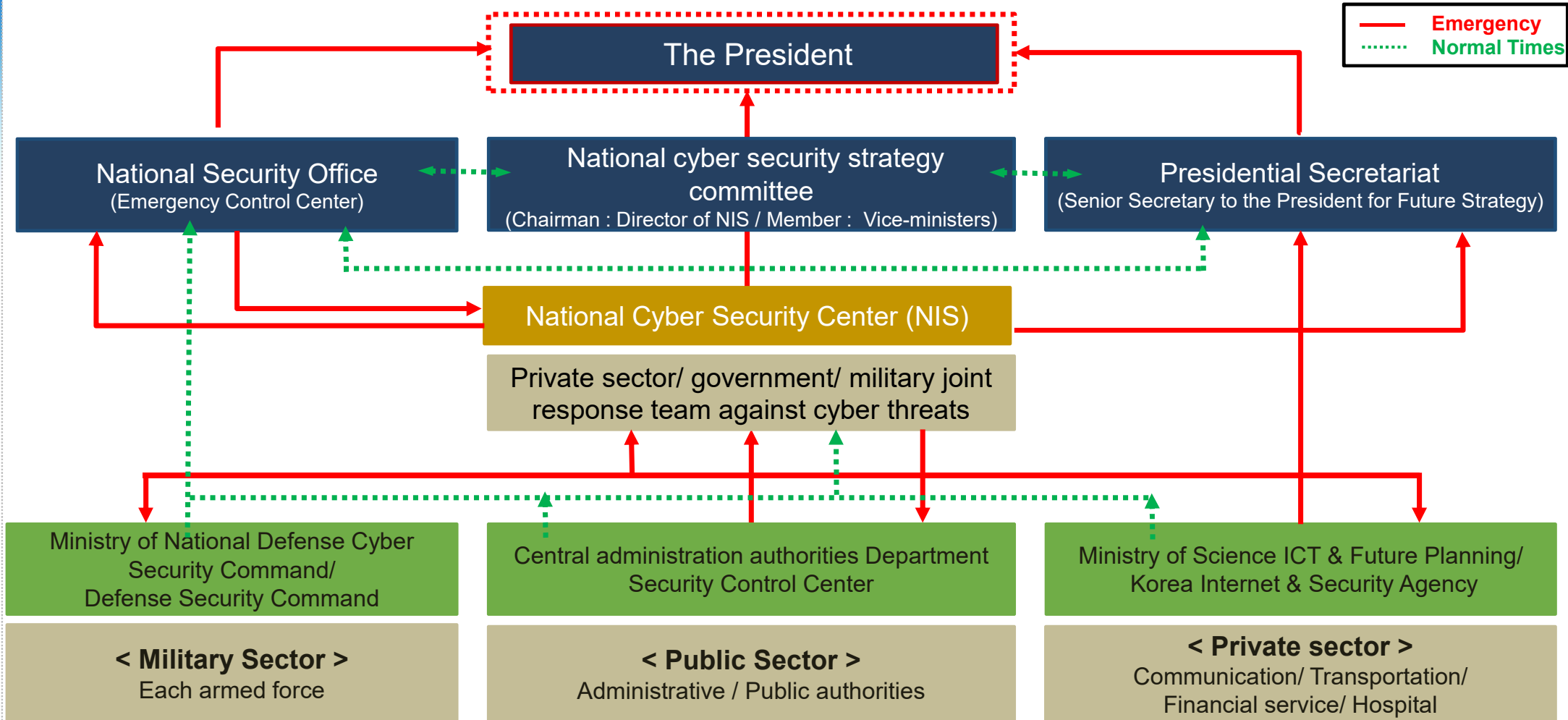
Establishment of the cooperation system for response against cyber threats

Removal of cyber security blind spots in public sector

Fostering of the information security industry and reinforcement of technology competitiveness

Main Tasks(1/9)

Establishment of the cyber security control tower



Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

- 1 **Enhance the prompt response system against cyber threats (Prompt)**
Build the smart cooperation system between the relevant authorities (Cooperative)
Enhance the robustness of protection of cyber space (Robust)
Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower

Activation of sharing of threat information among private sector, government and military

Enhancement of security level and awareness in private sector

Full-out enhancement and complementation of the situation propagation system

Enhancement of security of computer networks of the national Critical infrastructure

Recruitment, fostering and systematic management of cyber security experts

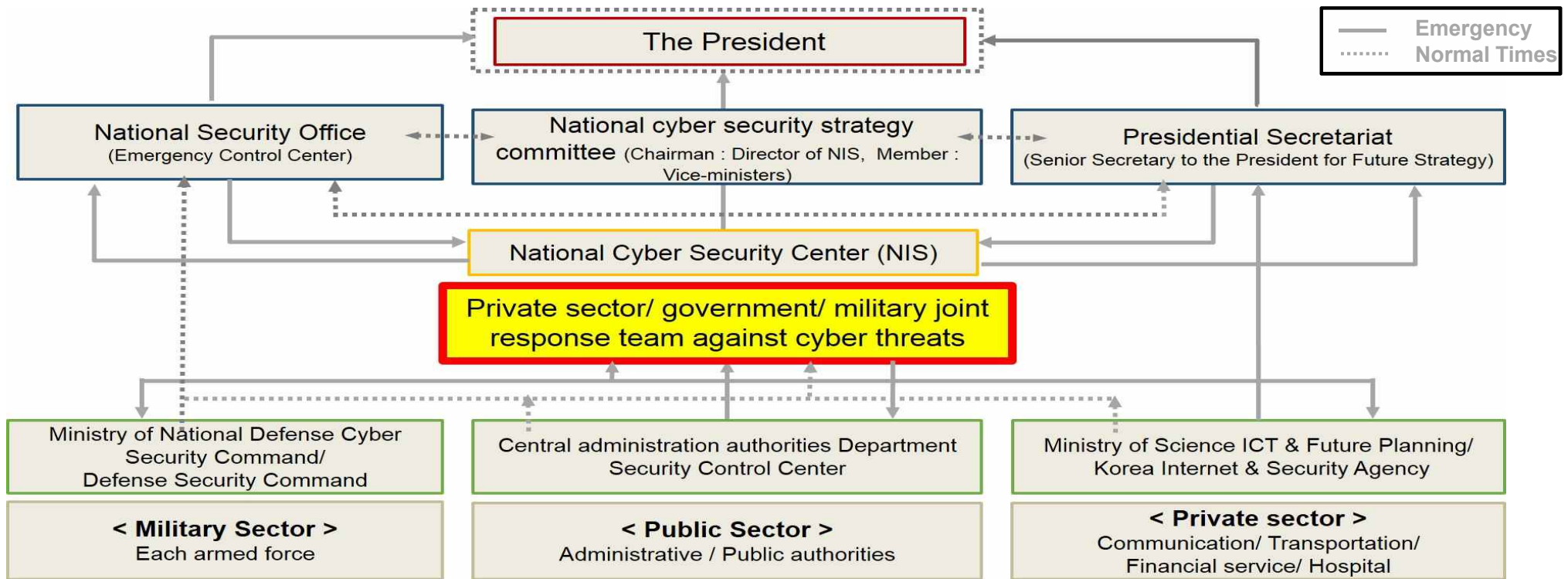
Establishment of the cooperation system for response against cyber threats

Removal of cyber security blind spots in public sector

Fostering of the information security industry and reinforcement of technology competitiveness

Main Tasks(2/9)

Full-out enhancement and complementation of the situation propagation system



- Enhance the cyber emergency report and propagation system (National Security Office, NIS, all authorities)
- Enhance the cyber threat warning system

Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

- Enhance the prompt response system against cyber threats (Prompt)
- 2 Build the smart cooperation system between the relevant authorities (Cooperative)**
- Enhance the robustness of protection of cyber space (Robust)
- Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower	Full-out enhancement and complementation of the situation propagation system	Establishment of the cooperation system for response against cyber threats
Activation of sharing of threat information among private sector, government and military	Enhancement of security of computer networks of the national Critical infrastructure	Removal of cyber security blind spots in public sector
Enhancement of security level and awareness in private sector	Recruitment, fostering and systematic management of cyber security experts	Fostering of the information security industry and reinforcement of technology competitiveness

▶ Establishment of the cooperation system for response against cyber threats

- Reinforce cooperation between cyber response authorities
- Reinforce operation of the 'Private Sector / Government / Military Joint Response Team Against Cyber Threats' 
- Reinforce international cooperation in relation with cyber security

▶ Activation of sharing of threat information

- Prepare the pan-national sharing system of information on cyber threats
- Improve the capability to detect/collect new cyber security treats

Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

Enhance the prompt response system against cyber threats (Prompt)
Build the smart cooperation system between the relevant authorities (Cooperative)
3 Enhance the robustness of protection of cyber space (Robust)
Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower

Activation of sharing of threat information among private sector, government and military

Enhancement of security level and awareness in private sector

Full-out enhancement and complementation of the situation propagation system

Enhancement of security of computer networks of the national Critical infrastructure

Recruitment, fostering and systematic management of cyber security experts

Establishment of the cooperation system for response against cyber threats

Removal of cyber security blind spots in public sector

Fostering of the information security industry and reinforcement of technology competitiveness

▶ Enhancement of security of computer networks of the national critical infrastructure

- Consider measures to protect specialized infrastructure by theme
- Expand designation of and intensively manage the key IT infrastructure

▶ Enforcement of security infrastructure and removal of cyber security blind spots

- Upgrade the voluntary security management level of the authorities
- Extend the information security system and verify security of the network equipment
- Propose preliminary security measures for smart mobile/cloud computing

▶ Enhancement of security level and awareness in private sector

- Preparation of enterprise information security management system and expand support
- Reinforce internal security control of external service contractors
- Enhance awareness of cyber security of the people

Goals and strategies of the plan



Goal

Advanced Cyber Security Nation

Strategies (PCRC)

Enhance the prompt response system against cyber threats (Prompt)
Build the smart cooperation system between the relevant authorities (Cooperative)
Enhance the robustness of protection of cyber space (Robust)

4 Make the creative basis for cyber security (Creative)

Main Tasks

Establishment of the cyber security control tower

Activation of sharing of threat information among private sector, government and military

Enhancement of security level and awareness in private sector

Full-out enhancement and complementation of the situation propagation system

Enhancement of security of computer networks of the national Critical infrastructure

Recruitment, fostering and systematic management of cyber security experts

Establishment of the cooperation system for response against cyber threats

Removal of cyber security blind spots in public sector

Fostering of the information security industry and reinforcement of technology competitiveness

▶ Recruitment, fostering and systematic management of cyber security experts

- Recruit and foster elite cyber experts (5,000 experts)
- Make the cyber warriors manpower pool, and foster/manage cyber warriors in a systematic manner
- Establish the 'National Cyber Simulation Center' to foster experts (Ministry of Science, ICT & Future Planning, NIS)

▶ Fostering of the information security industry and reinforcement of technology competitiveness

- Create and activate the information protection market (Ministry of Science, ICT & Future Planning)
- Develop the world-leading information protection technology and secure competitiveness of the product

International Cooperation

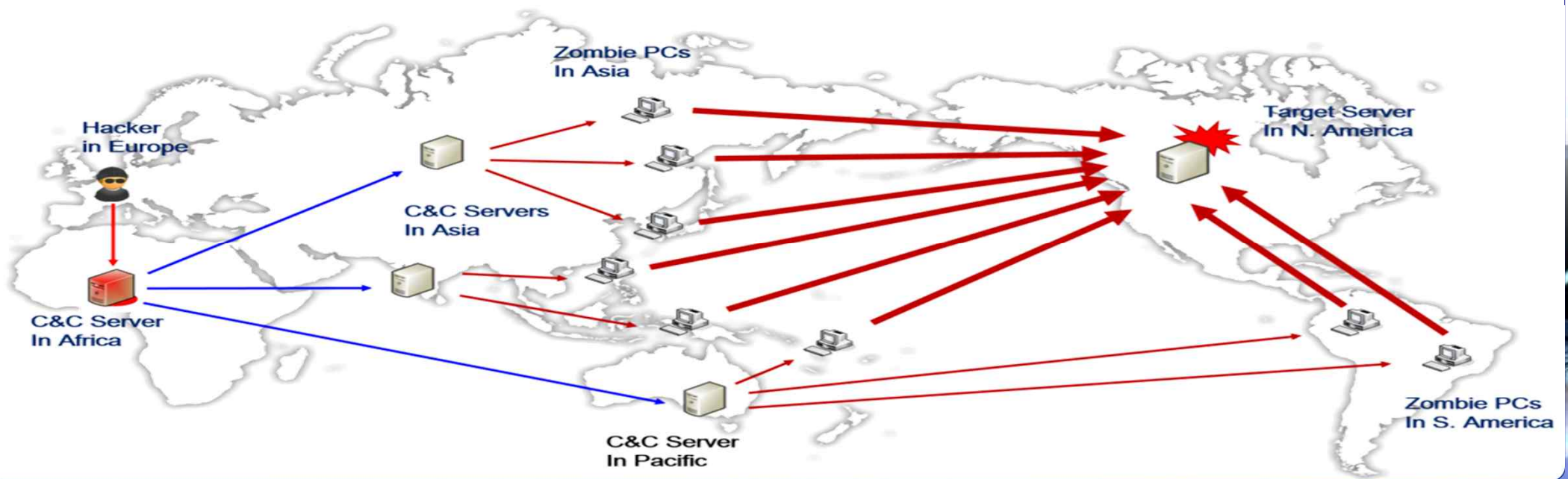


Importance of international cooperation in cyber security

Why we have to cooperate each other?

- As the globe is connected with the internet, transnational cyber attacks are possible
- International cooperation is becoming mandatory in cyber security field

< Possible scenario >



KISA activities for international cooperation

Improvement international activities for mutual response

FIRST

- Forum of Incident Response & Security Teams
- Global forum of 282 Teams from 62 Economies
- KISA sponsored 6 Korea members as Korean national CSIRT



APCERT

- Asia Pacific Computer Emergency Response Team
- Regional Forum of 25 Teams
- KISA hosted AGM & conference 2011 in Jeju
- Current Vice chair
- Moderated APCERT incident Handling drill



Security Training Course

- Training course for AP countries on CSIRT building & operation for strengthening capability & cooperation
- 203 trainees from 40 economies since 2005
- Diverse Instructors from abroad



Bilateral Cooperation

- Signing MoU with leading organizations to enhance cyber security cooperation
- Joint response to incident handling with global cyber security vendors
- Information sharing on cyber threats



Where should our collaboration go?

Meet & Talk & Raise our awareness

- Actively participation to the international organization to share threat information
- Need to reach for the common understanding among all of the economies





Thank You



DR.SIR, Jae-Chul
Sirjaechul@gmail.com