Present Status of Cyber-Terrorism and its Counter Measures in Korea

2002. 5. 21

Yang, Kunwon(yangkw@npa.go.kr)
Superintendent
Korea National Police Agency
Cyber Terror Response Center

Table of Contents

Introduction

Present Status and Analysis of Cyber Terrorism in Korea

Domestic Cyber Terrorism Cases

Countermeasures against Cyber-Terrorism

Introduction

Increasing Threats of Cyber Terrorism

- Critical Infrastructure's Increasing Dependence on IT
  - **Administration, Finance, Communication, Transportations, etc.**
  - **Integration of Information such as personal data etc.**
  - **Wide use of Internet**
- Increase of Damages by the Attacks such as System Destruction (Intrusion)
  - **Huge damages expected when Systems of Social Infrastructures attacked**
  - **Outflow, Counterfeit, or Forgery of National or Industrial Secrets and Personal Data**
- Using Cyber Terrorism as means of committing other crimes
  - **Connection with organized crimes such as Russian Mafia**
  - **Hacktivism**
- Possibilities of developing into Cyber war among countries
  - **For example, Hacker War between China and Japan**

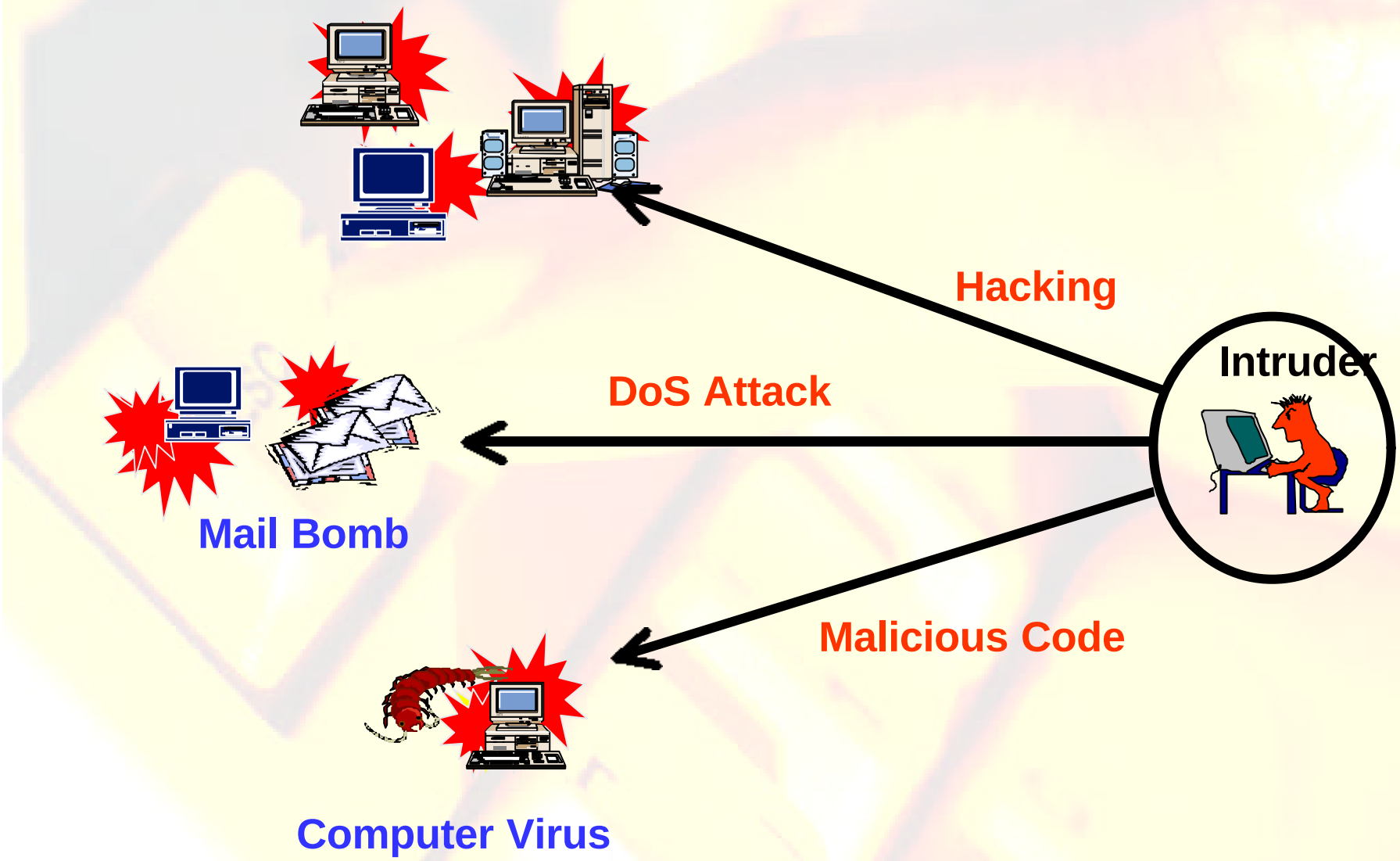
What is Cyber-Terrorism ?

- Necessity of Conceptualization
  - **Unique Characteristics of Cyber-Terrorism different from other cyber crimes and delinquencies**
  - **Special policy and legislation are needed**
- Opinions
  - Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives (Dorothy E. Denning)
  - Intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cyber systems, (Stanford University CISAC)
  - Manipulation of Information and Destruction of Network (National Counter-terrorism Activity Guideline)
  - Infringement of Critical Information Communication Infrastructures (Information Communication Infrastructure Protection Act)

Con't

- Cyber-Terrorism from the view point of Korean Police
  - **distinguished from ordinary cyber crime**
  - **Attacks such as hacking and virus against Information Communication Network itself, which cause national or social disorder or uneasiness**
    - **Korean National Police -> classifying cyber-terrorism as cyber-terrorism type crime (formal statistics)**
  - **Generally, cyber-terrorism is used as a wide concept which means aggressive activities against information communication network including cyber stalking**
- Methods
  - **Hacking, Circulation of Virus, DoS, etc.**

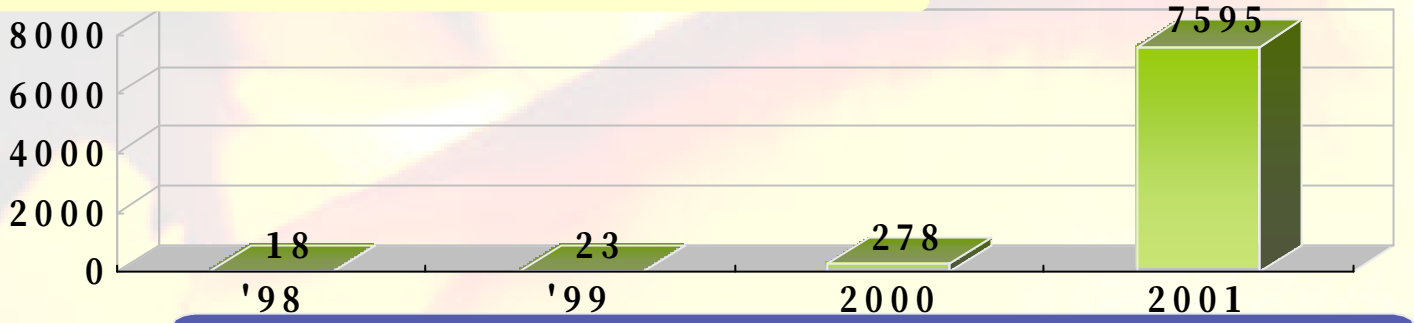
Methods of Cyber Terrorism



Present Status of Cyber-Terrorism in Korea

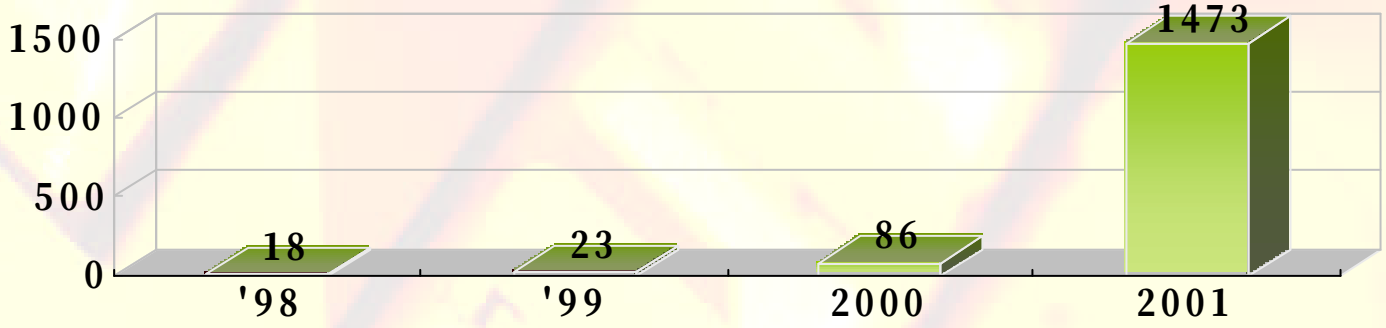
Statistics; Arrests of Hacking, Virus Crimes

Total Number of Hacking, Virus Arrests



☞ Hacking against PC and Network Game Systems
2000 : 192, 2001 : 6,122

Number of Cyber Terror cases arrested



☞ 17 times of increase in 2001
comparing to the previous year

Recent Major Case

Summary

In April 2002, detecting international hackers compromising the systems all over the world using W company's server as a route, investigators of CTRC traced them and found that they comprom-ised 11,222 systems of 95 countries from Aug. 2001 to March 2002

Damage Analysis summary

Index	Total	Identified Countries			Unidentified
		Sub-total	Korea	Other Countries	
No. of Servers	11,222	6,387	2,497	3,890	4,835
Percentage		100%	39%	61%	

☞ If the 39% of total victim systems belong to Korea, the number of Korean systems compromised is 4,300

Con't

Damage Analysis by countries

	Total	Korea	USA	China	Taiwan	Romania	India
No. of Servers	6,387	2,497	801	413	322	285	242
Percentage	100%	39.0%	12.5%	6.5%	5.0%	4.5%	3.8%
	Japan	Brasil	Canada	Hong Kong	Italia	Other Countries	
No. of Servers	196	160	115	107	91	1,158	
Percentage	3.1%	2.5%	1.8%	1.7%	1.4%	18.1%	

☞ Far from announcement of Predictive Co. of USA, Korea is rather the victim country of hacking not the hacker country according to the percentages in the table.

☞ It was found that generally, victim system is abused as route

☞ counter result of Korea's rapid increase in Information Communication Infras

(Internet users: 1.6 M in' 97 to 22 M in 2002)

Con't

Analysis of Hackers' Nationalities

	Total	Romania	Australia	Brazil	Germany	Russia
No. of Hackers	22	18	1	1	1	1

Characteristics

- ☞ Theft of critical data including credit card information
- ☞ Used automatic worm-style toolkit

  Scan, intrusion, Root compromising, sniffing, hiding processes,

  Second attack etc.
- ☞ Made Firewall, IDS useless

  (30% of victim system were equipped with security system)

  For security, management is more important than technology

Trends of Cyber-Terrorism in Korea

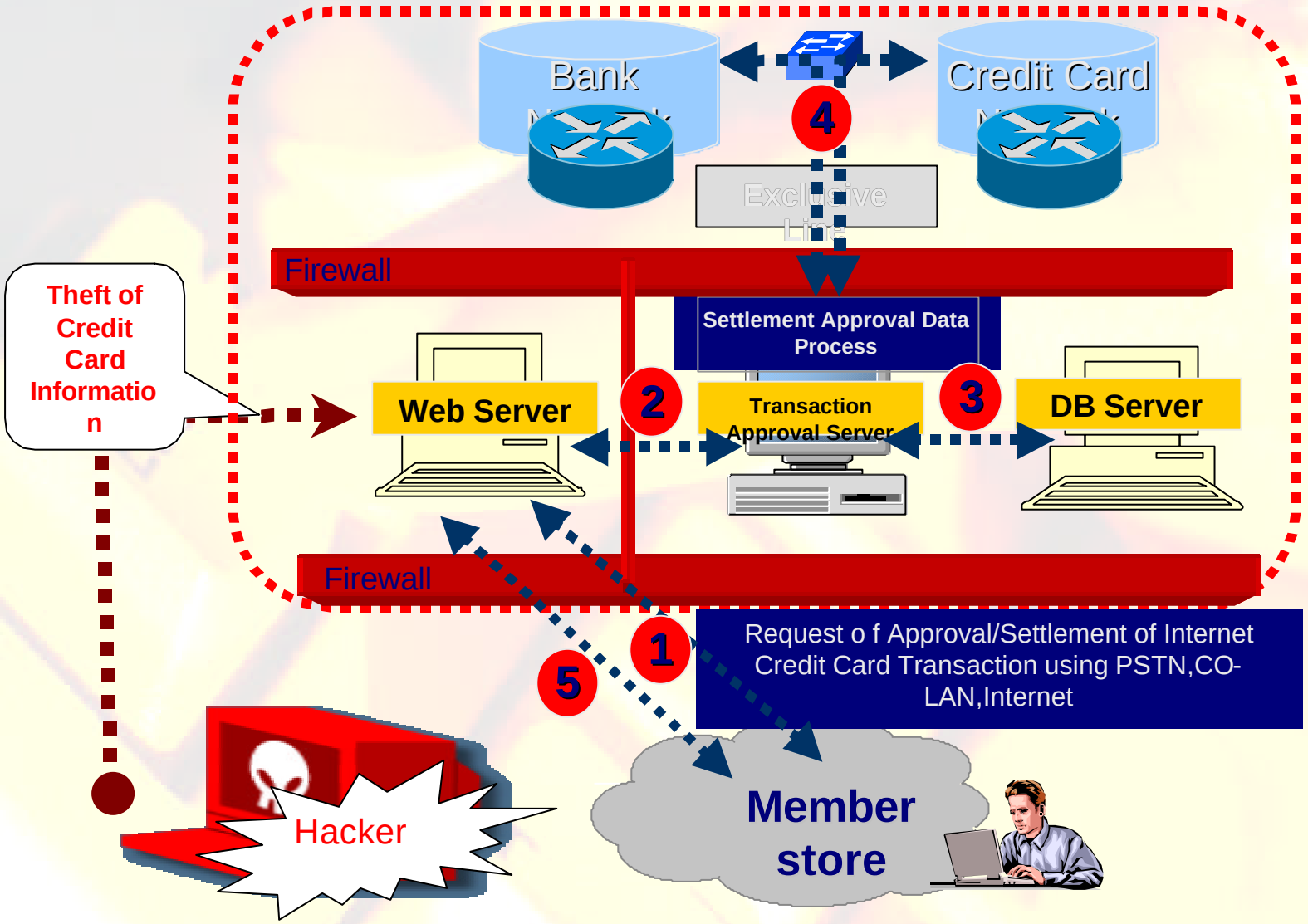
- Rapid Quantitative Increase of Damages as Information Communication Infrastructures grow
  - International Hackers abuse Korean servers as routes rather than direct target
    - Hackers usually use Korean servers which are relatively easy to attack and has good networks as routes to hide their crime
  - Many active domestic hacker community and script kiddies
- Increase in attacks against critical infras such as e-commerce network
- Huge, highly-integrated attacks against personal data
  - Gathering the personal data using web services
  - Abusing bugs in various web services such as cgi, php, asp
- International, organized hackers
- The advent of new attacking technologies which cannot be responded effectively with the traditional security systems
  - New intrusion techniques against security systems
  - Many intrusions resulted from improper management and administration of security systems
  - Techniques for avoiding the tracing

Con' t

- Increase of vandalism against domestic and overseas government agencies and NGOs
  - Increase of Vandalism such as repeating IE' s refresh(F5) key to cause overloads
  - Many communities of Portal sites, Game sites lead those activities
  - Difficult to regulate those activities legally or technically
  - Not committed by computer experts
- Increase of attacks against PCs and using PCs as route
  - IDC, super-high speed internet, PC
- Increase of property crimes using identity theft
  - Increase of fraud using personal data stolen from internet banking, online shopping mall, and game servers
  - Frauds through online P2P business
  - Internet PC rooms ubiquitous all over the country makes it more difficult to trace the perpetrators
  - Intimidation after theft of identity increased

Major Cases in Korea

Attack against Financial Network

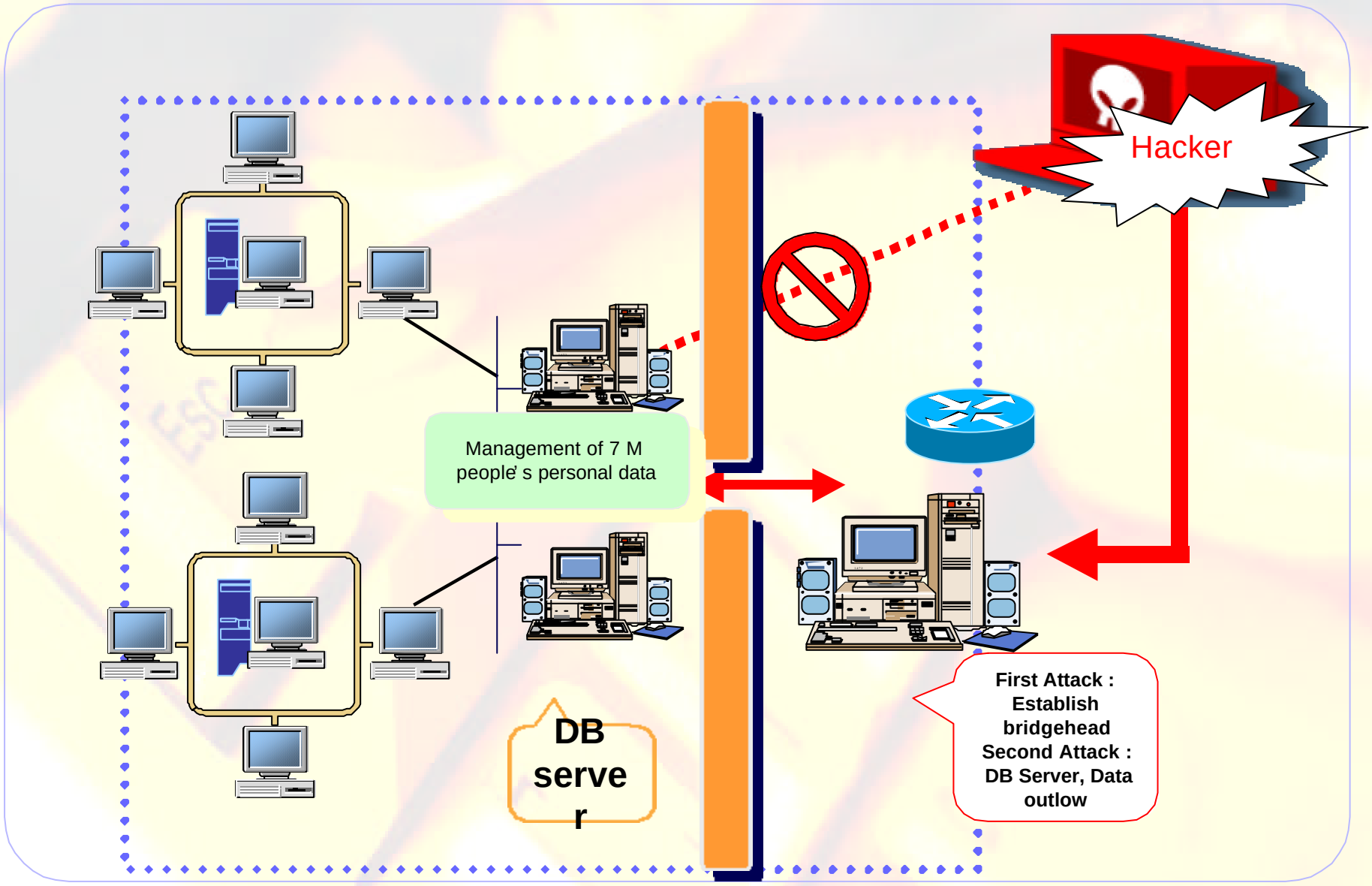


Con't

Analysis

- Arrested in April. 2001
- Attacks were concentrated on systems which manages information of high value
- Locating web server inside of firewall not on the separate network consequently caused the exposure of all network to the attacks
- In spite of security control service, they were attacked because the network IDS cannot detect the attack through web services

Large-scale Identity Theft



Con't

Analysis

- ☞ Arrested in April 2001
- ☞ Used the vulnerability of inevitable connection between web server outside of firewall and DB system inside of firewall
- ☞ The fact that cgi, php, and asp, which are widely used recently, have so many security problems is abused and web server was attacked first and then DB server was compromised

Miscellaneous

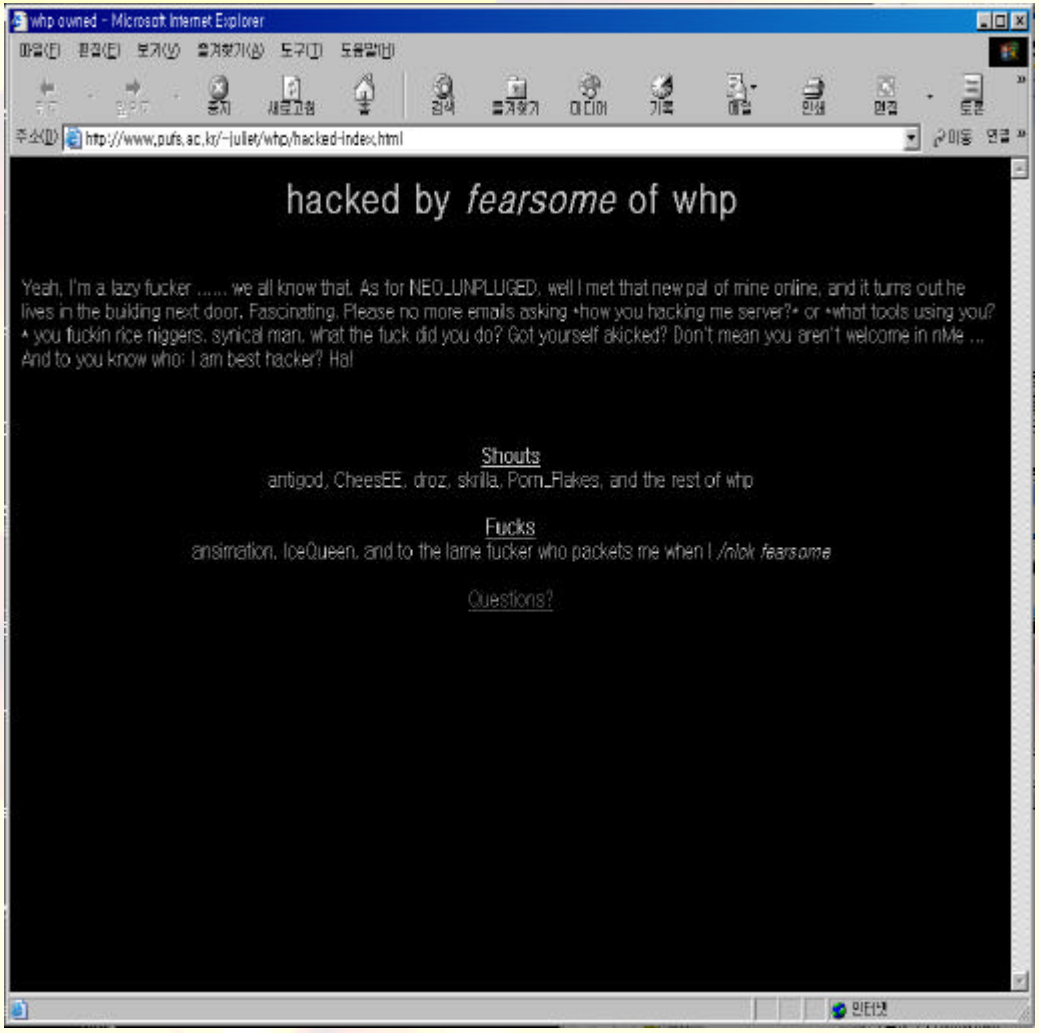
- ☞ 2000. 12
- ☞ Arrested suspect who stole 6.5 million personal data from an alumni association site

International Attack Case

International Hacking Group WHP

☞ Arrested in April 2001

International Hacking group WHP (one of its member was a service man of US Army in Korea) compromised 113 domestic systems indiscriminately. And the US service man was arrested for the hacking charge.



Organized Attack Case

Organized Hacking by Researchers of computer security company

☞ 9 were arrested in Dec. 2000

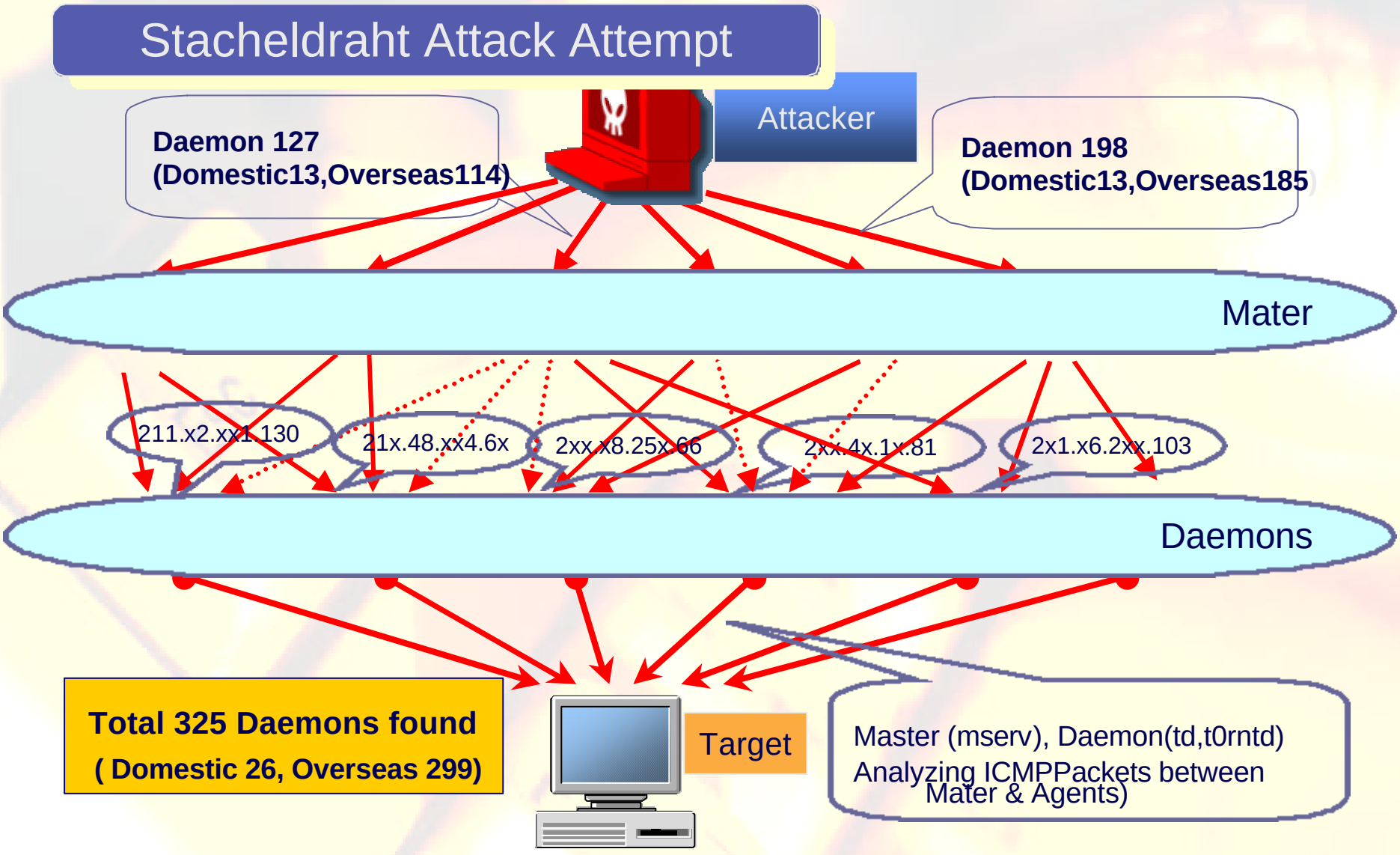
A domestic computer security company' s researchers (Tiger Team) were arrested for the hacking charge. They compromised about 80 business sites including banks and stole information in order to take security consulting orders from those victim companies

하지만, 여긴 Remote ODBC 설정이 가능한 버그가 존재 하였다. 이는 보통 로컬에서 ODBC를 설정 한 후 리모트로 DB에 직접 연결 하여 해킹 하는 방식 이였으나, DB Connection Port가 닫혀 있는 상황이라 80Port를 타고 들어 간 후 Remote로 ODBC설정이 되어 있는 DSN을 연결하여 mdb든 SQL이든, 모든 DB가 Query 가능 한 버그이다. 즉, 리모트에서 Table명을 알고 Query 한다면 그 Table은 RDS버그로 인해 우리에게 전송 되어 진다. 그뿐 아니라 편집 조작까지 가능한 버그라고 할 수 있다.

ASP 소스 누출이 쉽게 되는 버그가 있었다. +.htr이나 null.htw등 ASP소스 누출 하는 버그가 존재 한다는 건 보안에 어느 정도 무심했다고 볼 수 있을 것이다. 우리는 이런 버그를 통하여 DB Connetion부분의 DSN, User, Password등을 알 수 있었다.

```
<%
set DBcon1 = Server.CreateObject("ADODB.Connection")
DBcon1.open "DSN=stock;UID=appuser;PWD=appuser"
```

DDOS Attack


Stacheldraht Attack Attempt
Attacker
Daemon 127
(Domestic13,Overseas114)
Daemon 198
(Domestic13,Overseas185
Mater
211.x2.xx1.130
21x.48.xx4.6x
2xx.x8.25x.66
2xx.4x.1x.81
2x1.x6.2xx.103
Daemons
Total 325 Daemons found
(Domestic 26, Overseas 299)
Target
Master (mserv), Daemon(td,t0rntd)
Analyzing ICMPPackets between
Mater & Agents)

DDOS Attack

Trinoo Attack Attempt

- Found a master inside of a linux server in a Internet PC room located in Gangrung
- A file which contained 250 IP list used as agents was found
  After checking out 250 IPs, we found 97 servers were compromised and Trinoo deamons were installed in 30 servers
- Automated Tootkit was installed
  Synscan, Master, Agent, Wipe, and Kernel based Rootkit

Creating the computer virus

Arrest of a Virus Creating Group

☞ 7 members of CVC(Corean Virus Club) were arrested in Feb. ’98 and in Jan. ‘99

Korea’s biggest virus creating group Since 1996, they introduced techniques of Phalcon/SKIM(USA), NuKE (International), ‘29A’ Virus Group(Spain) and created and spread various computer viruses

Arrest of Worm Virus Creator

☞ Arrested white virus creator in Jan. 2000

☞ Spread it using MS Outlook Express

☞ While Melissa virus refer to address book of Outlook Express, White virus refer to inbox, send the infected messages every 15 minutes, and destroy the system on 31th, his birthday.

Countermeasures against Cyber-Terrorism

Factors to consider

Object of Protection

☞ Many vulnerable systems are abused before the direct attack to the critical information communication network

☞ Case by case countermeasures are needed

Techniques to evade tracing

☞ In addition to substantial legal countermeasures, it is necessary to have separate procedural laws to respond cyber-terrorism

(Kernel-based Rootkit, Web-based attack, Back door, Proxy, Anonymous Web, Browsing, IP Spoofing, PC Room, Free telnet account)

Con't

International Cooperation

- ☞ Legal countermeasures in accordance with international legal order
- ☞ Cooperation system considering legal rights, tracing(pursuit), and quick response comprehensively

Information sharing

- ☞ Information sharing and cooperation with law enforcement agencies, ISPs, ISAC, CERT, etc.

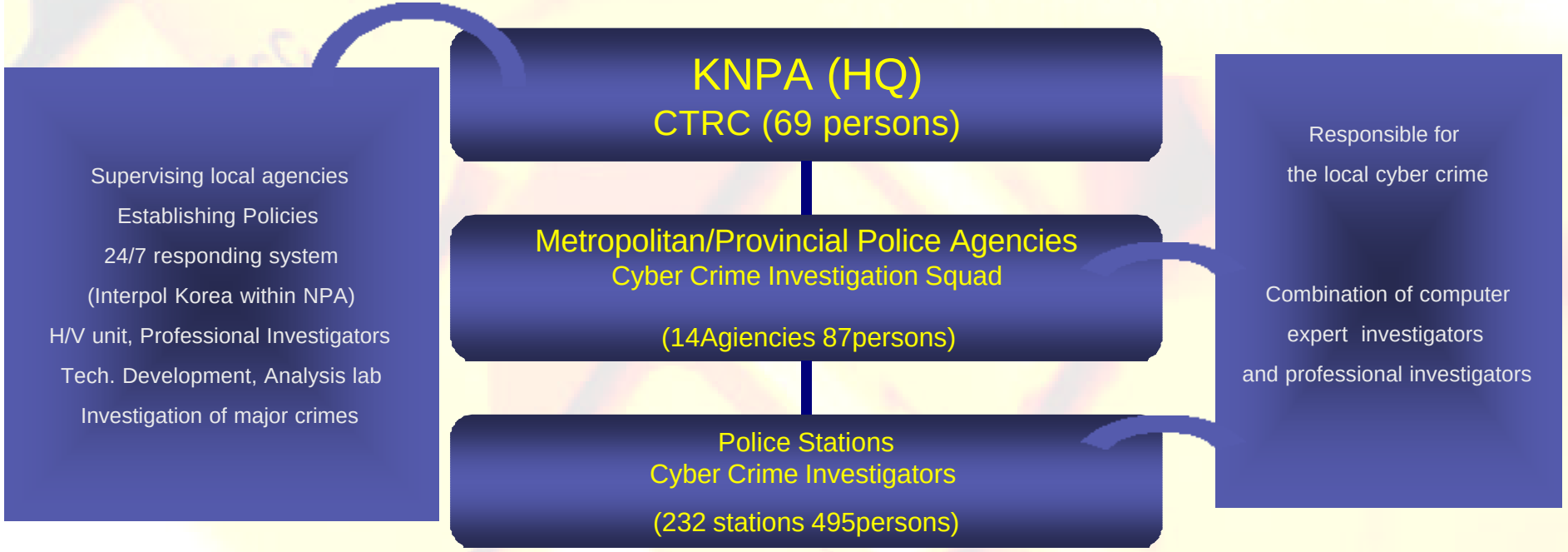
International cooperation paradigm

Organization

Response Agencies

- NPA(Interpol NCB-Cyber Terror Response Center), MIC, NIS
- KISA, ETRI

Police Force dedicated to Cyber Crime: 651 persons



Legal Countermeasures

Legal Countermeasures

☞ Penal Codes

Information Communication Infrastructure Protection Act, Act on Promotion of Utilization of Information and communications network And Information Protection Legislation of regulating cyber crime was in time considering International trend

☞ Countermeasures of criminal procedural law

Not sufficient procedural provisions especially for cyber terrorism, applies the same provisions as general criminal procedural law

☞ Alternative : **Legal countermeasures corresponding to international standards (quickness, mobility, easiness to destroy evidence)**

Meeting of the Justice and Interior Ministers of The Eight Dec. 9-10, 1997
- "PRINCIPLES TO COMBAT HIGH-TECH CRIME"

On November 23, 2001, in Budapest, Hungary, the United States and 29 other countries signed the Council of Europe Cybercrime Convention

Con't

Countermeasures of criminal procedural law (supplementary)

- ☞ Preservation of data saved on computer system (G8 Meeting)
- ☞ Method of acquiring data in transmission (G8 Meeting)
- ☞ Real-time collection of traffic data (G8 Meeting, Convention on Cyber Crime)

International Cooperation System

- ☞ International Cooperation is one of law enforcement activities

  KNPA have 24/7 cooperation system with interpol and 9 countries of Asia

  (hosted the 5th International Conference on Computer Crime in Oct. 2002.)

  Need to establish cooperation with private sectors

- ☞ Council of Europe Convention on Cyber Crime put emphasis on the importance of quick international cooperation

  Minimize the possibility of rapid international movement of criminal evidences through the close cooperation among member countries

International Cooperation

Special regulations on International Cooperation

☞ Council of Europe Convention on Cyber Crime provided special mechanism concerning electronic evidence

- **Quick preservation of stored computer data**
- **Open preserved traffic data to public quickly**
- **Cooperation on access to the stored computer data**
- **Access to the any country's stored computer data formally or with consent**
- **Cooperation on real time collection of traffic data**
- **Establish 24/7 Network**

☞ Korean police follows international paradigm regardless of compelling power of international law with the view point of reciprocity

☞ However, European countries, Canada, USA, and Japan are participating in the convention so that this convention is expected to be an international standard. Therefore, Korea has to hurry up to prepare legislation in accordance with this convention


경찰청 사이버테러대응센터
Cyber Terror Response Center
Thank you !