

Korean Cybersecurity Framework

23 Sep 2009

Hyderabad, India
2009 ITU Regional Cybersecurity
Forum for Asia-Pacific

Terrence Park
KrCERT/CC
Korea Internet & Security Agency

Conten

Cybersecurity Constituency in Korea

Code of Conduct in Korea

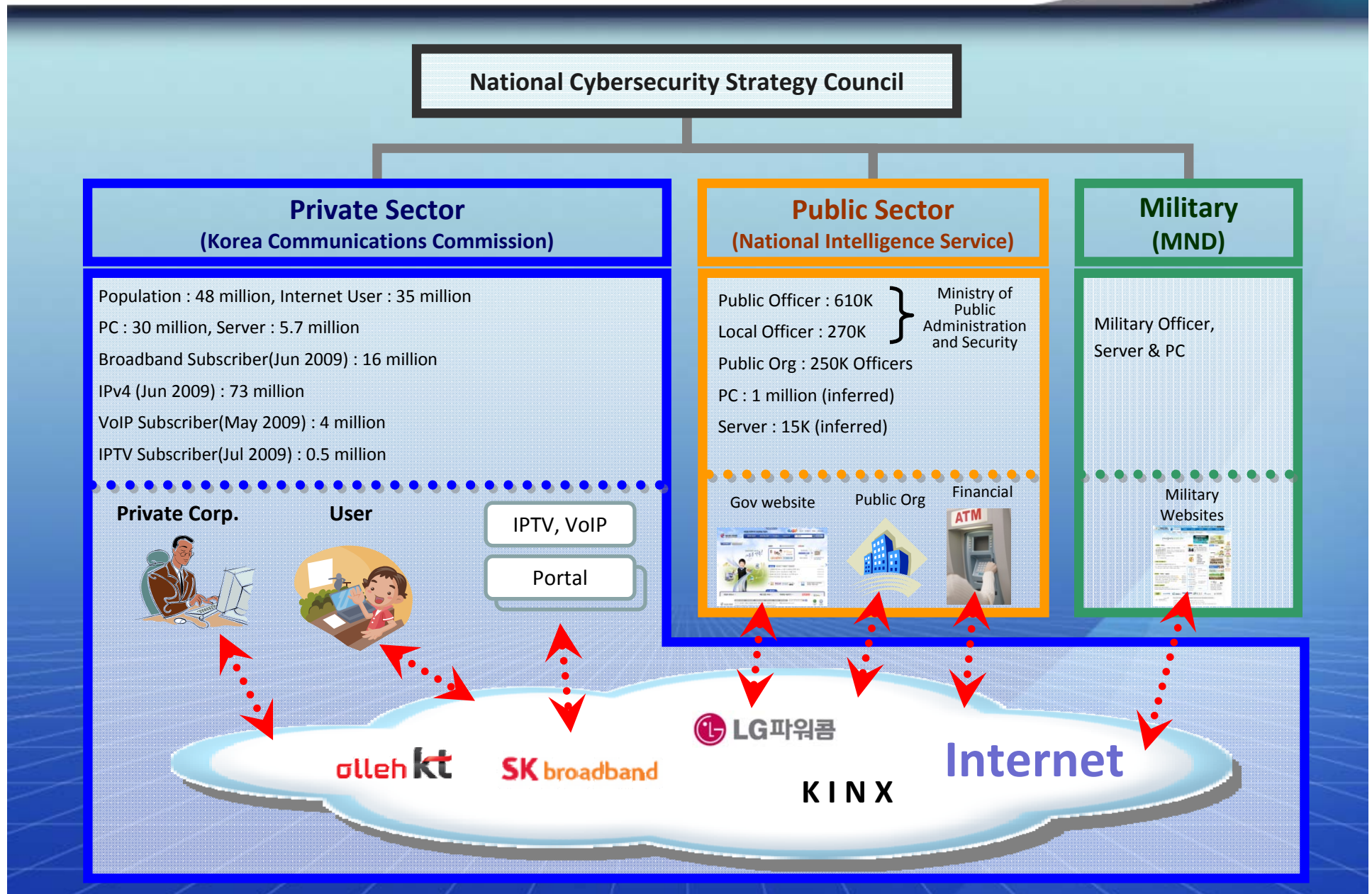
Evolution of Cyber Incident

National Cybersecurity Framework

KrCERT/CC Activity

7.7 DDoS

Cybersecurity Constituency in Korea



Code of Conduct Korea

Relevant Act : (Korea Communications Commission) The Act on Promotion of Information & Communication Network Utilization and Information Protection, etc.

Article 48-2 (Response, etc. to Infringement Accident)

(1) The Chairman of Korea Communications Commission shall perform the task falling under each of the following subparagraphs to properly cope with any infringement accident and may, if necessary, get the Security Agency to perform the task, in whole or in part:

1. The collection and dissemination of information on infringement accident;
2. The forecast and alert of infringement accident;
3. **Emergency measures against infringement accident; and**
4. Other measures prescribed by the Presidential Decree to cope with infringement accident.

(2) The person falling under each of the following subparagraphs shall furnish information pertaining to infringement accident, including the statistics of infringement accident by type, the statistics of traffic volume in the relevant information and communications networks and the statistics of uses by connection channel, to the Minister of Information and Communication or the Security Agency under the conditions as prescribed by the Ordinance of the Korea Communications Commission :

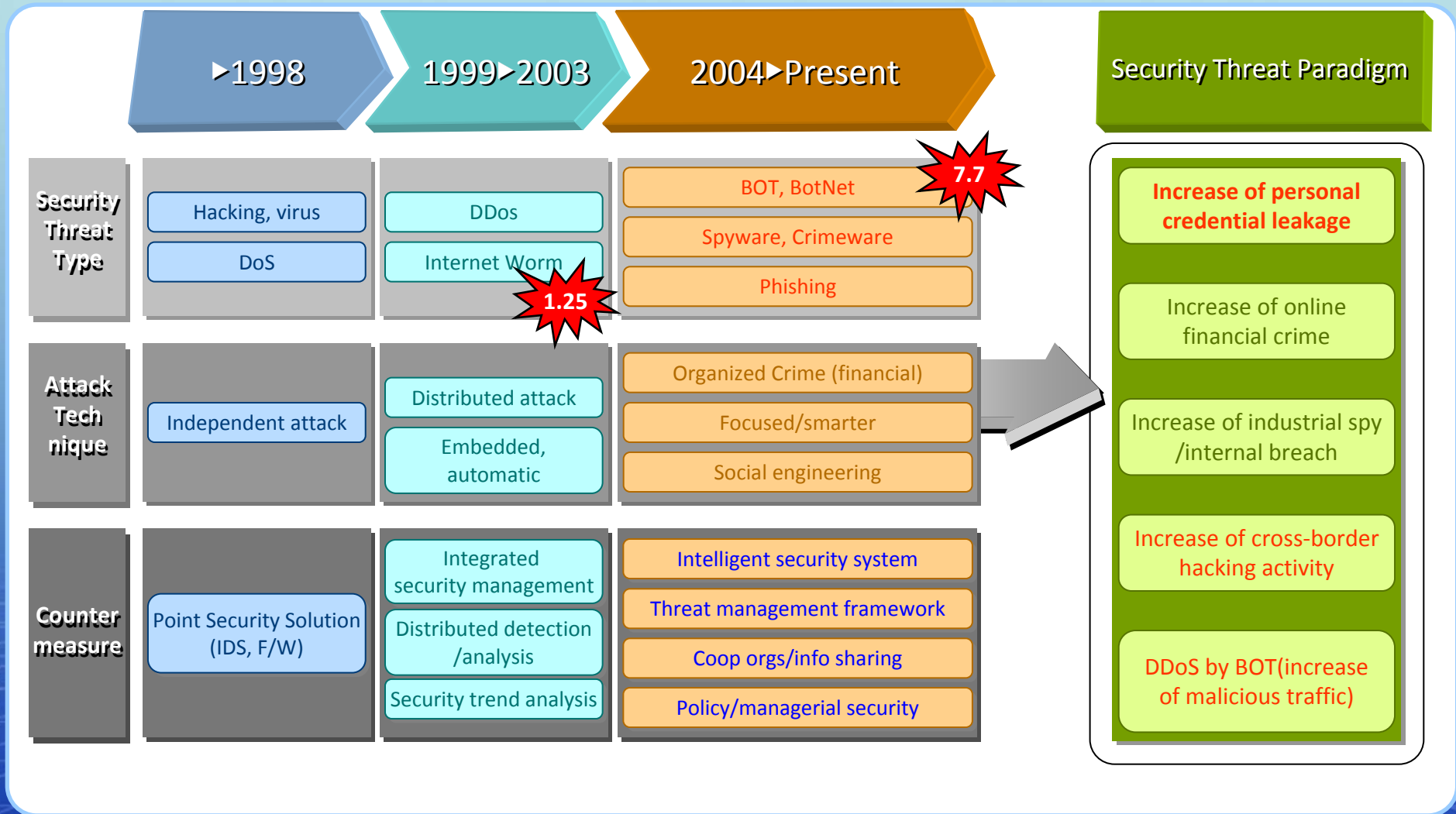
1. The provider of major information and communications services;
2. The business operator of agglomerated information and communications facilities; and
3. Other person who is prescribed by the Presidential Decree as the operator of the information and communications networks.

Article 48-3 (Report on Infringement Accident, etc.)

(1) The person falling under each of the following subparagraphs shall, when any infringement accident occurs or he finds signs of any infringement accident, report without delay the occurrence of such infringement accident or his finding of such signs to The Chairman of Communications Commission or the Security Agency. In this case, if any notice is served in accordance with Article 13 (1) of the Act on the Protection of Information and Communications Infrastructure, such notice shall be deemed the report referred to in the former part:

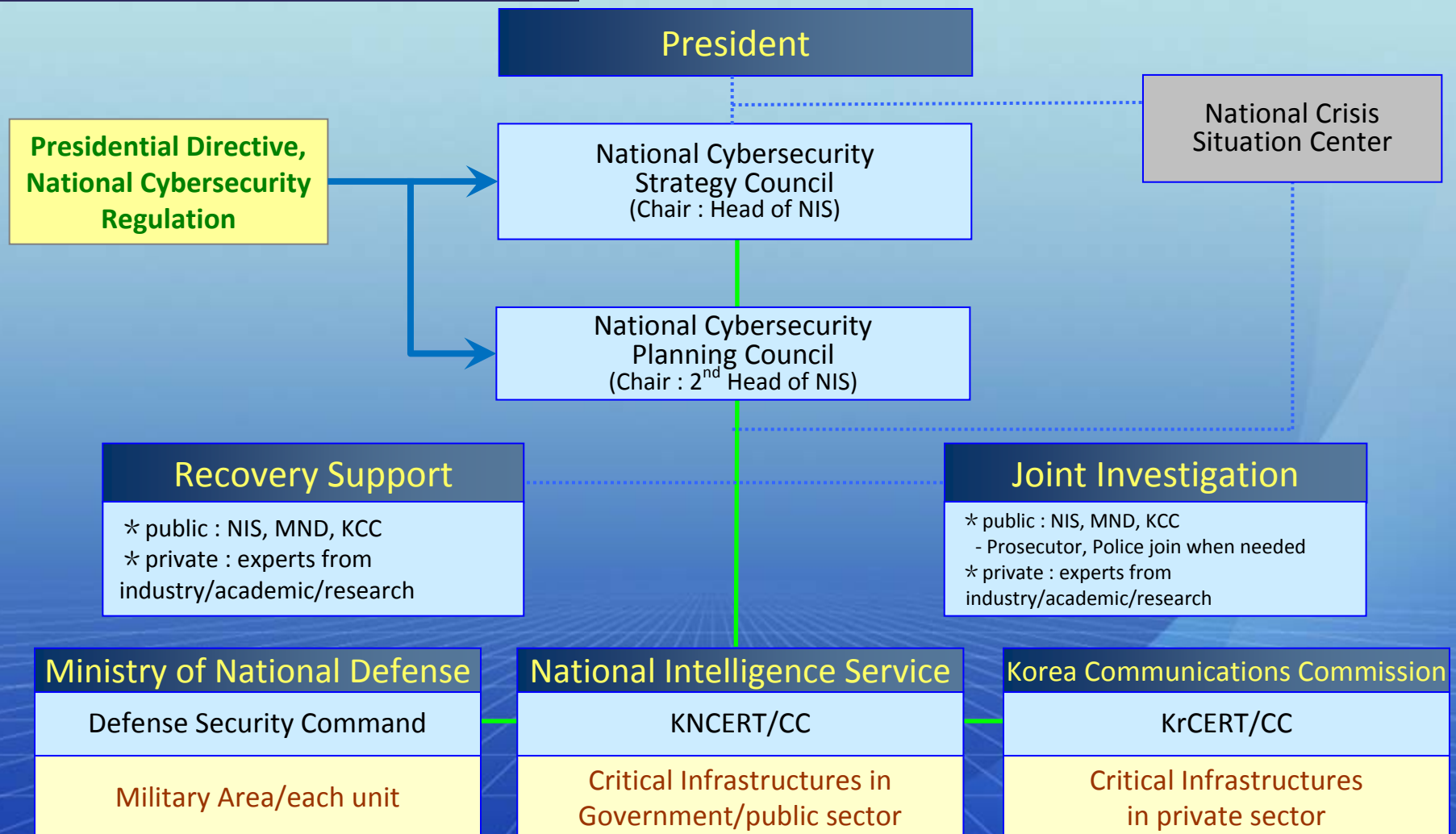
1. The provider of information and communications services;
2. The business operator of agglomerated information and communications facilities; and
3. Other person who is prescribed by the Presidential Decree as the operator of the information and communications networks.

Evolution of Cyber Incident



National Cybersecurity Framework

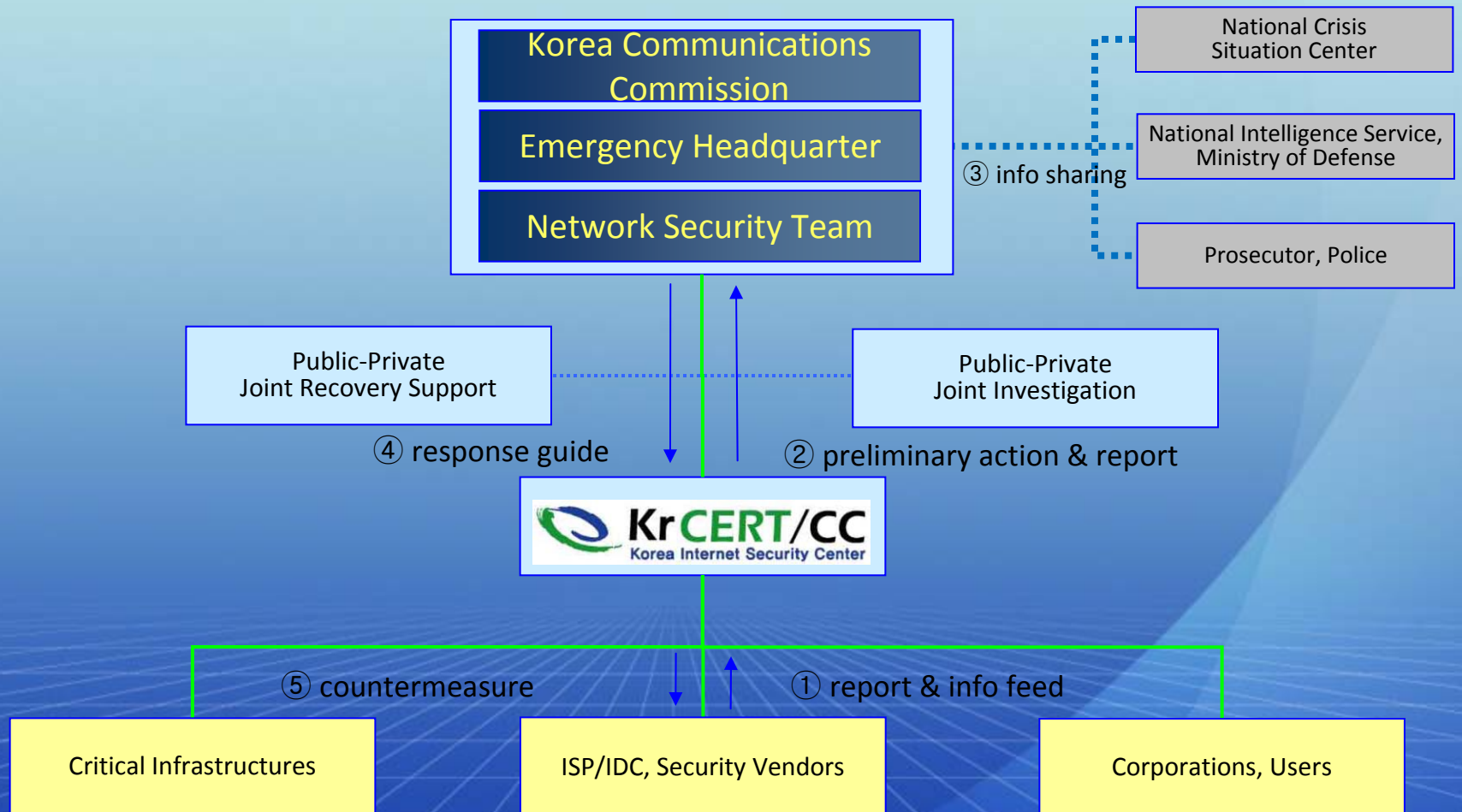
National Cyber Crisis Framework



Cybersecurity Crisis Management Standard Manual (Oct 2008)

National Cybersecurity Framework

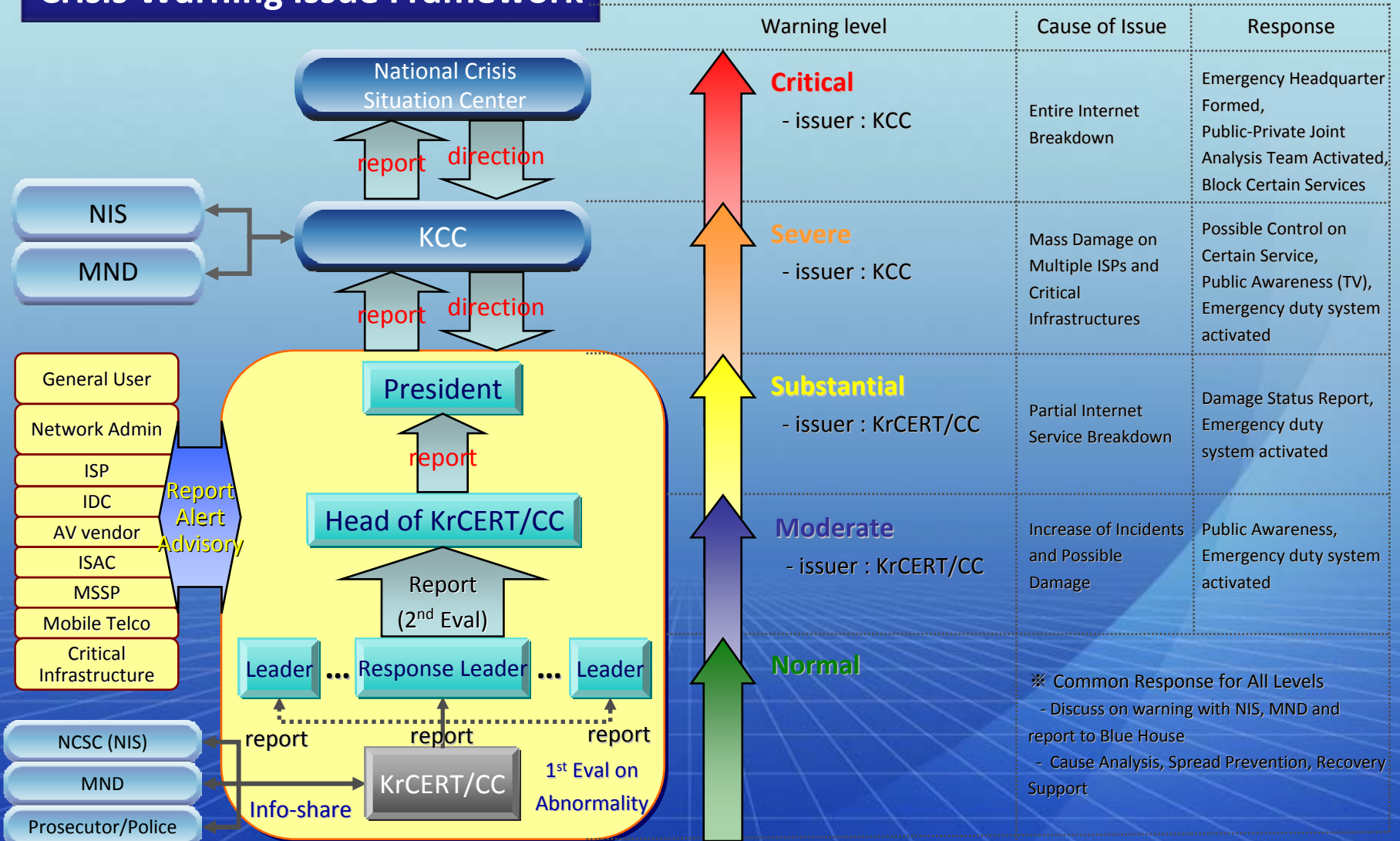
National Cyber Crisis Framework for Private Sector



Cybersecurity Crisis Response Manual for private sector (Jan 2009)






National Cybersecurity Framework

Crisis Warning Issue Framework



National Cybersecurity Framework

Internet Security Warning Level

LEVEL	CONTENTS
 Critical (Red)	<ul style="list-style-type: none"> o Traffic error occurs over all the Internet service areas of the nation. o Damages to major information and communication infrastructure facilities cause inconvenience in the service function to the general public. o Internet services in a private sector are paralyzed. o Collaborative response in a national level is required.
 Severe (Orange)	<ul style="list-style-type: none"> o Multiple ISP networks or major information and communication infrastructures impaired. o Hacking attacks and new security threats cause serious damages in private sector including major corporations, portal sites, laboratories, etc. o Private sectors suffers from widespread damages arising from worm, virus and hacking. o Collaborative response and action between a private sector and a government is required.
 Substantial (Yellow)	<ul style="list-style-type: none"> o Regional damage is incurred by worm, virus, hacking, etc. o Regional Internet communication errors or Internet service-related errors occurs or might occur. o Urgent security measures should be taken by ISP/IDC, general individual users and corporations.
 Moderate (Blue)	<ul style="list-style-type: none"> o The appearance of highly threatening worms, viruses, vulnerabilities, hacking methods and attacking codes might increase the possibility of damages. o Security incidents are spreading in other countries and the network of the nation is increasingly vulnerable to security threats. o The increased possibility of abnormal traffic in the domestic Internet
 Normal (Green)	<ul style="list-style-type: none"> o Internet communication traffic in a private sector is flowing smoothly o Unless they don't affect Internet communication or its usage <ul style="list-style-type: none"> - Malicious codes including worms and viruses were detected - New security flaws or hacking methods were announced o Possible existence of regionally abnormal traffic with low risk

National Cybersecurity Framework

Local Cooperation Framework

Public Sector: Government, Public Orgs



● Incident Escalation & Info Sharing



● Education support
● Internet Crime related Support



● Onsite Joint Investigation
● Incident Escalation for Serious Crime



● Technical Documents
● Hacking Analysis report

National Crisis Situation Center



Info-sharing

Private Sector: ISP, IDC, etc



KrCERT/CC Activity

Detection

Analysis

Dissemination & Support



ISP/ESM



Remote Agent



IDS/Firewall



Email feed



S/W, H/W



AntiVirus

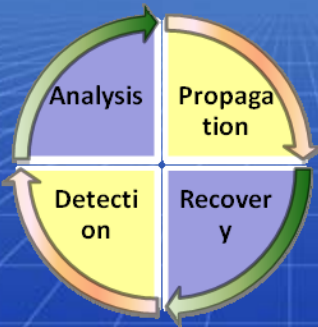


User

Malware

Vulnerability

Incident Reports



Mail



FAX



SMS



Web.



Messenger



TRS

Info-providing Org,
Hot Liners

ISP/IDC,
Mobile Provider,
Security/AV
Vendors

Private Corp.
(Portal, B2B, B2C)

General User

Broadcasting/
Media

Intelligence,
Military,
Police

Traffic Monitoring,
User Protection,
Malicious Traffic
Block,
Develop Vaccine,
Incident Reports

Attack Port Block,
Security Patch,
Log Analysis,
Damage Recovery

Security Patch,
Damage Recovery

Public Awareness

Info-sharing

7.7 DDoS

What is different?

Attack

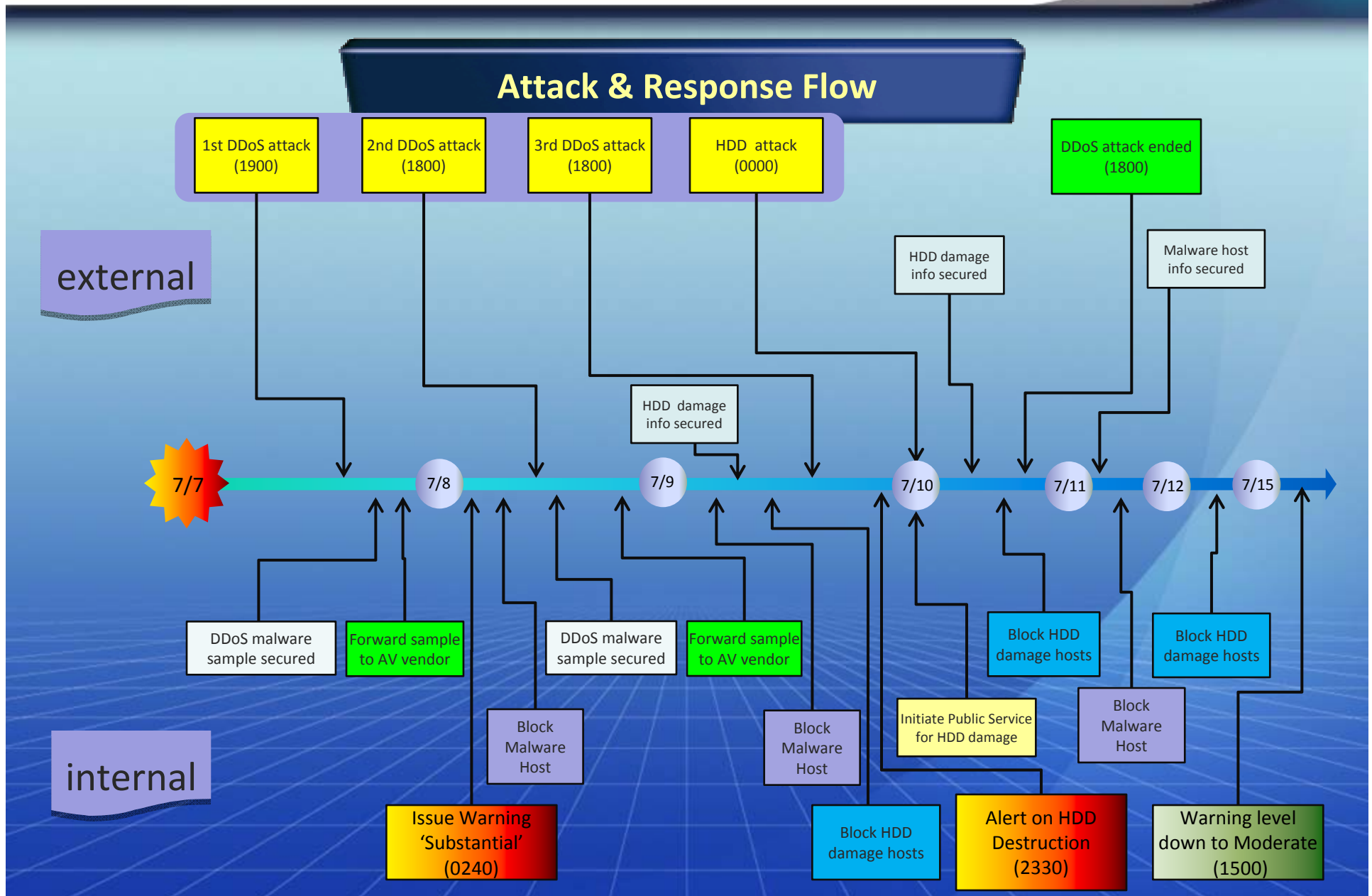
- Zombies do not act on real-time basis, no herder needed
- Crafted to act based on pre-designed scenario
- Damages fixed drive on certain time



Response

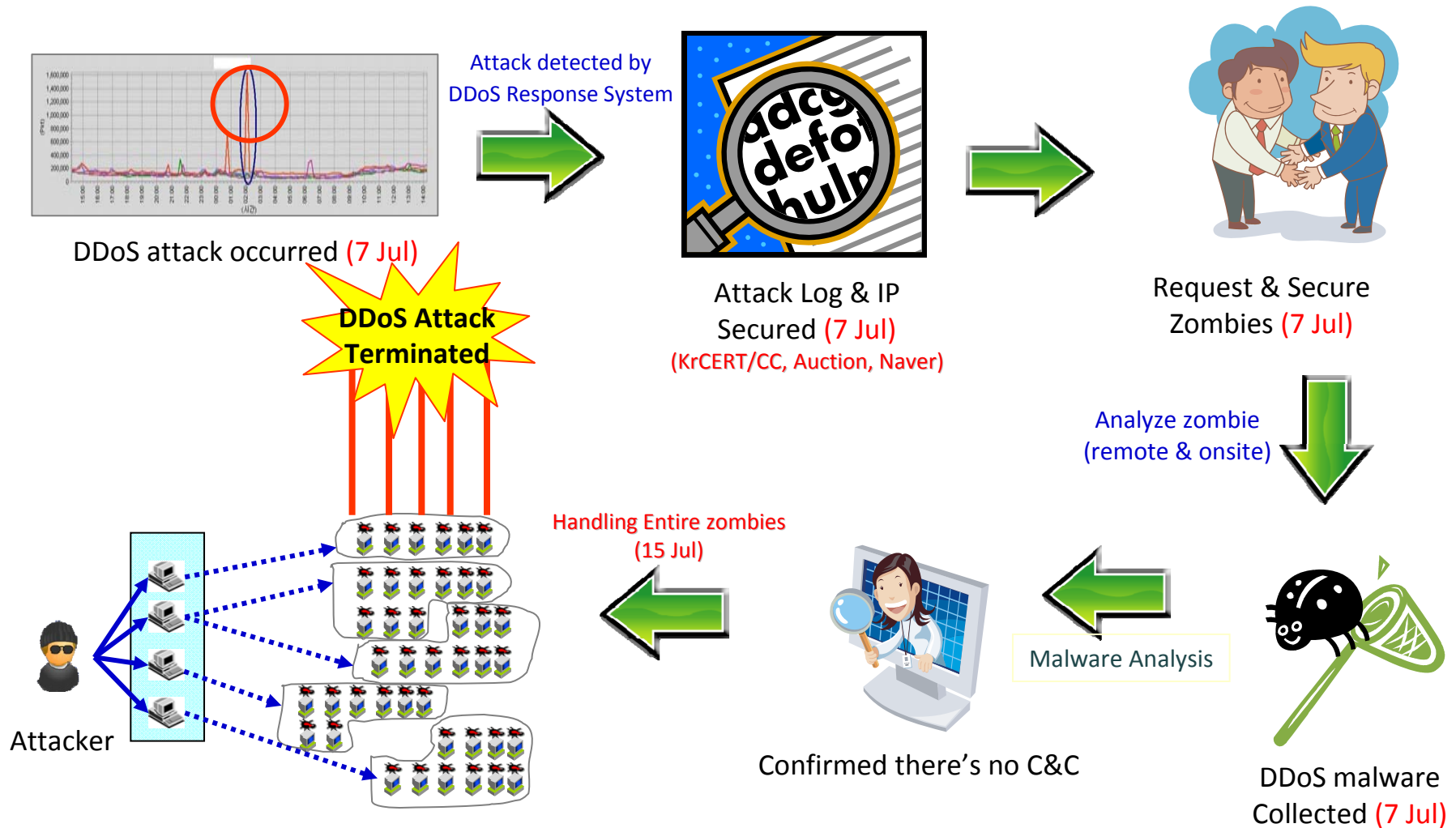
- C&C blocking does not work
- Clearing possible only when entire zombies are cured
- Limited countermeasure in network aspect

7.7 DDoS



7.7 DDoS

Attack & Response Timeline





Thank you

twpark@krcert.or.kr