

Security activities in Japan towards the future standardization



Side Event

Cybersecurity

Koji NAKAO KDDI, Japan

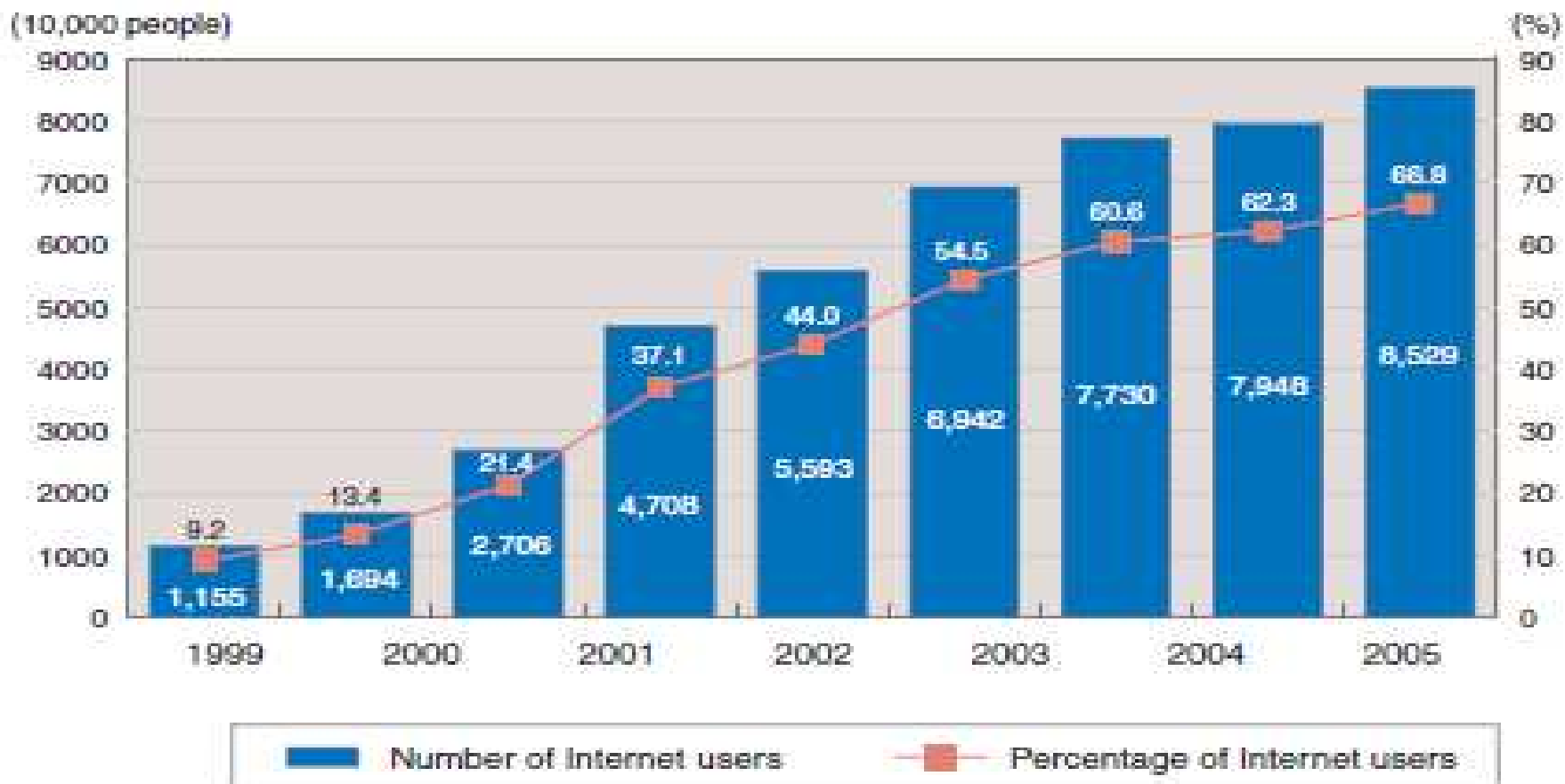
Content

- ❑ **Current threats**
 - Internet User in Japan
 - However, observation of many scans (by using Darknet monitoring)
 - Botnets threats
- ❑ **Security Activities against threats in Japan**
 - Bot countermeasure : CCC project
 - Trace-back project
- ❑ **Conclusion**



Number of Internet Users in Japan

Figure 1-2-1 Number of Internet users and penetration rate



Produced from MIC, "Communications Usage Trend Survey"



WTSA-08, Johannesburg, South Africa, 21-30 October 2008



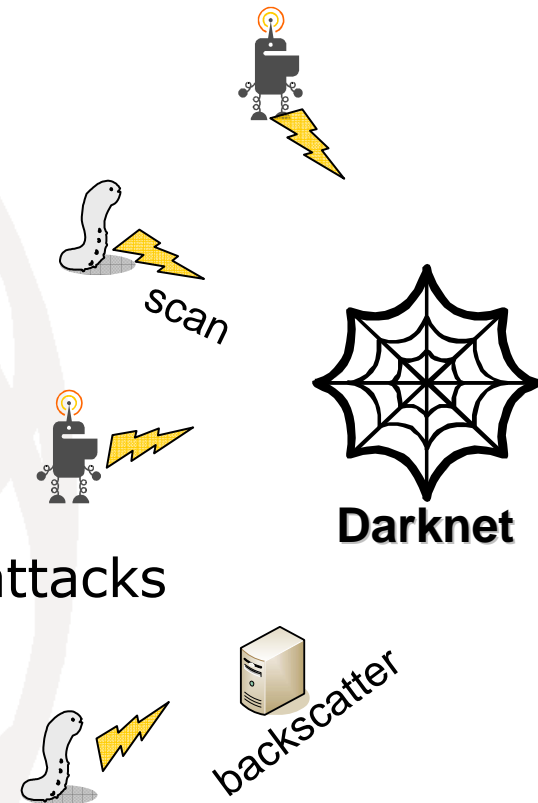
However, Monitor data through Dark-Net

❑ **Dark-Net**: Unassigned IP addresses space and they are not connected to the Real Servers/PCs.

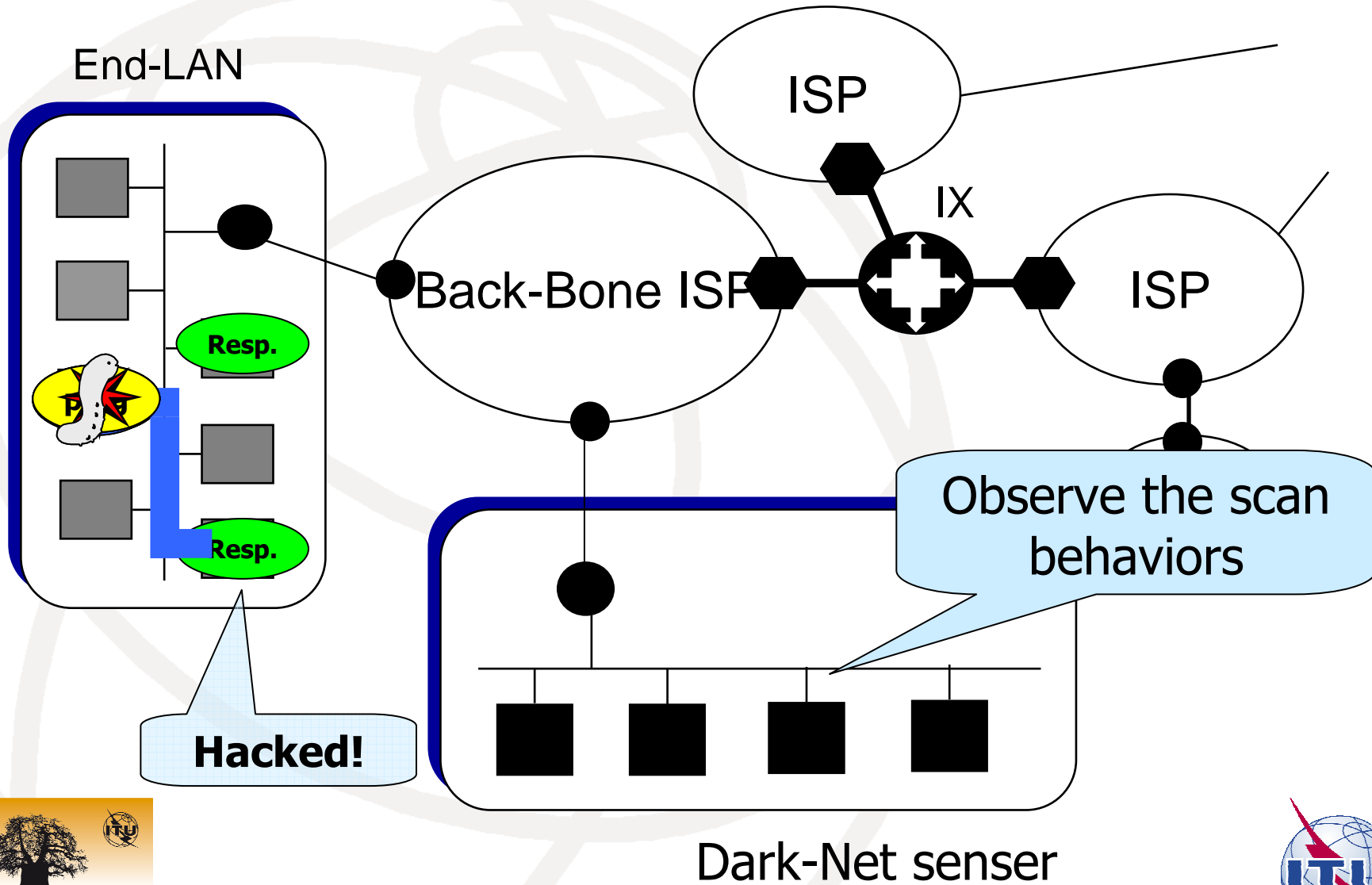
❑ Types of Packets arrived to the Dark-Net:

- Scans by means of Malwares;
- Malwares infection behaviors;
- DDoS attacks by Backscatter;
- Miss configurations/mistakes

❑ It is very useful to **Observe** the serious attacks behavior over the Internet.

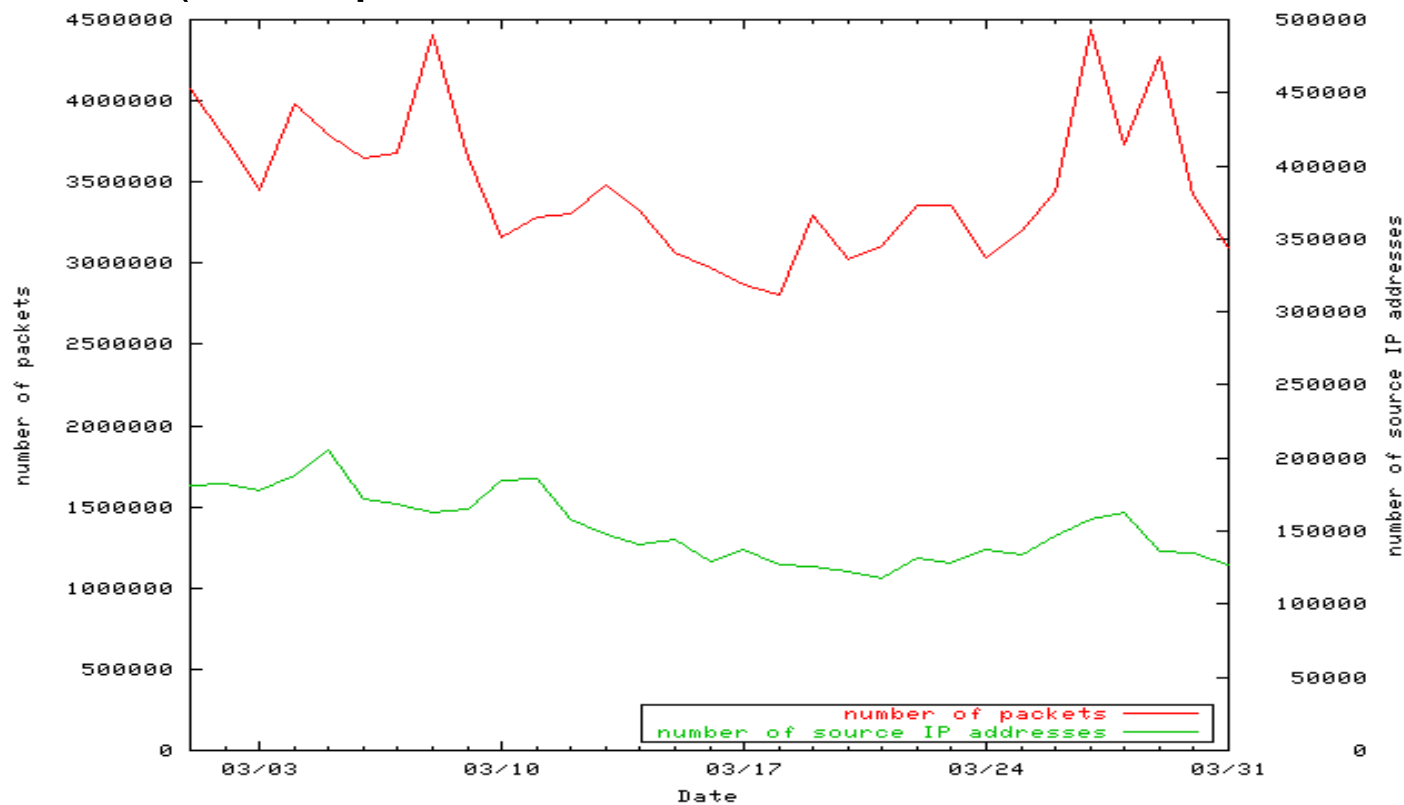


Malware infection behavior by means of Dark-Net monitor



How large packets can we get from the Dark-Net?

(Example: nicker /16 addresses block)



3.5 Million Packets from 150 Thousands Hosts per a day

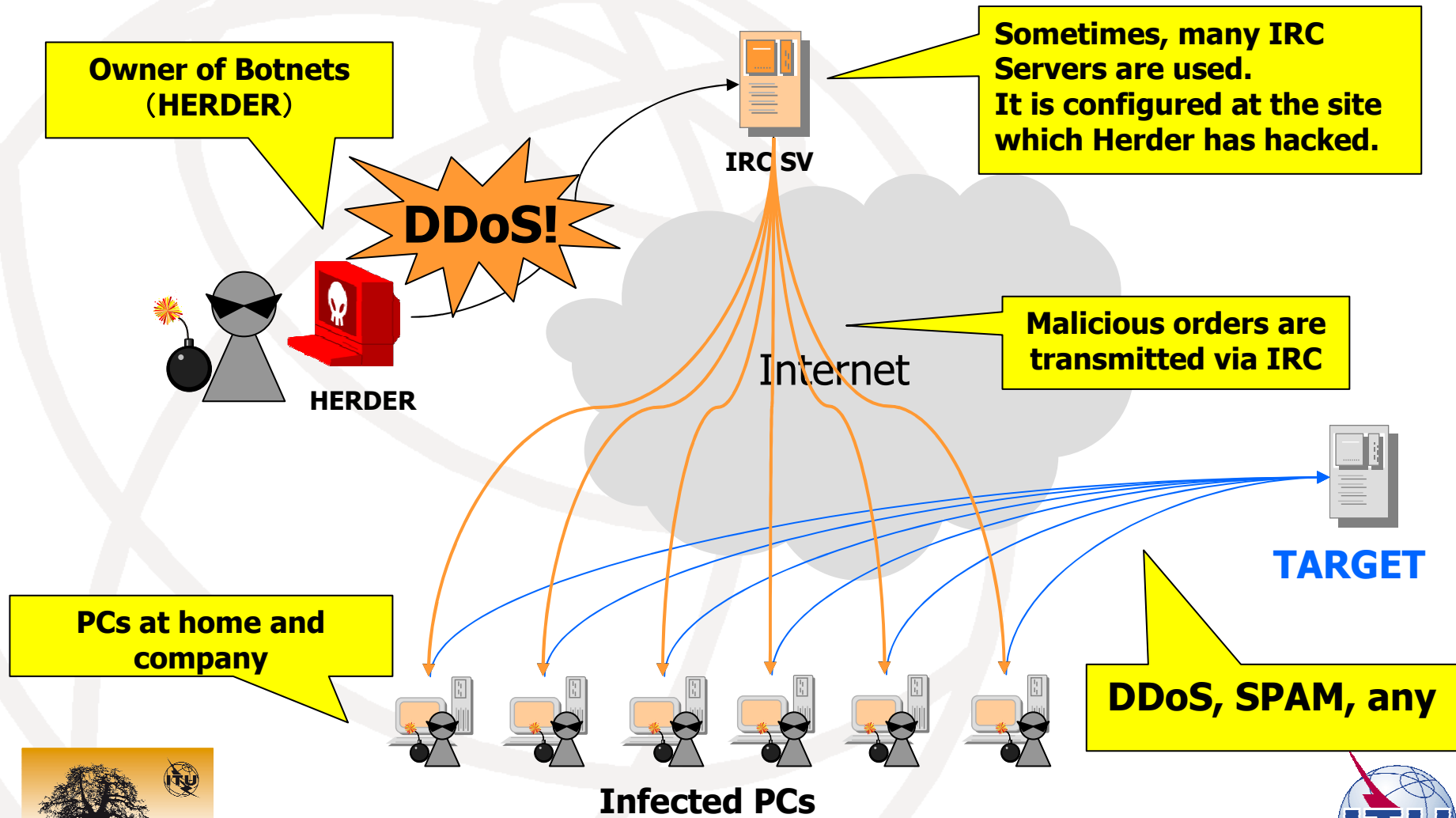


WTSA-08, Johannesburg, South Africa, 21-30 October 2008

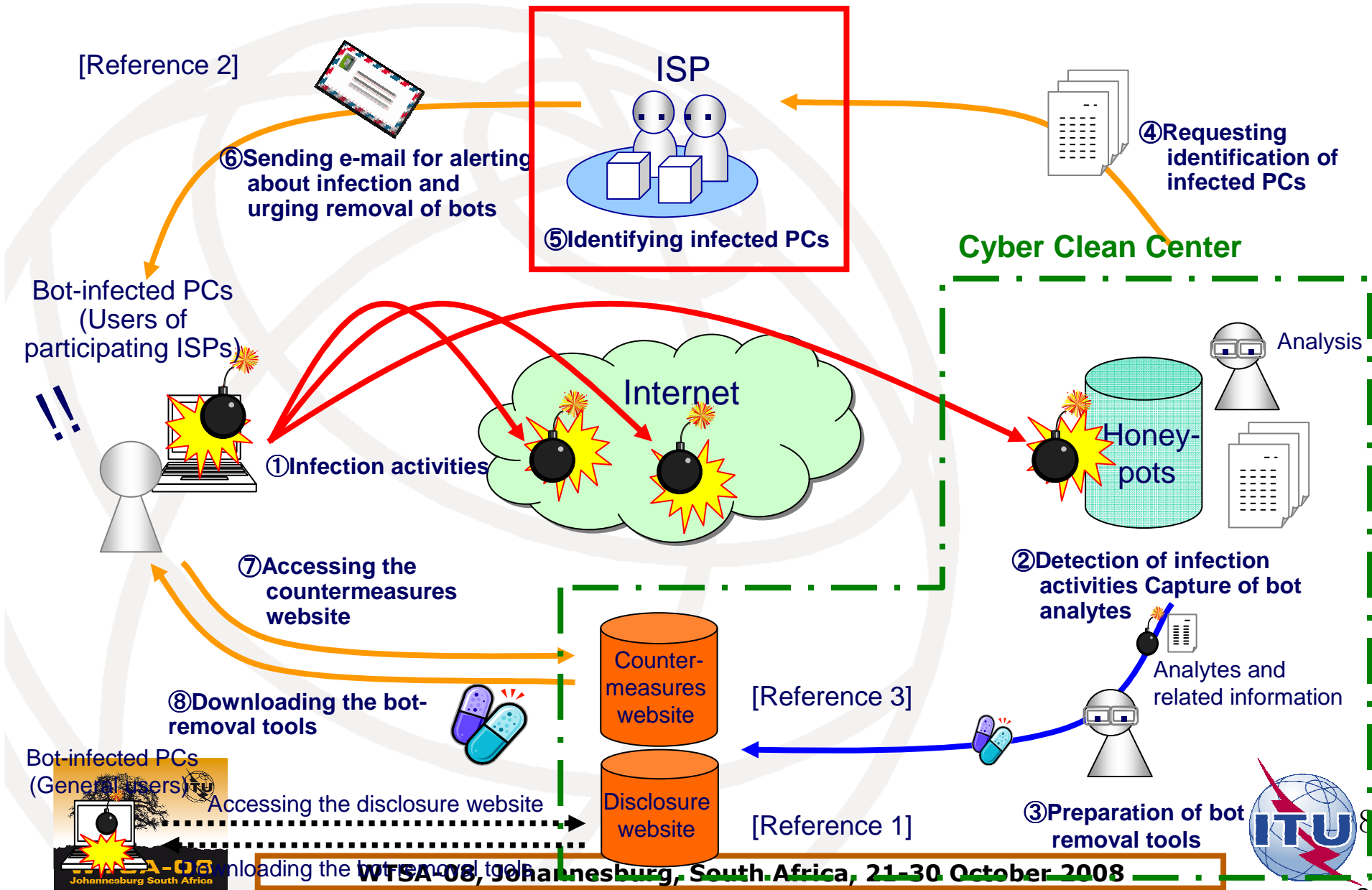


Basic concept of Botnets

According to analysis of Agobot source code.

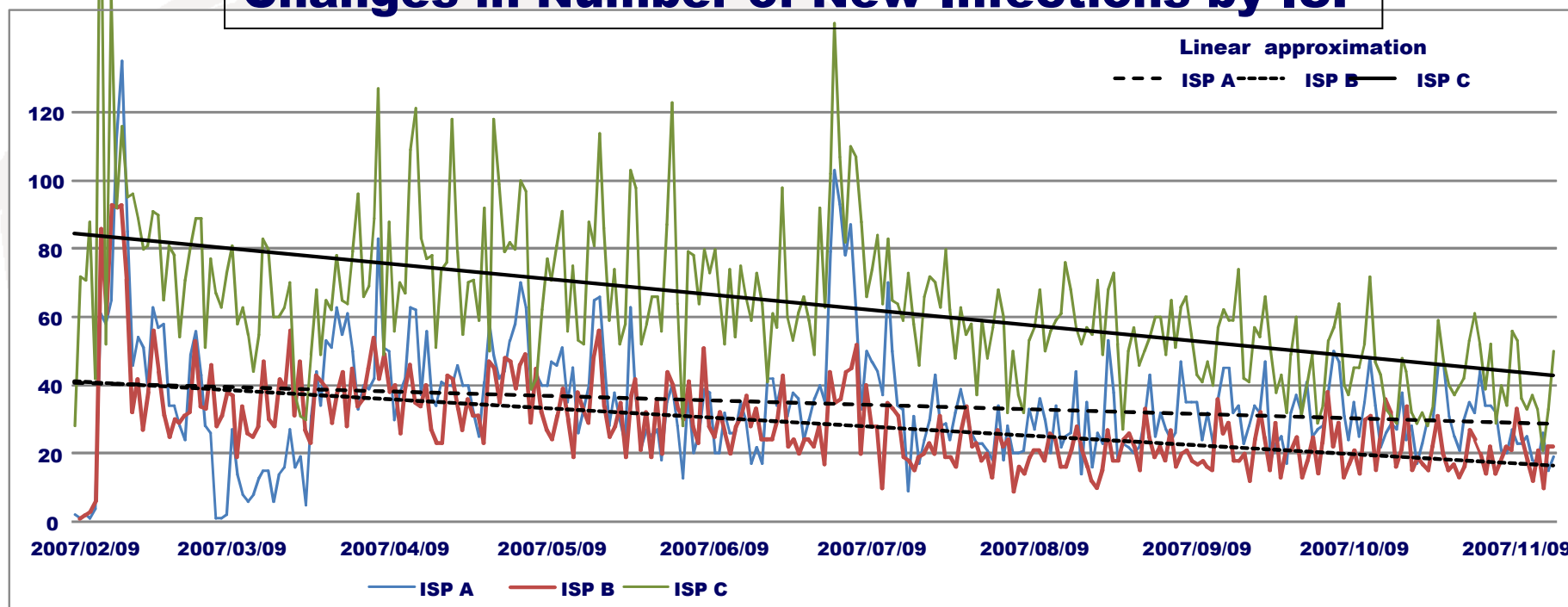


Workflow for Countermeasures against Bot-infected Users in Japan (Cyber Clean Center)



Effect of CCC Activities

Changes in Number of New Infections by ISP



There is a trend of a decline in the number of new users infected by malware



WTSA-08, Johannesburg, South Africa, 21-30 October 2008



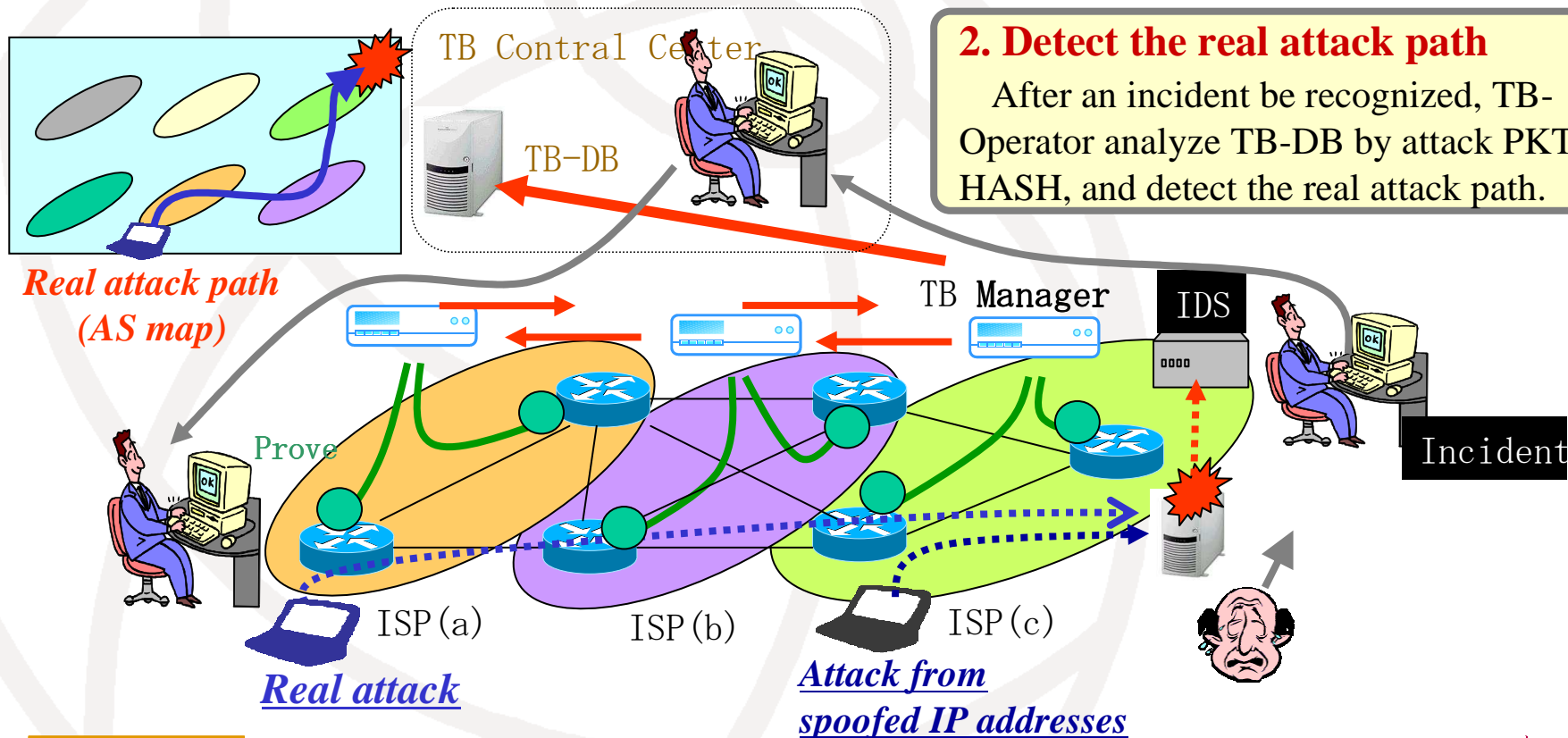
Outline of Traceback system studied in Japan

1. Store suspicious information.

Whenever IDS notify suspicious attacks, TB manager calculate the attack PKT's HASH, and automatically generate it's AS map recursively contacting with neighbor AS's TB manager, and the generated AS map is stored to TB-DB.

2. Detect the real attack path

After an incident be recognized, TB-Operator analyze TB-DB by attack PKT's HASH, and detect the real attack path.



0. Store HASH data temporary.

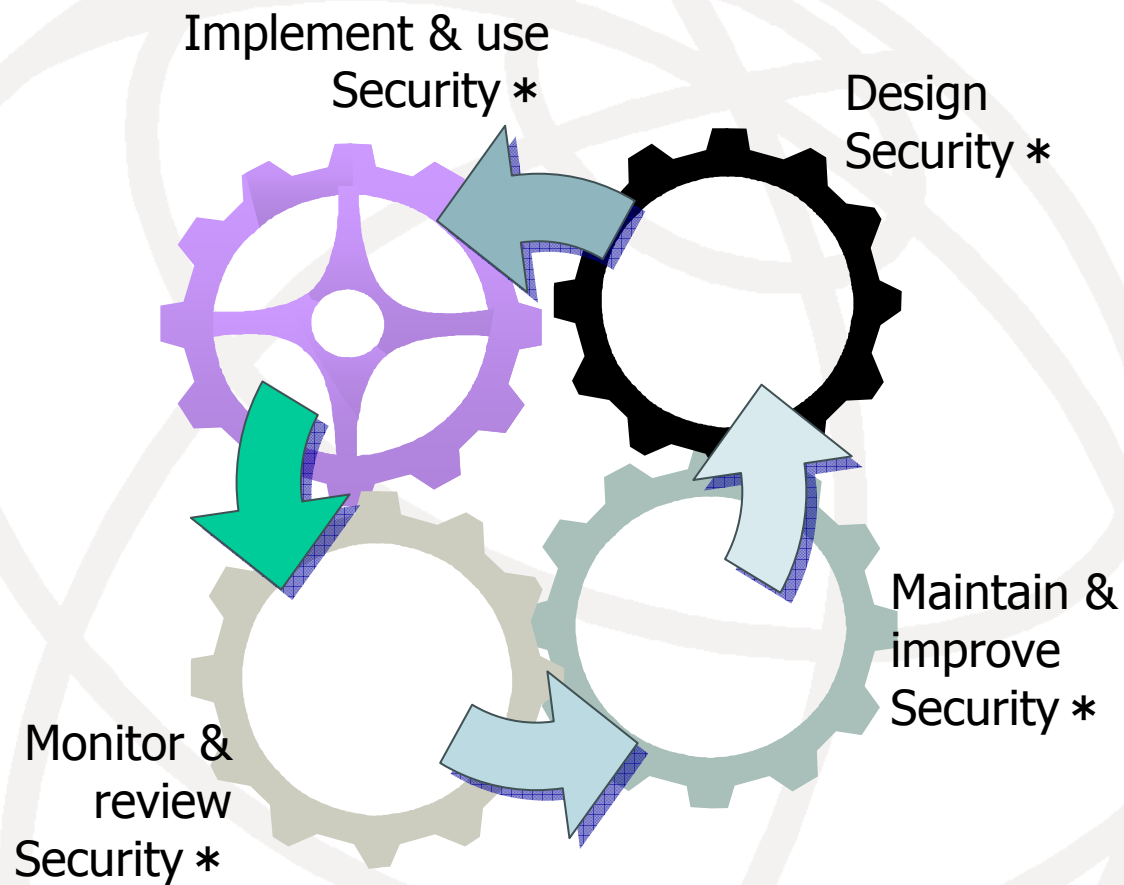
Each probe convert PKT to HASH, and store own cache automatically.

Activities related to ITU-T standardizations

- ❑ Since security issues are getting broad, diverse and complex, methodologies of standardization on security should also adapt to its diversification.
- ❑ Standardization of Bot countermeasures, information sharing and traceback technologies are recognized as new topics for ITU-T which apparently need **COLLABORATION**.
- ❑ Security standards are not only focused on high level requirements, but also focused on **frameworks** which jointly and actively work together (collaboratively) for **Cybersecurity**.



Thank you for listening



WTSA-08, Johannesburg, South Africa, 21-30 October 2008

