Fighting against a Big Monster: Cybercrime
Contents

1. Dark Side of IT Power

2. Cybercrime Investigation Department (CID)

3. Network among Government Agencies

4. Investigation Skills: Powerful Weapon

5. International Cooperation
1. Dark Side of IT Power

Benefits of Cyberspace: Age of Ubiquitous

Internet

Smartphone

SNS
1. Dark Side of IT Power

Dark side of IT Power: Cybercrime

Hacking

E-crime?

Smishing

Connected to Every Crime Everywhere
2. Cybercrime Investigation Department

CID under Supreme Prosecutors’ Office

- Effective response to “major” cybercrimes
- Support investigations for regional prosecutors’ offices
2. Cybercrime Investigation Department

[Manage Malware Analysis System]
Systematically collect the malware code
Correlative Analysis & Tracking

[Investigation & Support]
Support cybercrime investigation for field offices
2. Cybercrime Investigation Department

SPO / CID

Regional Offices

Seoul Central DPO
High Tech Crime Investigation Dept II

61 specialized prosecutors over the nation
3. Network among Government Agencies

[Wide Range of Network]
Consultative group consisting of 44 government agencies and public & private institutions
4. Investigation Skills : Powerful Weapon

- IP tracing
- Cellphone Call Records and Phone Call Location Analysis,
- Digital Forensic (National Digital Forensic Center, NDFC)
- “IDEAS” (an big data analysis system) Utilization
- Search and Seizure
- Bank Record
- Various Kinds of Computer Analysis Tool
5. International Cooperation

**Major Case**

- DDos Attack (Hacking)
- APT (Advanced Persistent Threat)
  - evolved hacking method, complex technical knowledge needed to both criminals and prosecutors
  - multiple jurisdiction

**International Smishing Organization Case**

- Korea, China, Japan were involved
- Used International Cooperation in Criminal Justice between Korea and China
Thank You

Office of Cybercrime Investigation