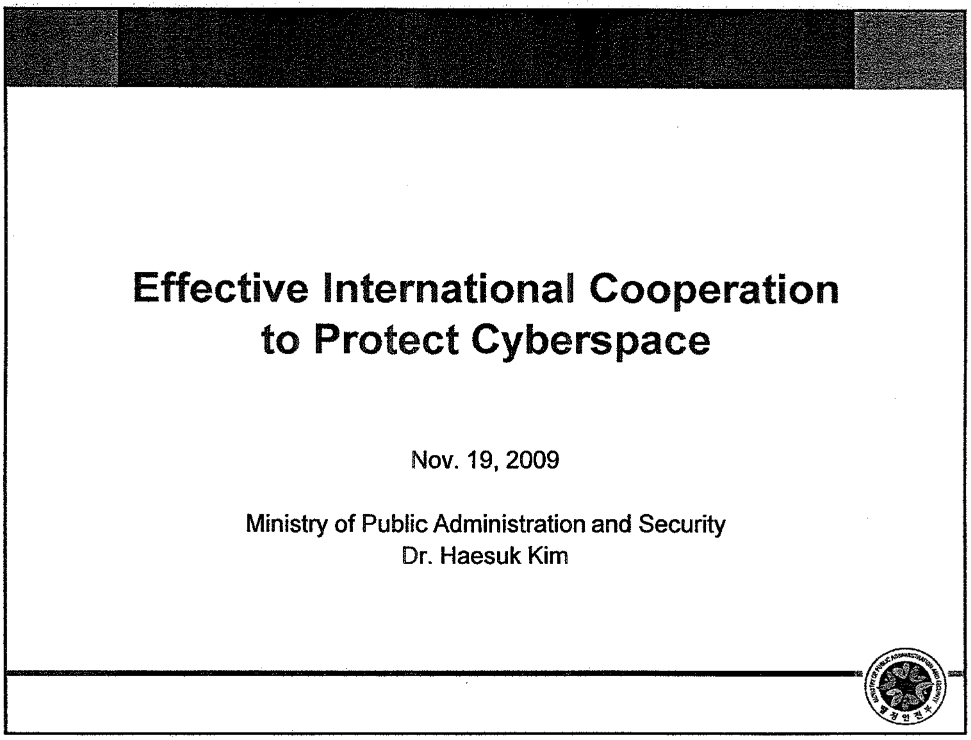
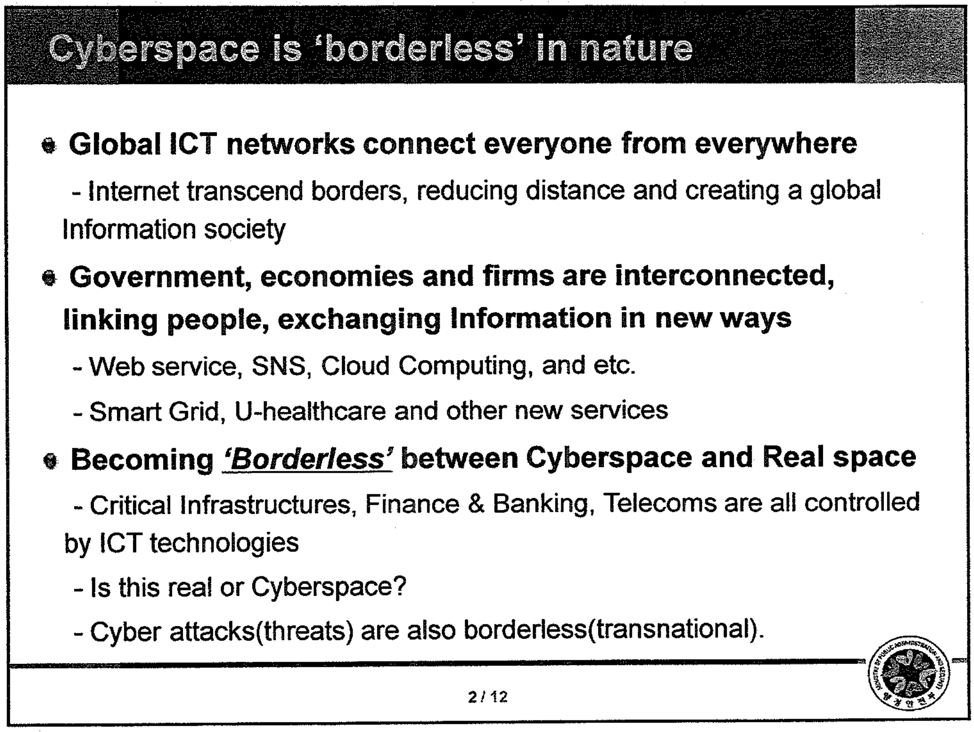


Effective International Cooperation to Protect Cyberspace

Nov. 19, 2009

Ministry of Public Administration and Security
Dr. Haesuk Kim



Cyberspace is 'borderless' in nature

- **Global ICT networks connect everyone from everywhere**
  - Internet transcend borders, reducing distance and creating a global Information society
- **Government, economies and firms are interconnected, linking people, exchanging Information in new ways**
  - Web service, SNS, Cloud Computing, and etc.
  - Smart Grid, U-healthcare and other new services
- **Becoming *'Borderless'* between Cyberspace and Real space**
  - Critical Infrastructures, Finance & Banking, Telecoms are all controlled by ICT technologies
  - Is this real or Cyberspace?
  - Cyber attacks(threats) are also borderless(transnational).

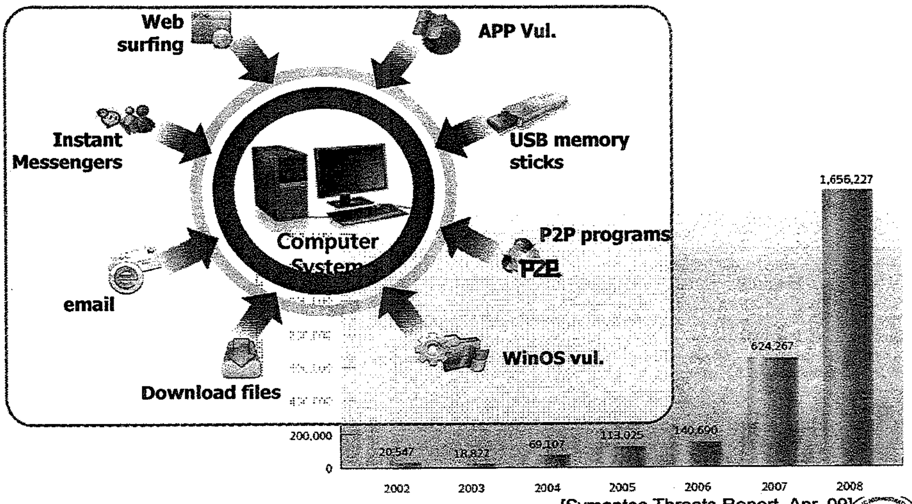
Recent Cyber Threat Features

- **Sophisticated Attacks**
  - DDoS Attacks : Organized and Professional
  - Malicious Codes, Botnets
  - Zero Day Vulnerabilities
  - Back to Hactivism
- **Targets are Expanding to All Sectors**
- **Botnet is most troublesome**
  - Spam, Clickfraud, Phishing & Pharming, Key Logging
  - DDoS Attacks
  - Anonymized Terrorist & Criminal Communication

  → Botnets are more than 10% of Internets

Threats are Exponentially Increasing

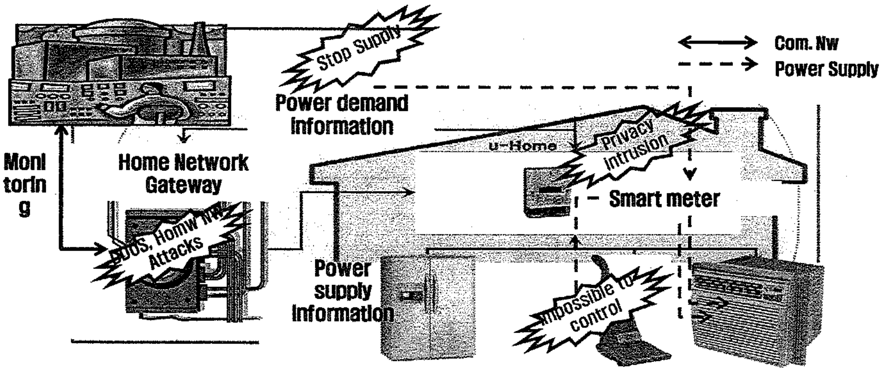
- Cyber threats are exponentially increasing, propagating in various ways



[Symantec Threats Report, Apr. 09]

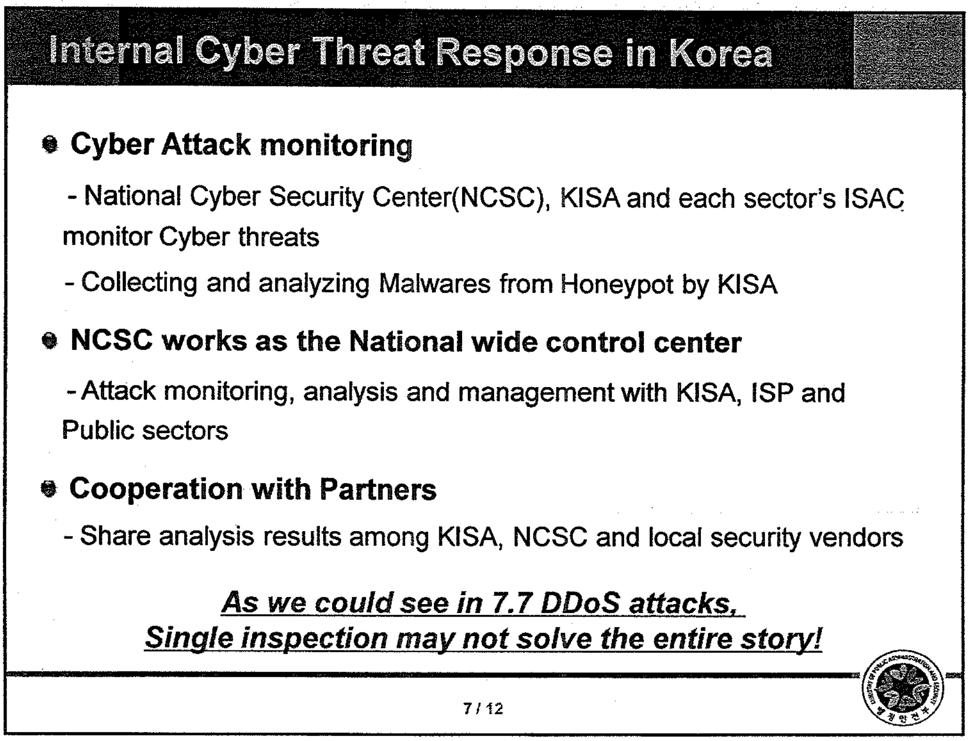
Digitalized Critical Infras are next Target

- **Malware, DDoS attacks and other cyber threats would stop the critical infrastructure services**



General Cyber Threat Defense Mechanism

- **Considering Points**
  - How accurate does the detection result?
  - How quickly can we detect the attack?
  - How efficiently can we block the attacks?
  - Isn't there any proactive attack defense mechanism at all?
- **Requirements to Defend**
  - **Malware propagation monitoring** : collecting and analyzing Zombies and sample files from honey pots and networks
  - **Collaborative tracing** : Vulnerable servers log, attack type, ..
  - (Inter)**National wide control center** for attack monitoring, analysis and management with networking components and security systems

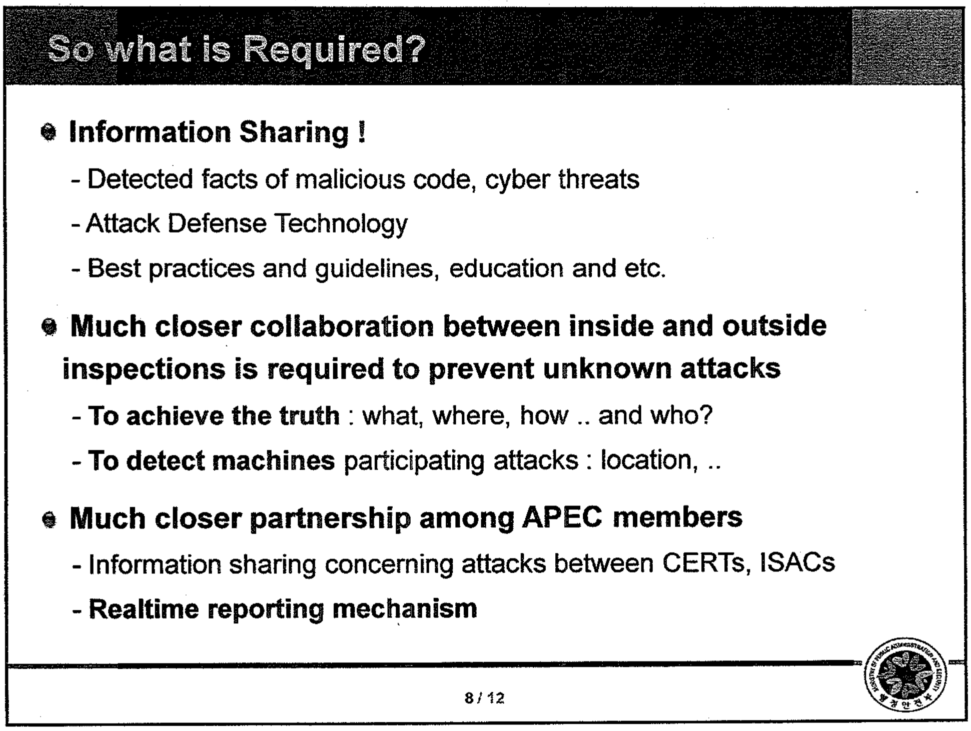


Internal Cyber Threat Response in Korea

- **Cyber Attack monitoring**
  - National Cyber Security Center(NCSC), KISA and each sector's ISAC monitor Cyber threats
  - Collecting and analyzing Malwares from Honeypot by KISA
- **NCSC works as the National wide control center**
  - Attack monitoring, analysis and management with KISA, ISP and Public sectors
- **Cooperation with Partners**
  - Share analysis results among KISA, NCSC and local security vendors

As we could see in 7.7 DDoS attacks,
Single inspection may not solve the entire story!

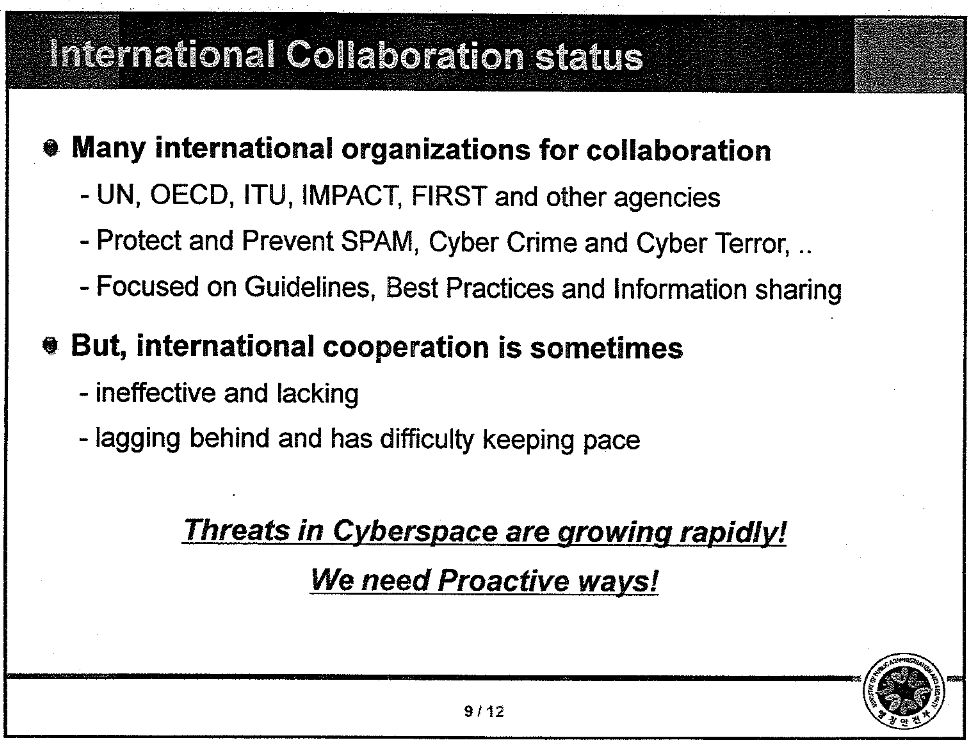
7 / 12



So what is Required?

- **Information Sharing !**
  - Detected facts of malicious code, cyber threats
  - Attack Defense Technology
  - Best practices and guidelines, education and etc.
- **Much closer collaboration between inside and outside inspections is required to prevent unknown attacks**
  - **To achieve the truth** : what, where, how .. and who?
  - **To detect machines** participating attacks : location, ..
- **Much closer partnership among APEC members**
  - Information sharing concerning attacks between CERTs, ISACs
  - **Realtime reporting mechanism**

8 / 12



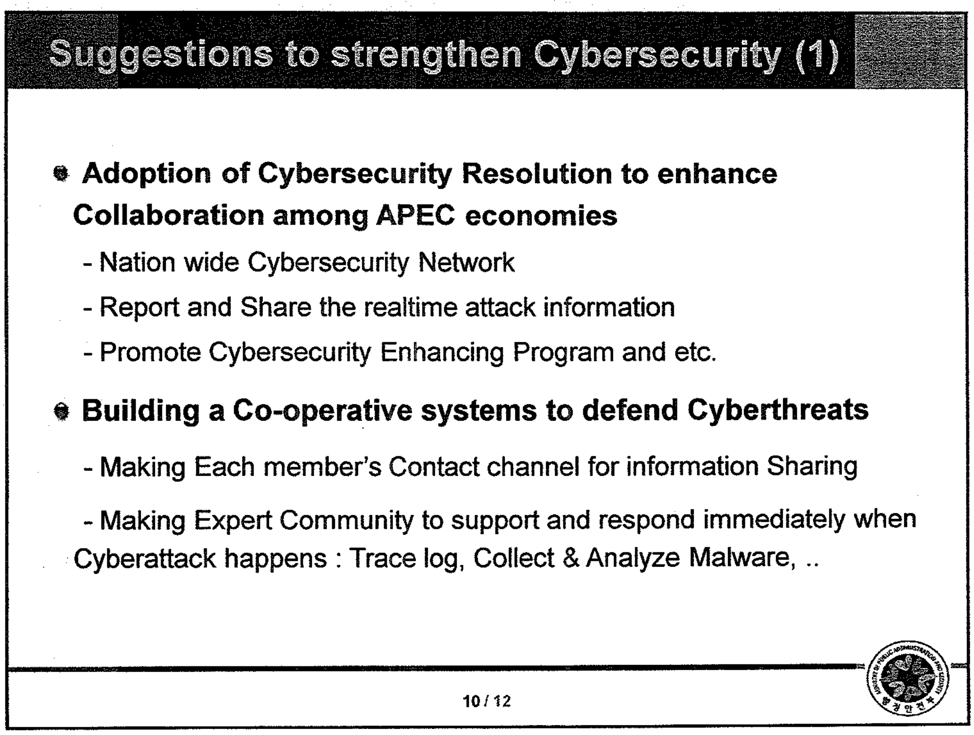
International Collaboration status

- **Many international organizations for collaboration**
  - UN, OECD, ITU, IMPACT, FIRST and other agencies
  - Protect and Prevent SPAM, Cyber Crime and Cyber Terror, ..
  - Focused on Guidelines, Best Practices and Information sharing
- **But, international cooperation is sometimes**
  - ineffective and lacking
  - lagging behind and has difficulty keeping pace

Threats in Cyberspace are growing rapidly!

We need Proactive ways!

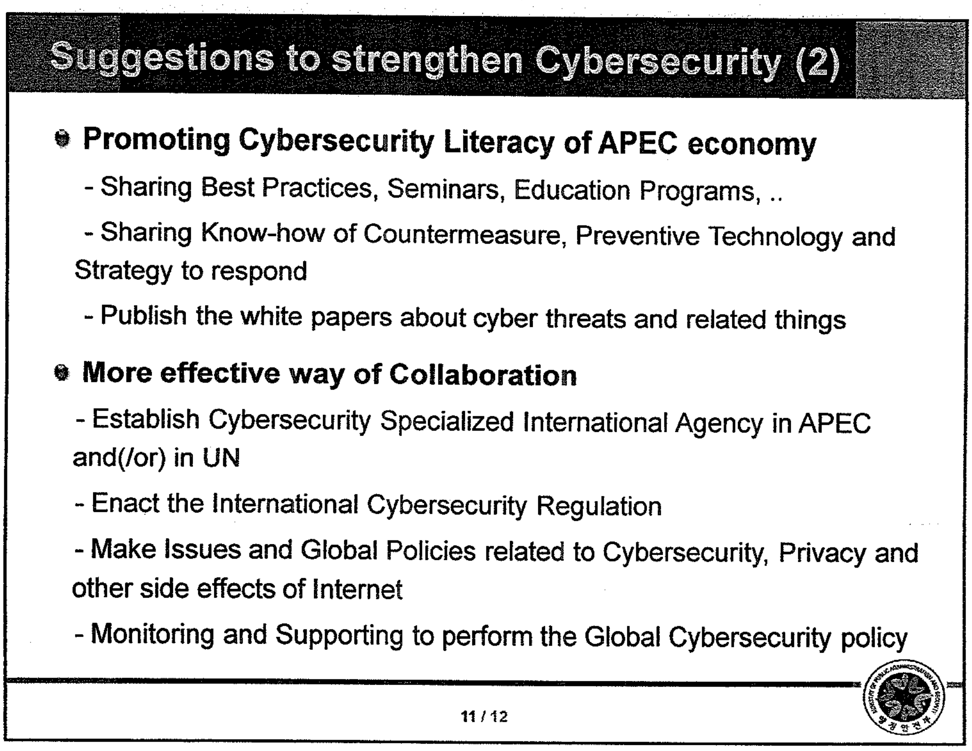
9 / 12



Suggestions to strengthen Cybersecurity (1)

- **Adoption of Cybersecurity Resolution to enhance Collaboration among APEC economies**
  - Nation wide Cybersecurity Network
  - Report and Share the realtime attack information
  - Promote Cybersecurity Enhancing Program and etc.
- **Building a Co-operative systems to defend Cyberthreats**
  - Making Each member's Contact channel for information Sharing
  - Making Expert Community to support and respond immediately when Cyberattack happens : Trace log, Collect & Analyze Malware, ..

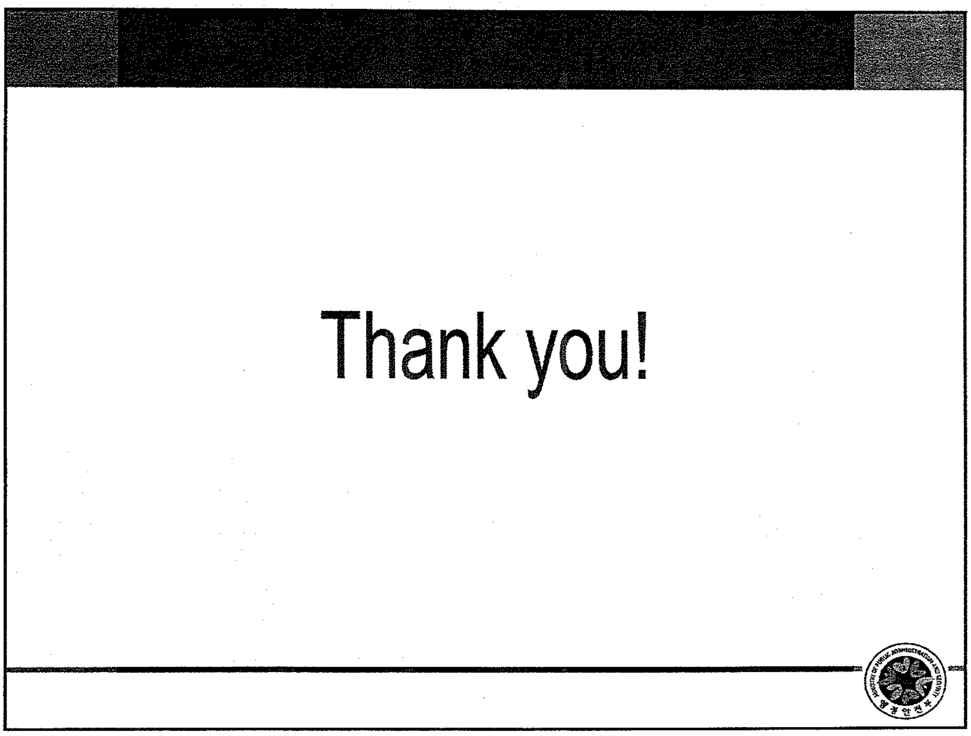
10 / 12



Suggestions to strengthen Cybersecurity (2)

- **Promoting Cybersecurity Literacy of APEC economy**
  - Sharing Best Practices, Seminars, Education Programs, ..
  - Sharing Know-how of Countermeasure, Preventive Technology and Strategy to respond
  - Publish the white papers about cyber threats and related things
- **More effective way of Collaboration**
  - Establish Cybersecurity Specialized International Agency in APEC and(/or) in UN
  - Enact the International Cybersecurity Regulation
  - Make Issues and Global Policies related to Cybersecurity, Privacy and other side effects of Internet
  - Monitoring and Supporting to perform the Global Cybersecurity policy

11 / 12



Thank you!