Cyber Security and International Cooperation

Special Adviser to the President for National Security

Lim, Jong In
The Sony Pictures Entertainment was hacked before the release of ‘The Interview’, a movie about the assassination of North Korea’s leader.

Overview of the Sony Pictures Hacking

- Sony Pictures Entertainment’s internal system was breached and some of data was leaked on November, 2014.
- The data included
  - personal information about employees
  - e-mails between employees
  - information about executive salaries
  - copies of unreleased Sony films, etc.
- The hackers called themselves the "Guardians of Peace" and demanded the cancellation of the planned release of the film ‘The Interview’, a comedy about a plot to assassinate North Korean leader Kim Jong-un.
Recent Issues – Sony Pictures Ent. (2014)

• U.S. pointed out North Korea as a perpetrator of the hacking and President Obama clarified N.K.’s hacking as a ‘Cyber Vandalism’

U.S. Government’s Reaction

• U.S. Government regarded the hacking against Sony Pictures Ent. was ‘Cyber Vandalism’, and took series of actions

• U.S. Government’s Reactions

  - 19th of December, 2014, F.B.I. published an investigation report of the hacking that North Korea was the perpetrator

  - President Obama said it was ‘Cyber Vandalism’ and claimed U.S. would take proportional action against the attack

  - Websites of North Korea were shut down, rumored to be cyber attack from U.S.

  - President Obama sanctioned North Korea’s Directorate of Reconnaissance
Recent Issues – Sony Pictures Ent. (2014)

February, 2015, the White House published the ‘National Security Strategy’ which reflects the Obama Administration’s security policies.

Outline of the National Security Strategy

- The second strategy paper regarded as Obama’s National Security Strategy 2.0
- Cyber threat is one of the new security challenges that U.S. and the international community face
- To defend Cyberspace, U.S. will
  - Legislate framework for Cyber Security
  - Impose cost on malicious cyber actor
  - Assist other countries
  - Cooperate both in International and domestic context
Korea Hydro & Nuclear Power (KHNP) was threatened to be destroyed by a hacker who claimed to have hacked KHNP and disclosed confidential data.

**KHNP Hacking Overview**

- **December, 2014**, Hacker who call himself as ‘Against Nuclear Power plant’ claims that he breached into KHNP and threatened KHNP to shut down the Nuclear Power plant.

- The Hacker exposed some confidential data of KHNP to prove that he/she succeeded to hack into KHNP internal control system.

- Korea Government and KHNP checked the control system of KHNP but could not find any evidence of the intrusion, and the cyber attack to the Nuclear Power plant did not happen.
Korea Government’s investigation unit claimed the hacking was perpetrated by North Korea using IP address in China, but failed to further the attribution.

Korea Government’s Reaction

- December 20, 2014, Government Combined Investigation Unit on Personal Information Crime took the investigation
- December 24, 2014, the Investigation Unit asked Chinese Police for cooperation
- March 17, 2015, the Investigation Unit presented midterm investigation report that the KHNP hacking was perpetrated by North Korea
- Hacker from N.Korea accessed VPN in S.Korea via proxy IP address in Shenyang, China, and failed to hack KHNP directly, so sent phishing emails to partners of KHNP and retired employees

Access via Proxy IP Address in Sunyang, China

Hacked partners of KHNP and retired employee’s of KHNP

Used vulnerabilities of Hangul (Wordprocessor)

Hacking Failed (Sent 6,000 Phishing Emails)

VPN in South Korea

Hacker in North Korea
Recent Issues – Implication

Difference between two hacking incidents: Sony Pictures Entertainments v.s. KHNP

U.S. Government
Response to Sony Pictures Entertainments Hacking
- F.B.I.
- Existing Cooperation - South Korea
- Request for Cooperation to - China

Investigation
International Cooperation

Attribution
Counter-Measures
- Attribution Succeeded - North Korea
- Financial Sanction
- Counter Attack?

South Korea Government
Response to KHNP Hacking
- Government Combined Investigation Unit on Personal Information Crime
- Request for Cooperation to - China

Investigation
International Cooperation

Attribution
- Attribution Failed - Some IP address in Shenyang, China?
South Korea has continuously suffered cyber attack but failed to attribute, arrest or prosecute any suspects

<table>
<thead>
<tr>
<th>Year</th>
<th>Cyber attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>• 1.25 Internet Intrusion : Korea’s major internet networks went down due to the Slammer Worm taking advantage of vulnerabilities of Microsoft’s SQL servers.</td>
</tr>
<tr>
<td>2009</td>
<td>• 7.7 DDoS Attack : Three DDoS attacks from July 7 to 10 paralyzed the major government sites including the Presidential Office and others.</td>
</tr>
<tr>
<td>2010</td>
<td>• GPS Disturbance : For three years from 2010, three incidents of GPS disturbance occurred, causing signal interference and damage to GPS receivers in private and military sectors including Korea Telecom’s base stations.</td>
</tr>
<tr>
<td>2011</td>
<td>• 3.4 DDoS Attack : DDoS attacks on 40 local web sites including major portals, government offices, the Ministry of National Defense and financial institutions.</td>
</tr>
<tr>
<td></td>
<td>• Attack on NH Bank's computer system : Extensive data on NH Bank’s computer system were damaged with service access paralyzed entirely or partially.</td>
</tr>
<tr>
<td>2013</td>
<td>• 3.20 Cyber Terror : Major local broadcasters’ and 6 financial institutions’ computer networks went down.</td>
</tr>
<tr>
<td>2013</td>
<td>• 6.25 Cyber Terror : The Presidential Office Website, major government websites, media and political parties were under cyber attacks.</td>
</tr>
<tr>
<td>2014</td>
<td>• Hacking on KHN P : KHN P’s blueprints and operating methods for nuclear power stations were leaked on the internet due to cyber attacks.</td>
</tr>
</tbody>
</table>
South Korea established a comprehensive national counter cyber threat system, which controlled and coordinated by the Presidential office.
ICT Development and Evolving Cyber Threat

As the development of ICT leads to new technologies such as IoT, Big Data and Cloud Computing

ICT Development

- Connection
- Personalized
- Data Digitalized
- Convergence

IoT
- Network of physical objects or "things" embedded with electronics, software, sensors and connectivity
- 26 billion devices on the IoT by 2020 (Gartner)
- Wearable Devices, Smart Car, etc.

Cloud Computing
- Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources
- IaaS(Infra), PaaS(Platform), SaaS(Service)

Big Data
- High volume, velocity, variety information assets that require new forms of processing to make more meaningful information
ICT Development and Evolving Cyber Threat

- European Commission’s Next Generation Computing predicts ICT will evolved to IoT Environment through Embedded system and CPS

Vision: Internet of Things, Data & Services
- (e.g. Smart Cities)

Cyber-Physical Systems
- (e.g. Intelligent Networked Road Junction)

Network Embedded System
- (e.g. Autonomous Aviation)

Embedded Systems
- (e.g. AirBag)

Source: NGC Study, 2013, EUTEMA
In a Hyper Connected Society where various new applications of ICT are being adopted, threats to the new applications are anticipated:

**Smart Home Appliance**
- ICT added home appliances for remote control and efficiency, and convenience
- Hacked or Demonstrated Cases
  - Refrigerator hacked to send spam emails (2014)
  - Philips LED Lighting hacking demonstration (Dhanjani, 2013)
  - Web Camera Exposed (BBC, 2014)

**Smart Car**
- IT component and services are integrated into automobiles for information gathering and remote control
- Hacked or Demonstrated Cases
  - U.S. Embedded Security Center Demonstration (2010)
  - Korea University Demonstration (2012)
  - BlackHat USA Demonstration (2014)

**Smart Healthcare**
- Using body-measured information by using wearable devices and medical equipment
- Hacked or Demonstrated Cases
  - Breakpoint Security Conference, Pacemaker Hacking Demonstration (2012)
  - BlackHat USA, Insulin Pump Hacking Demonstration (2013)

**Smart Energy**
- Increasing energy efficiency by managing information such as SmarGrid, Smart Buildings
- Hacked or Demonstrated Cases
  - Puerto Rico SmartMeter Tempering (2009)
Trends on Cyber Threat

Cyber threat is becoming more intentional, destructive, targeted, increasingly external in origin, and targeting human.

Source: Korea Internet & Security Agency
International Cooperation

The distinctive characteristics of the cyberspace makes investigation more difficult, and demands international cooperation.

**Real World**
- Based on Physical spaces such as building, street, city
  - Territory
  - Fixity
  - Embedded
  - Material
  - Visible
  - Tangible
  - Actual
  - Euclidean/Social Space

**Cyber Space**
- Based on Information Technologies such as S/W, Network
  - Network
  - Motion/Flux
  - Dis-embedded
  - Immaterial
  - Invisible
  - Intangible
  - Virtual/Abstract
  - Logical Space

Source: Sallie Westwood and John Williams, Imagining Cities
Various types of International Cooperation are being developed, yet the outcome of cooperation is insufficient to countering cyber threats.

**Bilateral Cooperation**
- Cooperation between two states that have common interests
  - China – Russia Non-aggression Pact for Cyberspace
  - U.S. – Japan Cyber Defense Policy Working Group

**Regional Cooperation**
- Cooperation within Nations in the Region
  - NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - ANZUS Treaty applies to Cyber attacks
  - Asean Regional Forum

**International Cooperation**
- Cooperation through International Organizations
- Cooperation by the International Conventions, Treaties or Laws
  - Budapest Convention on Cybercrime
  - UN GGE
International Cooperation

- Budapest Convention on Cybercrime came into force in 2001, which includes substantial/procedural articles of cybercrime regulation and international cooperation procedure

< Major Implications>

- The First legally-binding international instrument to comprehensively address the cybercrime issues
- Scope of the Convention
  - Criminalising Conduct
    - Illegal Activities / Fraud / Interference / Child Pornography / etc.
  - Procedural tools
    - Preservation / Search and Seizure / Interception of Data
- International Cooperation
  - Mutual Legal Assistance Treaties, Point of Contact

< Status as of June, 2015 >

- Radified: 20 European, Australia, Japan, Sri Lanka, United States
- Acceded: 15 European, Dominican Rep., Mauritius, Panama
- Invited to Accede: Argentina, Canada, Chile, Columbia, Costa Rica, Israel, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal, South Africa, Tonga
Capacity Building

- Effort to build capacity to defend their own cyberspace

### Governance, Role & Responsibility
- Setting a National Cyber Security Governance Framework
- Allocate each agency for a concrete role and responsibilities by their jurisdictional sector

### Research & Development
- Acquisition of various Cyber Security Technologies
  - Digital Forensic and Cyber Investigation Tools
  - Cyber Genome or Cyber map
  - Count Cyber Threat Technologies

### Education
- Securing well-trained human resources is key to Cyber security
  - Gifted Education for Teenagers
  - Cyber Security Department in University
  - Training Course for Employers

### Cooperation
- Internal Cooperation
  - Inter-agency cooperation
- Public-Private Partnership
- International Cooperation
  - International Organizations, Conventions or cooperation between states
To deter the fast growing cyber threats, it is important for each nation to build their own capacities and cooperate internationally.

- **Evolving Cyber Threats**
  - Cyber threats are getting more sophisticated and targeted
  - Cyber threats are one of the most serious threat that most nations face

- **Increasing Dependencies on ICT**
  - New technologies such as IoT, Big Data and Cloud computing are being used
  - Society increasingly dependent on ICT

---

**Each Nations effort to deter Cyber Threats**

- International Cooperation
- Capacity Building
International Cooperation and Collaboration on Cybersecurity

- Every State Cooperate in:
  - Cooperative Cyber Response
  - Judicial Cooperation
  - Critical Infrastructure Protection

- Every State Collaboration in:
  - Developing Cyber Norms
  - Develop a Interpretations of International Law
  - Confidence Building on Cyber Security
Thank you

jilim76@president.go.kr