Cyber Security of 2018 Pyeongchang Olympic Games

Feb 2019

OH, Sang Jin (osjin70@gmail.com)

Contents

1. Strategy of cyber security

** Source - http://www.pyeongchang2018.com*

Strategy of cyber security

① Develop & operate robust ICT Security Systems taking into account the unique nature of the Games specifics

② Protect Key Assets of Olympic ICT infrastructure

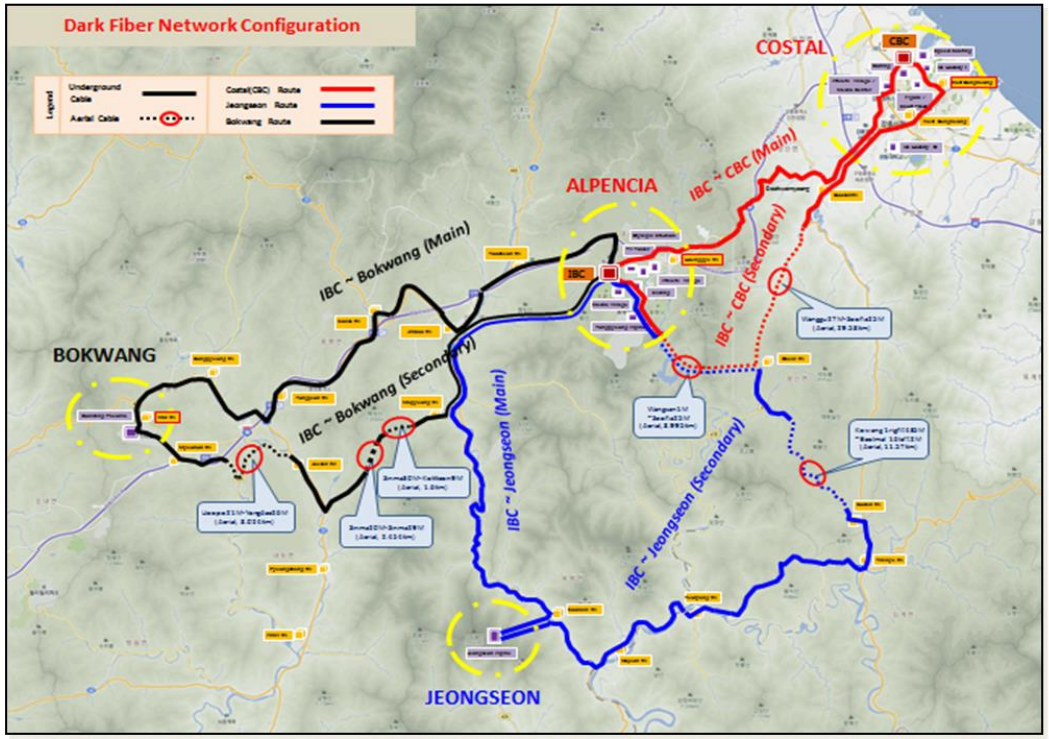
③ Develop IT Security Framework in compliance with local laws and international standards

④ Promote close cooperation between Organizing Committee, government agencies, and partner companies.

2. ICT Assets to Protect

** Source - http://www.pyeongchang2018.com*

Network Infrastructure (1/2)

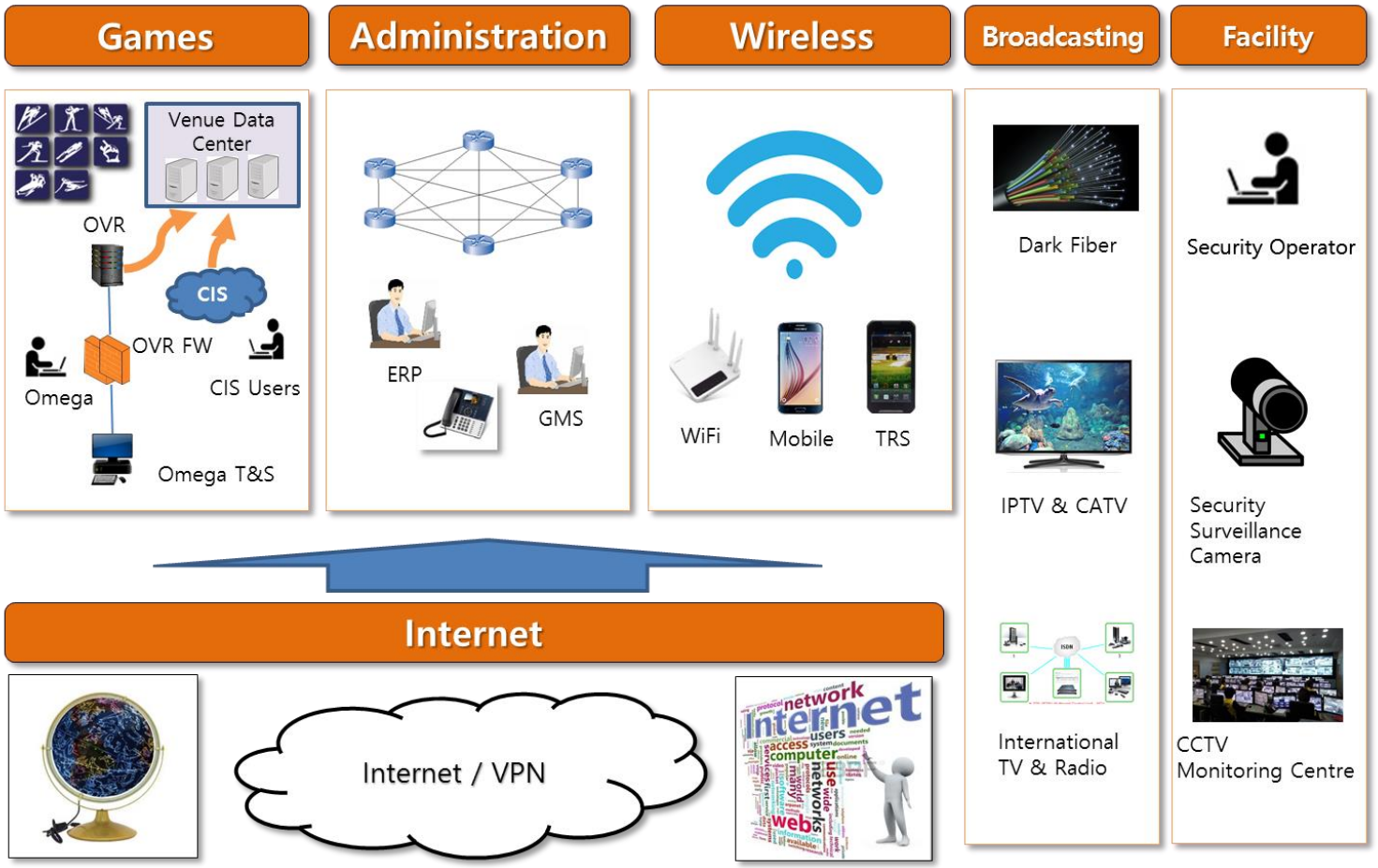


The total length of fiber optic cables: 775Km

2,943 of network equipment on POCOG N/W

1) Games N/W
2) Admin N/W
3) Wireless N/W
4) Broadcasting N/W
5) Facility N/W

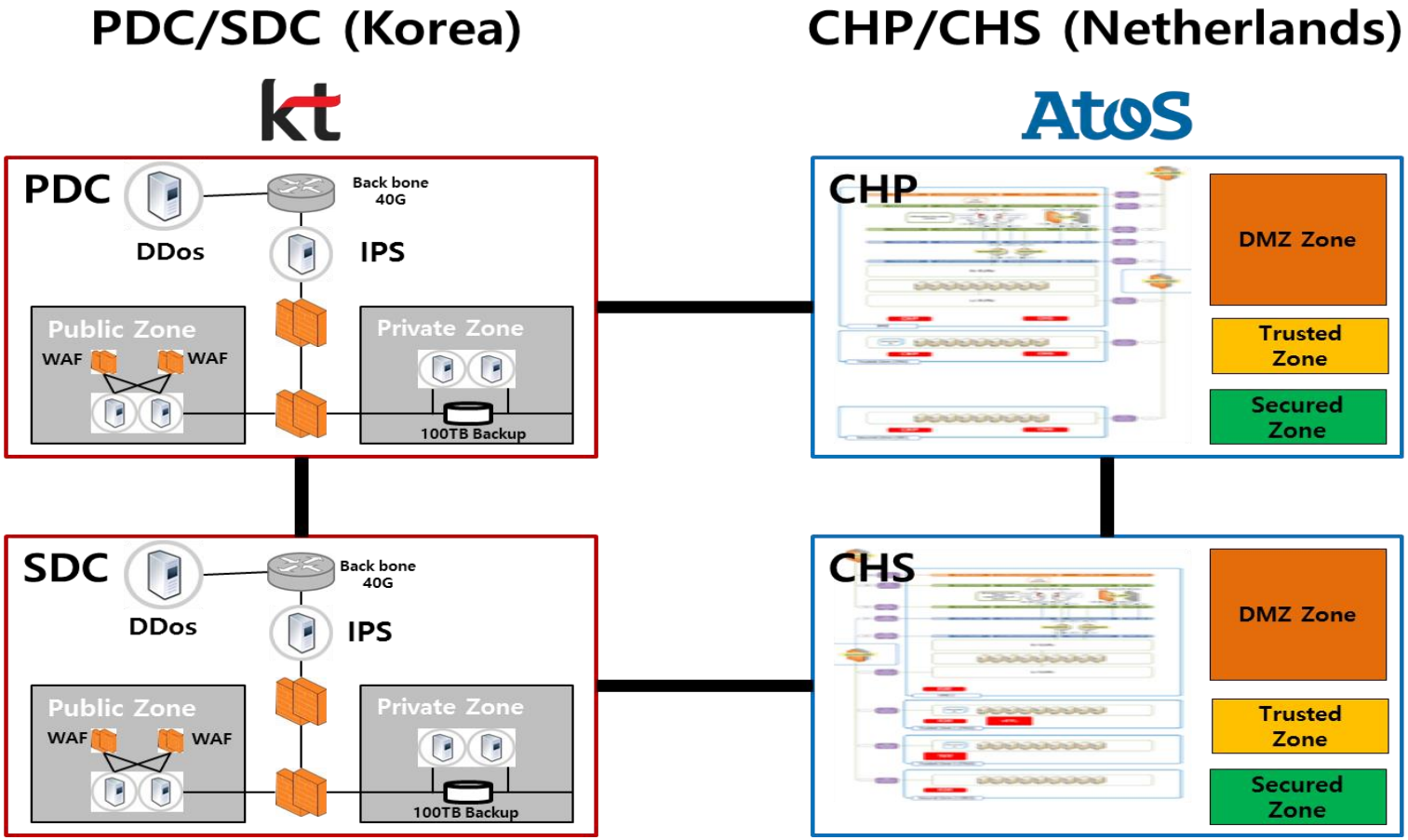
Network Infrastructure (2/2)



Olympic Application Services

- **Olympic Management System (OMS)**
  - ✓ Accreditation, Workforce Management, Competition, Schedule, Volunteer Portal (4)
- **Olympic Diffusion System (ODS)**
  - ✓ Info2018 / MyInfo, Commentary Information System, DATA Feed, etc. (9)
- **Games Management System / WEB**
  - ✓ GMS : Transportation, Accommodation, etc. (31)
    Web : Pre-Games, Games-Time, Test Event, etc. (10)
- **Administration System**
  - ✓ Management of Projects, Knowledge, Archive, Collaboration, Integrated Finance, Internal Portals, etc. (8)

Data Centre


PDC/SDC (Korea)
CHP/CHS (Netherlands)
kt
AtoS
PDC
Back bone 40G
DDos
IPS
Public Zone
WAF
WAF
Private Zone
100TB Backup
SDC
Back bone 40G
DDos
IPS
Public Zone
WAF
WAF
Private Zone
100TB Backup
CHP
DMZ Zone
Trusted Zone
Secured Zone
CHS
DMZ Zone
Trusted Zone
Secured Zone

ICT Devices

- Laptop, PC
  - *10,354*

- TV / Surveillance Cam
  - *7,130 / 810*

- Wi-Fi Router
  - 6,300

PyeongChang 2018

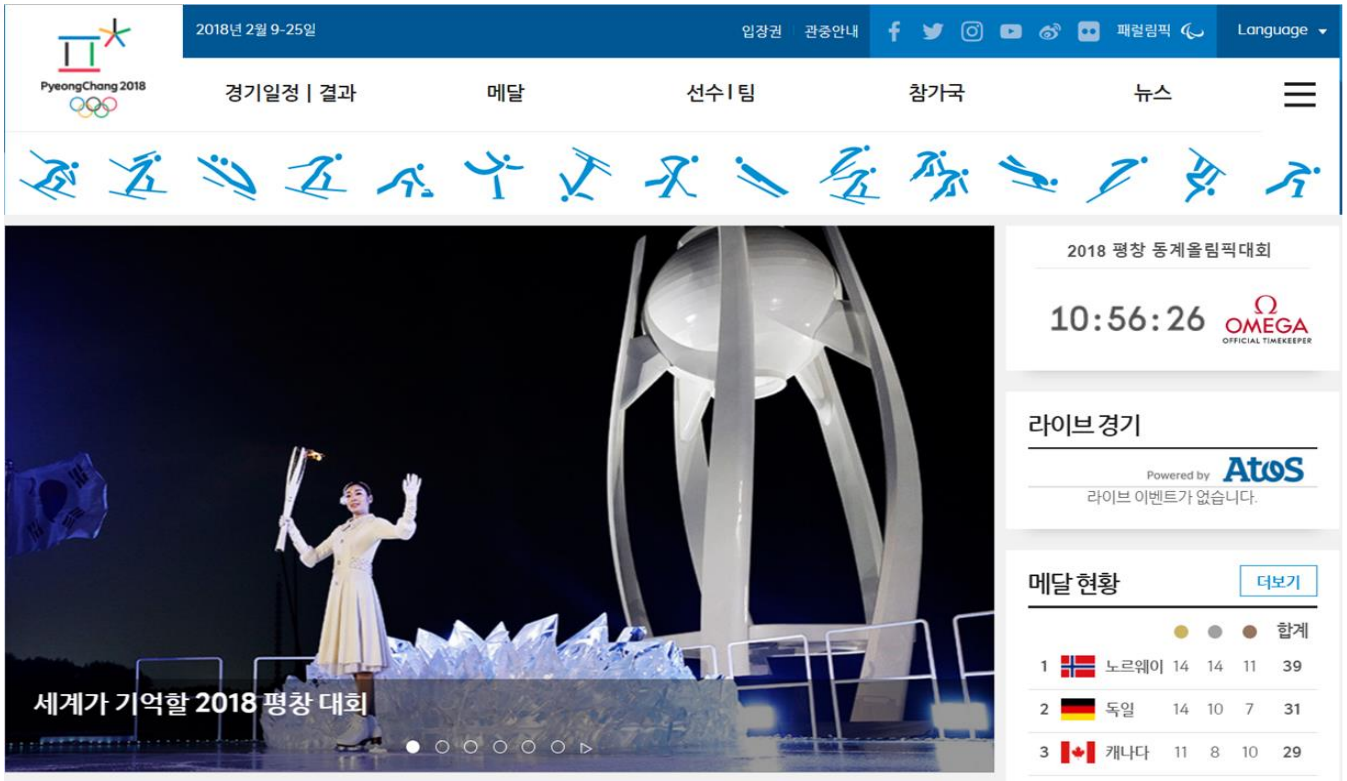
- Mobile Device, TRS, Radio
  - 21,000

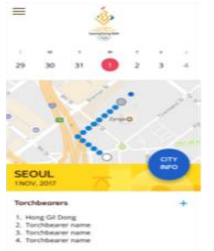
- Tablet
  - 2,372

- Reprographics Device
  - 2,665

Official Webpages

PyeongChang2018 Page on IOC's Official Website & Mobile Apps

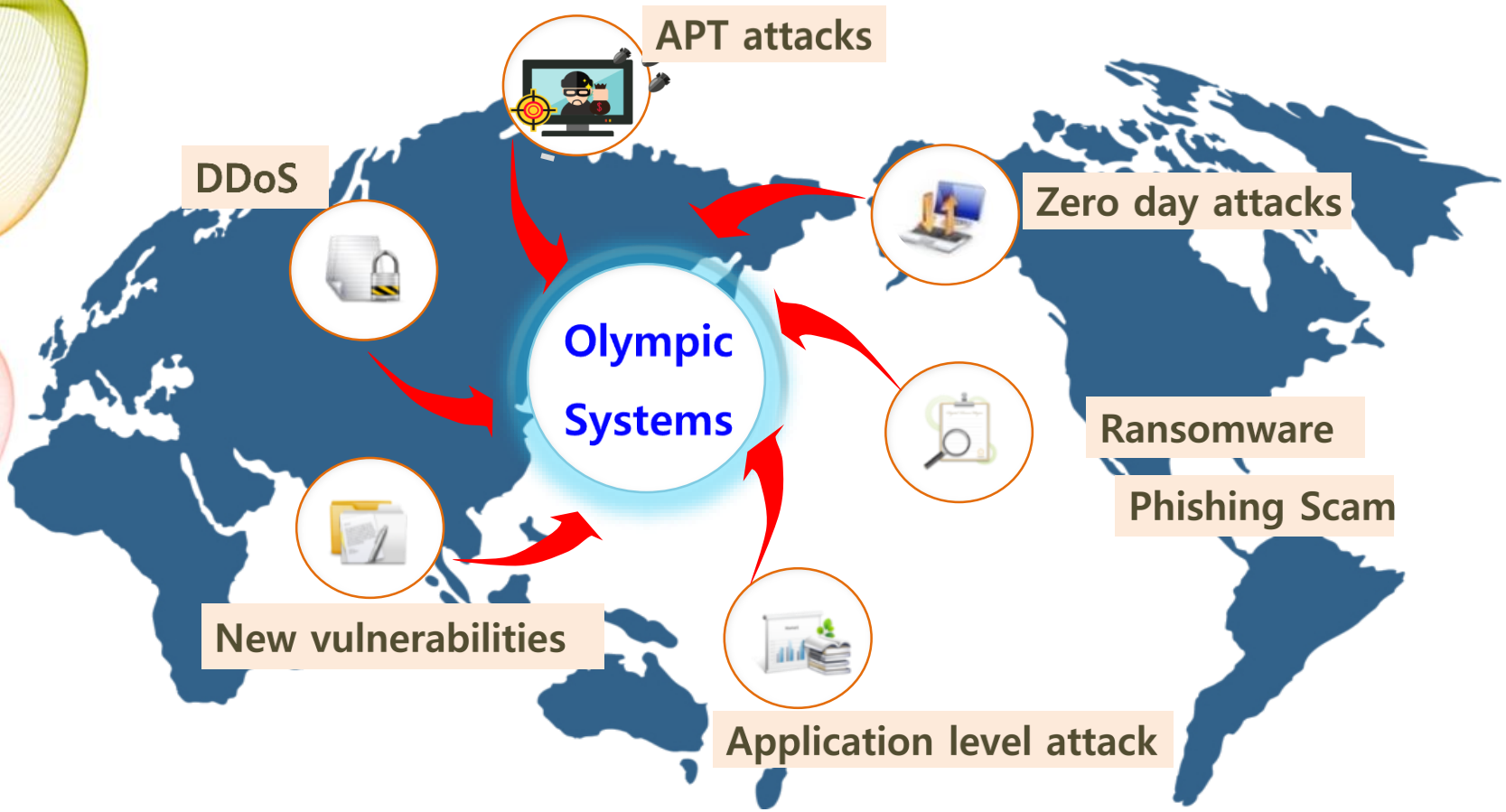




3. Security Threat & Governance

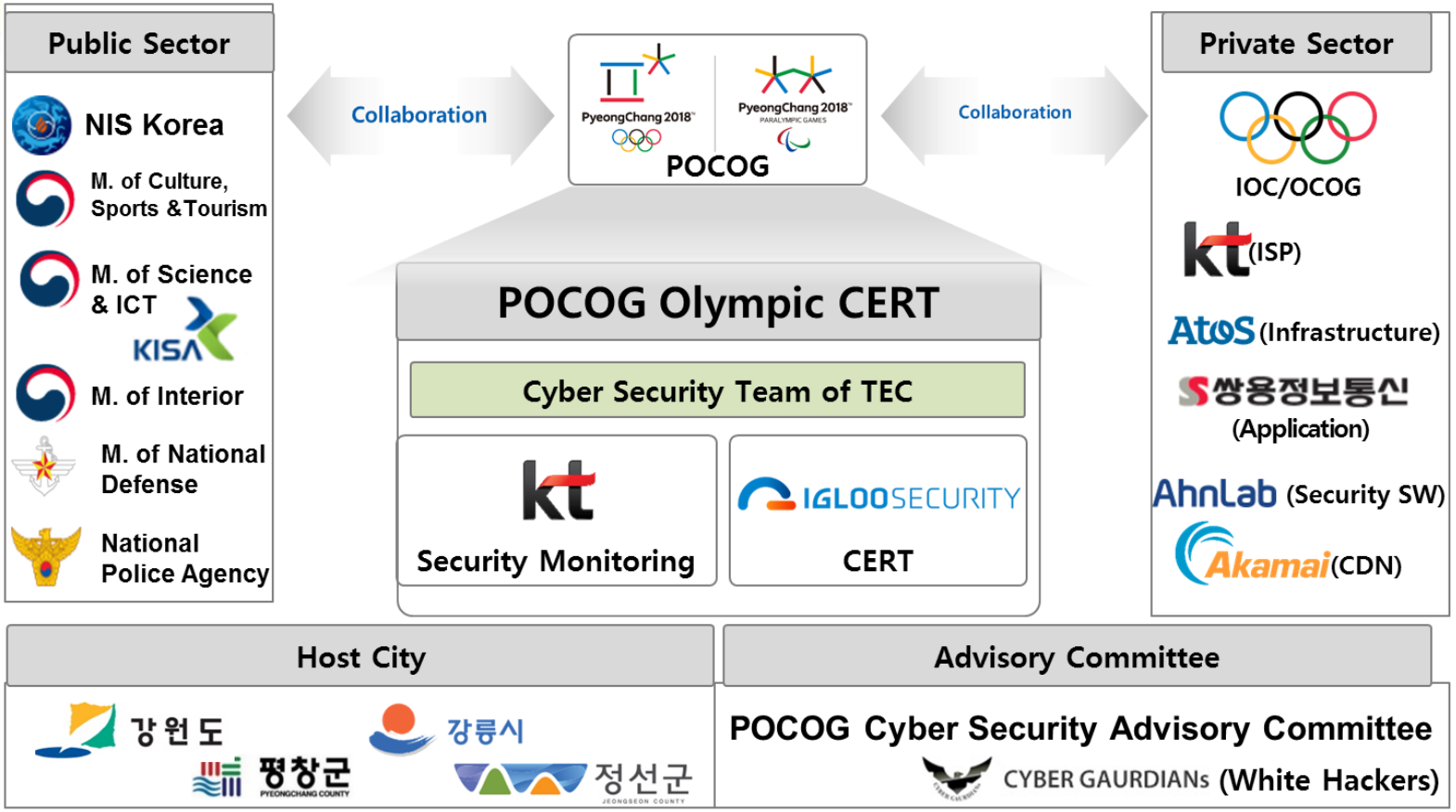
* Source - http://www.pyeongchang2018.com

Cyber Security Threats



Cyber Security Governance

▣ The nationwide cyber security governance was established and operated.



4. Cyber Security Measure

- Network Security
- Data Centre Security
- Device Security

** Souce - http://www.pyeongchang2018.com*

Network Security

Networks are physically partitioned to ensure security & reliability

Key Principles

A Independency

- Networks for 5 key services are partitioned

B Redundancy for network survival

- Redundant N/W Centre: MNC & SNC
- Redundant backbone & ISP N/W

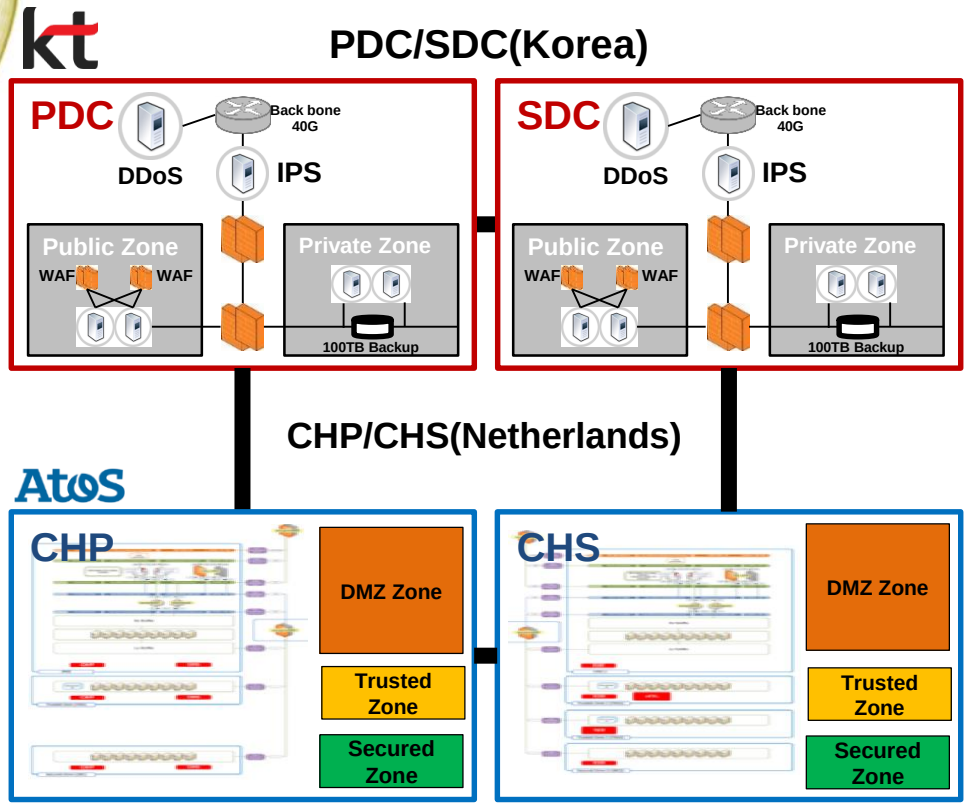
※ MNC (Main Network Centre) located in Gangneung
SNC (Secondary Network Centre) located in Pyeongchang

C Access Control

- Access Control by device
- Firewalls by network to control access

Data Centre Security

Comprehensive protection measures for 70 software critical for Games operations



Multi-layered Protection

- 1st: block DDoS attack in CDN
  * CDN(Content Delivery Network)
- 2nd: block DDoS attack by network service provider
- 3rd: block DDoS by POCOG
- 4th: Intrusion Prevention System
- 5th: Firewall
- 6th: Data Centre partitioned into three zones(DMZ, Trust, Secure)
- 7th: Web Application Firewall

Device Security (1/2)

Device Security (2/2)

End-point Security

- **Anti-APT(Advanced persistent threats) & Anti-Virus Solutions**
  - ✓ Monitor malware(email, web-based) in real time.
  - ✓ Two-layered email scanning [1st (virus detection)/ 2nd (attachments scanning)]
- **Software Restriction Policy (SRP, AppLocker)**
  - ✓ Utilized the default security features of Microsoft Windows
  - ✓ To prohibit the execution of unwanted S/W, or in unwanted directory
- **Centrally Managed End-point Security**
  - ✓ Adopt Patch Management System to strengthen end-point security
  - ✓ Monitor the security status of end-point devices and manage IP addresses
- **My PC-Safeguard solution(end-point) & Cyber Security Check Day**
  - ✓ Security check for every PC, which is centrally controlled.
  - ✓ Regularly reduce vulnerabilities in PCs & raise awareness on cyber security
- **Device Storage Control**
  - ✓ Prevent malicious code infection through USB, external storage, etc.
  - ✓ Secure USB distributed by POCOG are only allowed for use.

5. Proactive Prevention Activities

- Personal Information Impact Assessment
- Disaster Recovery Rehearsal
- Cyber Security Advisory Committee
- Olympics CERT

Personal Information Impact Assessment (2017)

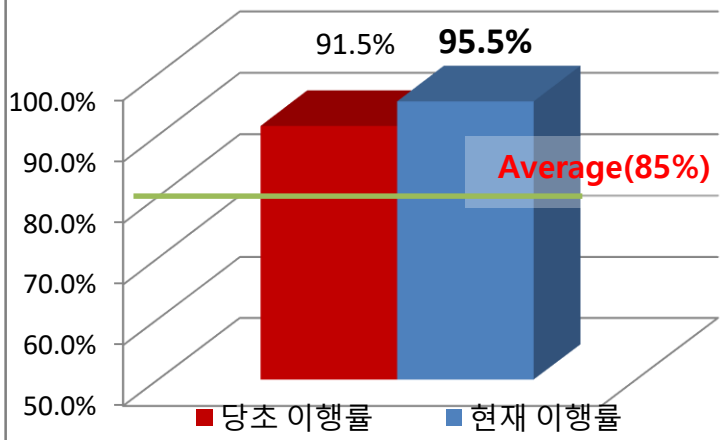
Overview

- To identify & improve risks in personal information management system.
- 56 systems in total, under assessment
- Apr.26.2017 - Aug.31.2017

Result

- 95.5% of systems have been properly installed in terms of information security

* Note: the average assessment rate among other organizations is 85%.



Disaster Recovery Rehearsals

Overview(4 rehearsals in total)

Aim	To Validate the disaster recovery plan & procedures for four(4) Data Centre & two(2) N/W Centre in case of disasters including cyber terror, fire, earthquake, etc.
1st	▪ Jun.9 / Aug.9 / Aug.12/ Aug.13. 2017
2nd	▪ Oct. 27~29. 2017

Result

Result

- Successfully complete the rehearsal.
- No issues in recovery procedures & manuals for Data Centre and N/W Centre.

Date	Target	Recovery Objective time	Result	
			Failover	Failback
'17. 8.12.	PDC	2 hours	3 hours	60min
'17. 8.13.	PDC	2 hours	1hr 20min	48min

Ref) Opening Ceremony Incidents

A cyber attack took place during the opening ceremony on 9th Feb, 2018. Internet access, IPTV, all other ICT services were damaged.

In collaboration with Olympic CERT, IOC, and Partners, Pyeongchang Organizing committee quickly recovered and stabilized the disrupted services.

Recovery Practices

- Disruption of Olympic services (9th Feb, 20:00 pm)
- Emergency service recovery for some Wi-Fi & IPTVs (9th, 22:00 pm)
- Completed the System Recovery procedures (10th Feb, 04:10 am)
- Checked the service availability & applied anti virus solutions (10th, 05:09 am)
- Changed passwords & applied additional security solutions (10th, 06:30)
- Fully recovered the disrupted services (10th, 07:50 am)

Cyber Security Advisory Committee

(20 meetings since 2015)

❖ **Activity**

① Assess the compliance by POCOG with the Information Protection & Personal Information Protection Standards.

② Review the configurations & security posture of N/W and systems.

③ Advise on how to monitor systems & respond to security incidents with proper procedures.

④ Advise & consult POCOG on major security issues.

Members of Committee

❖ **Committee Members**

- The total of 13 Experts from various sectors including public, private, Academy, related organization, and POCOG

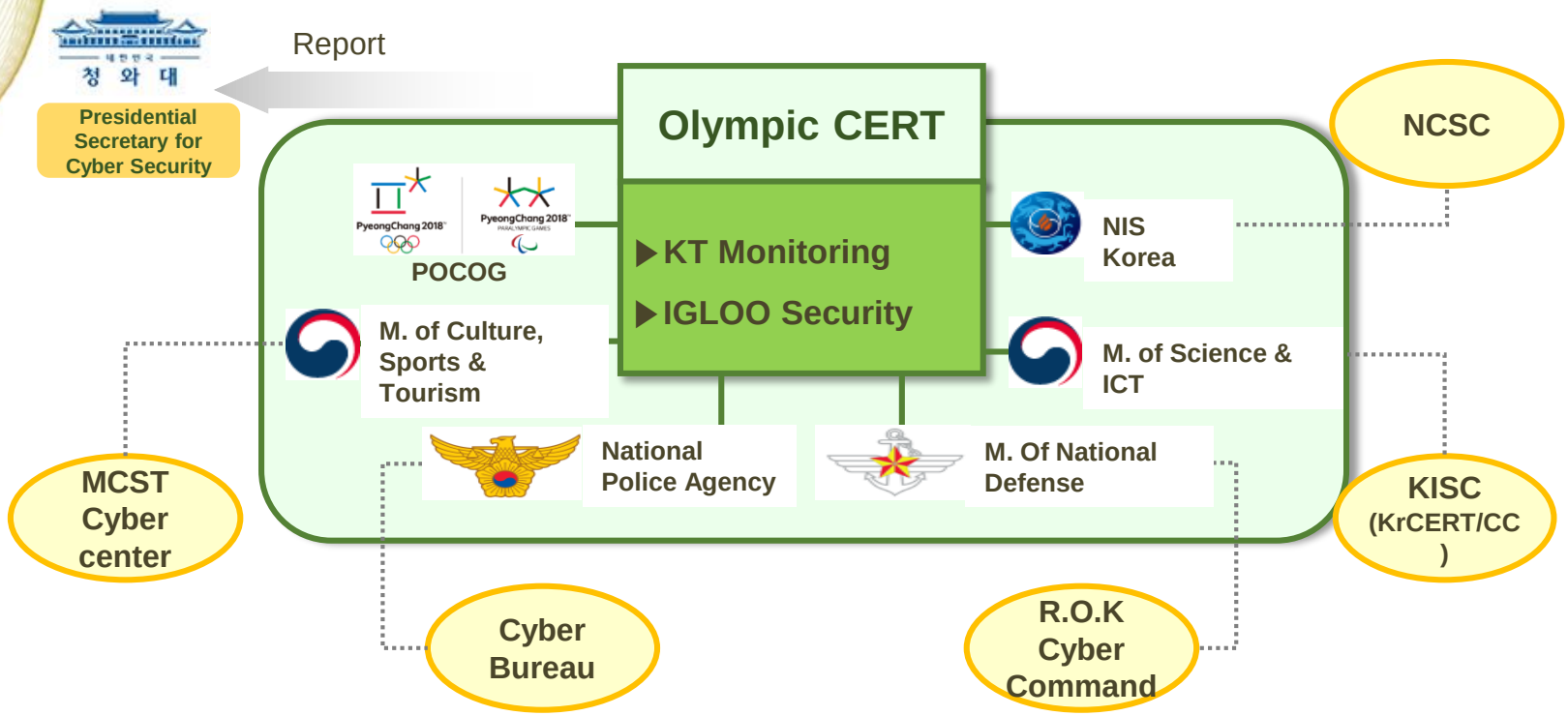
❖ **Technical Panel**

- 10 cyber security technology experts

❖ **POCOG CERT**

- Cyber Security Team of POCOG TEC (4 members)
- Igloo Security(Security Incident Response), KT(Monitoring), etc.

Structure of Olympic CERT



Thank you for your time!