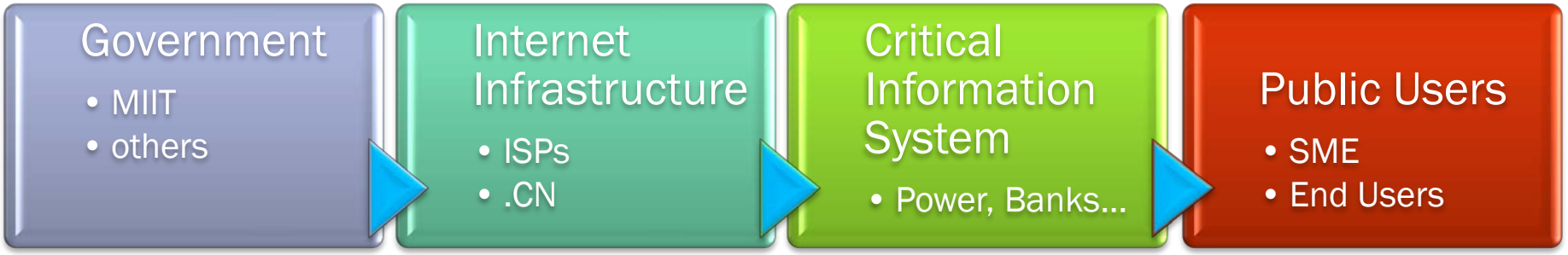
Information Security of the Beijing 2008 Olympic Games

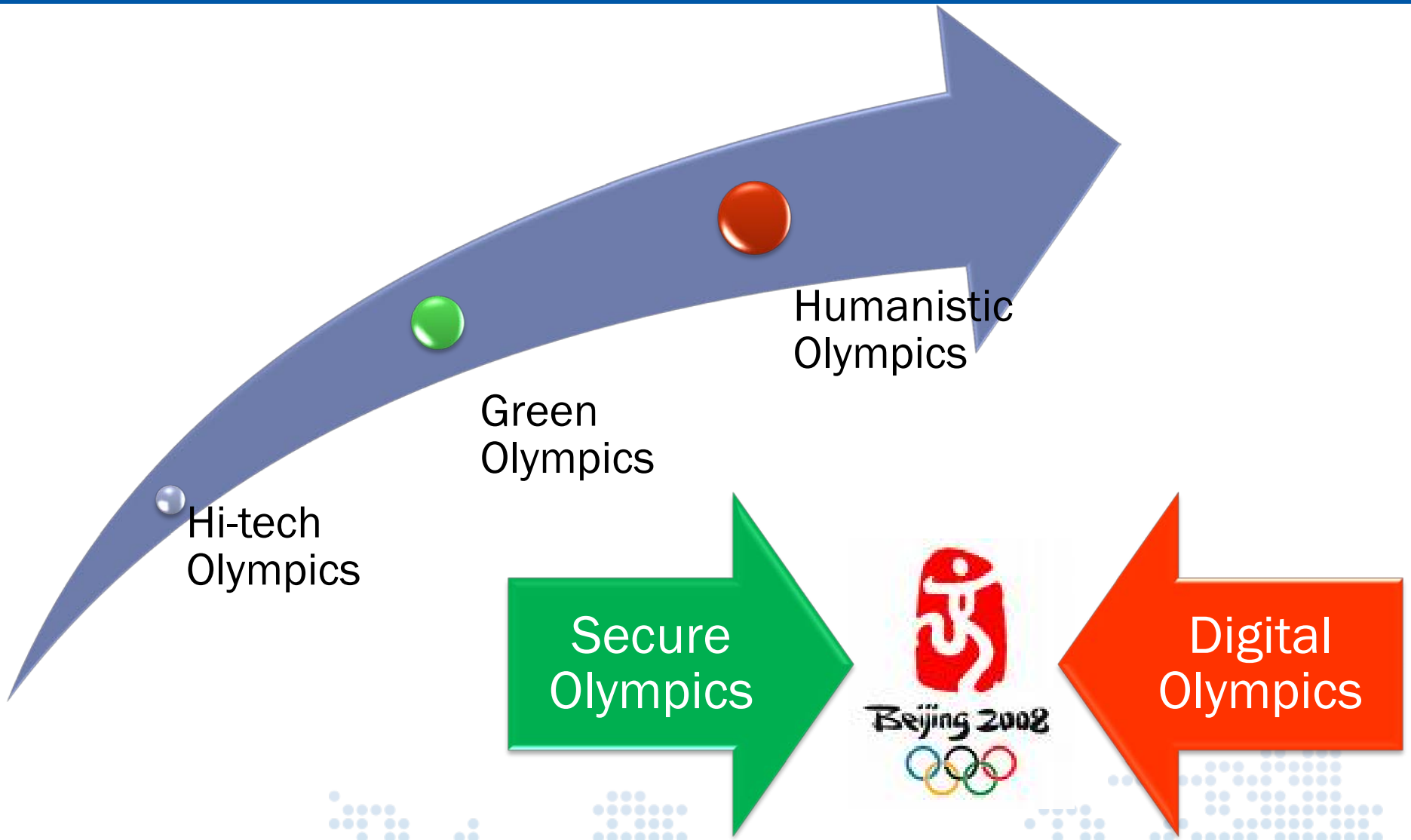
Yonglin ZHOU

About CNCERT



National computer network security team of China
Non-government agency
Non-profitable

Three Themes



Threats

CNCERT/CC

CNCERT/CC

Se
Int
Envir

Ho
Gr

Challenges

Scale

- Only the competition networks connected to more than 10 thousands of computers distributed around 66 venues.

Vulnerability

- Information Systems
- Operation Level
- Management Level

Risks

- After many times security evaluation, the systems were still found with high risks
- Operation faults, human damages, natural disaster

Situation

- Hacker groups
- Hostile group

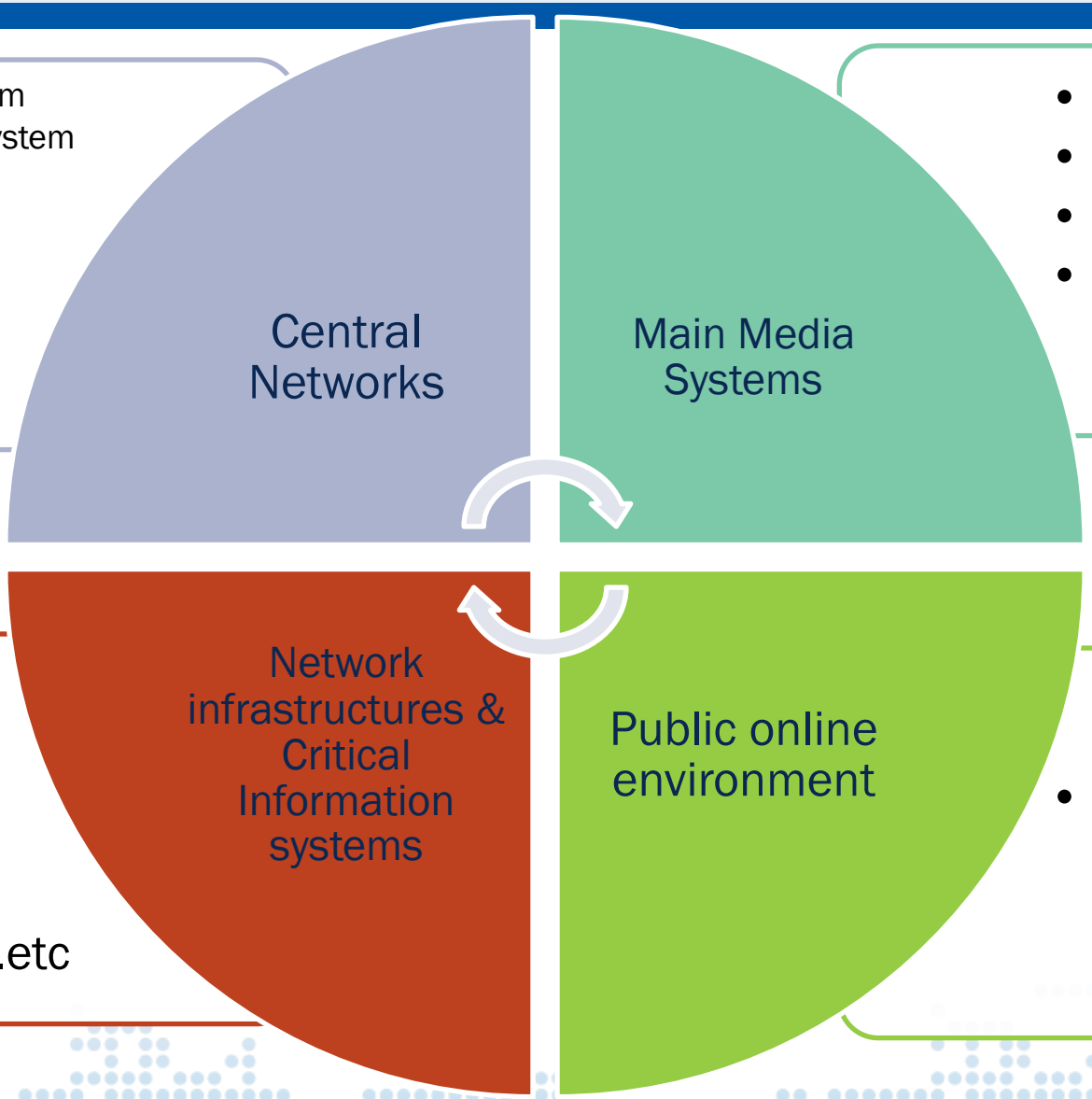
Experience less

- First time to hold such scale events
- Internet grew so fast and reach a statues that never appears before

Targets of protection

CNCERT/CC

CNCERT/CC



- Competition system
- Online ticketing system
- Office network
- Official Website

- CCTV
- Xinhuanet.com
- Sohu.com
- ...etc.

- ISP
- DNS
- Power, Civil Aviation , ...etc

- End user

General Goals

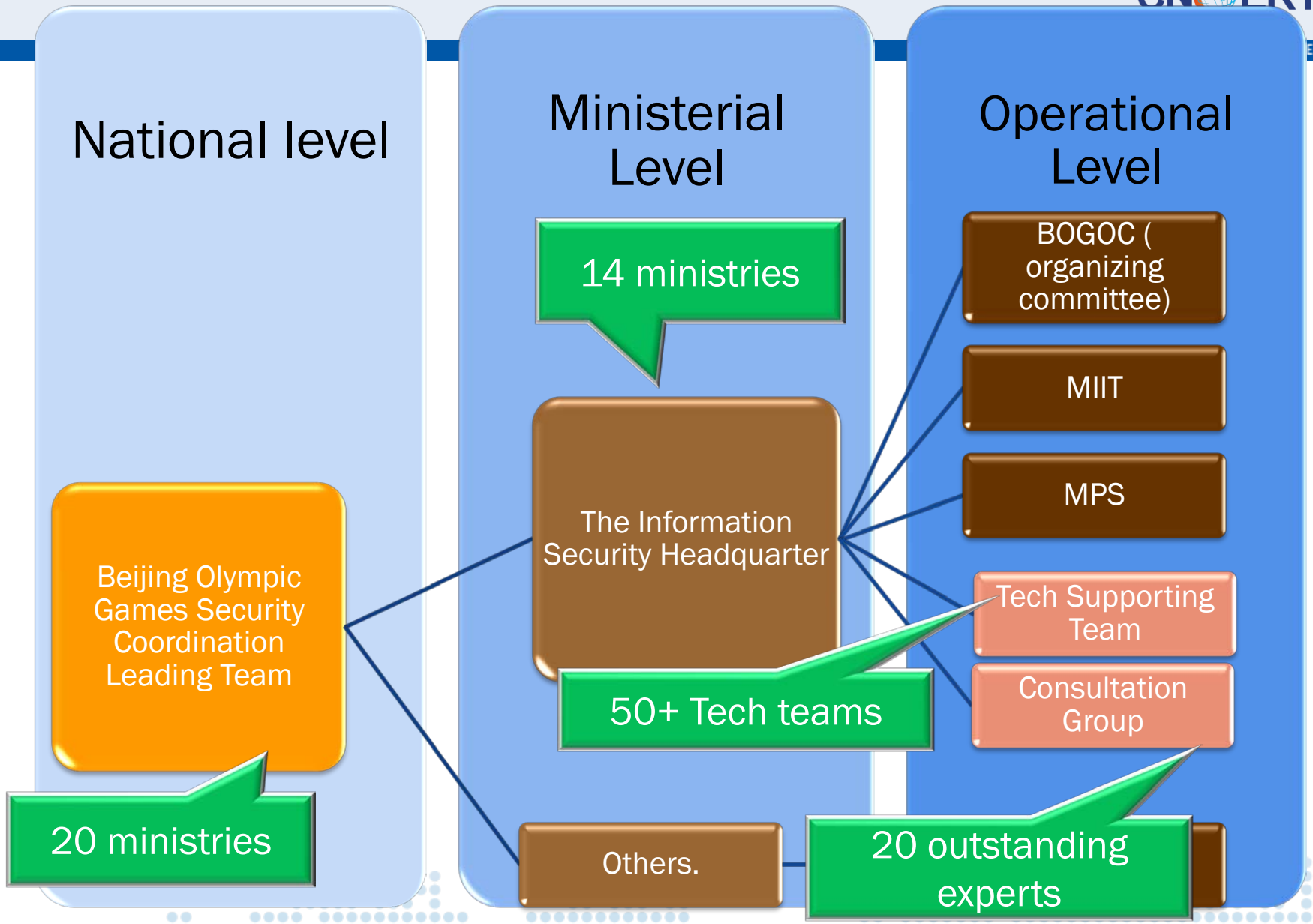
- The nation's leaders, including the president HU Jintao, issued many orders to enhance the information security of Beijing Olympics.
- In summary, the general goals are:
  - Keep the connectivity of networks
  - Keep the availability of information systems
  - Keep the order and safety of online environment
- **In short:**

  Try best to avoid serious incidents and make sure every common incidents can be solved appropriately.

Collaboration Framework

- Framework
  - In Dec 2004, the Beijing Olympic Games Security Coordination Team was founded, which consist of 20 departments, including Ministry of Public Security, Ministry of National Security, Ministry o f Defense, Ministry of Foreign Affairs, Ministry of Information Industry, the Government of Beijing, ...etc, to lead the safeguarding of Beijing 2008 Olympics.
  - Under the coordination team, instructing headquarters for 25 special fields and 10 regions were established. The Information Security Headquarter was responsible for the network security coordination, which consisted of 14 departments, such as MPS, MII, BOGOC (organizing committee), etc.
  - The information security headquarter organized more than 50 special technical teams and 20 famous experts to help as volunteers.

Collaboration Framework



Main Actions

CNCERT/CC

Classified Protection

- According to the classified protection regulation, the competition system, online ticketing system, office network, official Website have been strictly classified into necessary levels.
- Security countermeasures applied on those systems were even stronger than the requirements by the regulation.

Risk Assessment

- Many national professional teams were invited to evaluated and test the security of above systems.
- 13 vulnerability checks
- 6 formal risk assessment
- Tens of penetration tests

Instant Study

- Newly disclosed vulnerabilities (such as DNS vul), incidents.
- Grasp the situation and get professional advice at the first time.

Main Actions

Network Monitoring

- Official Website Provider (Sohu.com)
- Tech departments, BOGOC (organizing committee)
- China NetCom -- Internet Provider
- CNCERT – Cross network, national wide

Response Preparedness

- Multilevel and special ER plans
- Drills: for example, 7 times Anti-DDOS Drills. Each

Online Environment Cleaning

- Botnet and trojans sudden elimination
  - 2 times – before and in the middle of the games.
- Closed numbers of illegal websites (porn, violence, …)
- Strikes on cyber crimes

CNCERT's Activities

Help to learn experience

- Since 2006, invited experts who have joined the safeguarding of World Football Cup, Sydney Olympics… etc, to share their experience with BOGOC.
- Held meetings, forums to discuss what & how on Beijing Olympics protection

- Give professional suggestion on Olympic information system building, especially on security protection systems.
- Help handle many incidents : DDoS to online ticketing system

Give risk assessment and remote penetration tests.

Established collaboration agreements with BOGOC, ISPs, main medias, Critical Information System, CNCERT's supporting teams, and International partners

CNCERT's Activities

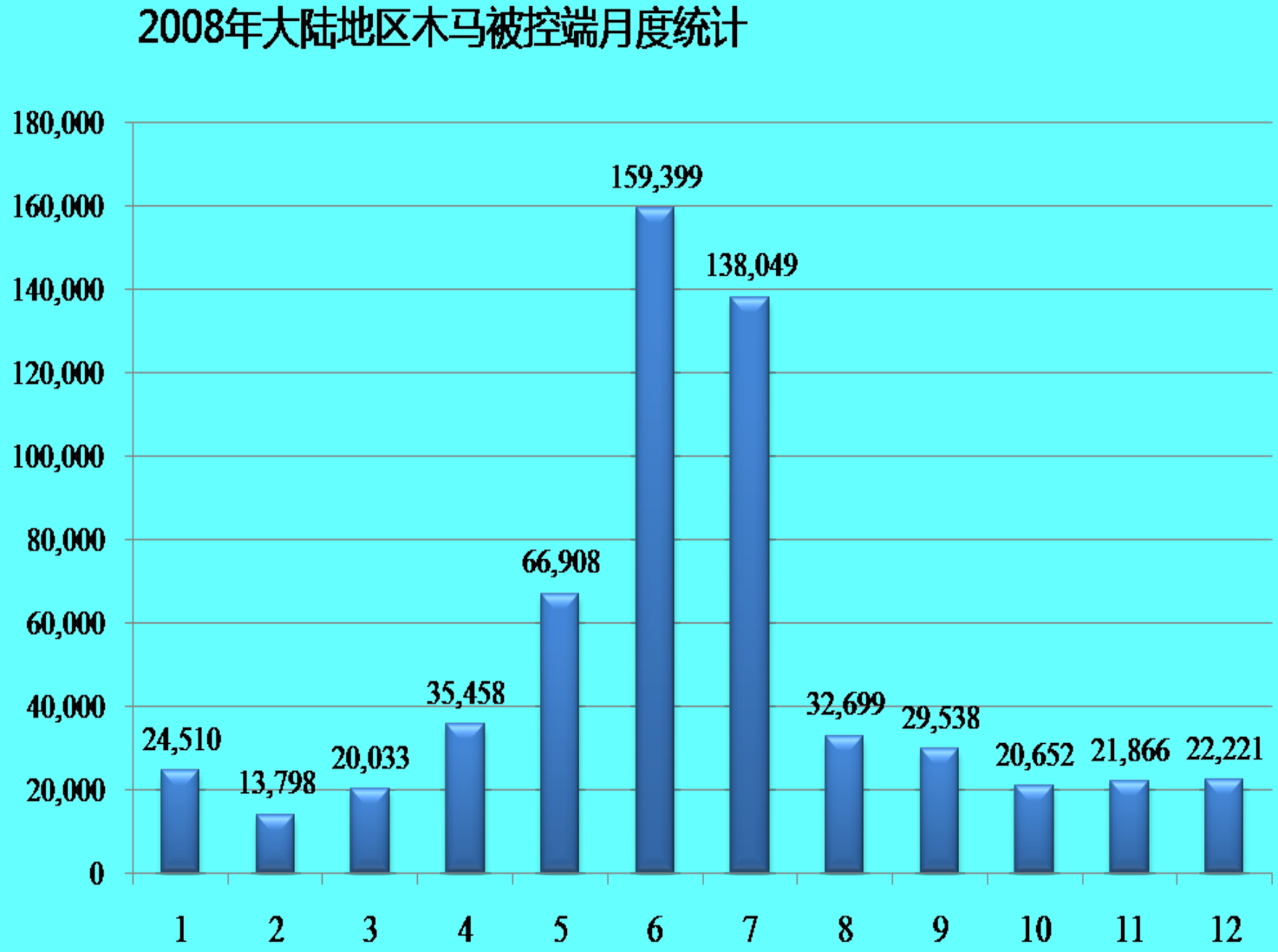
Upgraded network monitoring systems

Carried out 7*24 monitoring on 555 websites and more than 60 thousands IP addresses.

Distributed more than 400 monitoring reports to relevant departments

Organized 2 times sudden strikes on Botnet and Trojans, to mitigate the risk of large scale DDoS.

Results


2008年大陆地区木马被控端月度统计
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
24,510
13,798
20,033
35,458
66,908
159,399
138,049
32,699
29,538
20,652
21,866
22,221
1
2
3
4
5
6
7
8
9
10
11
12

Memories

Thanks

谢谢


Beijing 2008
北京欢迎你
The Official Website of the Beijing 2008 Olympic Games
www.beijing2008.cn