Network Security Activities in CERNET Backbone

Zhonghui Li
CERNET Network Center
Tsinghua University

Outline

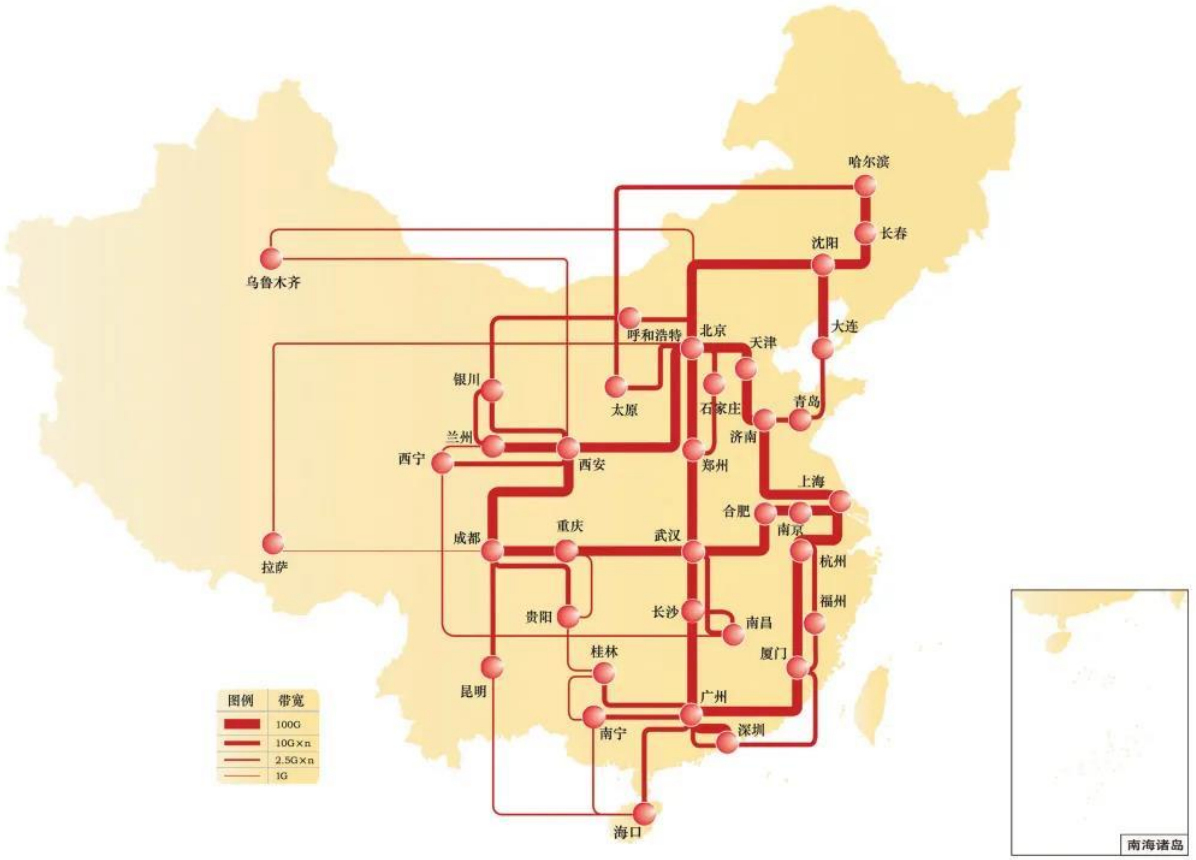
- Network security architecture
- Infrastructure security activities
- CCERT

Outline

- Network security architecture
- Infrastructure security activities
- CCERT

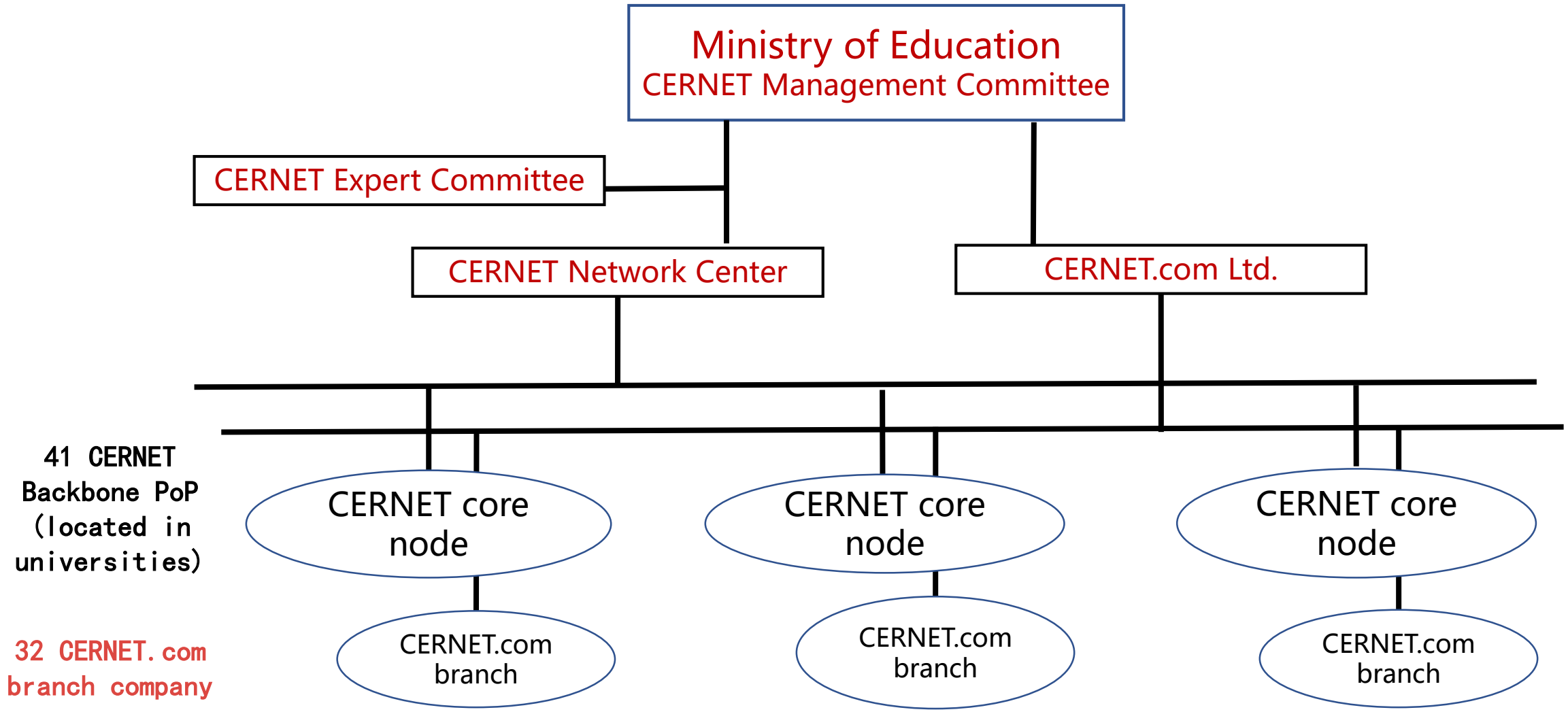
CERNET/CETNET2 backbones

CERNET backbone

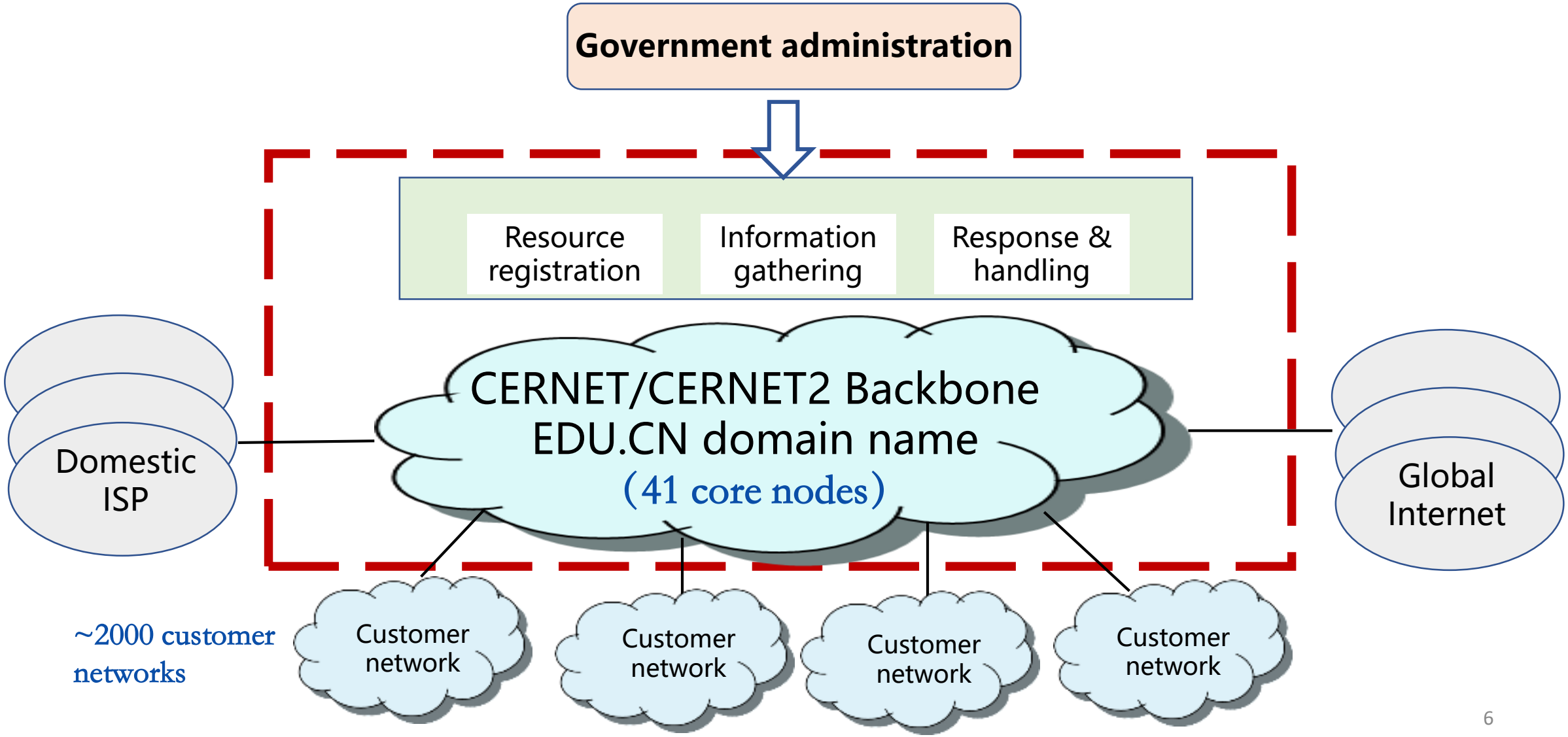


CERNET2 backbone

Architecture of CERNET organization and management



Management scope of CERNET network security



CERNET network security architecture

CERNET Management Committee

CERNET network center

- Emergency response CCERT
- Security operation SOC
- Network operation NOC
- Network information NIC
- System R&D Support

CERNET.com

- Customer service
- Technical service
- Technical R&D
- Security service

CERNET backbone core node (41)

CCERT members

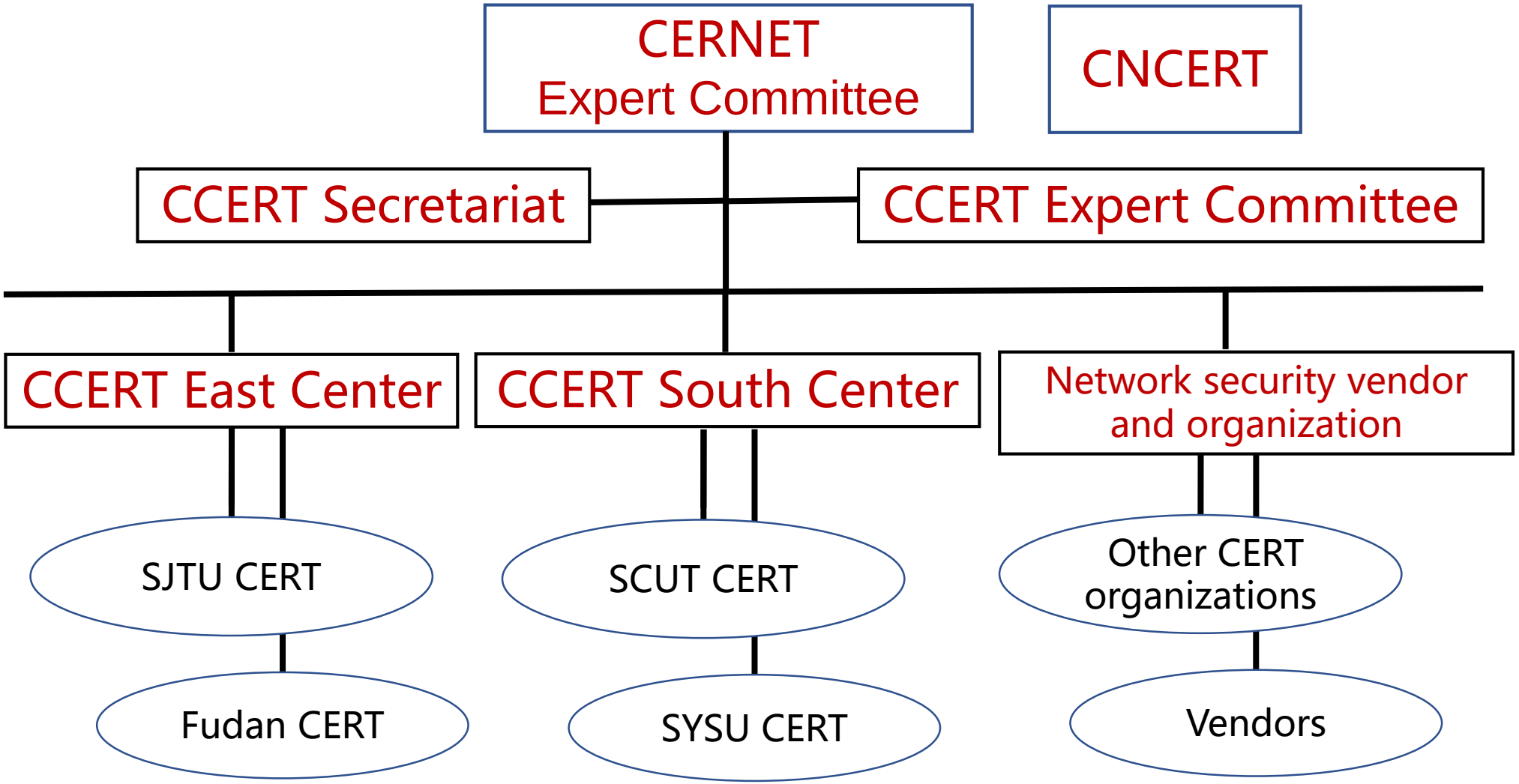
Tech support team in Tsinghua University

Core node	Core node	Core node	Core node
CERT/SOC/NOC/NIC	CERT/SOC/NOC/NIC	CERT/SOC/NOC/NIC	CERT/SOC/NOC/NIC
CERNET.com branch	**CERNET.com branch**	**CERNET.com branch**	**CERNET.com branch**

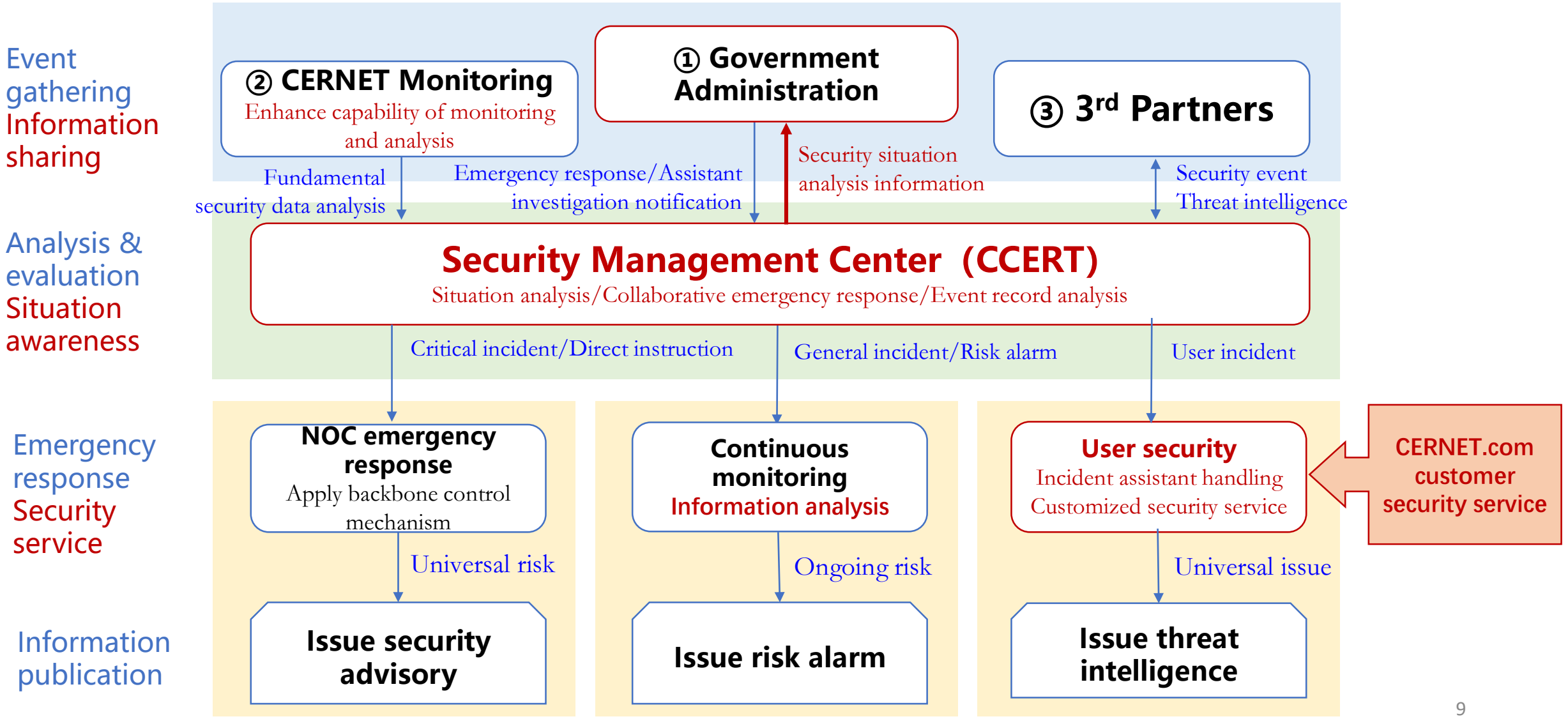
CERNET customer

- Collaborative handling
- Collaborative handling
- Collaborative handling
- Collaborative handling
- Collaborative handling
- Collaborative handling

CERNET network security emergency response and handling procedure

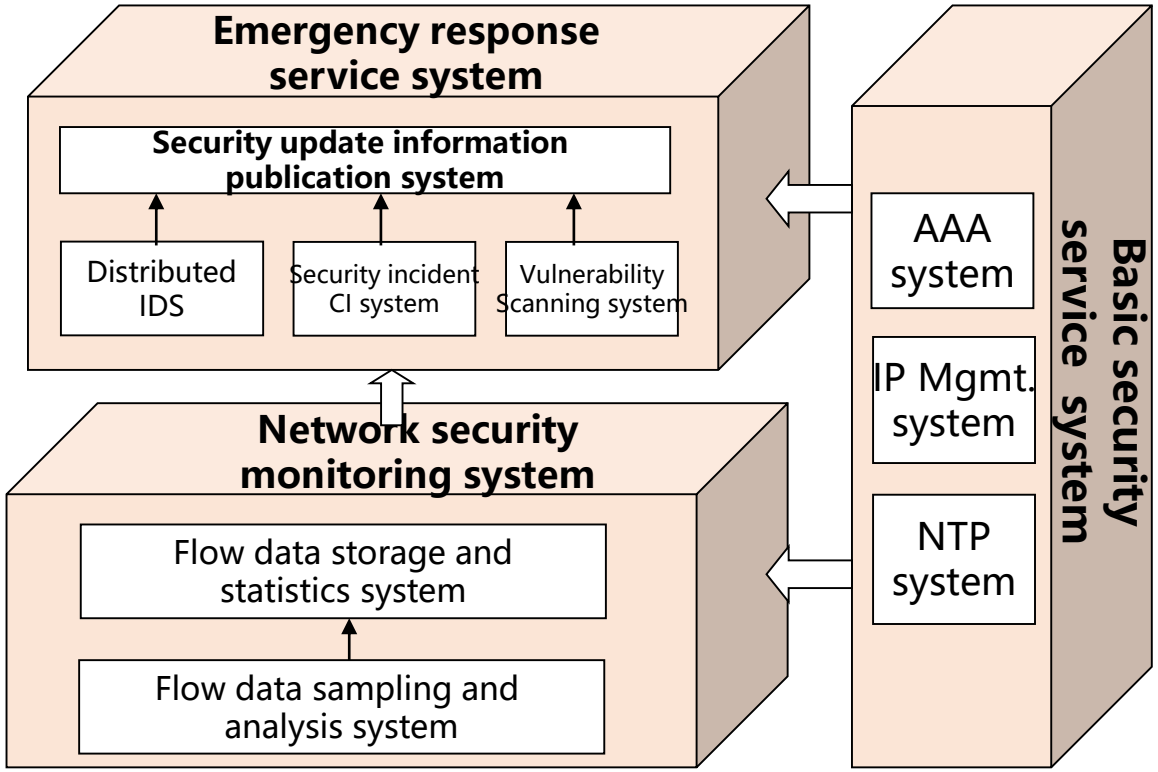


CERNET network security emergency response and handling procedure



CERNET operation security support architecture

CERNET backbone operation & security basic support system



CERNET high performance network management and security support system

Distributed NMS

- Distributed SNMP NMS
- Distributed flow analysis system
- Distributed bandwidth management and customer traffic control system
- E2E performance measurement system
- Network Op & Mgmt. service system

Backbone malicious behavior monitoring system

- Backbone malicious behavior monitoring system
- Distributed honeypot system

Emergency response collaborative service system

- IP address mgmt. system
- Emergency response collaborative service system
- Network service and situation information publication system

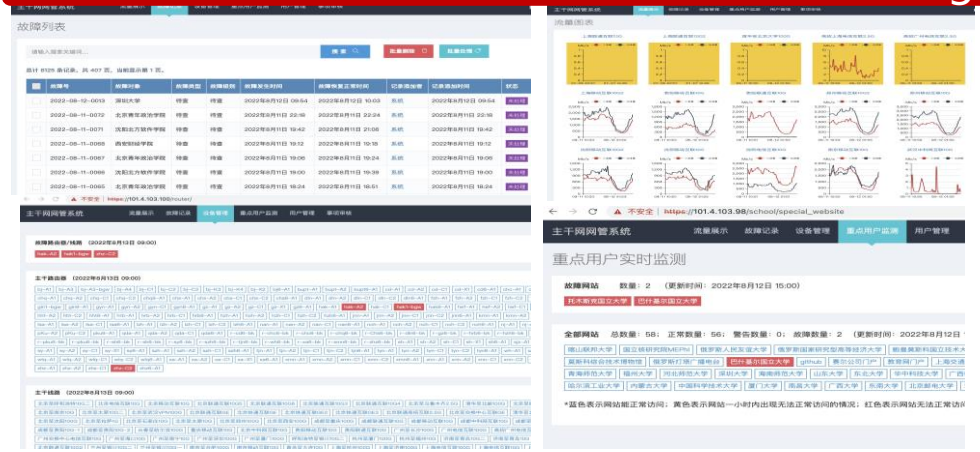
Outline

- Network security architecture
- Infrastructure security activities
- CCERT

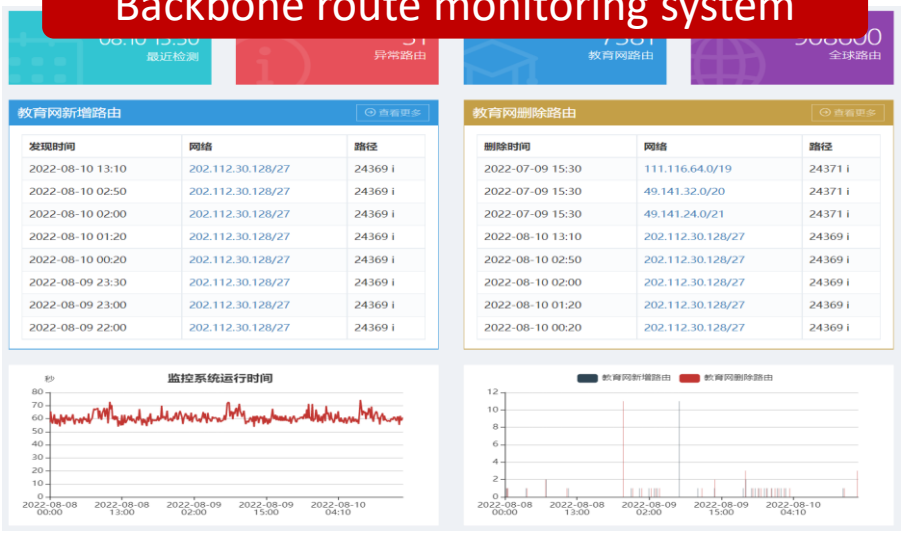
CERNET/CERNET2 backbone operation and monitoring

- Network traffic monitoring
  - Deploy threat detection system
- Application security monitoring
  - Deploy DPI device
- Node anomaly detection
  - Deploy device health monitoring system
- System operation monitoring
  - Deploy platform resource monitoring system
- Big data security analysis
  - Deploy situation awareness system with big data security analysis

Dual NMS：backbone node & link monitoring



Backbone route monitoring system



CERNET/CERNET2 backbone operation and monitoring

- Timely response
  - 7x24 monitoring and response
- Location
  - Fault & incident location
- Source trace
  - Detailed CLI commands of all operators in syslog
- Mitigation or counter measure
  - IP address blocking, BGP black hole

Backbone syslog ananlysis system

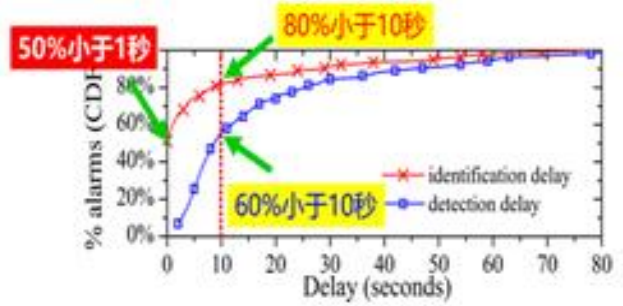
CERNET/CERNET2 backbone routing security mechanism

- Diversity on device vendors
- Self-developed NMS
- SAVA deployment
- Global inter-domain route hijack monitoring system
- MANRS initiative member
  - Filtering
  - Anti-spoofing
  - Coordination
  - Global validation

400+ probe

Cover 140+ countries

Handle 300M+ route updates message



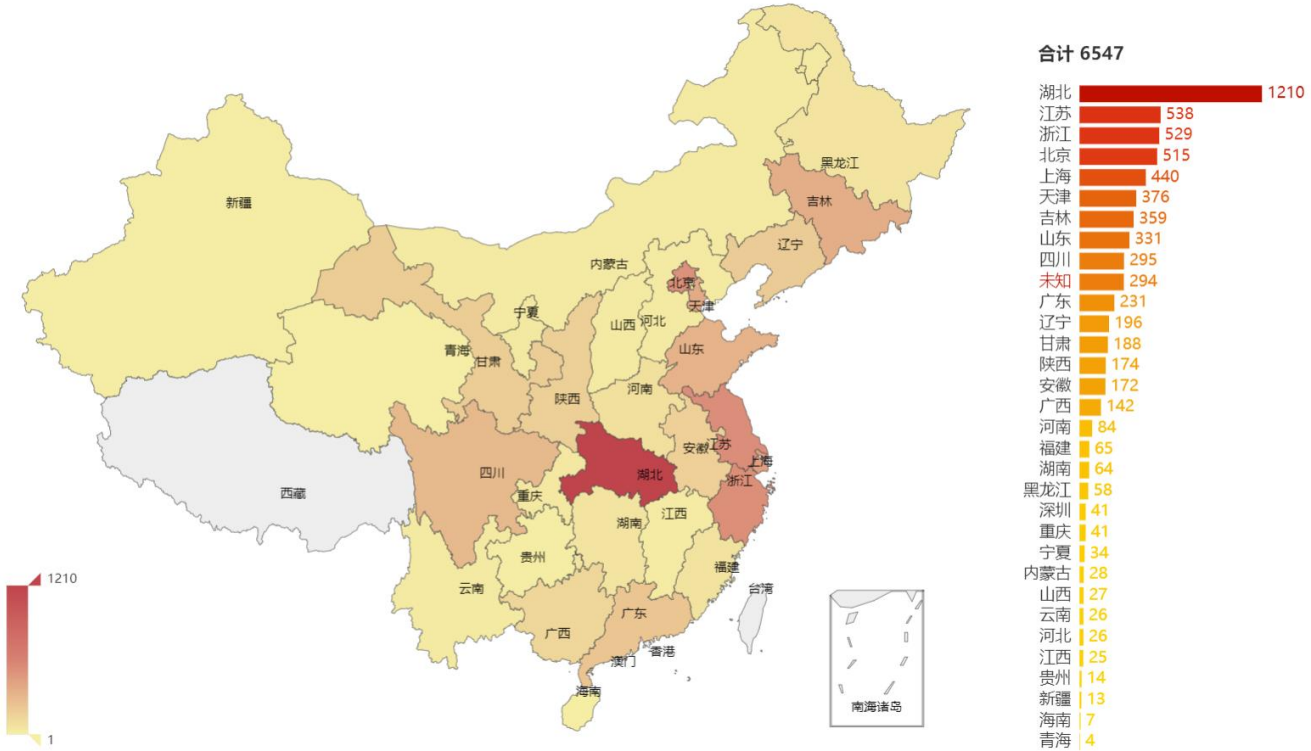
Incident detection in seconds

CERNET/CERNET2 backbone security monitoring

Virtual currency mining monitoring

2022-01-01 - 2023-01-10

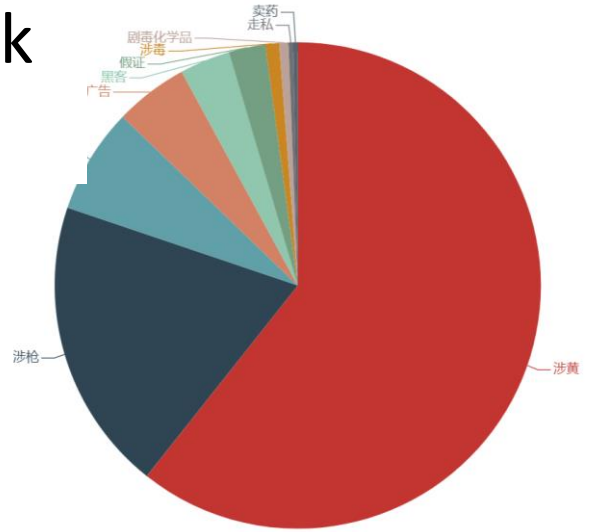
疑似矿工	波及学校	挖矿事件	活跃矿池
8796	667	532万	865



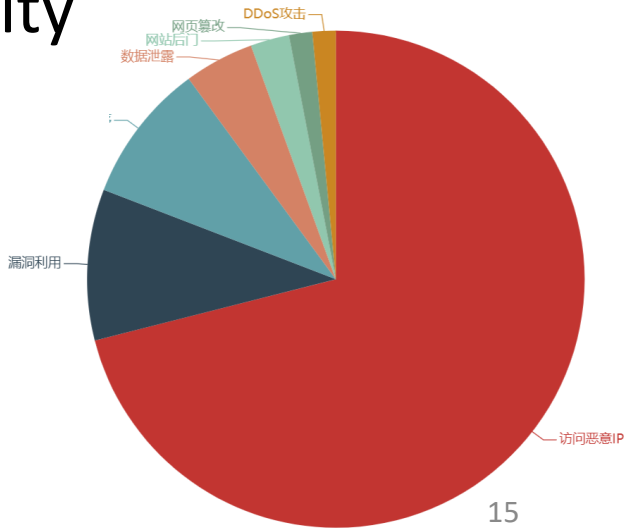
合计 6547

湖北	1210
江苏	538
浙江	529
北京	515
上海	440
天津	376
吉林	359
山东	331
四川	295
未知	294
广东	231
辽宁	196
甘肃	188
陕西	174
安徽	172
广西	142
河南	84
福建	65
湖南	64
黑龙江	58
深圳	41
重庆	41
宁夏	34
内蒙古	28
山西	27
云南	26
河北	26
江西	25
贵州	14
新疆	13
海南	7
青海	4

Network attack monitoring



Website security monitoring



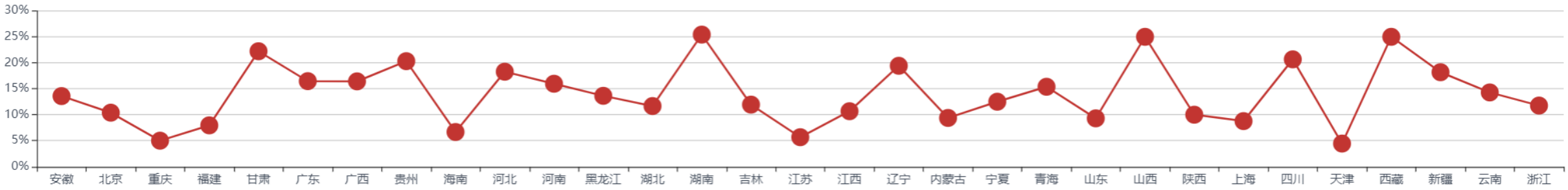
CERNET/CERNET2 backbone security service

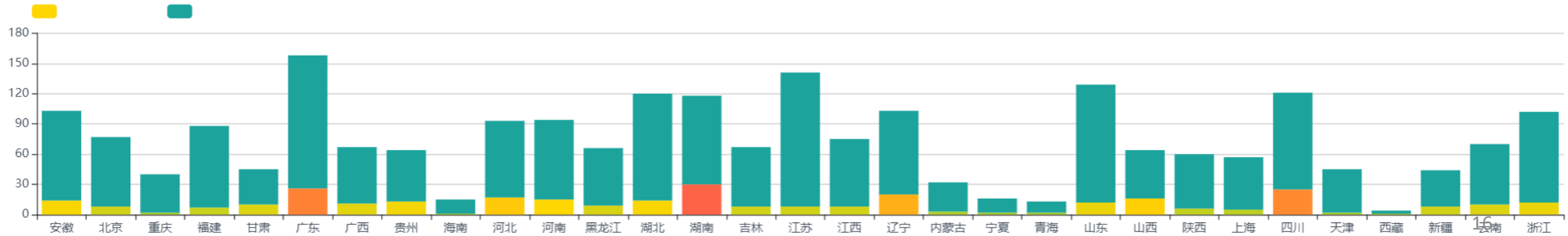
Security inspection for University & College enrollment website (since 2016)

1289 High vulnerability

4101 medium vulnerability

19607 Low vulnerability





Outline

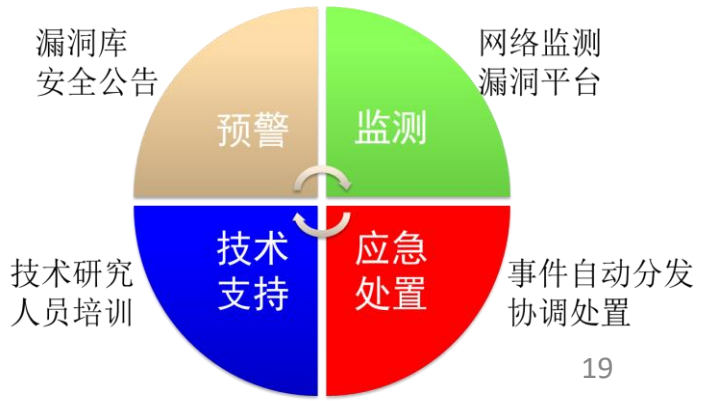
- Network security architecture
- Infrastructure security activities
- CCERT

Introduction of CCERT

- CERNET Computer Emergency Response Team
- The first CERT in China (1998)
- Provide security service and support to research and education customer networks
- CCERT national center is located in Tsinghua University, with the collaboration from other region/node CERT all over China
- *https://www.ccert.edu.cn*

Responsibility of CCERT

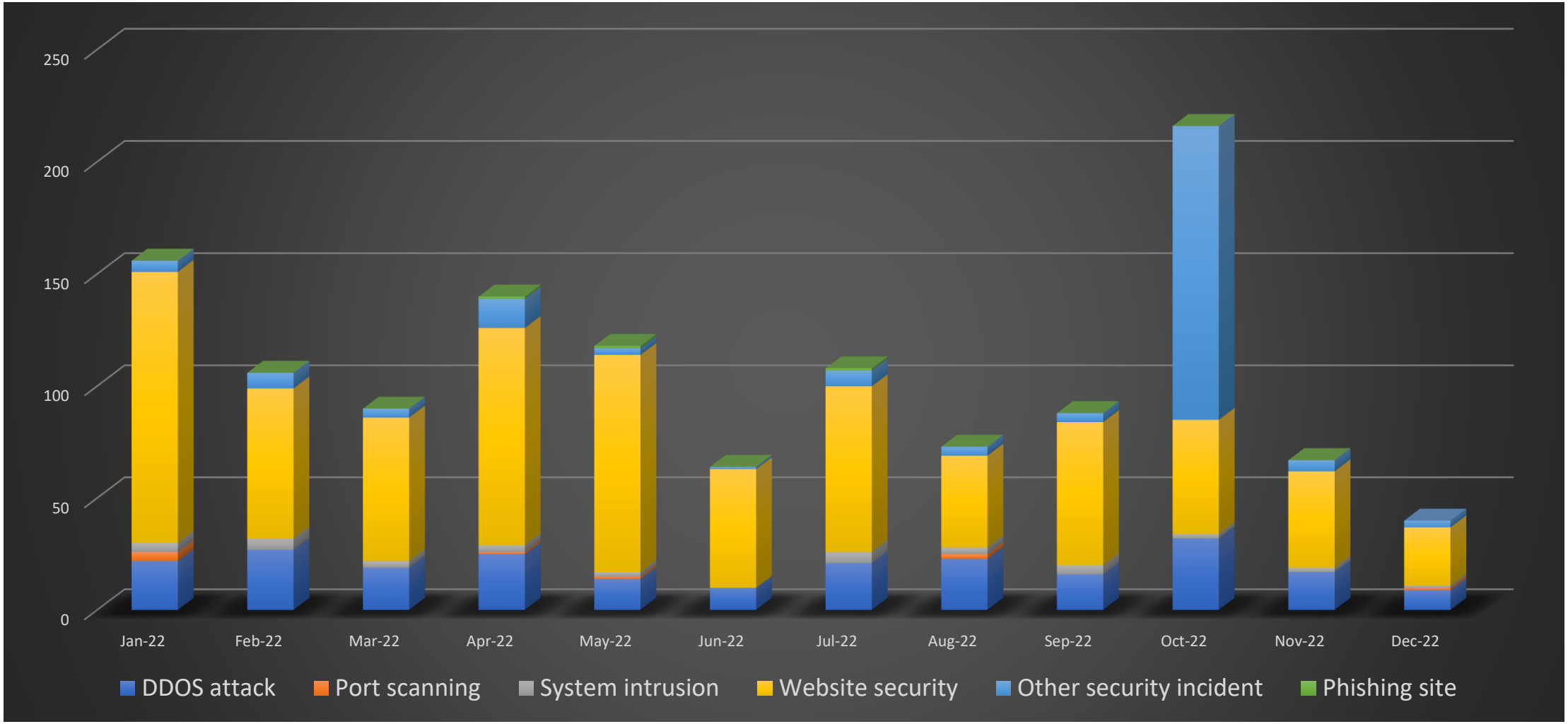
- Network security monitoring
- Security incident response
- Research on network security
- Security advisory publication
- Network security technology training



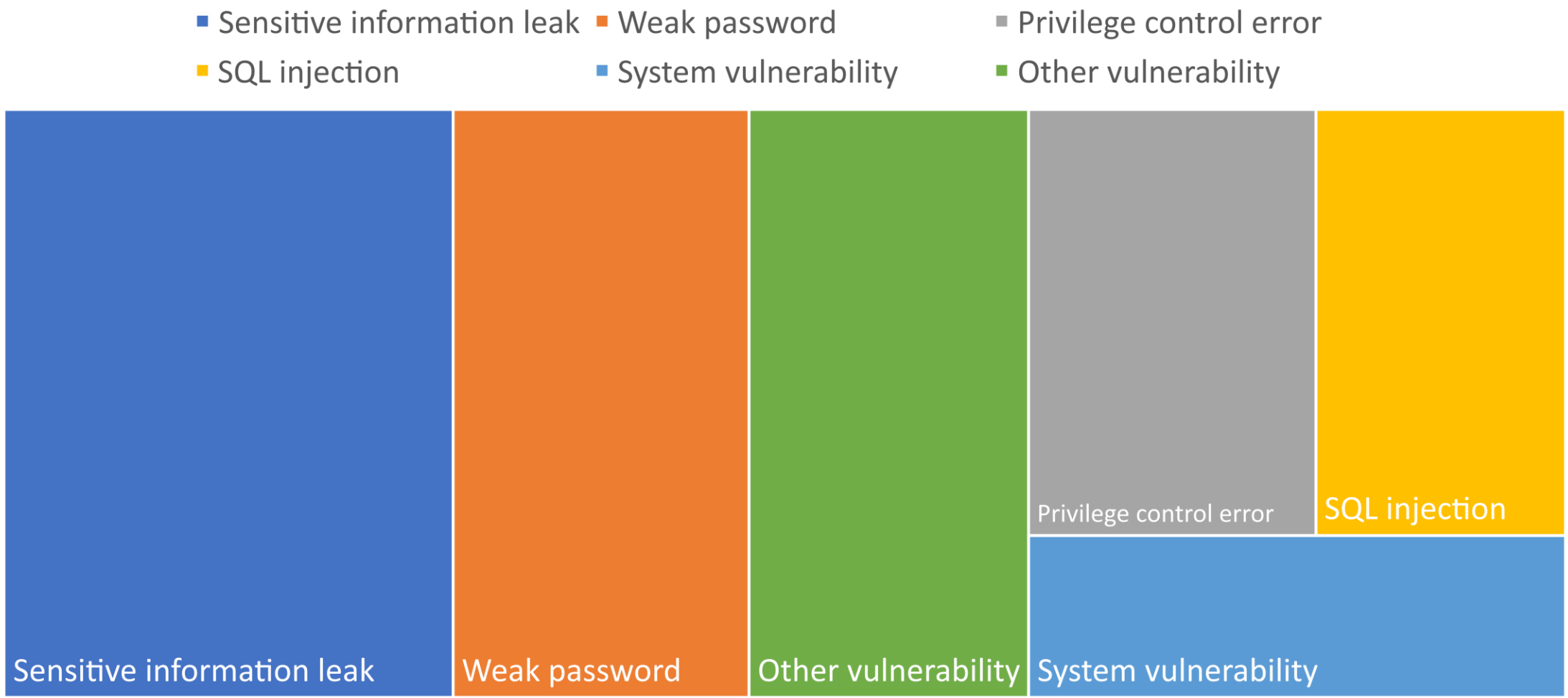
CCERT operation statistics for 2022

- Domestic network security complaint report
- Website security incident
- DDoS incident
- International network security complaint report

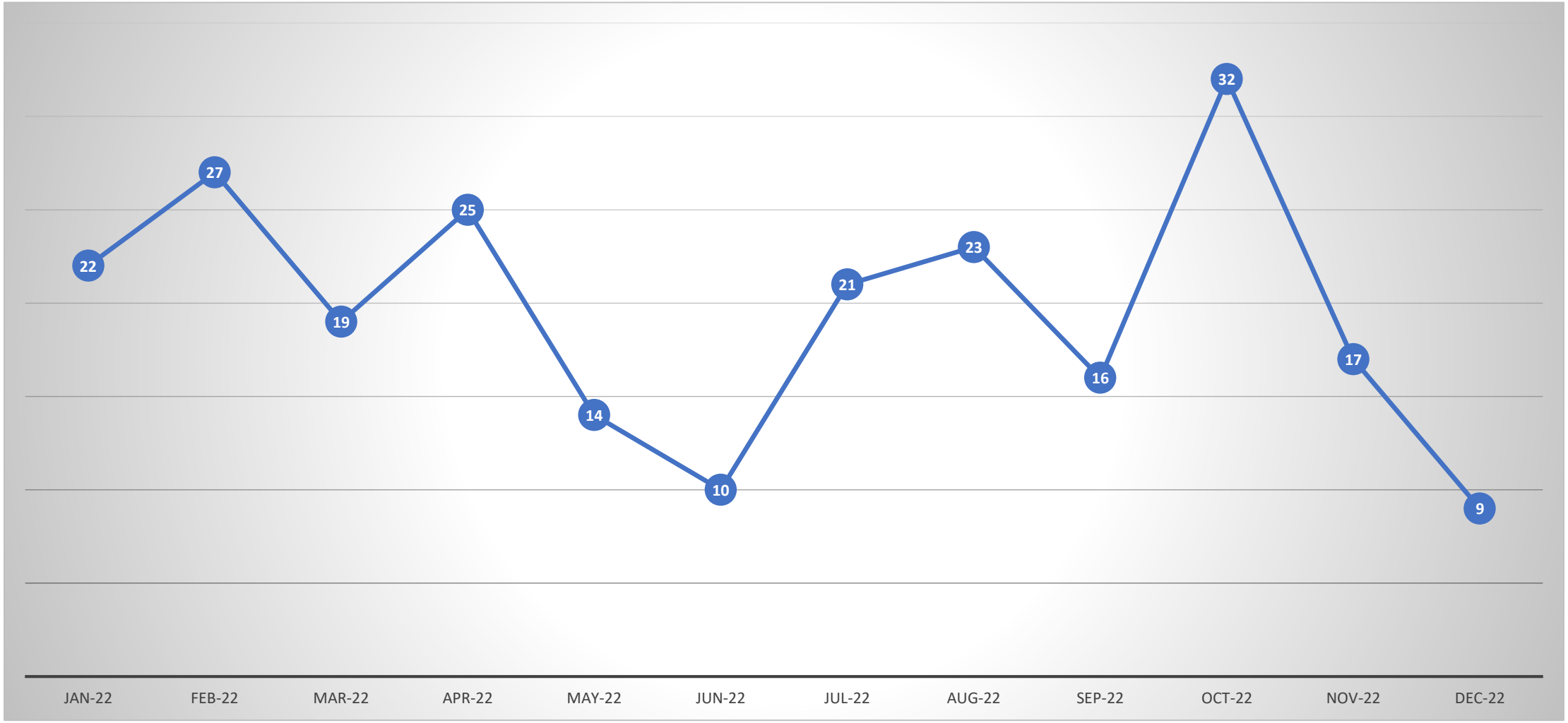
Domestic network security complaint report



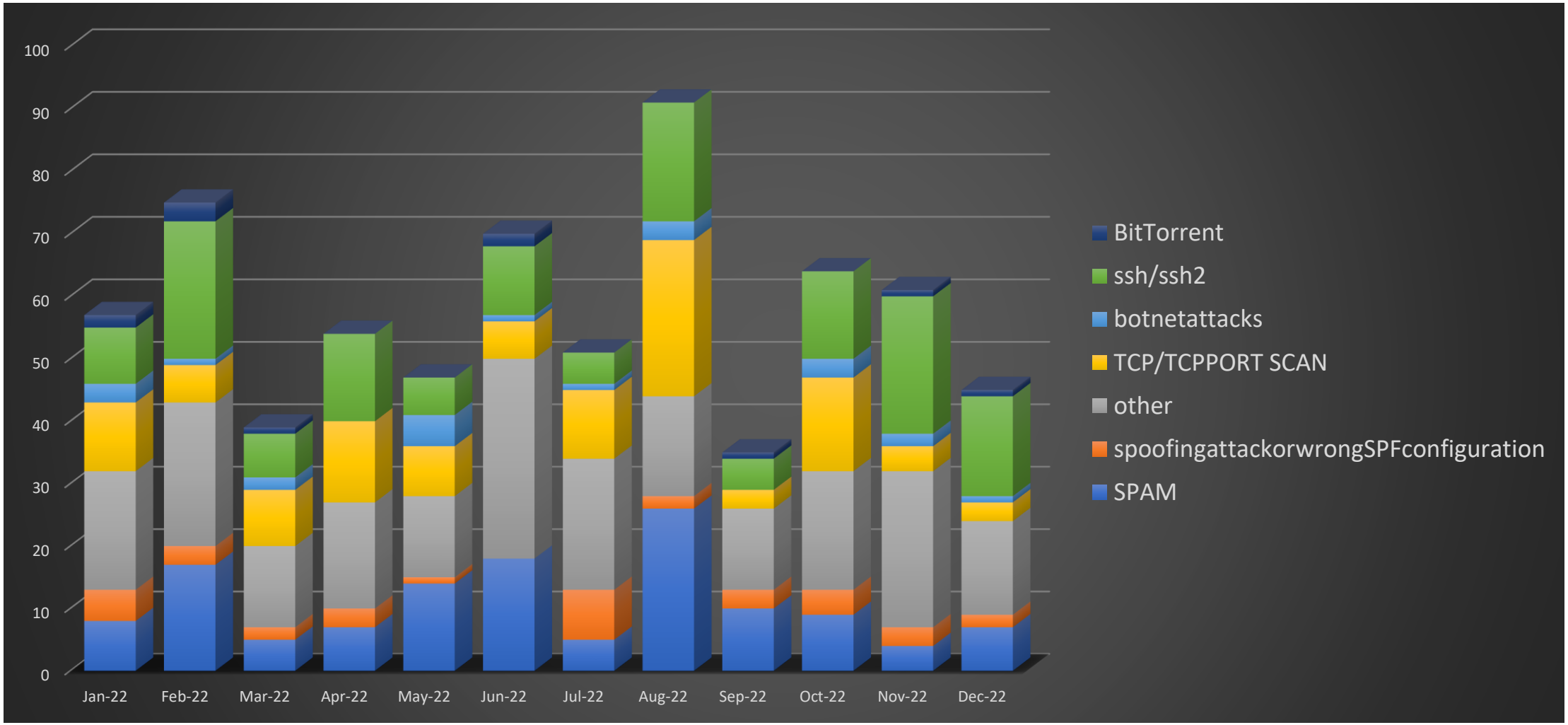
Website security incident



DDoS incident



International network security complaint report *(abuse@cernet.edu.cn)*



Thanks!