



# APCERT: 亚太地区应急合作经验

APCERT: Practice on CERT cooperation in AP area

杜跃进 博士

Yuejin Du. Ph.D

APCERT 副主席 & CNCERT/CC 副总工

2005年3月24日.CNCERT/CC'05



## 网络安全保障为什么需要合作

### Why we need cooperation for network security

- 攻击者和安全事件没有各种边界的限制，而管理者有  
for attackers & incidents, there is no borders, but we have
- 过于庞大的客户群和工作量，对服务质量的要求  
too many users too much works, need QoS
- 涉及太多的技术分支，需要产业界内的合作  
too many tech. issues, need too much resources
- 涉及到技术以外的很多领域，需要跨行业合作  
not only tech. issues are included in
- 全球化的问题，要全球解决  
Global Problem, Global Solution



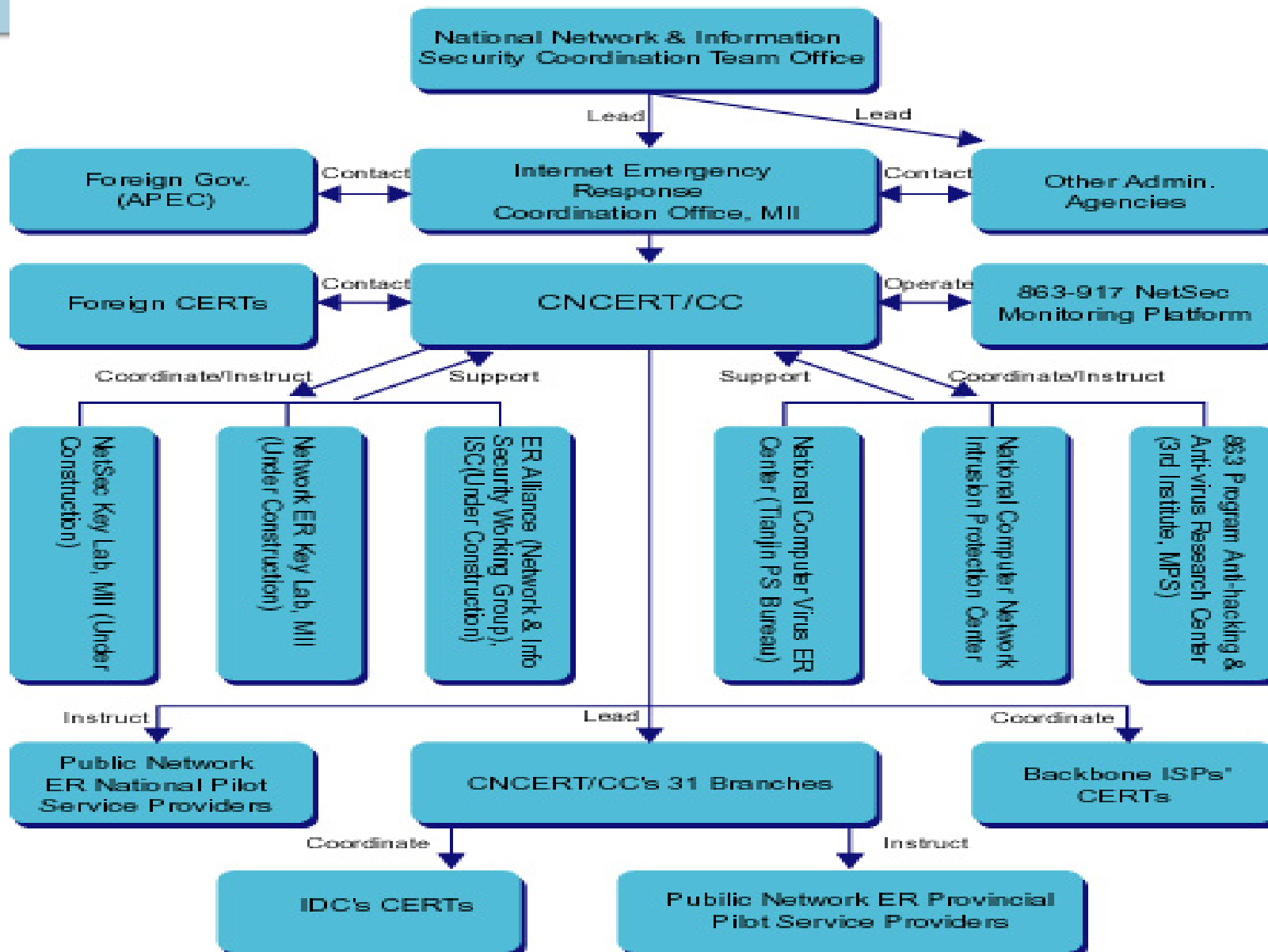
# 技术领域的合作框架

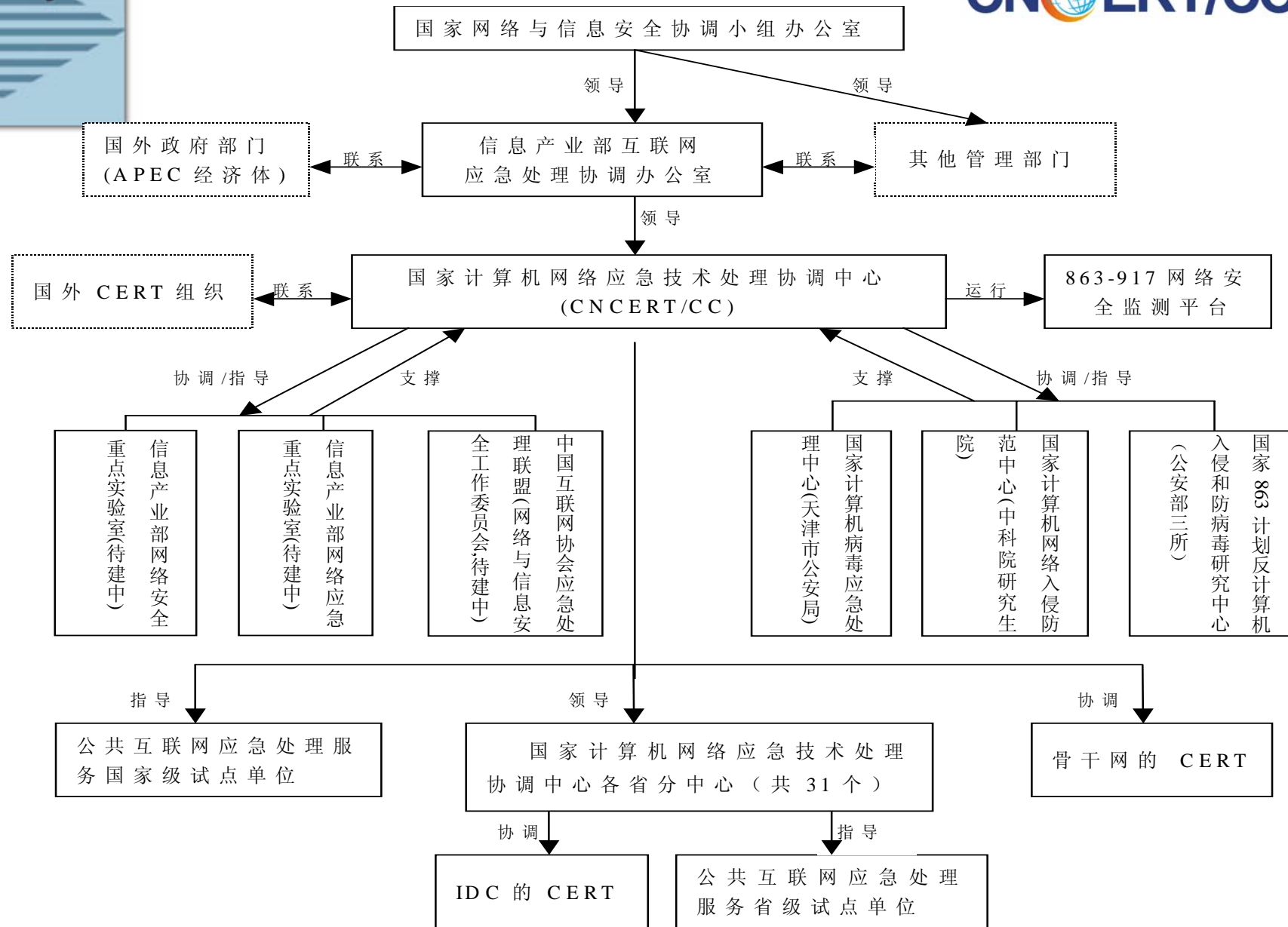
## Cooperation Scheme on Technical Side

- 2002年形成的合作体系曾经让我们很好地限制了2003年的蠕虫SQL SLAMMER  
With the scheme established in 2002, we successfully restrained SQL SLAMMER in 2003.
- 但是对新的经验教训的总结，使我们意识到需要进一步扩展和完善应急合作体系  
New incidents made us realized that the scheme was not good enough
- 2004年我国形成的国家公共互联网络应急处理体系  
In 2004, the scheme was enlarged

# NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM

C







## 多边合作框架的必要性

### cooperation scheme among multiple sides

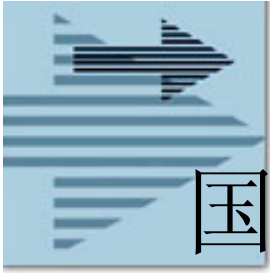
- 政府、网络供应商、应急组织/安全服务商、学术研究力量、专业化组织、产品供应商等的多边合作：

#### Cooperate among multiple sides:

- Government: laws, LEA, standard, etc. related
- ISPs: network related
- Various CSIRTs/security service providers: cover more end users
- Labs: analysis, research, development related
- Organizations with specialities: more professional support
- Industry side: patch, tools, products, upgrade, etc.

- 只有通过多领域广泛、有效的合作，才可能真正有效地应对各类安全事件

***Only by multi-parties' cooperation according to a well-planned scheme can Internet security incidents be handled quickly and effectively***



# 国际合作:国际化的问题要国际化解决

International cooperation: 'Global problem, global solution'

- 国际合作的好处  
With global cooperation, we can:
  - Get earlier warning
  - Data sharing (increase the analysis capability)
  - Tech. and info. sharing
  - Stop the attacking from other country or trace the sources of attackers
- **CNCERT/CC的实例**  
*CNCERT/CC :*
  - *got early information from JPCERT/CC and AusCERT for MSBLAST(DDoS traffic) and NACHI(abnormal traffic increasing)*
  - *confirmed the situation during each large-scale incidents with CSIRTs in Europe, America, and other places*
  - *helped other CSIRTs to handle hundreds of phishing incidents*
- 更多的国际合作组织成立  
*More and more international organizations now: FIRST, APCERT, EGC, TF-CSIRT, etc.*



# 行业以外的合作

## Cooperation among various fields including LEA

- 针对特定威胁形成的跨行业合作，例如AntiPhishing:  
金融、商业、应急组织等  
organizations for fight with particular threat, etc phishing
- 司法部门在打击违法犯罪方面的合作，例如，在内部与所有行业部门合作，在国际上开展执法部门之间的合作（例如G8网络）  
cooperation org. for anty-cybercrime, eg. G8
- 行业以确保安全生产为目标；司法部门以打击违法犯罪为目标。  
探讨应急组织和执法部门的合作模式，一直是一个重要的交流话题  
cooperate with LEA is always a hot topic



# 合作组织或体系的形成

## Cooperation organizations & schemes

- FIRST
- APCERT
- EGC/TF-CSIRT
- 泛美国家的合作框架
- 我国的公共互联网络应急处理体系
- 韩国等周边国家的类似体系



# Europe

- European Government CERT : EGC
  - Comprised of the Government CERTs from
    - UK, France, Germany, Finland, Sweden, Netherlands.
- TF-CSIRT: cooperation organization with focus on research issues



# America

- Inter-American CSIRT Watch and Warning Network,  
(2004.4 Framework)
  - Establish CSIRTs in each of the Member States;
  - Identify national points of contact in each State;
  - Establish protocols and procedures for the exchange of information;
  - Rapidly disseminate notice of such attacks throughout the region;
  - Provide rapid regional notice of general vulnerabilities in the system;
  - Provide regional warning of suspicious activities, and develop the cooperation needed for analysis and diagnosis of such activities;
  - Provide information on measures for remedying or mitigating attacks and threats;
  - Strengthen technical cooperation and training in computer security aimed at establishing national CSIRTs; etc.
- 23 countries participated, to make up national POC operate 24x7



# Asia-Pacific

- APCERT: 17个成员，来自13个经济体
  - 澳大利亚 (AusCERT)、日本(JPCERT/CC)、韩国 (KrCERT/CC)、中国 (CNCERT/CC)、马来西亚 (MyCERT)、泰国(TaiCERT)、新加坡 (SingCERT)、菲律宾(PH-CERT)、文莱 (BruCERT)、中国香港(HKCERT)、 etc



# APCERT POC Scheme

- Initially created for APCERT members.
- Used for serious and time critical incidents only. This means, each POC must give the requests made via this arrangement highest priority.
- APCERT will provide APCERT POC Arrangements to CSIRT groupings outside the AP region if certain criteria are met.
- APCERT POC Arrangements will not be exchanged with individual CSIRTs or vendor CSIRTs.
- One POC per one economy.



# APCERT与其他国际组织的合作 cooperate with other organizations

- FIRST
- EGC
- APEC
- Etc.

• *CNCERT/CC* 是作为中国大陆与外界、国内政府与业界、以及业界各方力量之间的桥梁，  
而 *APCERT* 则作为亚太区域经济体之间的合作桥梁，亚太区域和世界其它区域之间的桥梁



## 构建主动、开放、有效的网络应急体系

*Establishing Positive, Open, and Effective  
Network Emergency Response Systems*

Questions?

[www.cert.org.cn](http://www.cert.org.cn)

[dyj@cert.org.cn](mailto:dyj@cert.org.cn)



# Proposals for the cooperation in network security (newly added)

- CERT capability building
- Training & HR building
- Forum and related conferences to share experiences and discuss related problems
  - CNCERT/CC Annual Conference; APCERT conferences , etc
- POC exchange
- Information exchange issues (depends on):
  - Building up the trusted relationships
  - Strand and the implementation, e.g. IODEF and IHS
  - Secure and convenient platform for information exchange
- MOU & NDA (in the future)