Alibaba Group
阿里巴巴集团

Challenges of Cybersecurity in the new era of Internet+

---Differences and new challenges of cybersecurity issues from the angle of Alibaba)

Yuejin Du Ph.D
Alibaba Group

SWISS Cyber Strom 2015.10.21

About me:

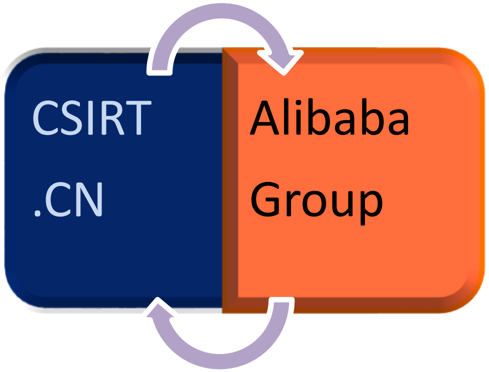
CSIRT community

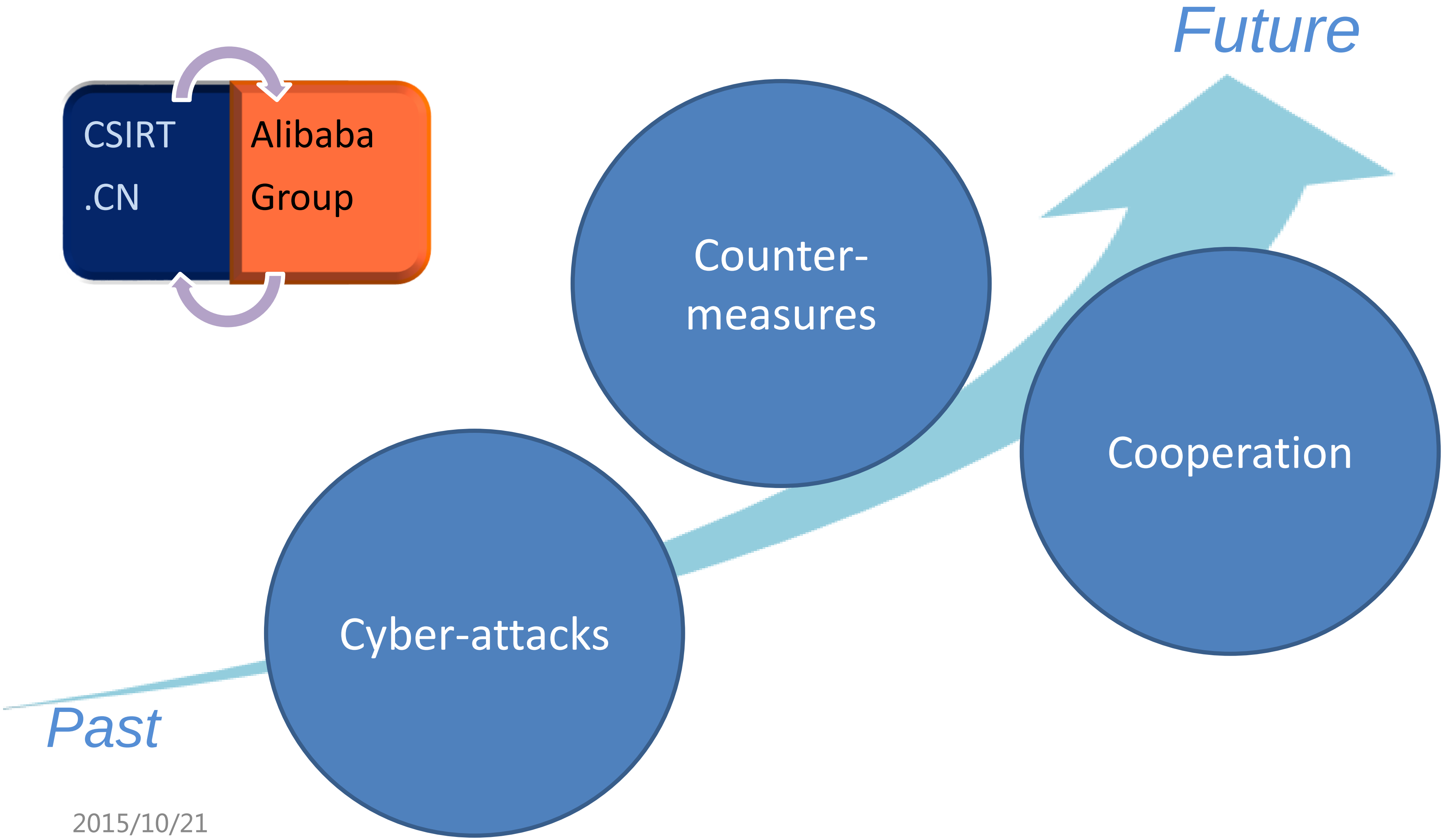
- Incident handling
- Capacity building
- Domestic cooperation system building
- International cooperation / coordination

Alibaba Security

- Data security
- Threat intelligence integration
- Standard
- Cooperation & Ecosystem building

Topics might be interested





2015/10/21

Cyber Attacks follows Benefit

China is a good target:

- Huge amount of users and online hosts
- Very active on Internet economy
- Wealthy
- Weak awareness and protection

» Websites in China defaced /intruded

» 2005: >13K

» 2007: >61K

» 2008: >54K

» 2011:>37K

» 2013:>24K (backdoors >76K)

» IPs in China controlled by botnets or trojans

» 2007: >4.5million

» 2010: >5 million

» 2011: 8.9million

» 2012: 14 million

» 2013: >11.3 million

According to CNCERT/CC

- Personal Information leakage
- Online ID theft
- Mobile Security / malicious APP
- Critical information infrastructure
- APT
- ……

2000w开房数据下载在线查询

原 | 浏览：8435 | 更新：2014-01-30 09:14

>30K phishing websites toward Chinese companies
FTC: Online ID Theft caused US 1.52 billion $ in 2011

Severe DNS attacks

>700K mobile malwares
Many app-stores have problems

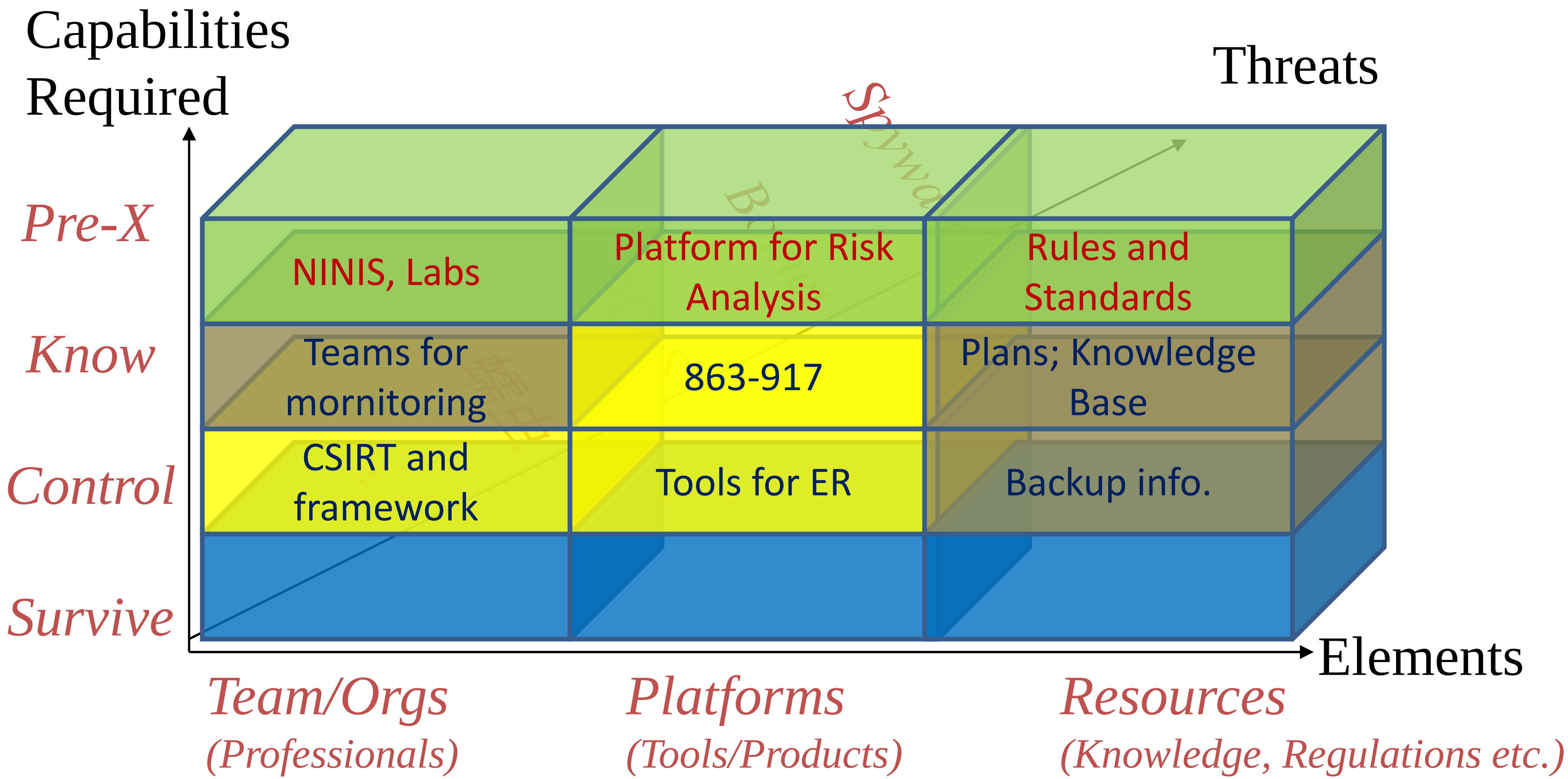
According to CNCERT/CC

Alibaba is a good target

- Largest e-commerce platform and still growing very fast
- More than 400 million registered users
- More than 10 million people living in this ecosystem
- Financial giant: Alipay
- Infrastructure: AliCloud
- Valuable data
- **Strong Security Team** (*but consumers could be the weakness)*

Countermeasures

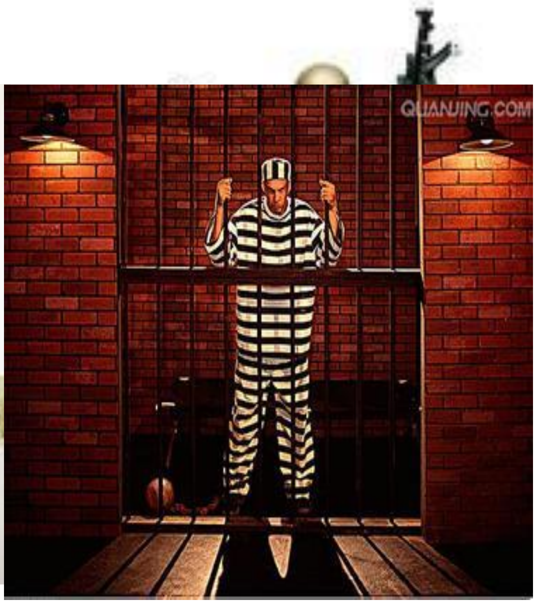
- Capacity model



	Team/Orgs (Professionals)	Platforms (Tools/Products)	Resources (Knowledge, Regulations etc.)
Pre-X	NINIS, Labs	Platform for Risk Analysis	Rules and Standards
Know	Teams for mornitoring	863-917	Plans; Knowledge Base
Control	CSIRT and framework	Tools for ER	Backup info.
Survive			

Countermeasures

- 3 Stages: you can never make it by yourself

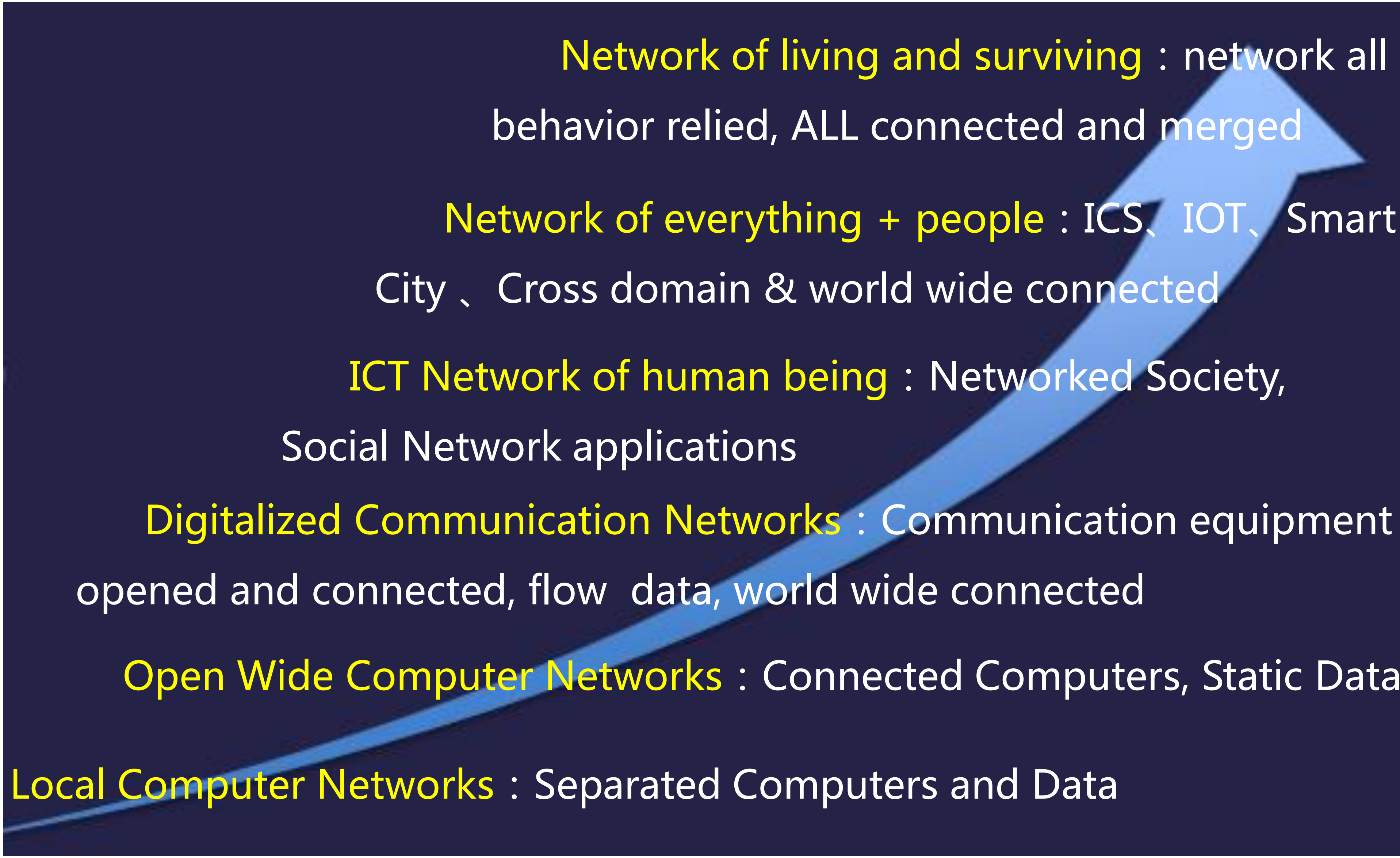


Countermeasures

New angle to look at cybersecurity from Alibaba:

What's different from such a company?
What's new in our current era?
What's the challenges in the future?

Security: From Computer to Cyberspace



Network of living and surviving：network all behavior relied, ALL connected and merged

Network of everything + people：ICS、IOT、Smart City 、Cross domain & world wide connected

ICT Network of human being：Networked Society, Social Network applications

Digitalized Communication Networks：Communication equipment opened and connected, flow data, world wide connected

Open Wide Computer Networks：Connected Computers, Static Data

Local Computer Networks：Separated Computers and Data

Key features that make difference

inter-connection, smart, mergence

interconnection：online into one network all time, all devices, no gap

Smart： “Smart means changes”

Mergence：different domains interrelated

Challenges

- Boundaries of space, time, and management in real world vanished
- Different hardware, software, protocols, platforms, etc.
- Very complicate relations
- Threat is spreading into EVERY domain, but they are far from ready

Normal news in the coming few years:

Been hacked

Find new vulnerability

Because :

- Problems generated faster than founded, not to speak of been fixed
- The motivation, capacity, and numbers of our adversaries will keep rising

New features we have to live with

Dynamic : Data, Application, Asset, Boundaries, Transections, Adversaries

Big : Huge amount of everything to deal with

Complex : Long chain, wide front line, many weak points, too much out of control

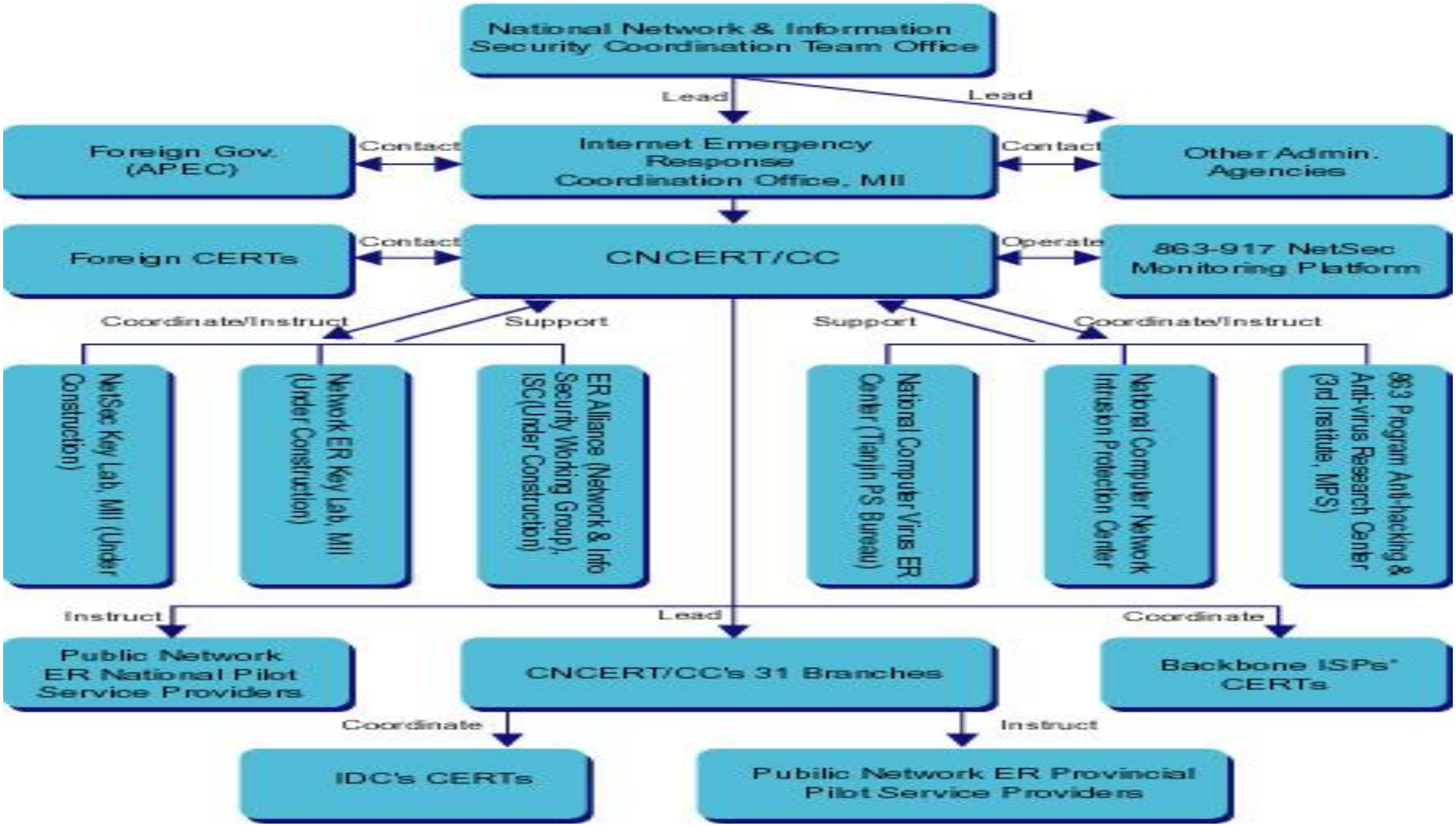
Business : Security becomes blood inside business, high requirement on performance, stability, and easy using

One of the key problems today

Different languages: what are you talking about?

Cooperation

NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM



National Network & Information Security Coordination Team Office

Foreign Gov. (APEC)

Internet Emergency Response Coordination Office, MII

Other Admin. Agencies

Foreign CERTs

CNCERT/CC

863-917 NetSec Monitoring Platform

NetSec Key Lab, MII (Under Construction)

Network ER Key Lab, MII (Under Construction)

ER Alliance (Network & Info Security Working Group), ISC(Under Construction)

National Computer Virus ER Center (Tianjin PS Bureau)

National Computer Network Intrusion Protection Center

863 Program Anti-hacking & Anti-virus Research Center (3rd Institute, MPS)

Public Network ER National Pilot Service Providers

CNCERT/CC's 31 Branches

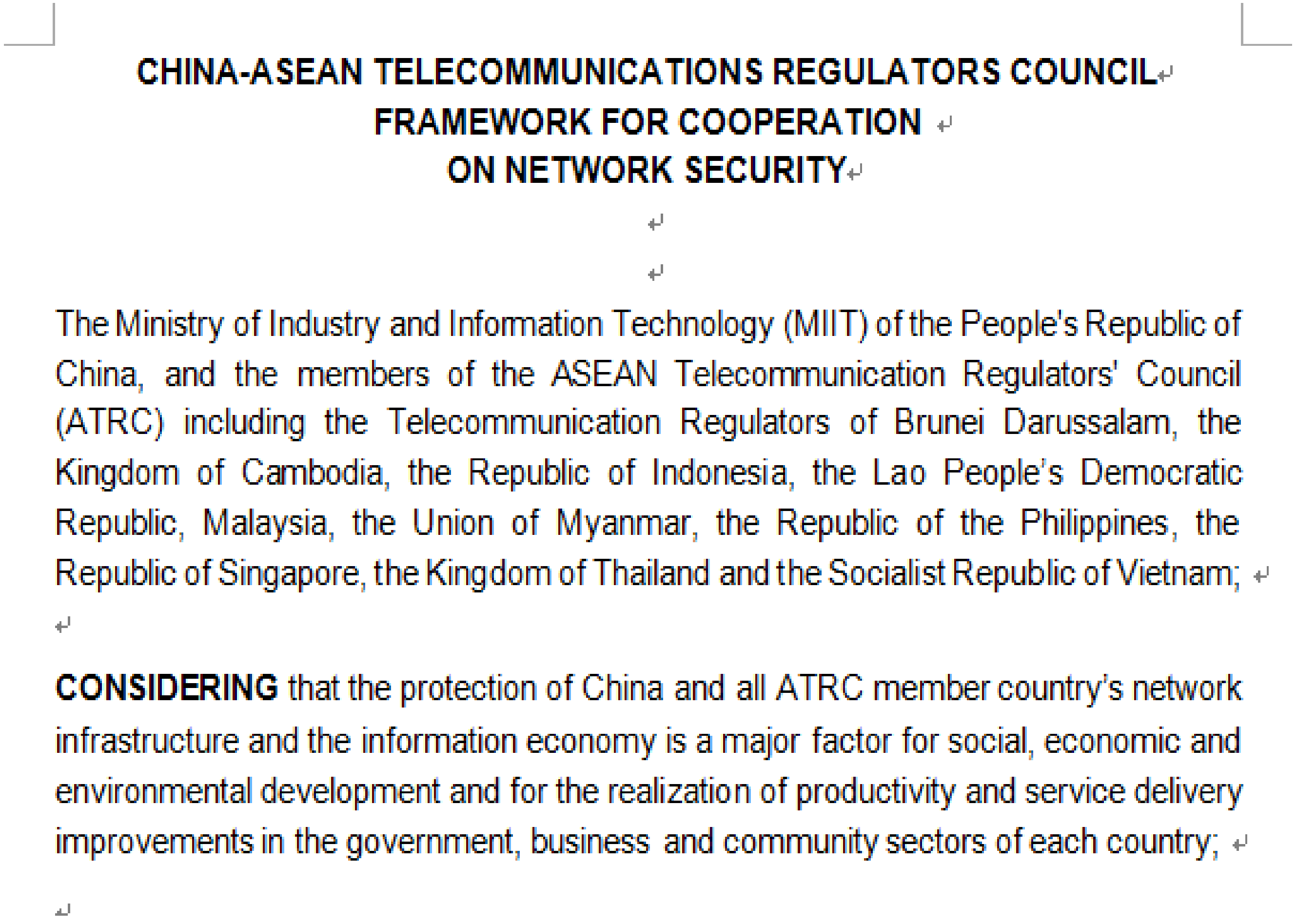
Backbone ISPs' CERTs

IDC's CERTs

Public Network ER Provincial Pilot Service Providers

Global Problem, Global Solution

- CNCERT/CC
- FIRST
- APCERT
- APEC-TEL
- CJK
- China-ASEAN Framework
- Capacity building



CHINA-ASEAN TELECOMMUNICATIONS REGULATORS COUNCIL
FRAMEWORK FOR COOPERATION
ON NETWORK SECURITY

The Ministry of Industry and Information Technology (MIIT) of the People's Republic of China, and the members of the ASEAN Telecommunication Regulators' Council (ATRC) including the Telecommunication Regulators of Brunei Darussalam, the Kingdom of Cambodia, the Republic of Indonesia, the Lao People's Democratic Republic, Malaysia, the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Kingdom of Thailand and the Socialist Republic of Vietnam;

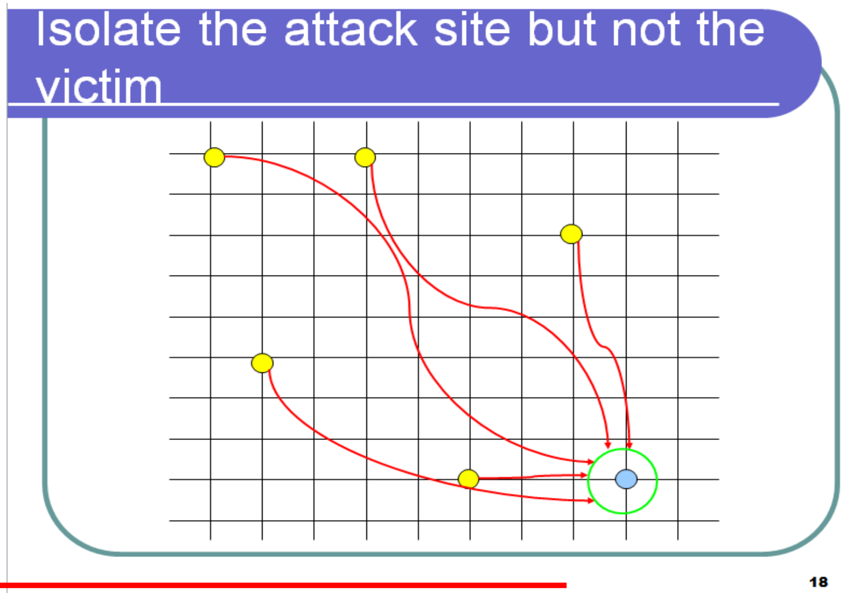
CONSIDERING that the protection of China and all ATRC member country's network infrastructure and the information economy is a major factor for social, economic and environmental development and for the realization of productivity and service delivery improvements in the government, business and community sectors of each country;

We tried

Anti-cybercrime depend upon the community working together

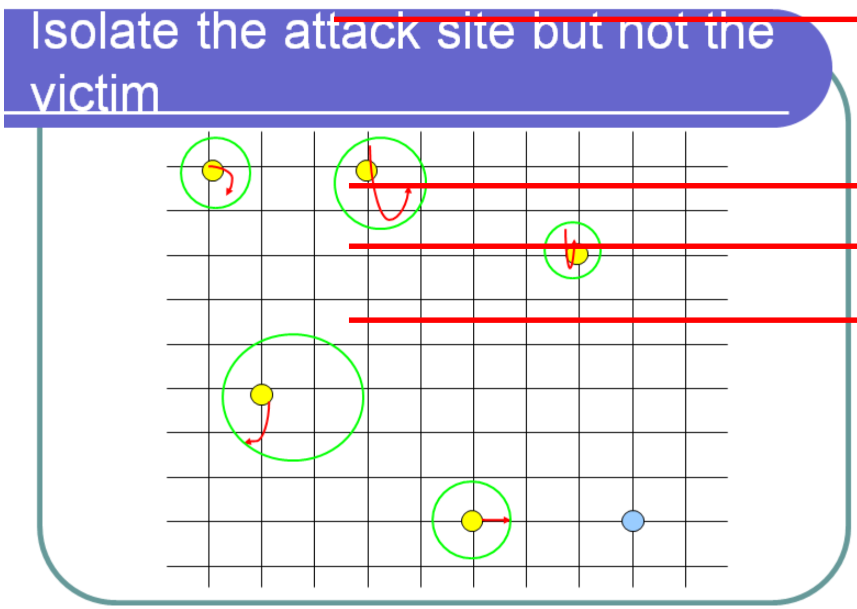
Yuejin Du
Internet Emergency Response Coordination Office, MII, China
Bangkok, July. 23, 2003

1

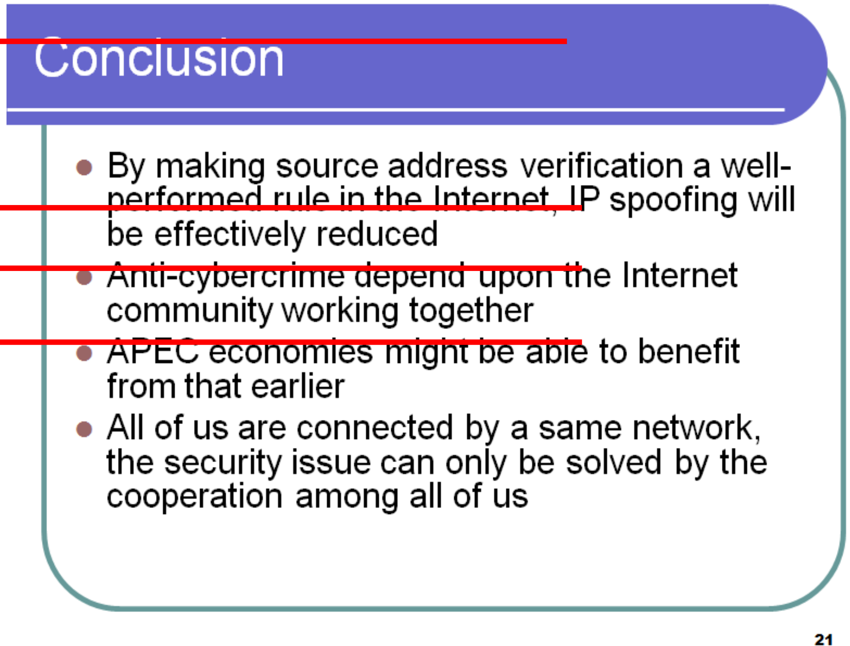


Isolate the attack site but not the victim

18



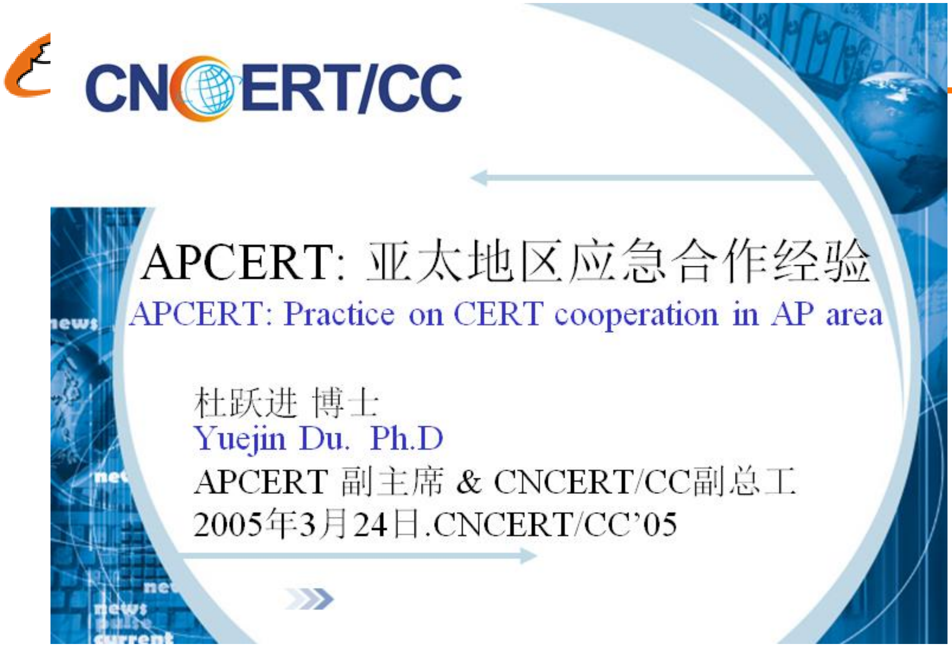
Isolate the attack site but not the victim



Conclusion

- By making source address verification a well-performed rule in the Internet, IP spoofing will be effectively reduced
- Anti-cybercrime depend upon the Internet community working together
- APEC economies might be able to benefit from that earlier
- All of us are connected by a same network, the security issue can only be solved by the cooperation among all of us

21

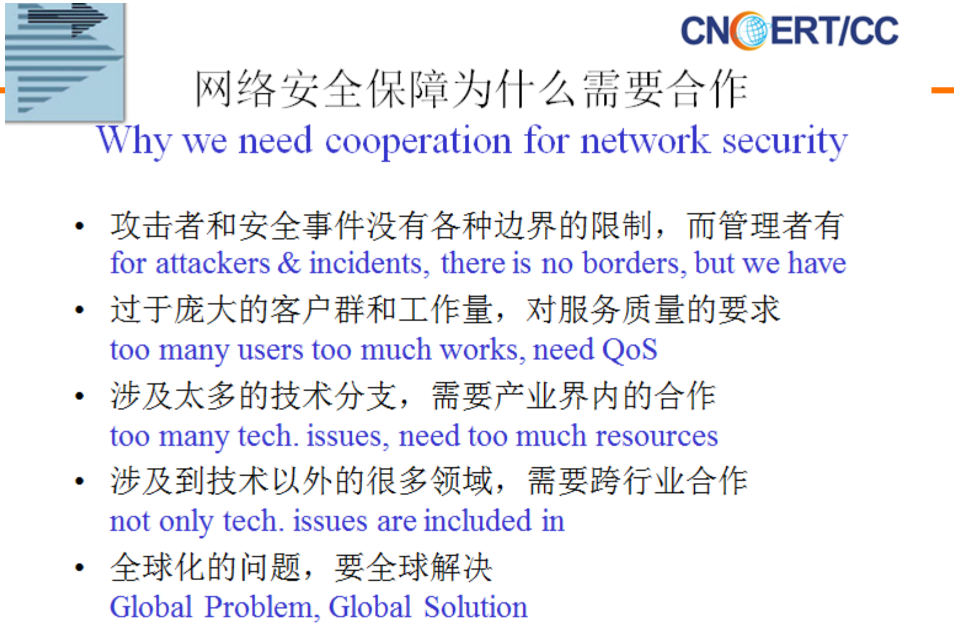


CNCERT/CC

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

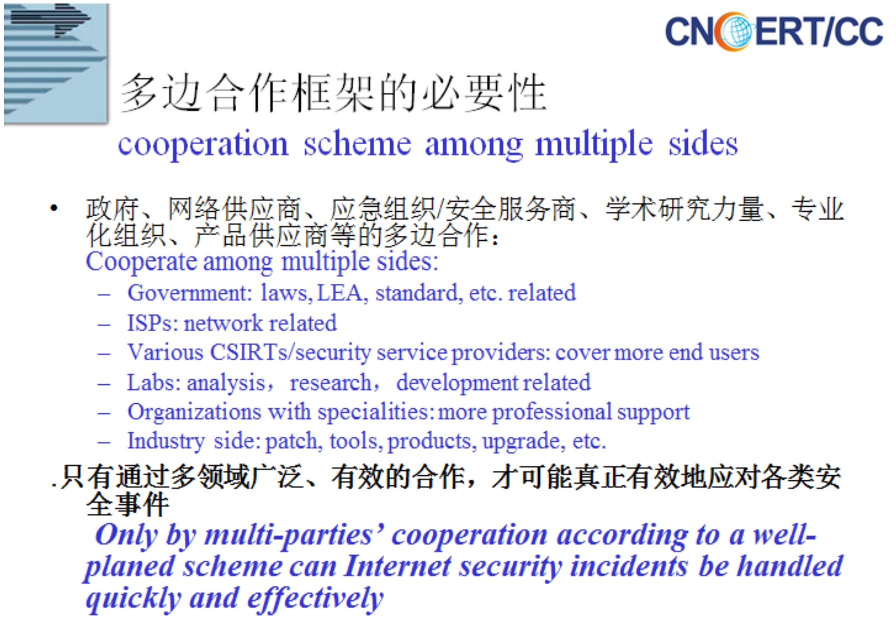


CNCERT/CC

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



CNCERT/CC

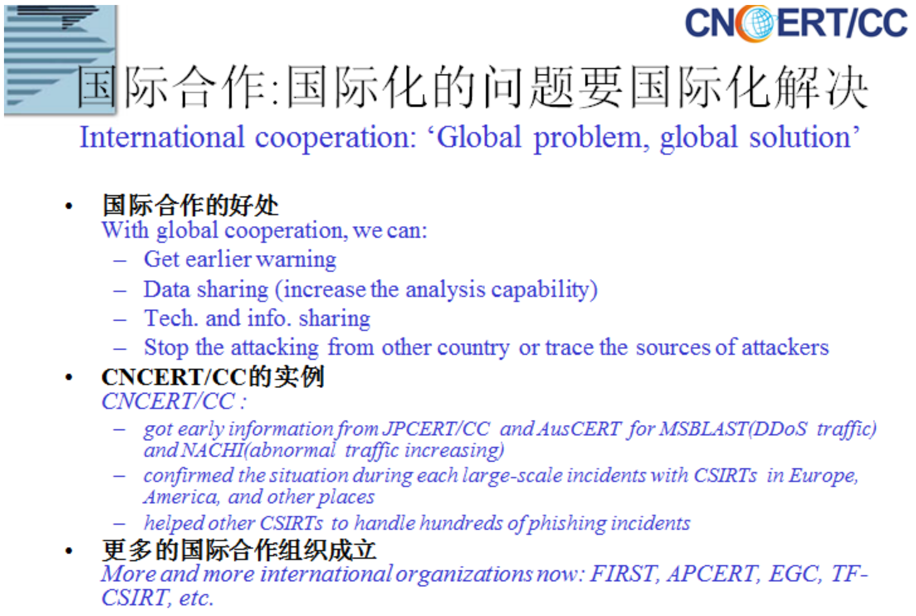
多边合作框架的必要性

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-planed scheme can Internet security incidents be handled quickly and effectively



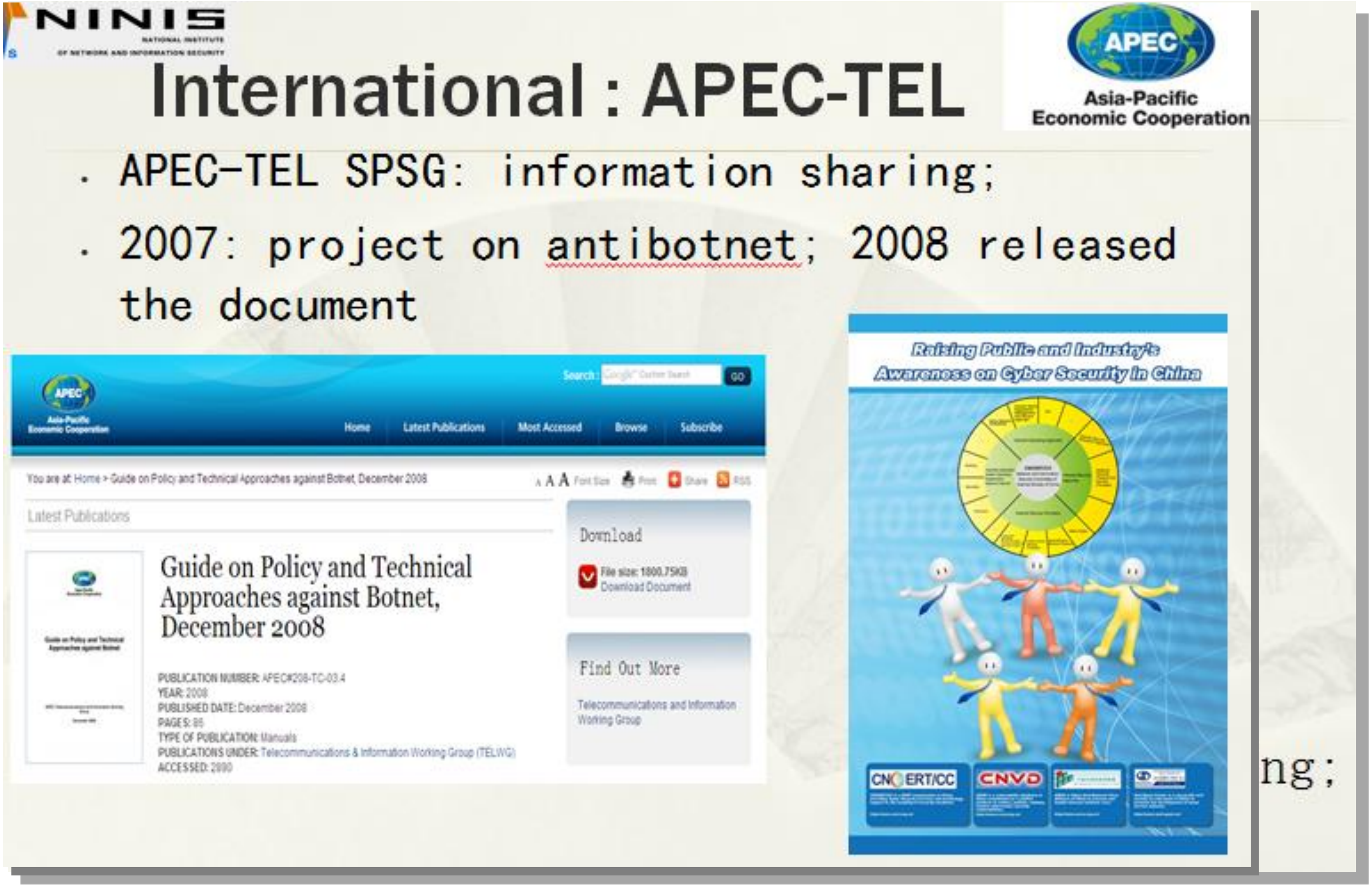
CNCERT/CC

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.

We had good time before



NINIS
NATIONAL INSTITUTE OF NETWORK AND INFORMATION SECURITY
APEC
Asia-Pacific Economic Cooperation

International : APEC-TEL

- APEC-TEL SPSG: information sharing;
- 2007: project on antibotnet; 2008 released the document

APEC
Asia-Pacific Economic Cooperation
Search:
GO
Home
Latest Publications
Most Accessed
Browse
Subscribe
A A A Font Size
Print
Share
RSS

You are at: Home > Guide on Policy and Technical Approaches against Botnet, December 2008

Latest Publications

Guide on Policy and Technical Approaches against Botnet, December 2008

PUBLICATION NUMBER: APEC#208-TC-03.4
YEAR: 2008
PUBLISHED DATE: December 2008
PAGES: 86
TYPE OF PUBLICATION: Manuals
PUBLICATIONS UNDER: Telecommunications & Information Working Group (TELWG)
ACCESSED: 2890

Download

File size: 1800.75KB
Download Document

Find Out More

Telecommunications and Information Working Group

Raising Public and Industry's Awareness on Cyber Security in China

ng;

Mutual Benefit

- Besides the efforts we’ ve done to help other parts of the world, we also learnt a lot and got many help from International cooperation
  - Trends of new threats
  - Information of incidents
  - Handling of incidents
  - Trust relationship building
  - Etc.

Alibaba still believes

- And we are going to try our best to
  - Protect the benefit of the users, which would reach to 2 billion in the whole world
  - Protect their money and their data
  - Build a secure and trust-worthy global e-commerce infrastructure, make it the most valuable platform for all users
- Thus
  - We would like to share
  - We would like to cooperation

Conclusion

The Internet is no longer just a platform of ICT

Social

Entertainment

Shopping

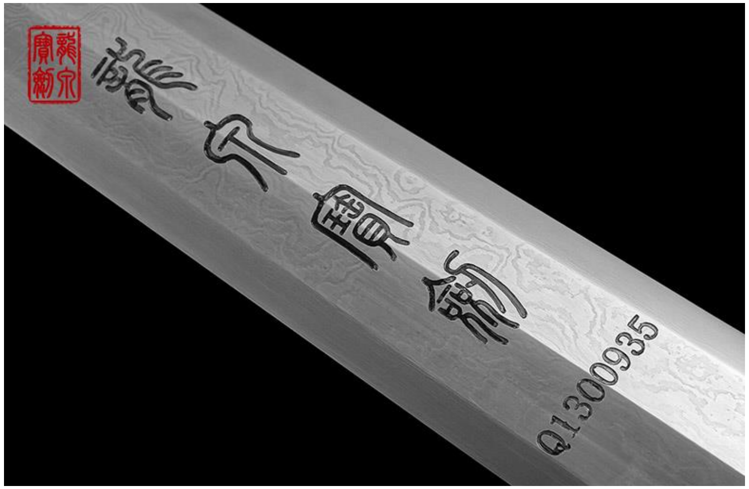
Education

Healthcare

	Social	Entertainment	Shopping	Education	Healthcare
PAST	Boring life Office / Home	Wired TV Go to cinema	Shopping outside Short distance	Go to school Buy books	Prescription Go to hospital
↓	Online chat Online video	Online movies Online games	Stay at home Online shopping	Online courses Online education	E-prescription Consolidated mgmt
NOW	Mobile chat Rich communications	Mobile movies Mobile games	Easy shopping Mobile shopping	Mobile learning Any time	Mobile health Remote medical

Conclusion

Cyber Security is no longer the old concept



Conclusion

- The KEY is to adapt the new cyber-world better than the bad guys
- The KEY is to build up trust and work together again

Thank You

yuejin.dyj@alibaba-inc.com

阿里指数 交易直播厅 日志分析 流计算 即时计算 生意参谋 One Data Open API 营销高手 企业361

Thank U

数据安全

Alibaba Group
阿里巴巴集团