


Capacity Building on Cybersecurity

Yuejin Du Ph.D

Director of NINIS
Deputy CTO of CNCERT/CC

2013.9.11 Beijing



Content

- Current Situation & Trend
- Capacity Model & Practice
- Future & Proposal

国家网络信息安全技术研究所



Cybersecurity : better or worse?

- * *It's BETTER!*
 - * More governments and people are talking it
 - * More strategies, laws and investment
 - * New technology is applying
 - * Security industry is growing
 - * Hacking is not as easy as before
 - *

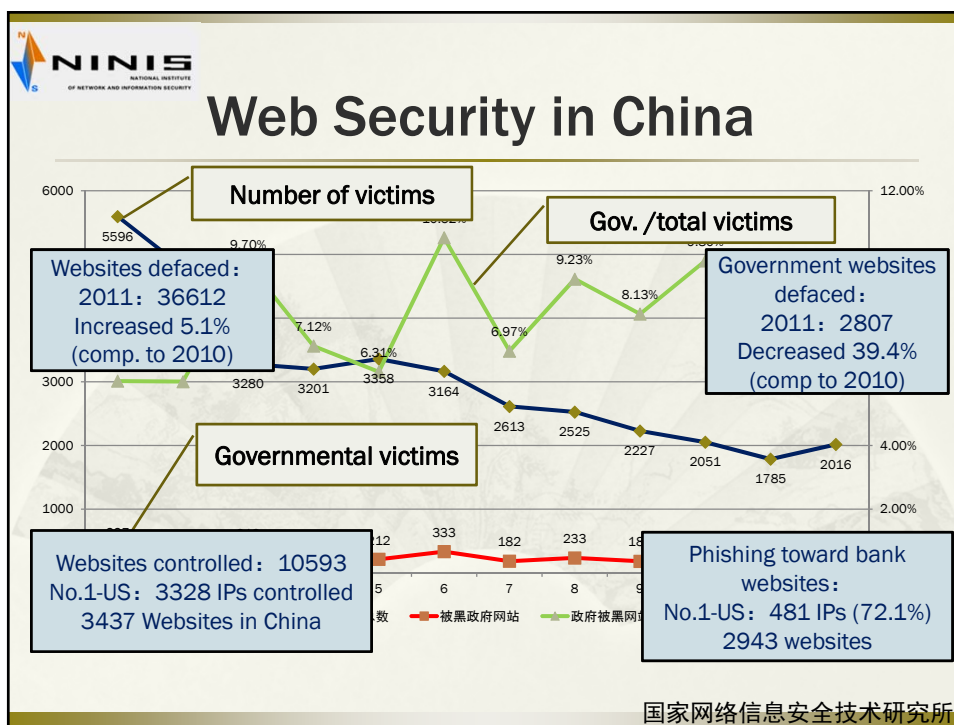
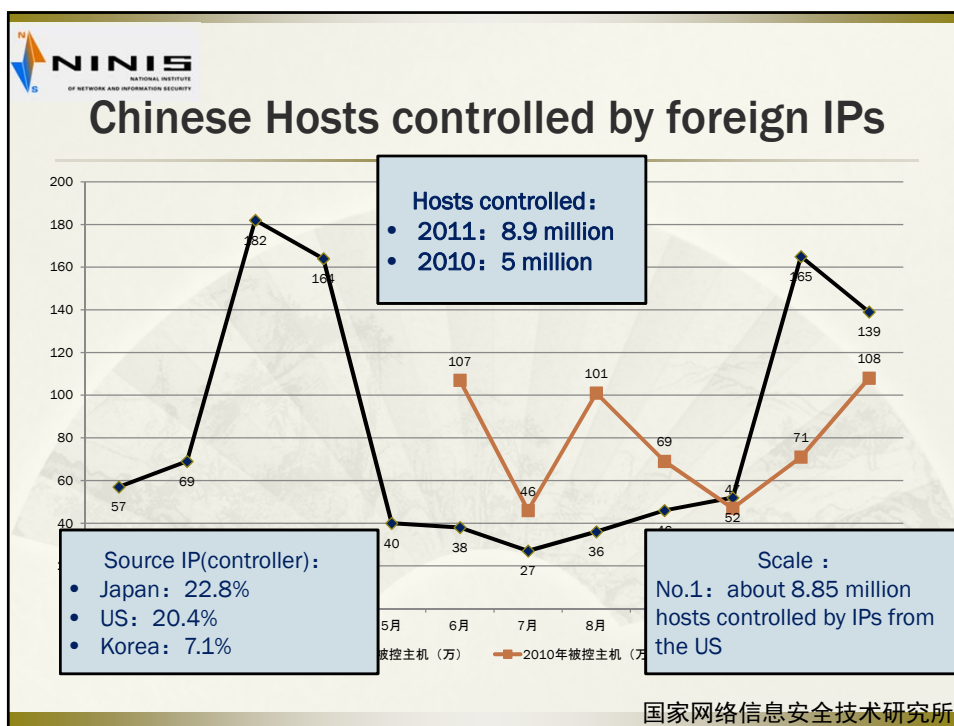
国家网络信息安全技术研究所




Cybersecurity : better or worse?

- * *It's WORSE!*
 - * More governments and people are talking it
 - * More strategies, laws and investment
 - * New technology is applying
 - * Security industry is growing
 - * Hacking is not as easy as before?
 - * Growth on the number of users
 - * Informationalization!

国家网络信息安全技术研究所






Other statistics of China

- * Mobile Security
 - * New malware: 6249, increased 2 times with 2010
 - * About 7.12 million to several billions of smart phone affected mobile malware
- * Phishing incidents reported to CNCERT/CC
 - * 2011: 5459
 - * 2010: 1566
- * New vulnerabilities collected in CNVD
 - * 2011: 5547, High risk 2164
 - * 2010: 3447, High risk 649

国家网络信息安全技术研究所



Several Typical Incidents

- * 2011: Information Leakage/CSDN
 - * Huge amount of personal information stolen and spread on the Internet
 - * *Application Security*
- * 2010: Web “defacement”/Baidu
 - * Billions of Internet users affected
 - * *Domain Name Security (Data)*
- * 2009: DNS broke down/DNS-POD & Baofeng
 - * More than half of our Internet broke down
 - * *Critical Information Industry Security*

国家网络信息安全技术研究所



Take this issue more serious

- * All those are just something we CAN see
- * Potential damage is different
- * We do not know the 'enemy', we do not know ourselves either!
- * We have no idea about the real RISK!
- * Global problem, need global solution, but we are losing the most important thing: TRUST

国家网络信息安全技术研究所



Trend of Cybersecurity

- * Tech:
 - * ICS
 - * Mobile security
 - * Big Data and Cloud
 - * Financial
 - * Weaponized malware and attack
- * Non-tech:
 - * More confliction than cooperation
 - * Less trust and industrial cooperation


国家网络信息安全技术研究所



What we need most now

- * Strengthen our own capacity
- * +
- * Build larger cooperation framework
- * +
- * Help each other
- * +
- * Try to rebuild trust

国家网络信息安全技术研究所



Content

- Current Situation & Trend
- Capacity Model & Practice
- Future & Proposal

国家网络信息安全技术研究所



Capabilities Needed

- * Capability of 'yu' (预): take precautions
 - * Prevention, Early warning, evaluation etc. Before real incident happen
- * Capability of 'zhi' (知): knowing what's happening
 - * monitoring
- * Capability of 'kong' (控): controllability
 - * Incidents or emergency response / crisis management
- * Capability of 'sheng' (生): recover and survive
 - * Recover from incidents, survivability of the core function

国家网络信息安全技术研究所



Elements Needed to Build the Capabilities

- * Infrastructure (Tools or platforms)
 - * Products, tools/devices
 - * *"You cannot make bricks without straw" (If you want to do the job well, you must sharpen your tools) 工欲善其事，必先利其器, Confucius, 551BC -479 BC*
- * Teams
 - * Professional security teams & cooperation framework
- * Resources
 - * Knowledge and database on vulnerabilities, attacking behaviors, information of infrastructure and important systems you need to protect, methodology, procedure, regulation and laws, etc.
 - * *"No flour, No Bread" (without hands you can not make fists) 巧妇难为无米之炊*

国家网络信息安全技术研究所

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

The Third Dimension

- * *“Not only know yourself, but also know your enemy, that’s the rule of win”– 知己知彼，百战不殆，The Art of War*
- * Threat is the third dimension:
Study and learn from new threats constantly:
 - * Purpose: check out if the capabilities are able to handle the new threats or not, escalate your capabilities (through the elements) if necessary.

国家网络信息安全技术研究所

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

Capacity Model of Cybersecurity

Required Capabilities (y)

Pre- X

Knowing

Controlling

Surviving

Threats (z)

Spyware

Botnet

DDoS

蠕虫

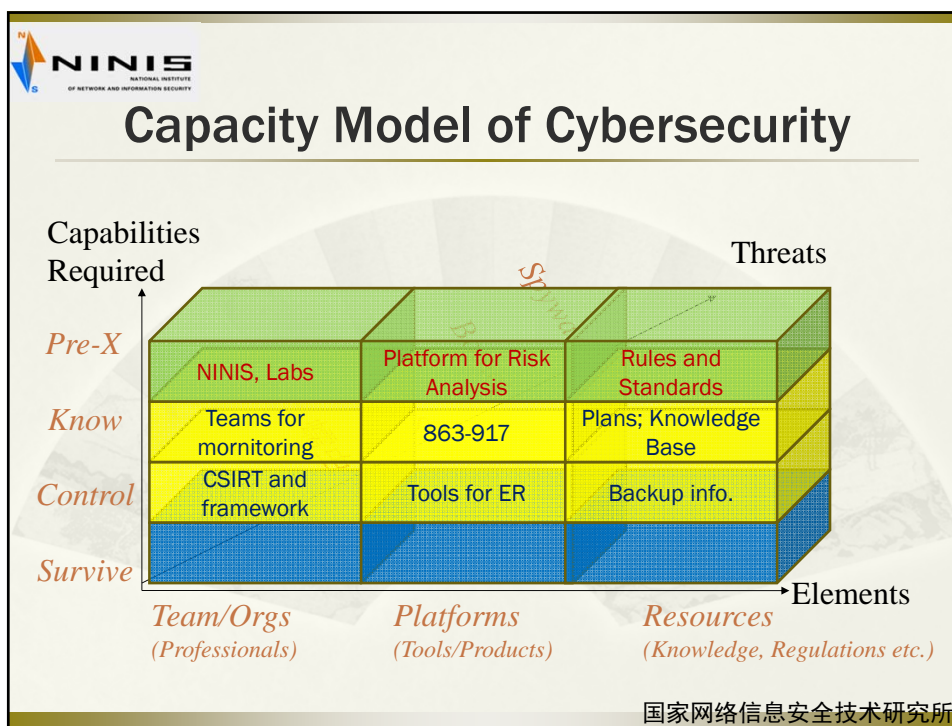
elements (x)

Teams/Orgs (professional)

Platforms (products)

Resources

国家网络信息安全技术研究所

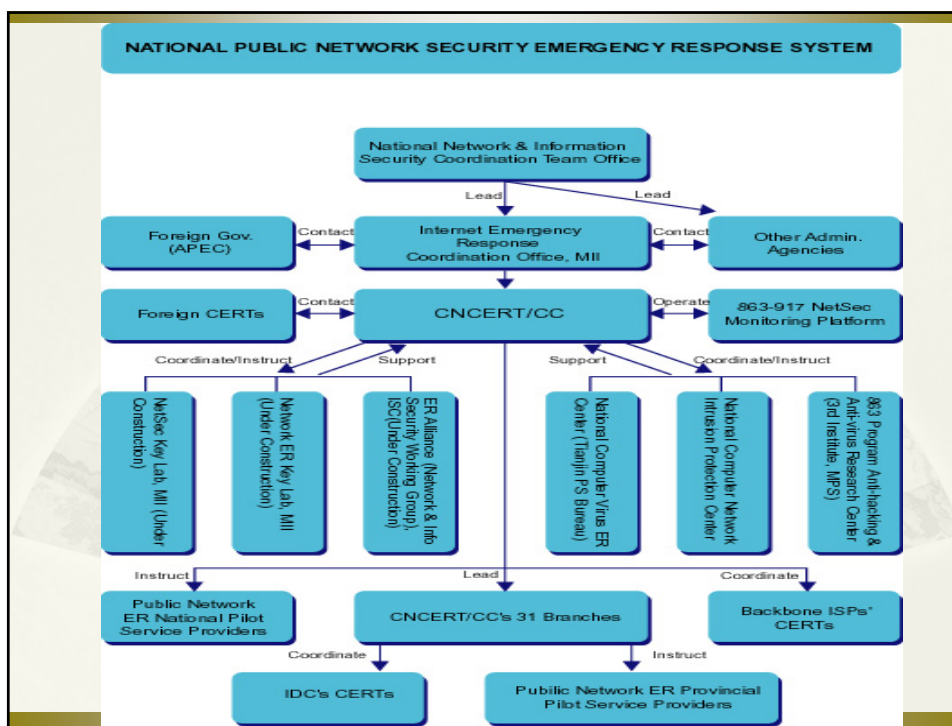


NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

CNCERT/CC

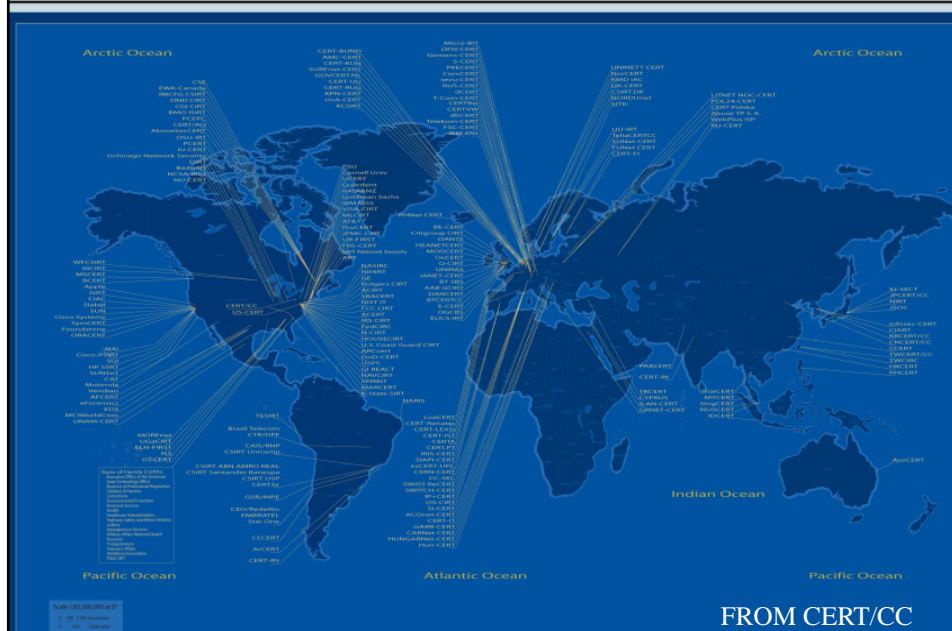
- * Established in 2000
- * became a full member of FIRST in 2002
- * At APSIRC2002, initiated APCERT (Asia Pacific Computer Emergency Response Team) with AusCERT, JPCERT/CC.
- * At APSIRC2003, was nominated and elected as the Steering Committee member of APCERT
- * In 2004, built up 31 branches across the country.

国家网络信息安全技术研究所



Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



Anti-cybercrime depend upon the community working together

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

Isolate the attack site but not the victim

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

国家网络信息安全技术研究所

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 specialties: 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

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 NACH (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.

国家网络信息安全技术研究所



Something we did before

International : APEC-TEL



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




.ng;

国家网络信息安全技术研究所



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.


国家网络信息安全技术研究所



International Cooperation

- **APCERT**
- **FIRST**
- **ASEAN**
- **APEC**
- **TF-CSIRT, CERT/CC**
 - Training cooperation
- **Law enforcement department**
 - one of POC
- **International Companies :MS, eBAY**
 - cooperation in incident handling and information exchange

国家网络信息安全技术研究所



Content


- Current Situation & Trend
- Capacity Model & Practice
- Future & Proposal

国家网络信息安全技术研究所

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

Global Problem, Global Solution

- * We are all connected
- * Cannikin Law: without secure neighbor, can not get our own
- * There are still many economies do not have enough capacities
- * Help each other: eliminate the 'digital divide' on security is crucial
- * What we've done



国家网络信息安全技术研究所

NINIS
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

The weather went bad since 2007

Four stages:


Cyber threats

- * Script Kids/Cyber Knights: before 2004
- * Cyber Criminals: 2004-
- * Information Stealing: 2007-
- * Cyber War/Conflict: 2010-

International cooperation on anti-cyber-threats

- * Starting: before 2001
- * Good: 2001-2007
- * Bad: 2007-2010
- * Worse: After 2010

国家网络信息安全技术研究所

 **NINIS**
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

Rebuild trust is the key

- * Trust is the key for cooperation/collaboration
- * Trust is being hurt
- * Debate and point fingers does not help
- * Need to find a way to rebuild the trust, or all of us will lose the real battle

The most important? Say NO to Cyberwar!

国家网络信息安全技术研究所

 **NINIS**
NATIONAL INSTITUTE
OF NETWORK AND INFORMATION SECURITY

How can public sectors join: Cross border and multilayer cooperation framework

Policy Level	Governmental Agencies: Policy making; resource; Law issues; Regulations	Build and Share: Common understandings; MOUs; LEA cooperation
Operational Level	CSIRTs, Industries: Keep efficiency; Ensure effectiveness	Build and Share: Related information; Incident handling;
Research Level	Research institutes: Understand new challenges; Provide new suggestions	Build and Share: Projects on Trends and new challenges; Knowledge sharing

国家网络信息安全技术研究所

