网络空间的信任模型：现状与挑战

之——DNS信任体系

段海新，清华大学

阿里安全峰会2015，北京

提纲

- 网络空间和信任根
- DNS信任体系的攻击面
- ICANN和DNSSEC
- 总结

网络空间（Cyberspace）

- 通过互联网和计算机进行通信、控制和信息共享的虚拟空间
- 网络空间里没有明确的、固定的边界，也没有集中的控制权威

--《网络空间安全一级学科论证报告》，2015年5月

国务院学位委员会
教育部 文件

学位〔2015〕11号

国务院学位委员会 教育部
关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委）、新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

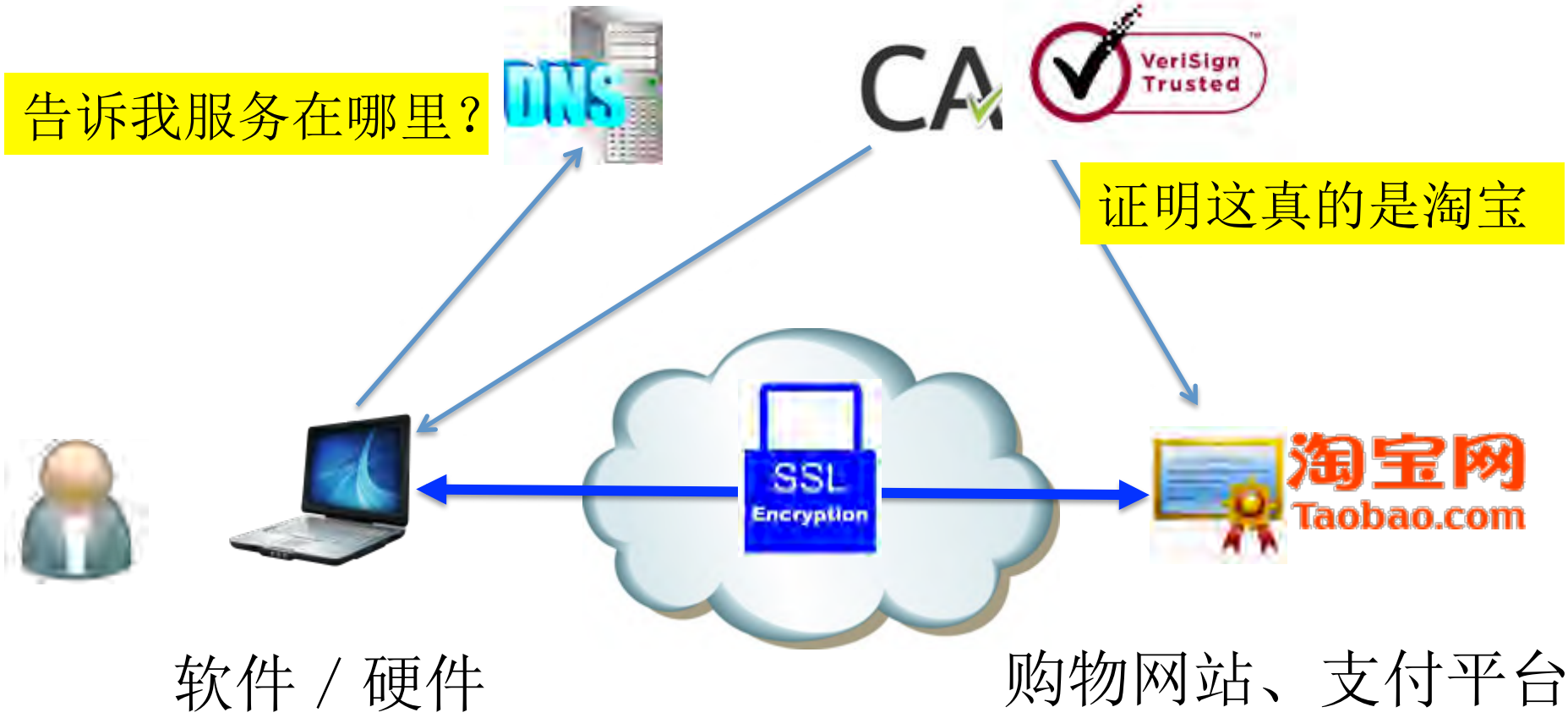
信任（Trust）

- 相信某人（组织）或某物：
  - 真实（Truth）
  - 可靠（Reliability）
  - 有能力（Ability）或有强度（Strength）

Trust Fall

Firm belief in the reliability, truth, ability, or strength of someone or something--oxford dictionary

信任举例：网上购物

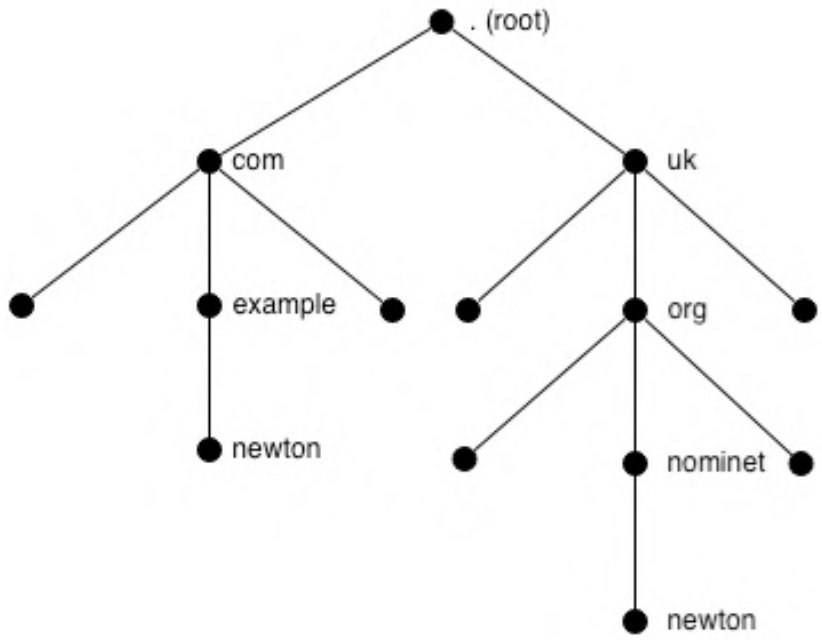

告诉我服务在哪里？
DNS
CA
VeriSign Trusted
证明这真的是淘宝
SSL
Encryption
淘宝网
Taobao.com
软件 / 硬件
购物网站、支付平台

信任根（Trust Anchors）

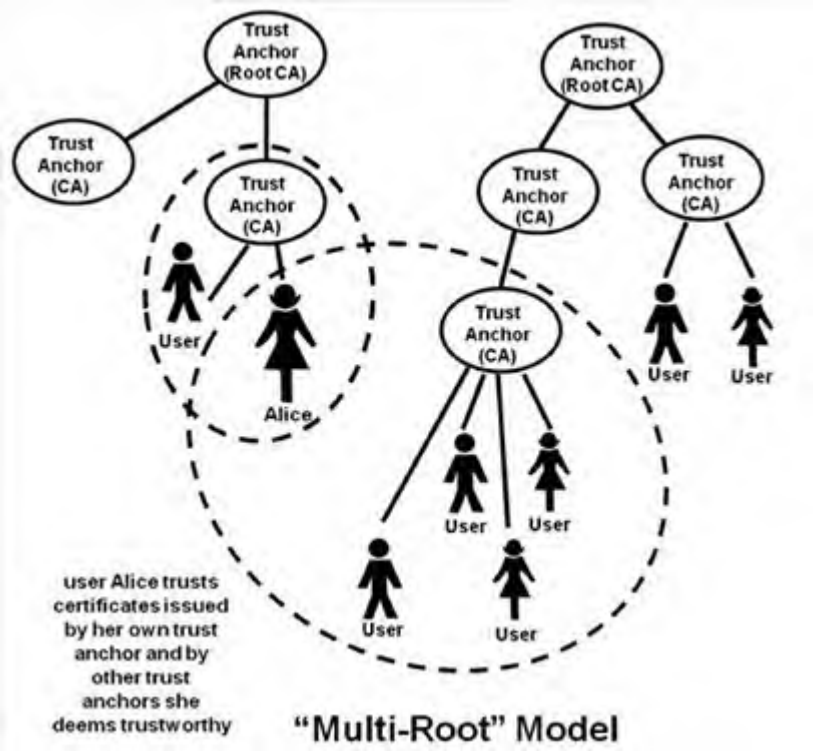
- 域名服务系统（DNS）
  - IP地址：你在哪里？
  - 真实：不能给出假的、错误的地址
  - 可靠：运营者必须诚实，不能故意造假
  - 强壮：在受攻击的情况下仍可以工作
- 公钥证书权威（Certificate Authority, CA）
  - 身份认证：怎么证明你的身份？
  - 互联网保密、完整性通信的前提条件
  - 对CA的真实、可靠、强壮要求更高

DNS和CA的信任模型

DNS : 树形结构



CA：森林结构



你的浏览器信任多少个 CA?

提纲

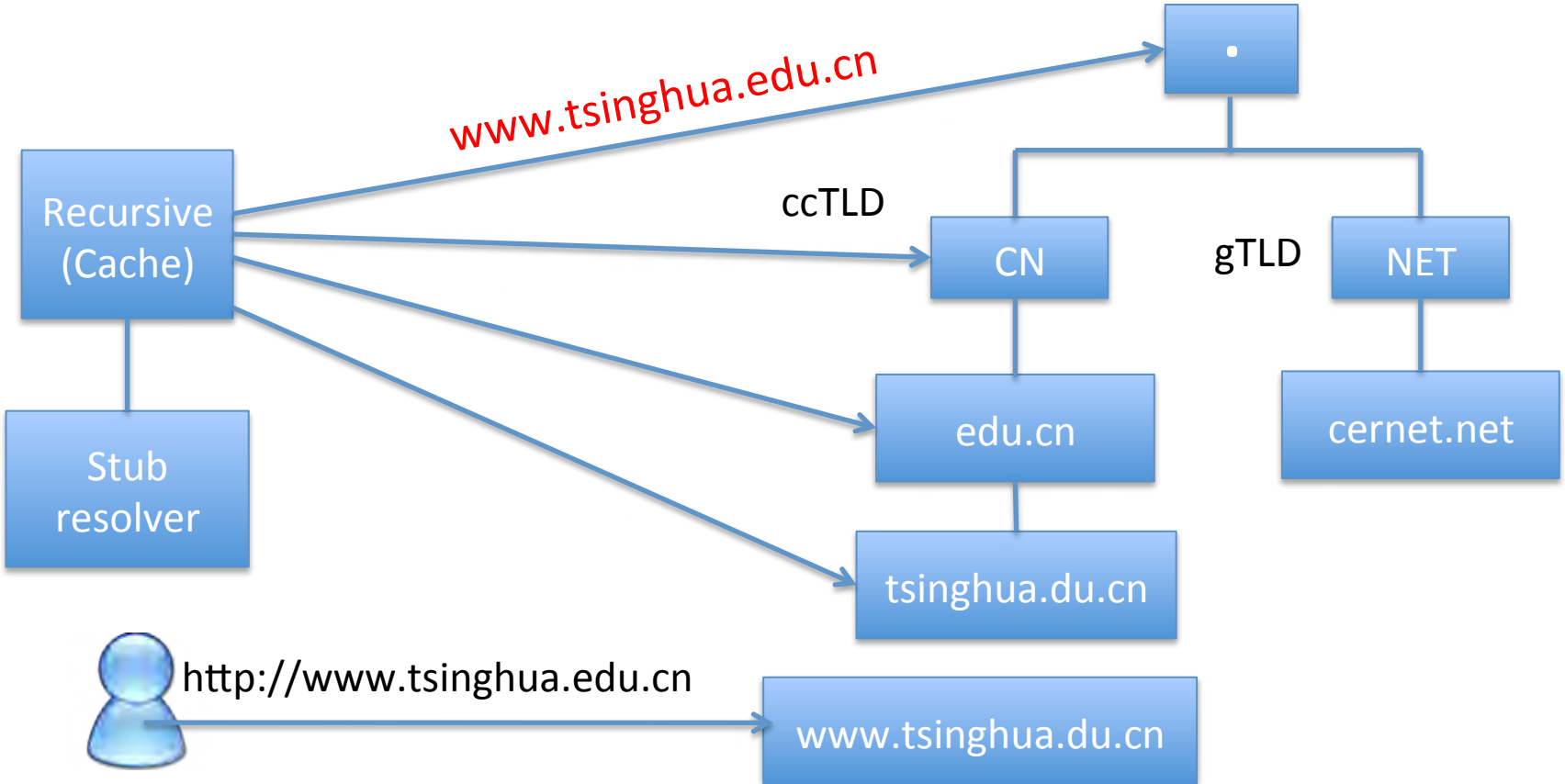
- 网络空间和信任根
- DNS信任体系的攻击面
- ICANN和DNSSEC
- 总结

DNS工作过程

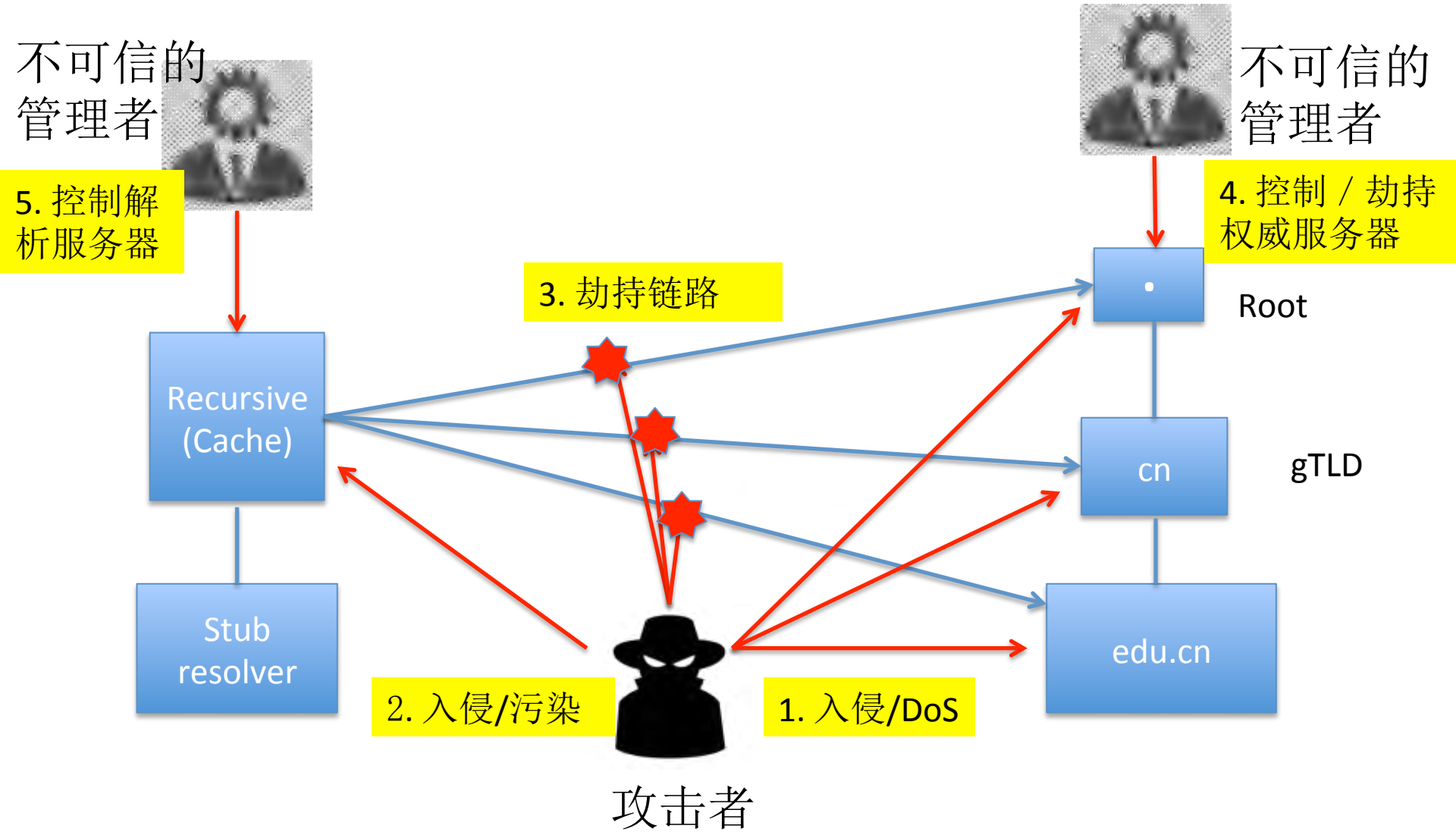
客户端：递归/缓存
- Cache, Recursive

UDP

权威服务器（Authoritative），Root, TLD, …



DNS信任的攻击面（attack surface）



DNS信任体系的攻击面之一：

控制/劫持/权威服务器（Server），
比如Root

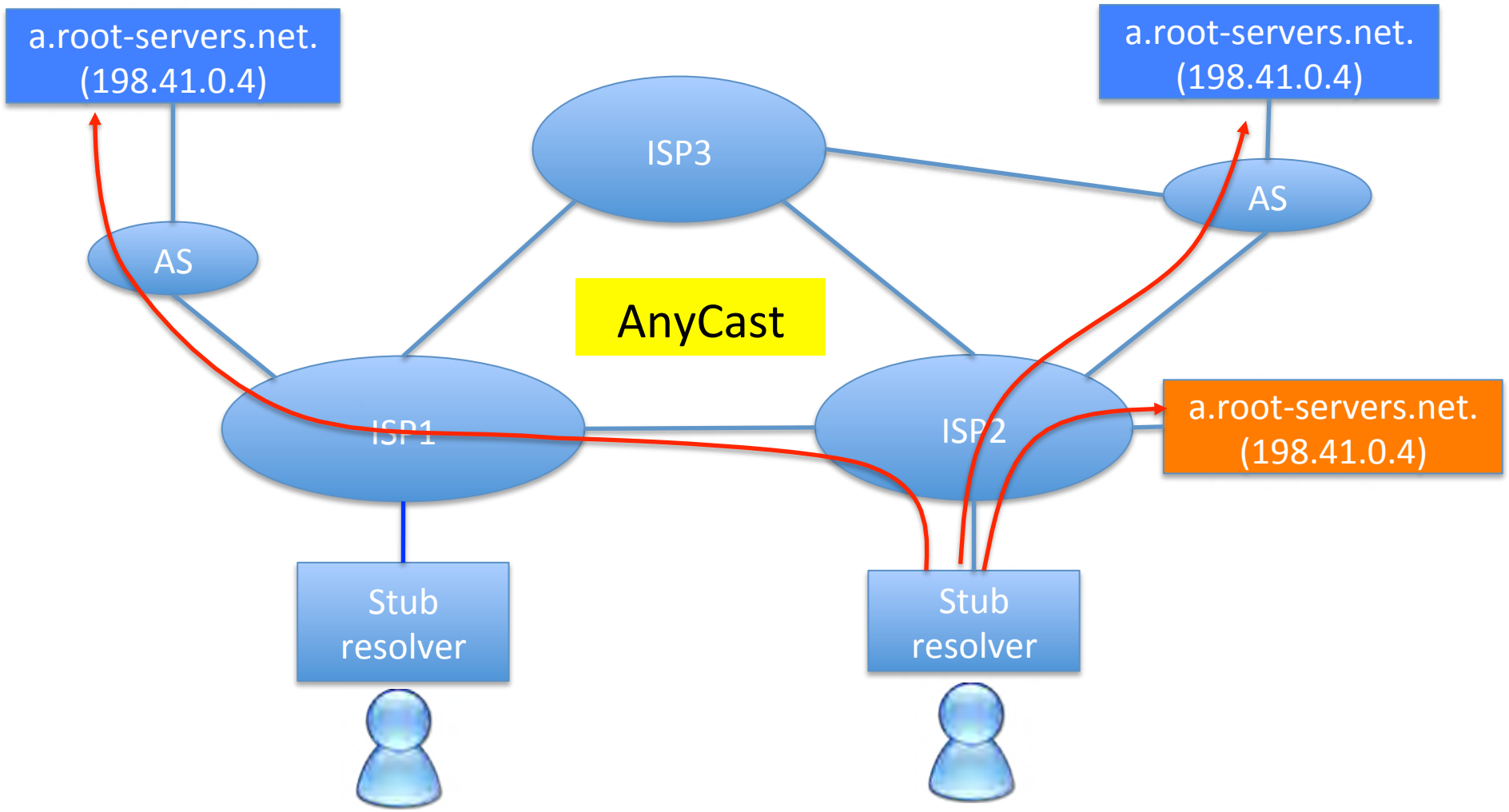
控制/劫持权威服务器，如Root

- US GOV -> NSF -> Network Solutions Inc.(NSI)
  - 从政府补贴、到收费、到被告
- ccTLD => Jon Postel, RFC 1591(1994)
  - 先来先得的政策
  - IAB Review Committee 没有成立
  - .IQ（伊拉克）被授予美国的恐怖分子
- Hijacking of Root by Jon Postel, 1998
  - 邮件通知8个root管理员同步IANA而非NSI
  - 政府命令Jon 停止，同时坚强了对Root控制权

段海新，伊拉克域名IQ被美国删除的背后以及早期的根域名管理
http://netsec.ccert.edu.cn/duanhx/archives/1850

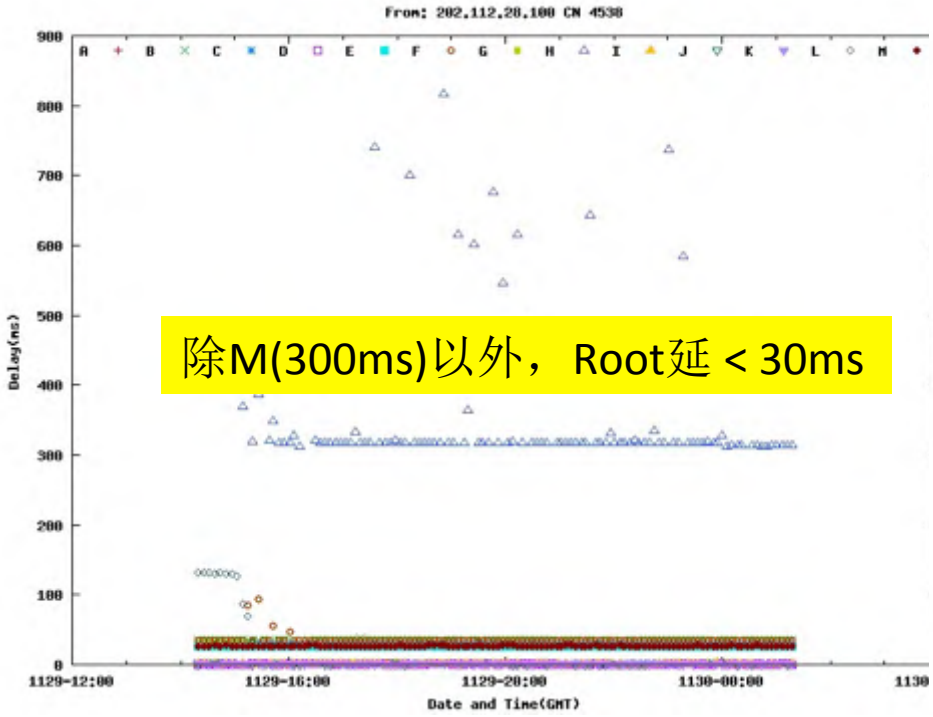
Root Servers (anycast instances)

山寨一个Root，自己控制



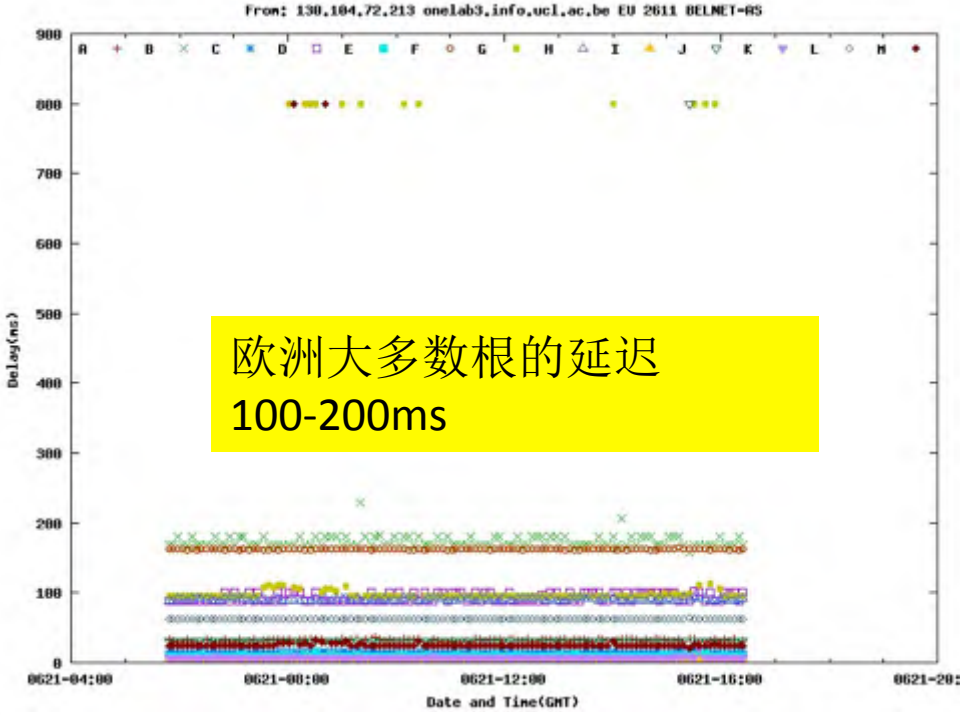
到Root的延迟： CERNET & Europe, 2012

- Root DNS delay in CERNET



除M(300ms)以外， Root延 < 30ms

- Root Delay in Europe



欧洲大多数根的延迟
100-200ms

J. Liang, J. Jiang, H. Duan, K. Li, and J. Wu, “Measuring query latency of top level DNS servers,” presented at the PAM'13: Proceedings of the 14th international conference on Passive and Active Measurement, 2013.

DNS信任体系的攻击面之二：

控制解析服务器

如果你可以控制解析服务器...

From:Paul A Vixie[SMTP:paul@vix.com]
Sent:Thursday, October 31, 1996 12:56 PM
To:newdom@vrx.net
Subject:requirements for participation

I have told the IANA and I have told InterNIC -- now I'll tell you kind folks.

If IANA's proposal stagnates past January 15, 1997, without obvious progressand actual registries being licensed or in the process of being licensed, I will declare the cause lost. At that point it will be up to a consortium of Internet providers, probably through CIX if I can convince them to take up this cause, to tell me what I ought to put into the "**root.cache**" file that I ship with BIND.

https://www.ietf.org/mail-archive/text/ietf/1996-11

Paul Vixie
Author of BIND
Chair of SAC of ICANN

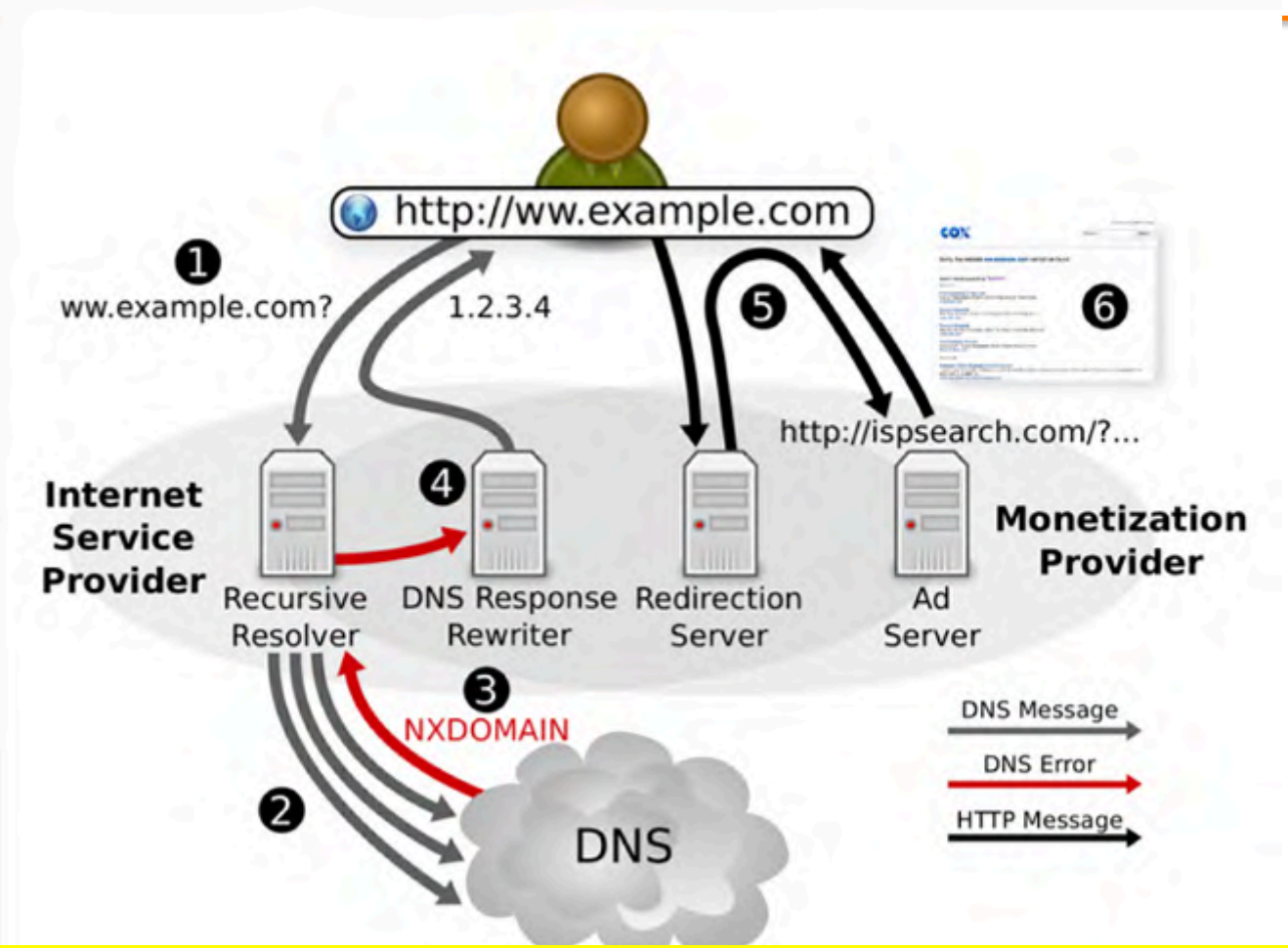
ORSN (2002-2008, 2013-)
(Open Root Server Network)

As a long time supporter of the universal namespace operated by IANA, it may come as a surprise that I have joined the Open Root Server Network project (ORSN). I'll try to explain what's going on and what it all means.

香港某酒店，DNS查询都被重定向

```
$ dig  @1.1.1.1 www.edu.cn

; <<>> DiG 9.6-ESV-R4-P3 <<>> @1.1.1.1 www.edu.cn
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12501
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.edu.cn.                    IN  A

;; ANSWER SECTION:
www.edu.cn.         124 IN  A   202.205.109.203
www.edu.cn.         124 IN  A   202.112.0.36
www.edu.cn.         124 IN  A   202.205.109.205

;; Query time: 6 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Fri Mar 22 07:01:35 2013
;; MSG SIZE  rcvd: 76

$ dig  @2.2.2.2 www.edu.cn

; <<>> DiG 9.6-ESV-R4-P3 <<>> @2.2.2.2 www.edu.cn
; (1 server found)
```

有些ISP利用解析服务NXDOMAIN赚钱



N. Weaver, V. Paxson, and C. Kreibich, “Redirecting DNS for Ads and Profit,” presented at the Proceedings of the 20th USENIX Security Symposium“s Workshop on Free and Open Communications on the Internet (FOCI ”11), 2011.

DNS信任体系的攻击面之三：

控制解析路径 / 链路

[dns-operations] Odd behaviour on one node in I root-server (facebook, youtube & twitter)

Hi there! A local ISP has told us that there's some strange behavior with at least one node in i.root-servers.net (traceroute shows mostly China) It seems that when you ask A records for facebook, youtube or twitter, you get an IP and not the referral for .com

It doesn't happen every time, but we have confirmed this on 4 different connectivity places (3 in Chile, one in California)

This problem has been reported to Autonomica/Netnod but I don't know if anyone else is seeing this issue.

This is an example of what are we seeing:

$ dig @i.root-servers.net www.facebook.com A ;
….
ANSWER SECTION: www.facebook.com. 86400 IN A 8.7.198.45

Mauricio Vergara Ereche
Santiago CHILE

https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005260.html

智利用户访问facebook.com的域名解析可能经过中国

Root Servers in China

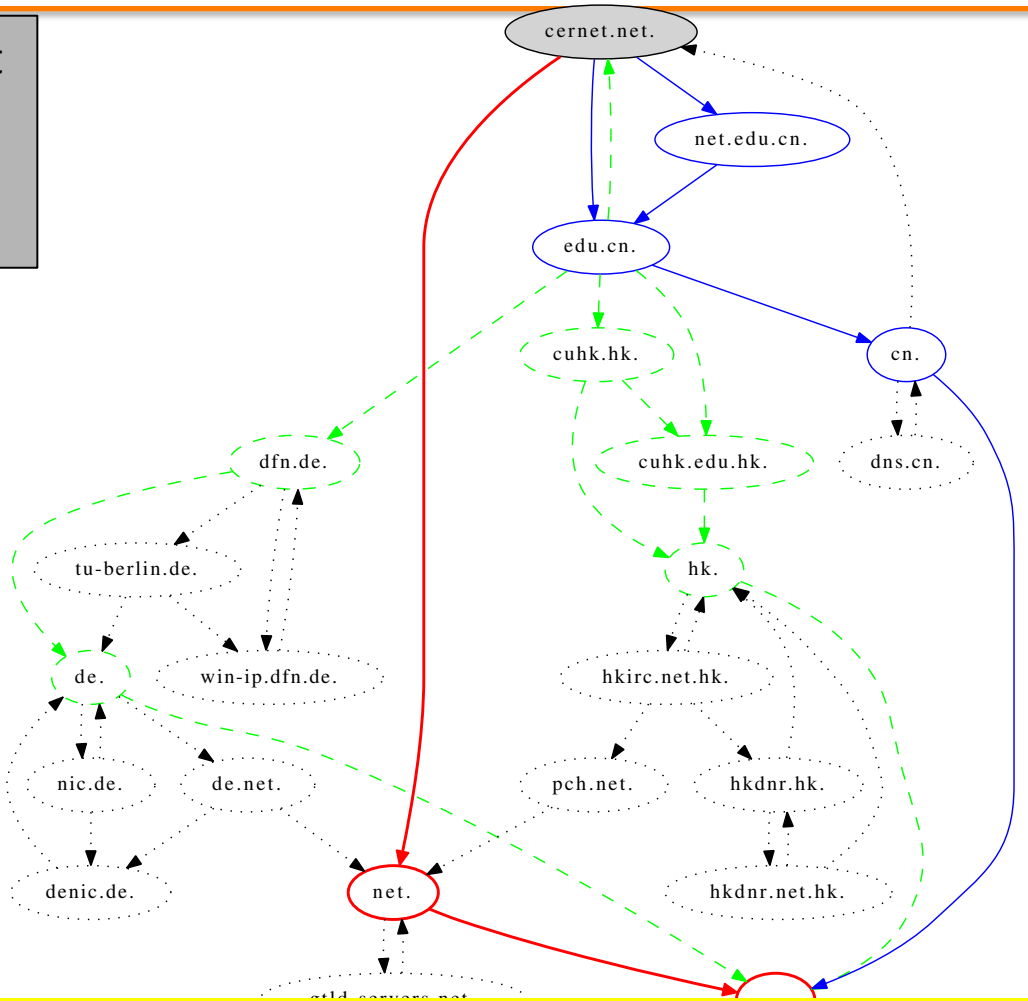
2013: 4(BJ) + 5(HK) + 3(TW) = 12

2013: 4(BJ) + 5(HK) + 3(TW) = 12

域名解析可能经过哪些链路？

```
$ dig ns  cernet.net @a.gtld-servers.net
;; AUTHORITY SECTION:
cernet.net.      NS    ns2.net.edu.cn.
cernet.net.      NS    dns.edu.cn.
```

```
$ dig ns  edu.cn
;; ANSWER SECTION:
edu.cn.    NS    S6.edu.cn.
edu.cn.    NS    NS2.CUHK.EDU.HK.
.....
edu.cn.    NS    DENEB.DFN.DE.
```



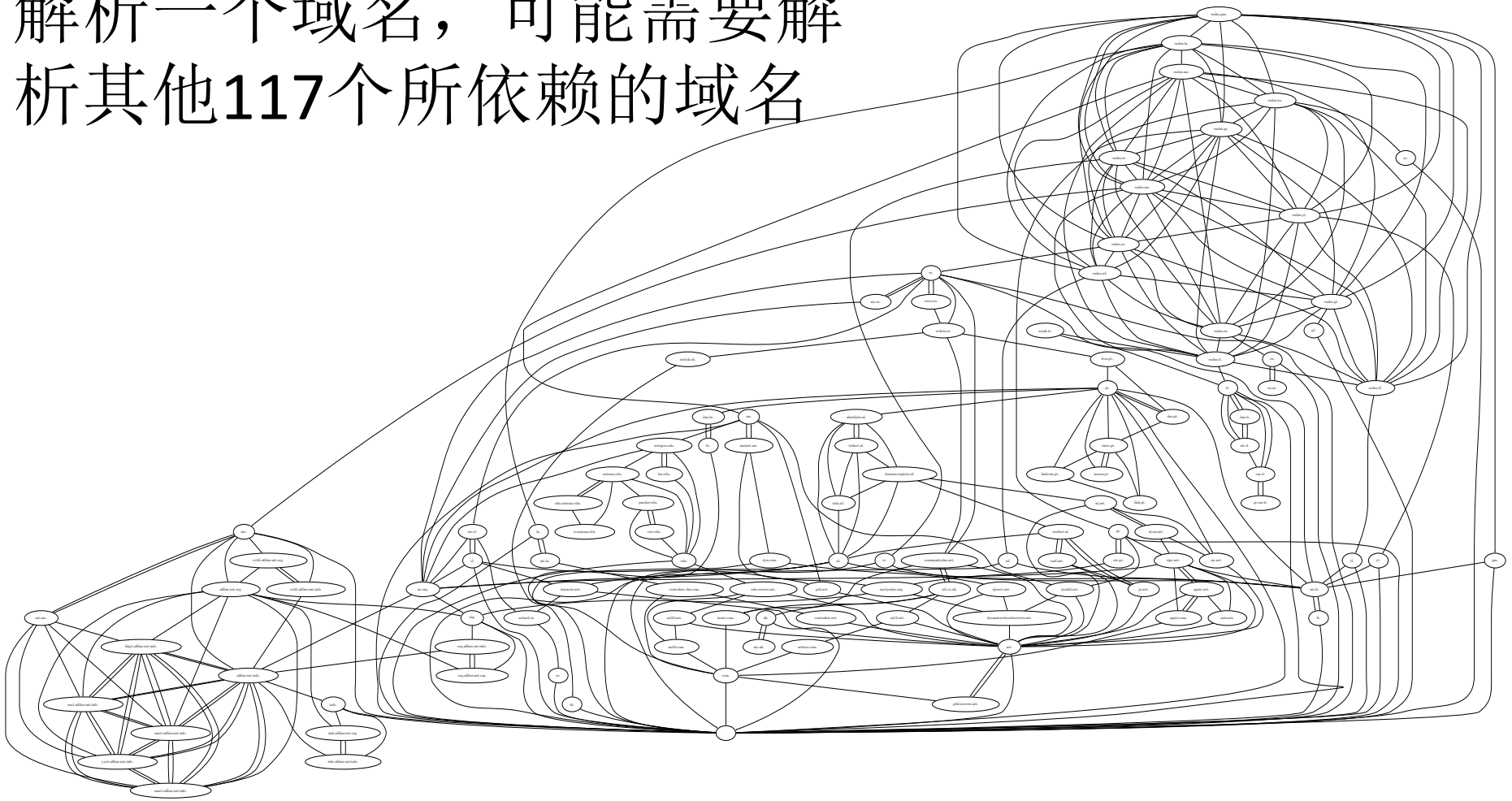
J. Jiang, L. Jinjin, D., Haixin, Analysis and Measurement of Zone Dependency in the Domain Name System, 2013

.CN 的域名解析会如何？

```
$ dig   ns   ac.cn


;; QUESTION SECTION:
;ac.cn.                  IN   NS

;; ANSWER SECTION:
ac.cn.          86400  IN   NS  d.dns.cn.
ac.cn.          86400  IN   NS  cns.cernet.net.
ac.cn.          86400  IN   NS  a.dns.cn.
ac.cn.          86400  IN   NS  e.dns.cn.
ac.cn.          86400  IN   NS  b.dns.cn.
ac.cn.          86400  IN   NS  c.dns.cn.
```

域名空间中，国家的边界在哪里？

解析一个域名，可能需要解析其他117个所依赖的域名




你以为
DO YOU THINK
WHAT YOU THINK
YOU THINK?
你以为的就是
你以为的吗?

提纲

- 网络空间和信任根
- DNS信任体系的攻击面
- ICANN和DNSSEC
- 总结

ICANN: DNS新的Trust Anchor

美国政府控制着ICANN吗？

Department of Commerce: Relationship with ICANN, 2000

The question of whether the Department has the authority to transfer control of the authoritative root server to ICANN is a difficult one to answer. Although control over the authoritative root server is not based on any statute or international agreement, the government has long been instrumental in supporting and developing the Internet and the domain name system. The Department has no specific statutory obligations to manage the domain name system or to control the authoritative root server. It is uncertain whether transferring control would also include transfer of government property to a private entity. Determining whether there is government property may be difficult. To the extent that transition of the management control to a private entity would involve the transfer of government property, it is unclear if the Department has the requisite authority to effect such a transfer. Since the Department states that it has no plans to transfer the root server system, it has not examined these issues. Currently, under the cooperative agreement with Network Solutions, the Department has reserved final policy control over the authoritative root server.

http://www.gao.gov/new.items/og00033r.pdf

XXX域名美Gov反对，ICANN最后批准

- 2000, ICANN 启动新TLD的POC
- 2000, 美国公司ICM Registry 申请 .kids 和 .xxx
- 2003, ICM 根据ICANN意见修订，申请sTLD
- 2005, ICANN考虑多方的反对，拒绝了XXX
- …
- 2010, ICANN 批准了ICM的XXX申请

[0] .xxx域名在icann讨论被美国一票否决的case: http://netsec.ccert.edu.cn/duanhx/archives/1881
[1] Delegation of the .XXX top-level domain， http://www.iana.org/reports/2011/xxx-report-20110407.pdf
[2] Accountability and Transparency at ICANN An Independent Review. Appendix D: The .xxx Domain Case and ICANN Decision-Making Processes http://cyber.law.harvard.edu/pubrelease/icann/pdfs/AppendixD_xxx.pdf

ICANN与GAC（政府咨询委员会）

- ICANN目前是Root DNS的Trust Anchor
- 政府咨询委员会（GAC）的角色
  - GAC只能提意见，它可以派人参加ICANN理事会的会议、参与讨论或辩论，但是没有投票权。
  - 理事会对于可能影响公共政策的决策，必须听取GAC的意见，但可以不按GAC的意见做决定，但必须给出解释

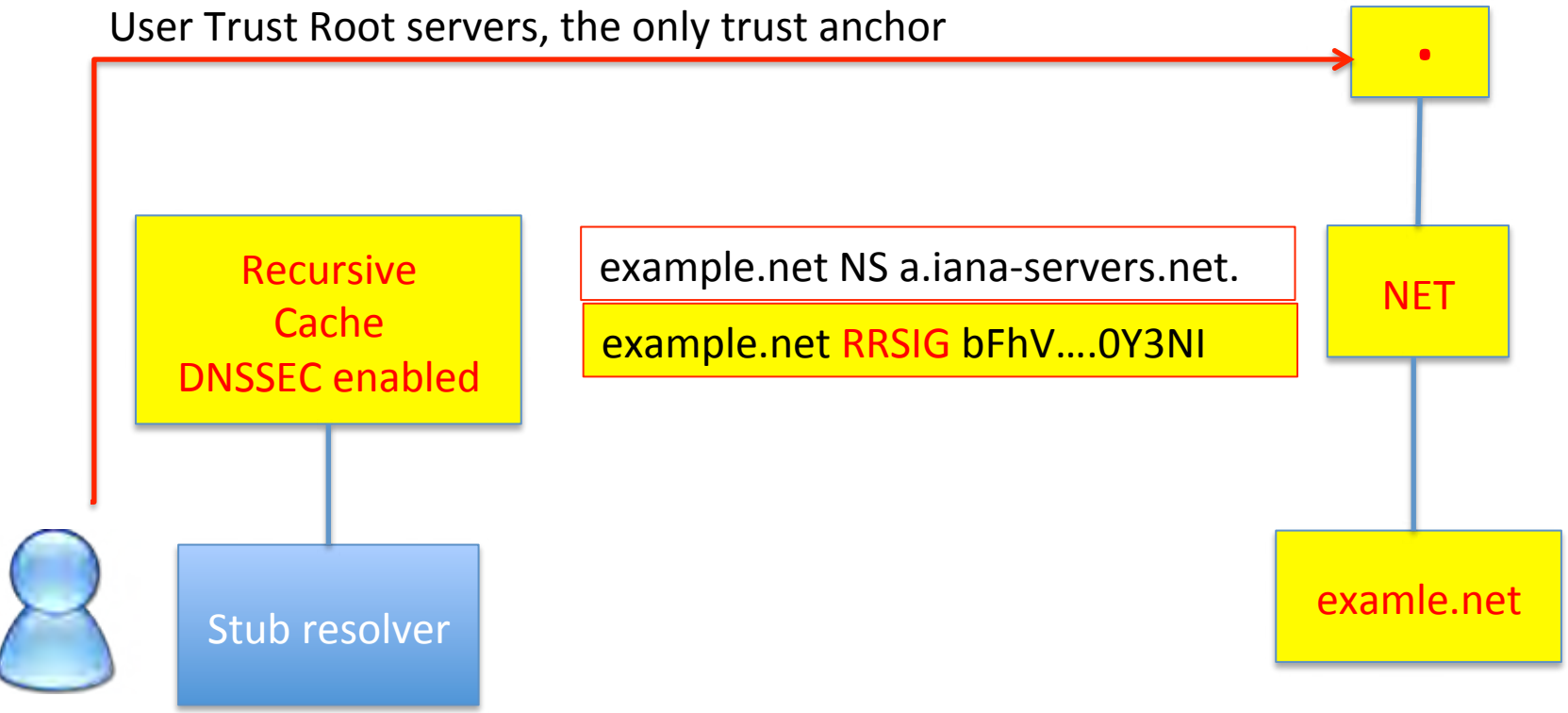
ICANN的章程： https://www.icann.org/resources/pages/bylaws-2012-02-25-zh#XI

DNSSEC : DNS 安全就安全了

事实是这样的吗？

DNSSEC：防止链路劫持、缓存污染

- Clients(resolvers) validate the signature with their public keys
- Servers sign all the DNS records with their private Keys



Paul Vixie, June 1995:

> This sounds simple but it has deep reaching consequences in both the protocol and the implementation—which is why it's taken more than a year to choose a security model and design a solution. We expect it to be another year before DNSSEC is in wide use on the leading edge, and at least a year after that before its use is commonplace on the Internet.

BIND 8.2 blurb, March 1999:

> [Top feature:] Preliminary DNSSEC.

BIND 9 blurb, September 2000:

> [Top feature:] DNSSEC.

Paul Vixie, November 2002:

> We are still doing basic research on what kind of data model will work for DNS security. After three or four times of saying "NOW we've got it, THIS TIME for sure" there's finally some humility in the picture . . . "Wonder if THIS'll work?" . . .
>
> It's impossible to know how many more flag days we'll have before it's safe to burn ROMs . . . It sure isn't plain old SIG+KEY, and it sure isn't DS as currently specified. When will it be? We don't know. . . .
>
> 2535 is already dead and buried. There is no installed base. We're starting from scratch.

DNSSEC
Trusted Community Representatives

Crypto Officers for the US East Coast Facility

- Alain Aina, BJ
- Anne-Marie Eklund Löwinder, SE
- Frederico Neves, BR
- Gaurab Upadhaya, NP
- Olaf Kolkman, NL
- Robert Seastrom, US
- Vinton Cerf, US

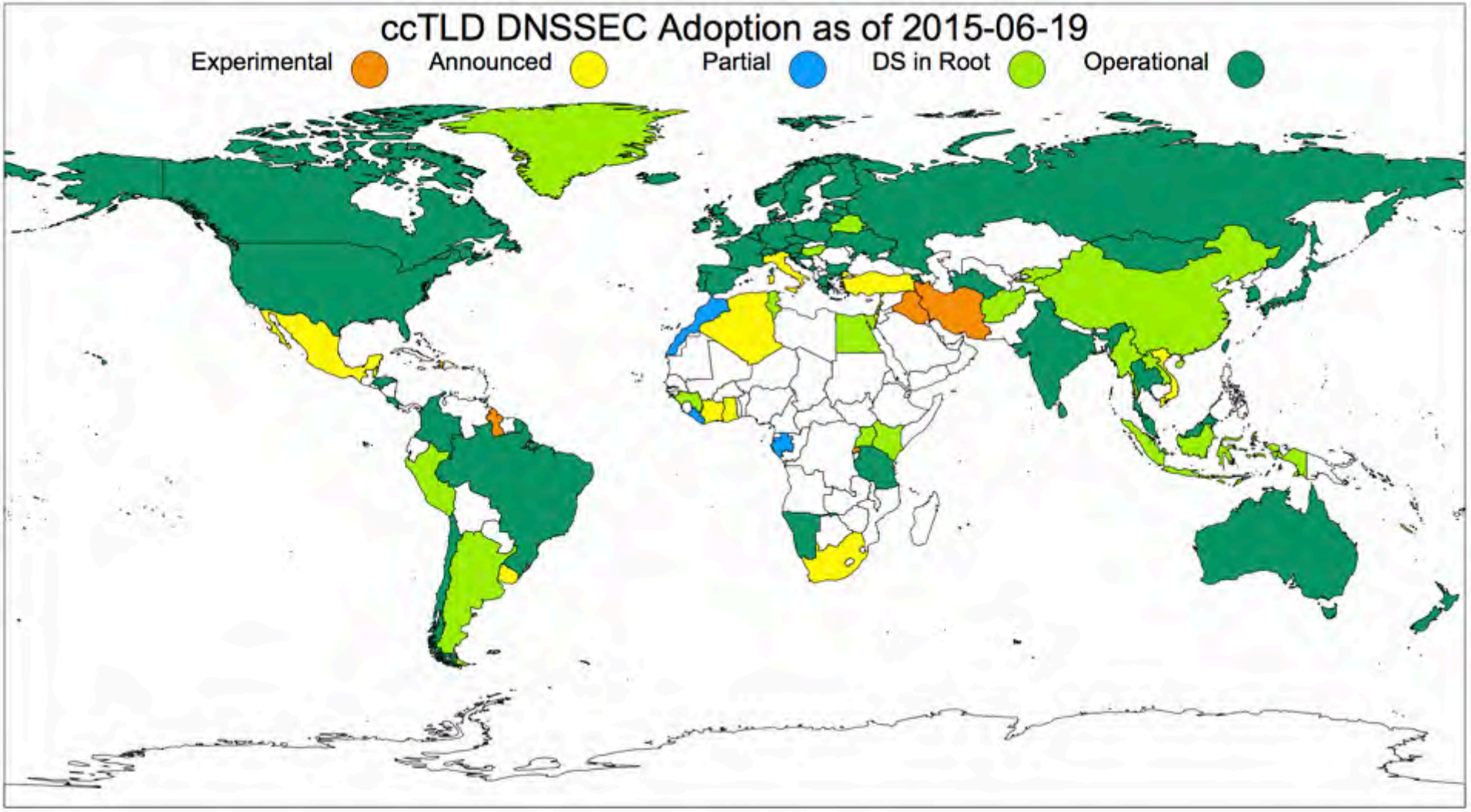
Crypto Officers for the US West Coast Facility

- Andy Linton, NZ
- Carlos Martinez, UY
- Dmitry Burkov, RU
- Edward Lewis, US
- João Luis Silva Damas, PT
- Masato Minda, JP
- Subramanian Moonesamy, MU

Recovery Key Share Holders

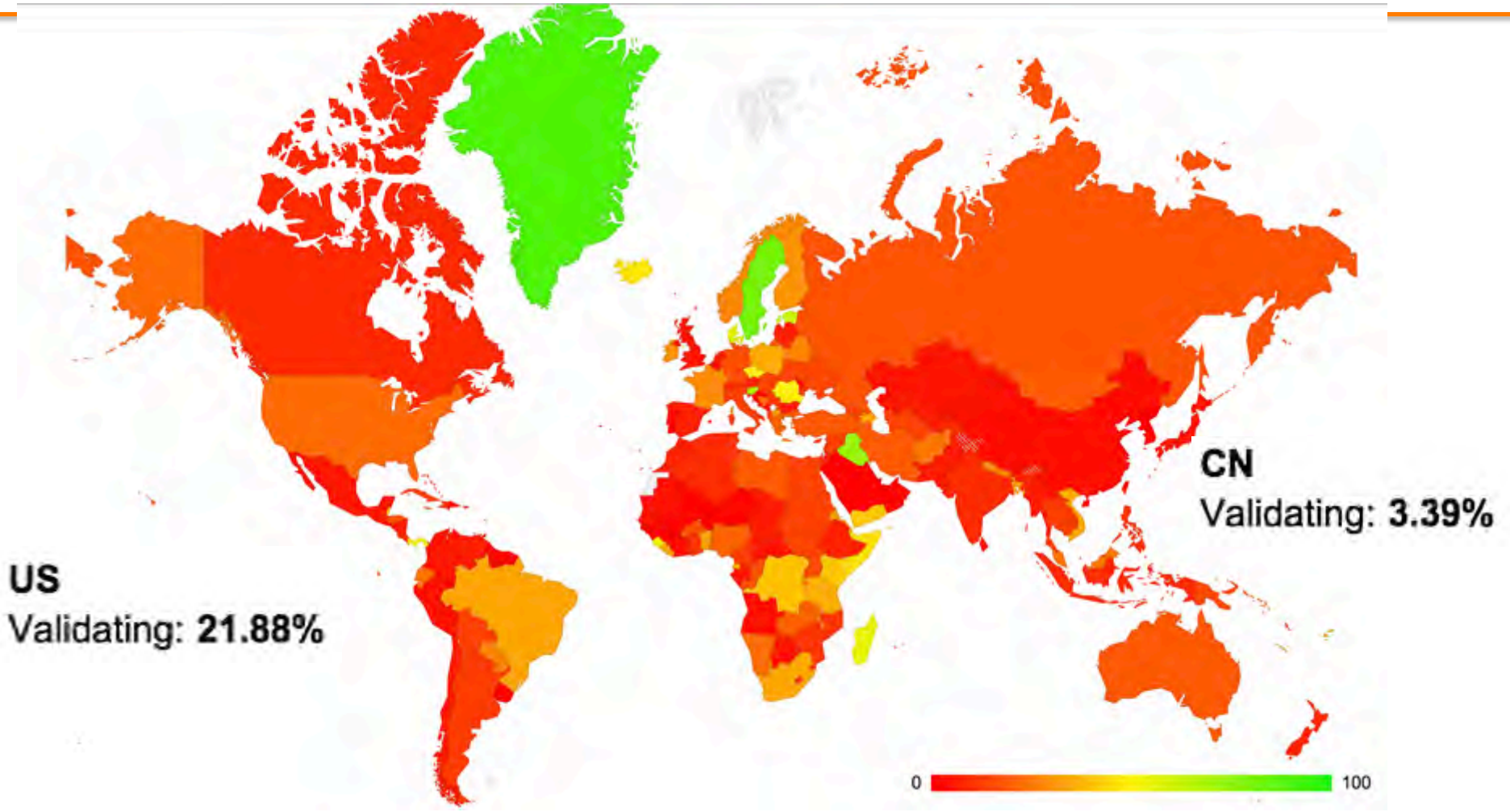
- Bevil Wooding, TT
- Dan Kaminsky, US
- Jiankang Yao, CN
- Moussa Guebre, BF
- Norm Ritchie, CA
- Ondřej Surý, CZ
- Paul Kane, UK

http://www.root-dnssec.org/index.html



Experimental -- Internal experimentation announced or observed (9):	GY HK HT IQ IR MS MU RW TO
Announced -- Public commitment to deploy (11):	CI DZ GH IL IT MX SG TR UY VN ZA
Partial -- Zone is signed but not in operation (no DS in root) (4):	GA LR MA VC
DS in Root -- Zone is signed and its DS has been published (34):	AD AF AG AR AW BY BZ CC CN EG FO GD GI GL GN HU ID KE KG KI KY LA LB LC MM NC NU PE PW SJ TN TV UG VU
Operational -- Accepting signed delegations and DS in root (67):	AC AM AT AU BE BG BR CA CH CL CO CR CX CZ DE DK EE ES FI FR GR GS HN HR IE IN IO IS JP KR LI LK LT LU LV ME MN MY NA NF NL NO NZ PL PM PR PT RE RU SB SC SE SH SI SX TF TH TL TM TT TW TZ UA UK US WF YT

DNSSEC Validation Rate by country (%)



http://stats.labs.apnic.net/dnssec

DNSSEC部署现状意味着什么？

- 尽管权威服务器.CN已经签名，但是绝大多数中国的解析服务器仍然不做验证

- 防止假冒的权威服务器、防止链路上的劫持、缓存污染攻击，还有漫长的路

总结

- 互联网源于一个相互信任的群体，脆弱的DNS支撑着今天的互联网快速发展
- 在充满冲突、相互不信任的环境中，如何管理DNS这种公共资源？
- 政策、技术的开放、透明，融入现有互联网治理体制
- 对信任权威的不信任，是防止权威被滥用、保证权威可以被信任的重要手段

Do you trust what you think you can trust ?
你信任你以为你可以信任的吗?

duanhx@tsinghua.edu.cn