The future of DNS Security

By Ram Mohan
EVP & Chief Technology Officer
Afilias

SANOG Meeting
Chenai
July 22, 2009

The future of DNS security

- DNS is the technology that underpins the development and functionality of the Internet
- Since DNS was developed, the use and effect of the Internet has fundamentally shifted
  - The Internet is now mission critical to EVERYONE and ALL communications

Future looking:

DNS and DNS networks need to be based on:

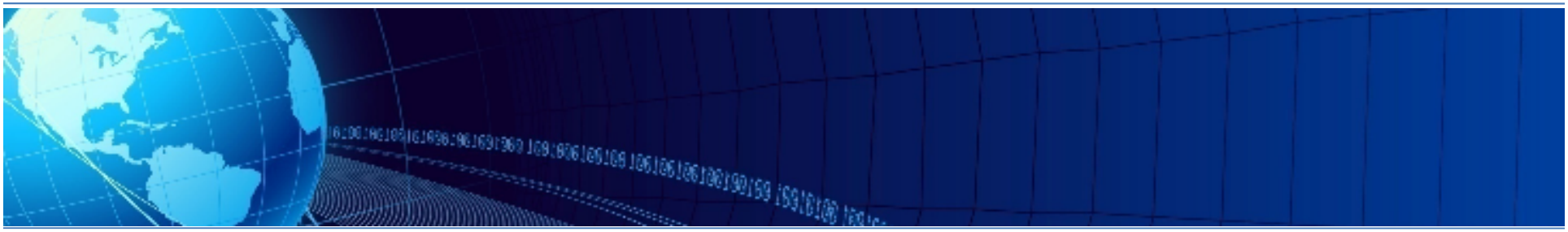
1. **a stable, reliable security model to thwart criminal attacks**
2. **a diverse, scalable network with no single points of failure**

Will the DNS and the root be stable?

Several deployments:

- IPv6 (and IPv4 depletion)
- New TLDs
- IDN TLDs (iTLDs)
- DNSSEC deployment

Not a technical scaling question alone



Creating a stable, reliable security model to thwart criminal attacks…

DNSSEC: A new security model for DNS

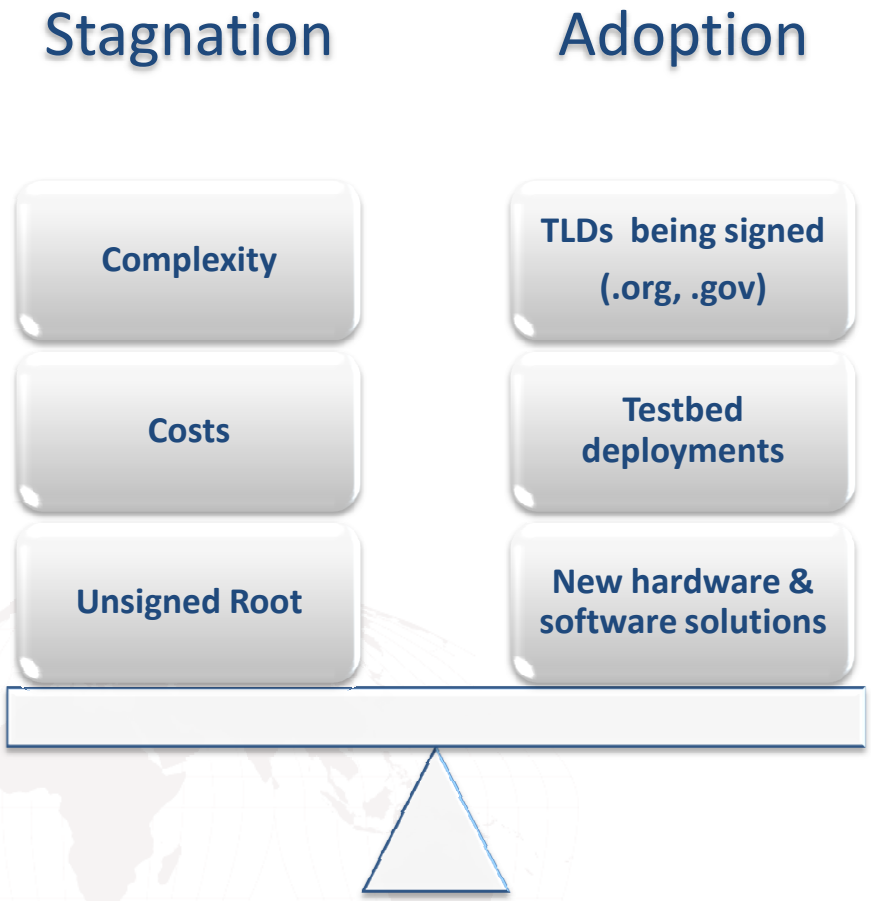
- DNS Security Extensions (DNSSEC)
  - Best way to protect from a man-in-the-middle attacks and cache poisoning (a.k.a. “the Kaminsky bug”)
- DNSSEC introduces digital signatures to the DNS infrastructure, allowing end users to more securely navigate the Internet.
- Provides effective verification that applications, such as Web or email, are using the correct addresses for servers they want to reach.

Current state of implementation

- .ORG signed by Afilias, on behalf of PIR, June 2
  - The .ORG key was pushed to the Interim Trust Anchor Repository (ITAR) on June 26, 2009 and picked up by the DNSSEC Look-Aside Validation (DLV) on July 6, 2009.
  - 18 domains successfully signed in the Friends & Family phase
  - The first scheduled Zone Signing Key (ZSK) rollover was successfully completed on July 2, 2009.
- 12-14 other TLDs are also signed; Root to be signed by end of 2009; .COM expected 2011

SANOG.org is signed!!!

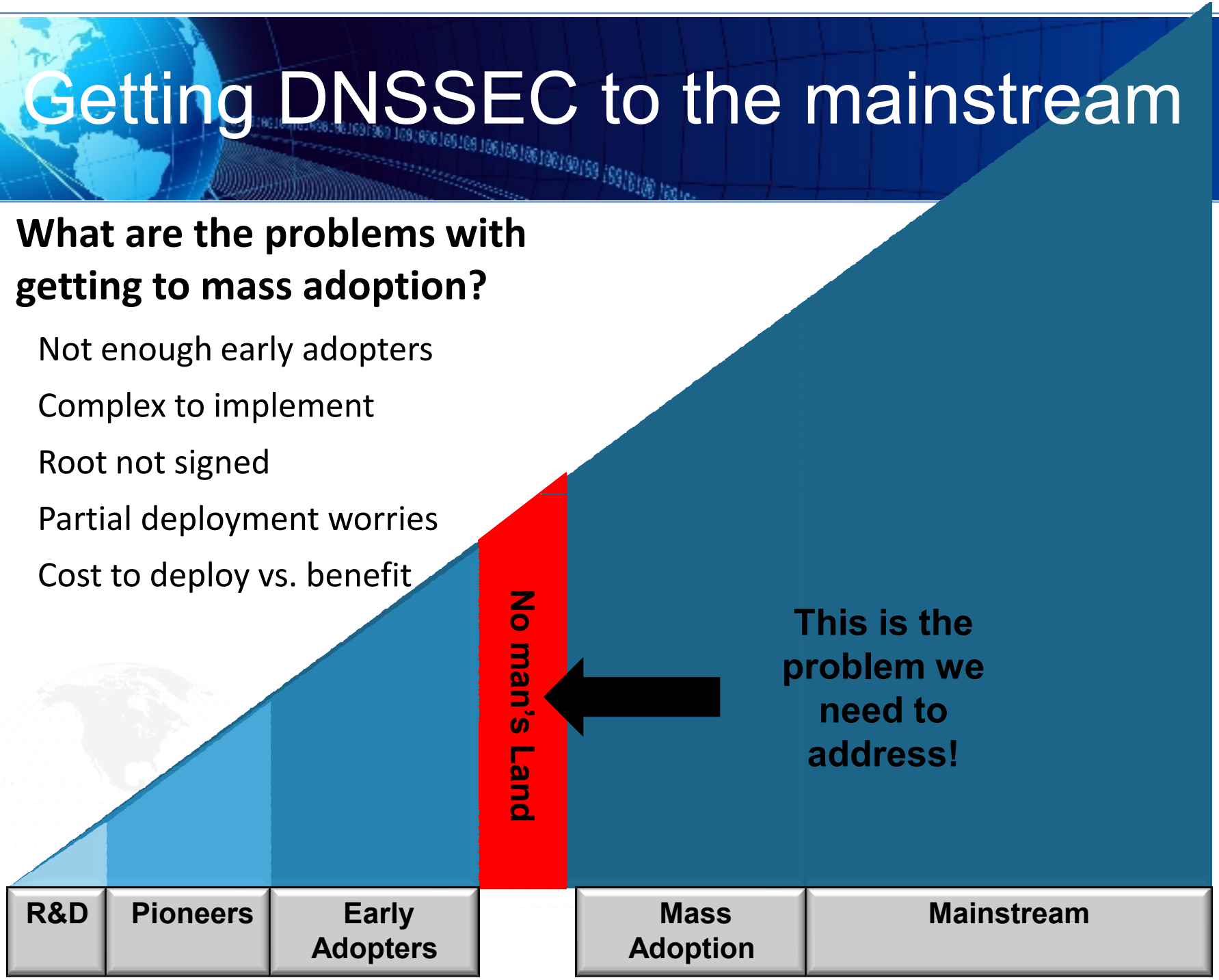
What's the tipping point for DNSEC adoption?



Getting DNSSEC to the mainstream

What are the problems with getting to mass adoption?

- Not enough early adopters
- Complex to implement
- Root not signed
- Partial deployment worries
- Cost to deploy vs. benefit



Choices to adopt DNSSEC

- Option 1: Do it yourself requires:
  - Hardware and software costs
  - Overcome complexities of key distribution
  - In-house expertise, typically not mission critical
  - Risks of website being inaccessible , if done incorrectly

If a site owner selects this they will have to manage:

- New DNSSEC software
- New DNSSEC hardware
- Generating keys – KSKs, ZSKs
- Loading keys for each zone
- Generating and storing DS records at the registrar
- Key rollover

This is NOT a core business function for most organizations!

Choices to adopt DNSSEC

- Option 2: Outsource
  - Fixed cost
  - No expertise needed
  - Complete end- to-end solution

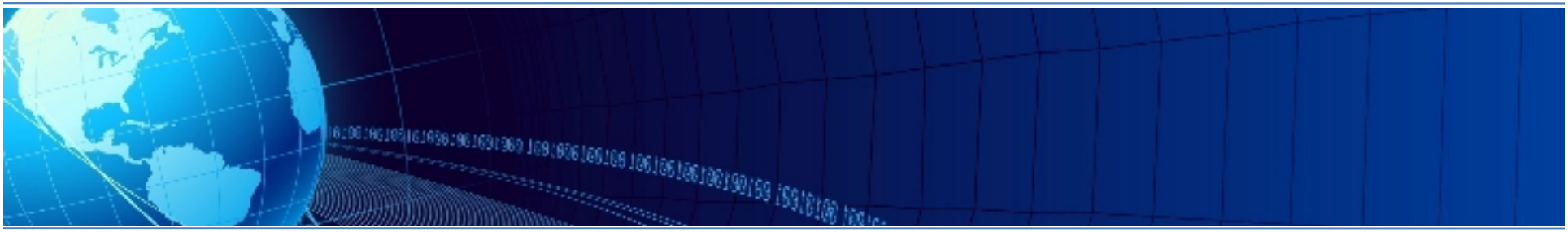
Requires:

- Known provider with global DNS infrastructure and experience in DNSSEC
- Simple interface for signing and management
- Relationships with Trust Anchors and DNSSEC industry leaders
- Service Level Agreement and Contract

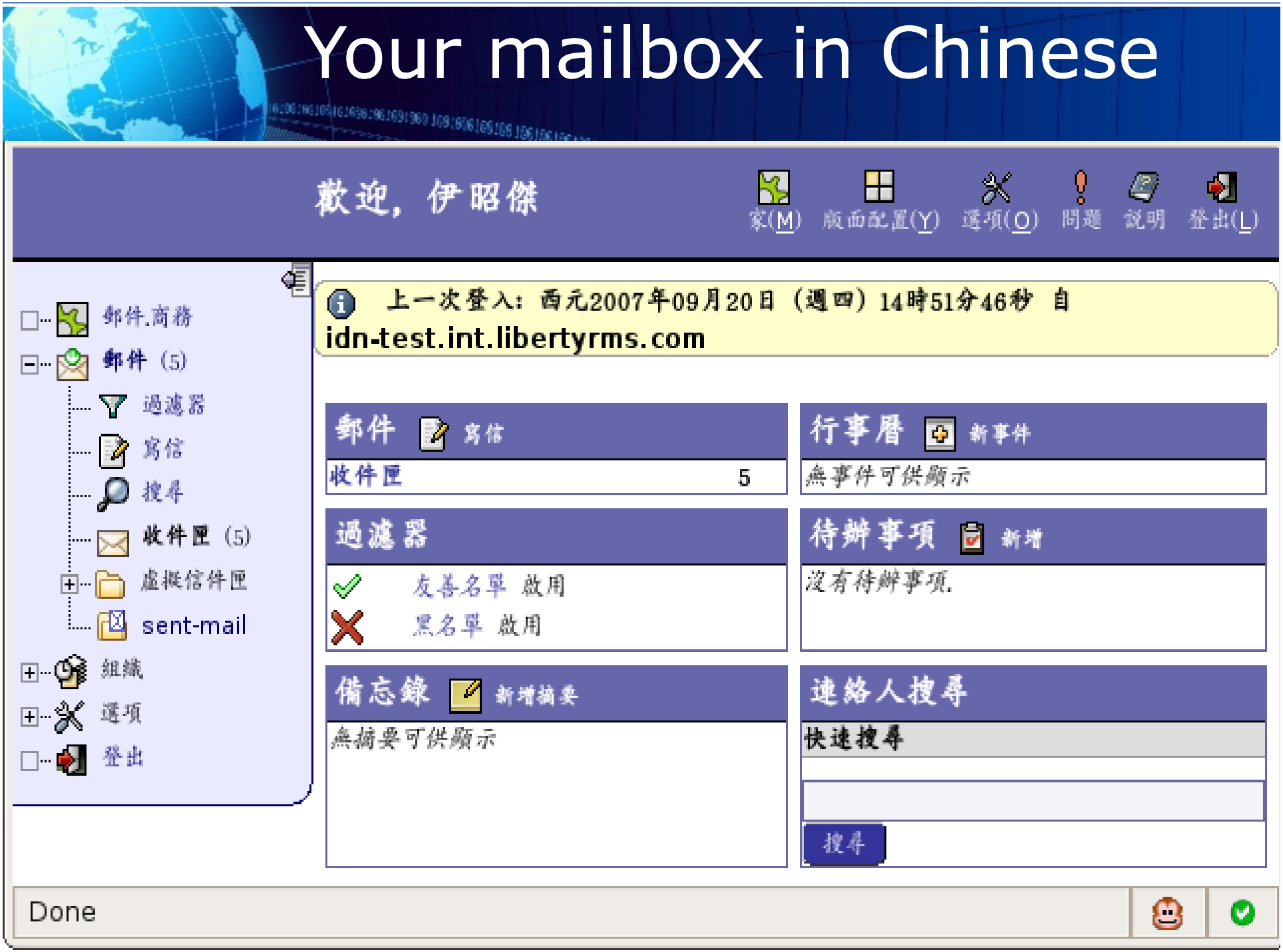
Need for an easy solution

To get DNSSEC to the mainstream DNSSEC needs to be **made easy** with managed services and deployment down the chain of trust

- Afilias beta testing 1-Click DNSSEC™
  - Security of DNSSEC and the convenience of effortless management, in one solution.
- Opportunity for new DNSSEC products to
  - Securing Email
  - E-Commerce applications
  - RFID networks, etc.

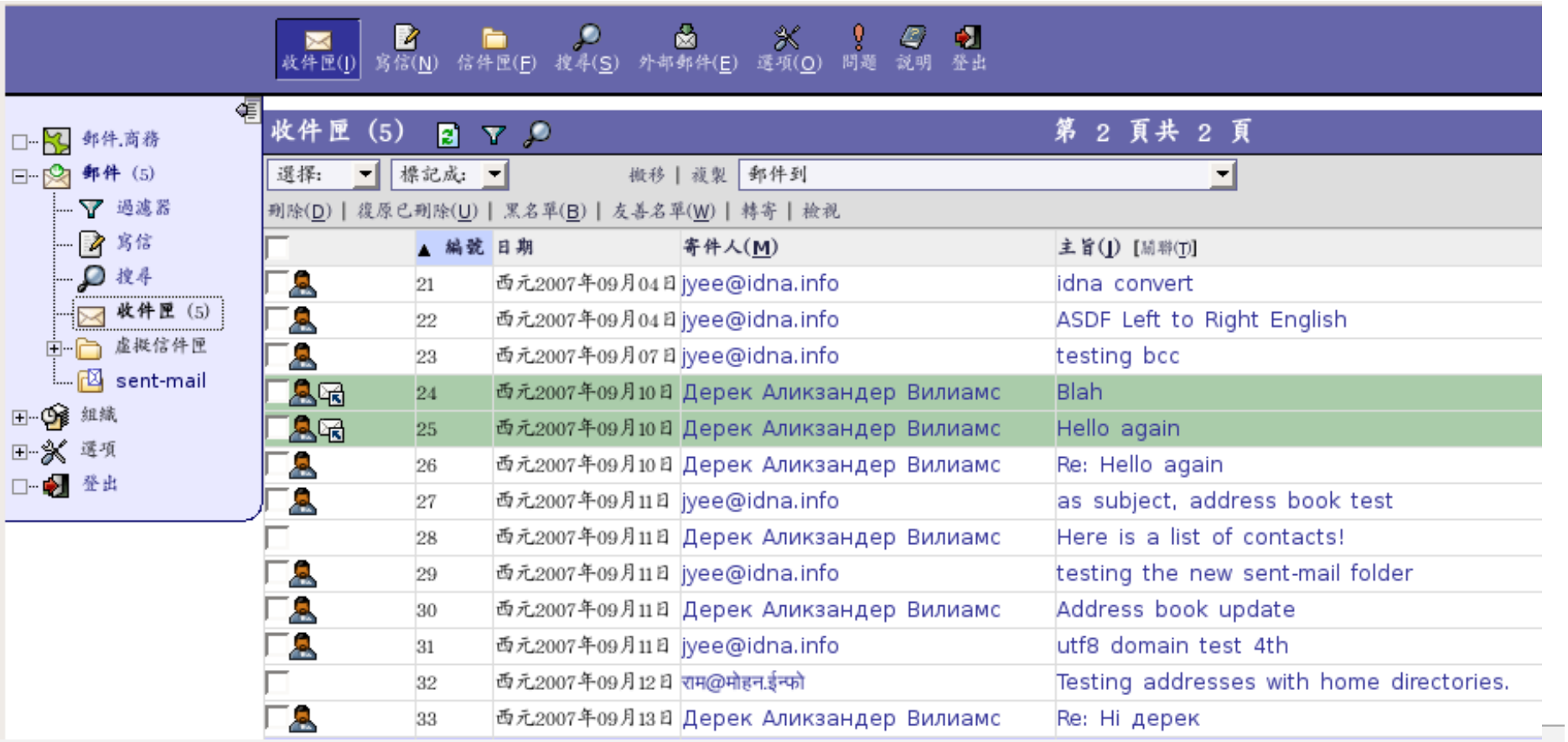


A future where all domains and all content is in your local language…


Your mailbox in Chinese
歡迎, 伊昭傑
家(M)
版面配置(Y)
選項(O)
問題
說明
登出(L)
郵件.商務
郵件 (5)
過濾器
寫信
搜尋
收件匣 (5)
虛擬信件匣
sent-mail
組織
選項
登出
上一次登入: 西元2007年09月20日 (週四) 14時51分46秒 自
idn-test.int.libertyrms.com
郵件
寫信
收件匣 5
行事曆
新事件
無事件可供顯示
過濾器
友善名單 啟用
黑名單 啟用
待辦事項
新增
沒有待辦事項.
備忘錄
新增摘要
無摘要可供顯示
連絡人搜尋
快速搜尋
搜尋
Done

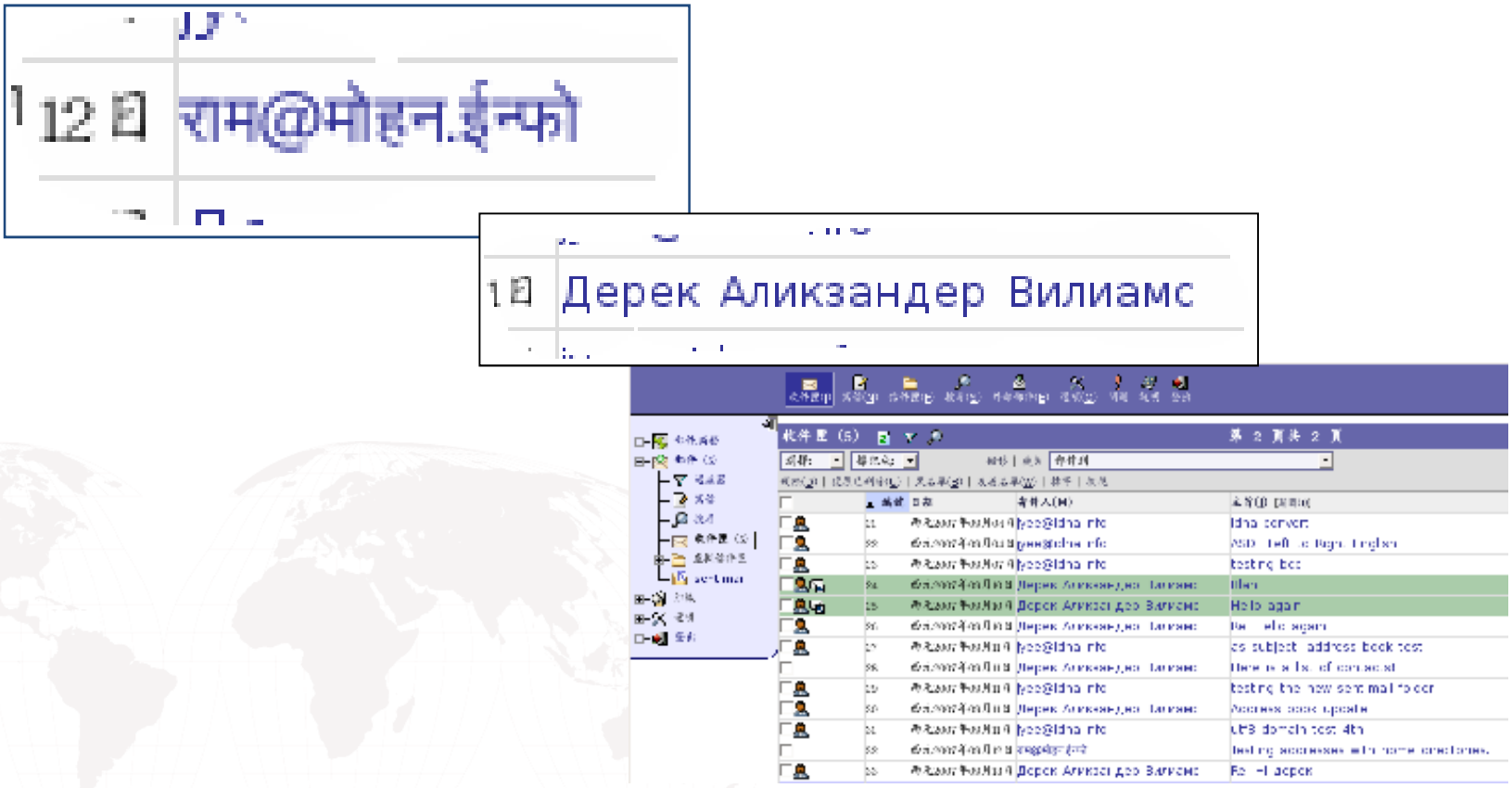
How Do You Know Who Is Writing To You?

- Internet applications must handle messages in multiple languages



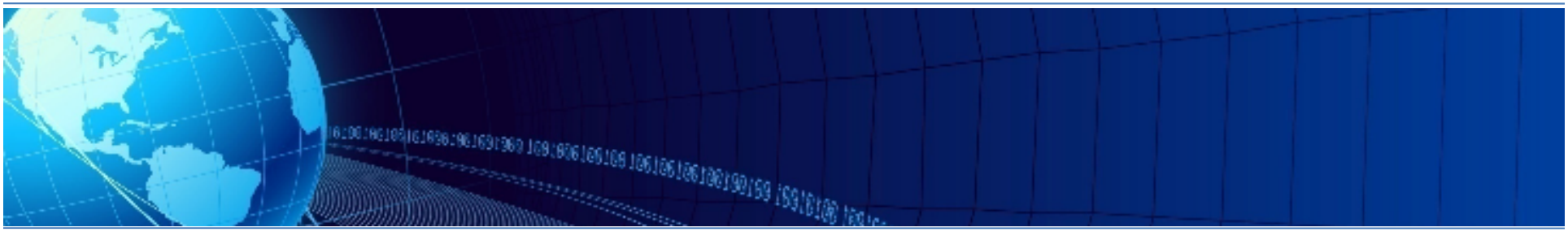
Can You Write To Someone In Another Language?

Applications must allow users to enter text in multiple languages



What About Content?

Applications must handle content in multiple languages



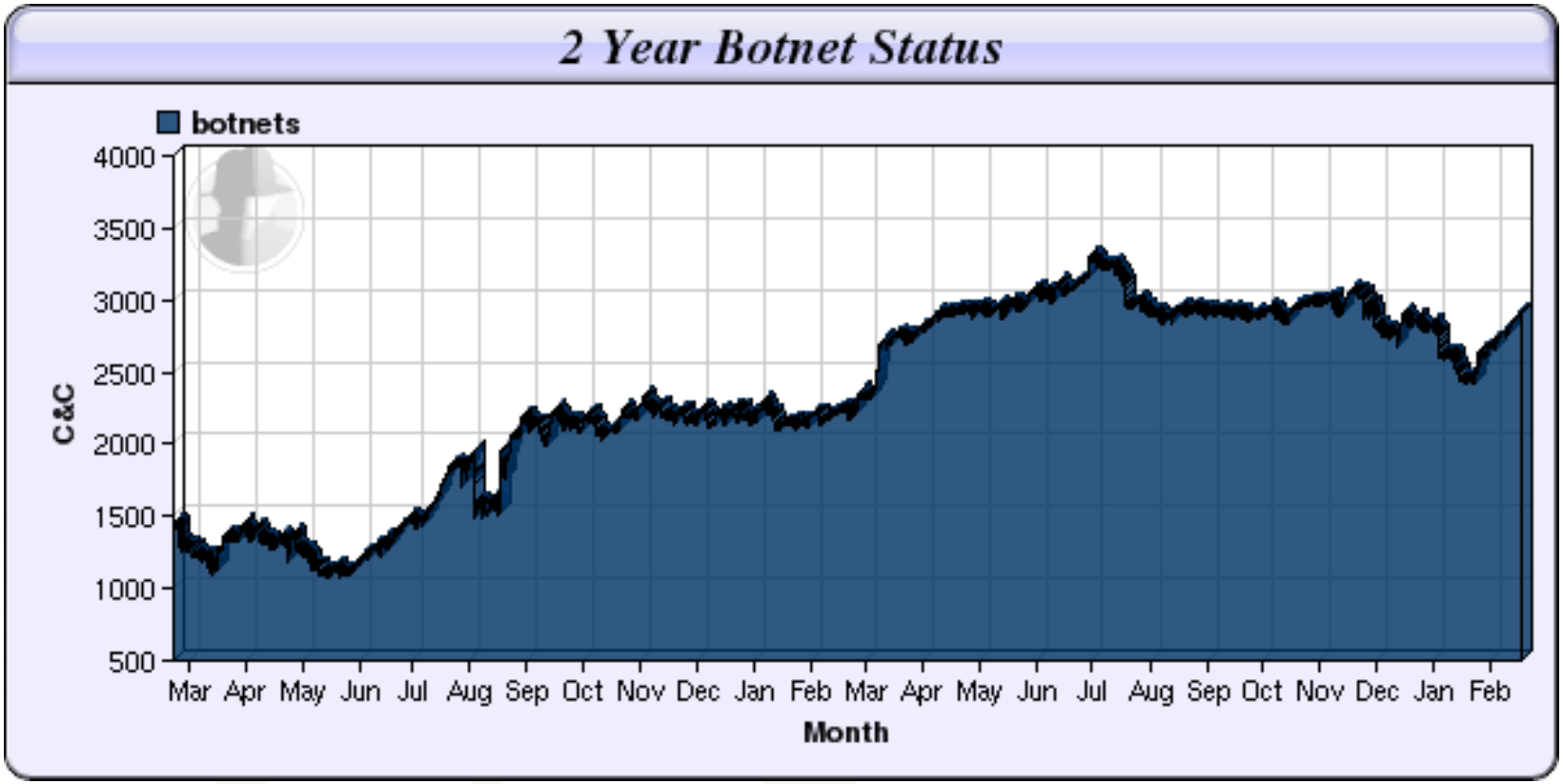
Designing a diverse, scalable network with no single points of failure…

Why your DNS needs to worry

- It's not just companies being targeted anymore!
- The DNS is growing more and more susceptible to attack through
  - Continued and larger scale DDoS attacks aimed at the Root and TLD operators
  - Regionalized attacks focusing on countries or specific governments / government agencies
- DNS is being victimized by new malicious activity (e.g.: Worms like Conficker)
- Small DNS networks being tasked with heavy load from new services (e.g.: URL shortening)

Botnets are here to stay

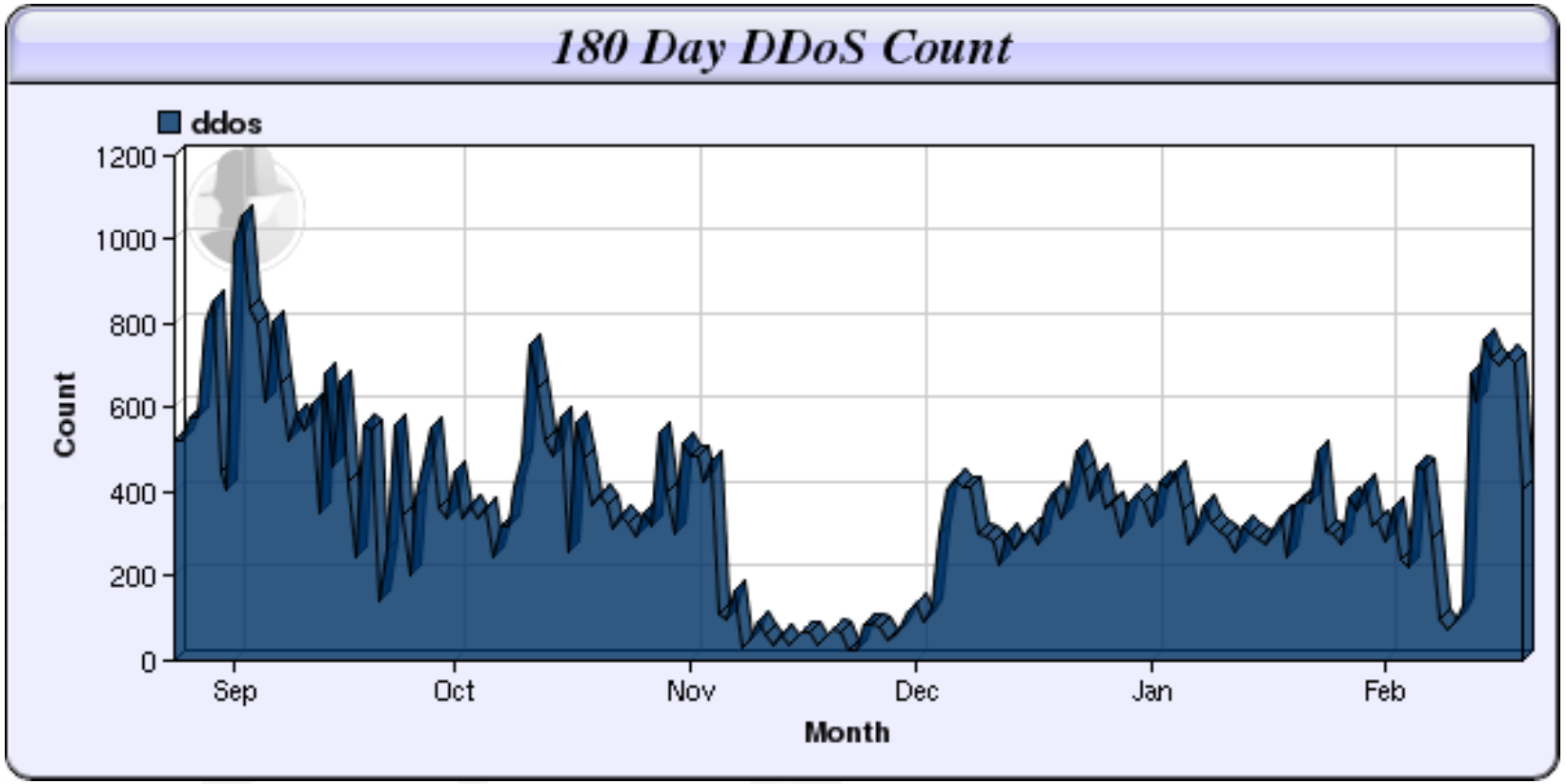
- Larger attacks, more sophistication



Source: http://www.shadowserver.org

DDOS Remains Serious Threat

- Increasing frequency and sustained activity

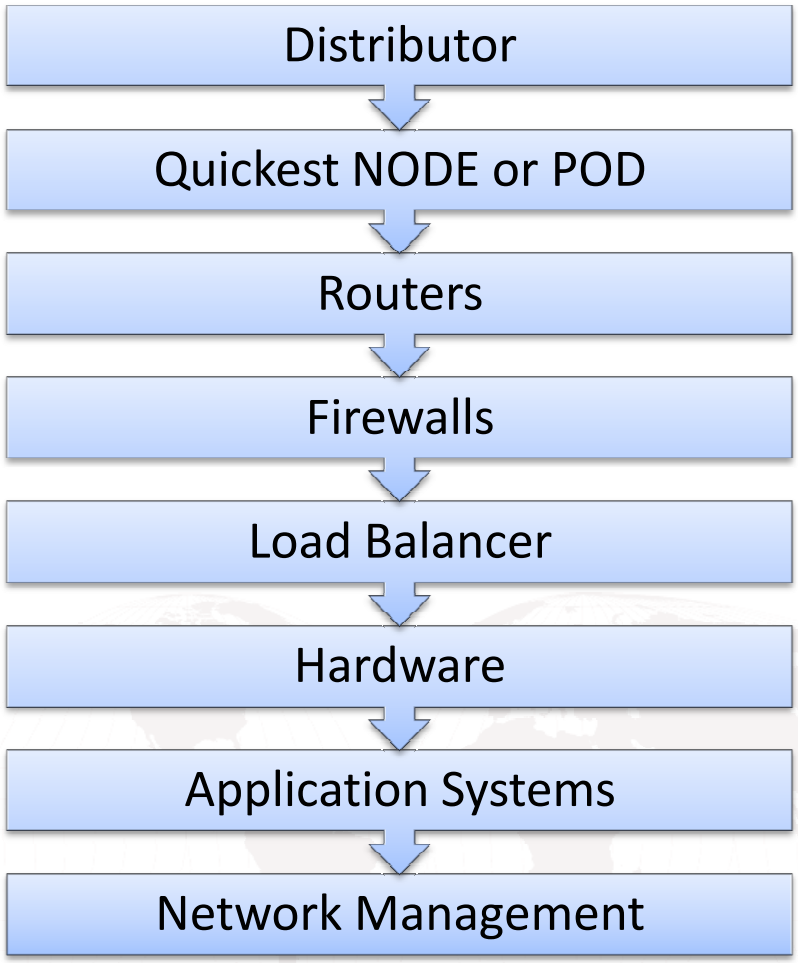


Source: http://www.shadowserver.org

Build your network with diversity

- No other Internet technology matters if users can not get to the Web site, or the e-mail can not be delivered.
- Treat your DNS like you do any other technology – **build it with redundancy, scalability and ensure no single points of failure**
- To deploy diversity across your DNS your options include:
  1. Internal development
  2. Adding an outsourced provider

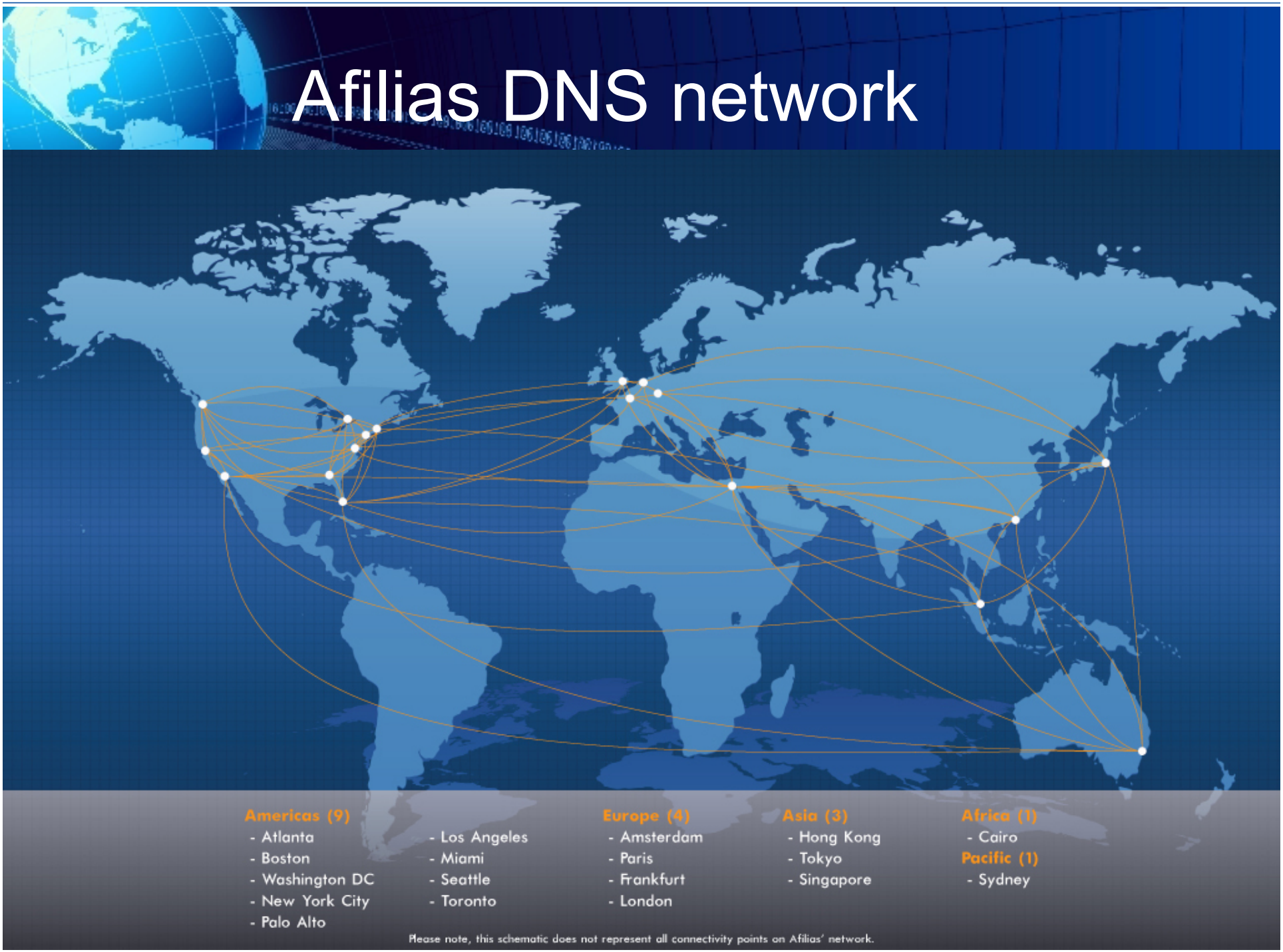
Implementing DNS Diversity



Diversity at all levels

- Multiple DNS providers
- Multiple types of DNS software (e.g. : Bind + NSD)
- Geographically diverse datacenters and NOCs
- Geographically diverse DNS node constellation on multiple continents
- Nodes configured with Anycast technology
- Multiple bandwidth providers w/ min. 1 gbps
- Multiple brands of hardware (e.g: both Cisco and Juniper Routers)
- No single OS or other software
- Diversity in Personnel and expertise

Afilias DNS network



About Afilias

- World class domain name registry services
- Scale/Knowledge/Experience of 14 million+ registrations & 15 TLDs
- Global DNS network available to TLDs + Managed DNS for end users

Generic & Sponsored TLDs

.info Where the World Goes for Information.

.org advance your mission

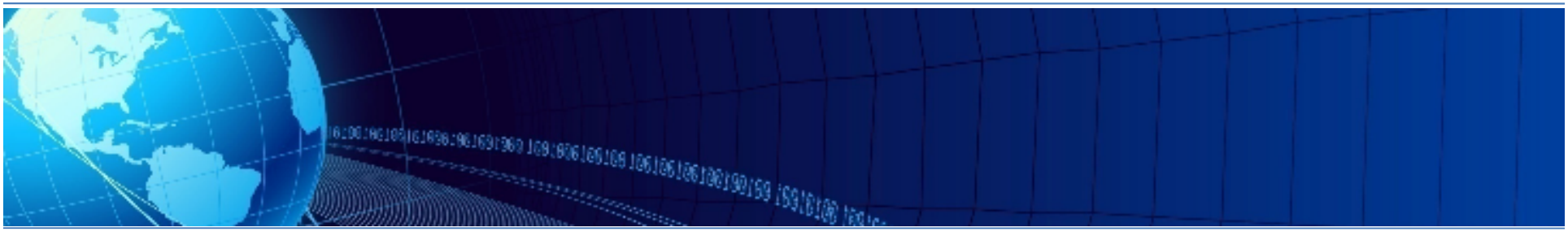
.mobi Internet Made Mobile

.Asia

.aero the domain of aviation

Country Code TLDs

.bz .NI .HN .GI .in .VC .LC .MN .SC .Me



Thank you!

Ram Mohan
Afilias
rmohan@afilias.info
www.afilias.info