Current Counter-measures and Responses by the Domain Name System Community

Paul Twomey
President and CEO

22 April 2007

APEC-OECD Malware Workshop
Manila, The Philippines

What we want you to do today

- Understand the risks to the Internet as we have known it for over 30 years
  - Security and stability of addressing and routing
- Become partners in managing these risks
- Understand how your interests are affected by ICANN’s policy work
- Get involved in creating the policy that sets how the Net connects you to your customers
- Understand the opportunities and risks the upcoming liberalising of gTLDs offers

Internet’s unique identifiers were coordinated through the Internet Address Naming Authority

Jon Postel
1943–1998

Need for change circa 1996–97

- **Globalisation** of the Internet
- **Commercialisation** of the Internet
- Lack of **competition** in the domain name space
- Trademark-domain name **conflicts**
- Need for a new model of **governance**

ICANN mission statement

- To coordinate, overall, the global Internet's system of unique identifiers, and to **ensure stable and secure operation** of the Internet's unique identifier systems. In particular, ICANN coordinates:
  1. Allocation and assignment of the three sets of unique identifiers for the Internet:
     - Domain names (forming a system called the DNS)
     - Internet protocol (IP) addresses and autonomous system (AS) numbers
     - Protocol port and parameter numbers
  2. Operation and evolution of the DNS root name server system
  3. Policy development reasonably and appropriately related to these technical functions

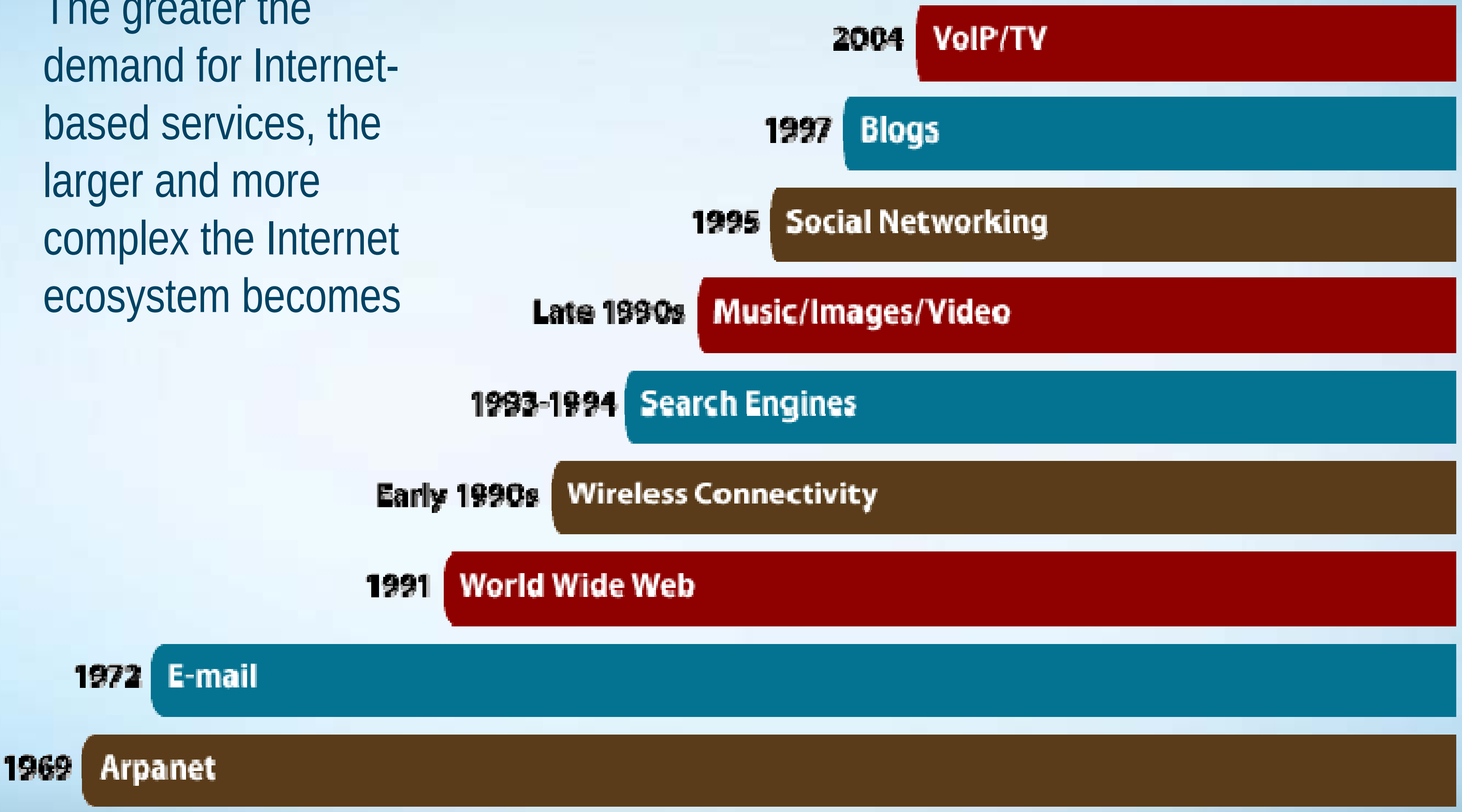
Principles of operation

1. Contribute to stability and security of the unique identifiers system and root management
2. Promote competition and choice for registrants and other users
3. Forum for multi-stakeholder bottom-up development of related policy
4. Ensure on a global basis an opportunity for participation by all interested parties

ICANN

From Thin Pipe to Fat Pipe

The greater the demand for Internet-based services, the larger and more complex the Internet ecosystem becomes



2004 VoIP/TV

1997 Blogs

1995 Social Networking

Late 1990s Music/Images/Video

1993-1994 Search Engines

Early 1990s Wireless Connectivity

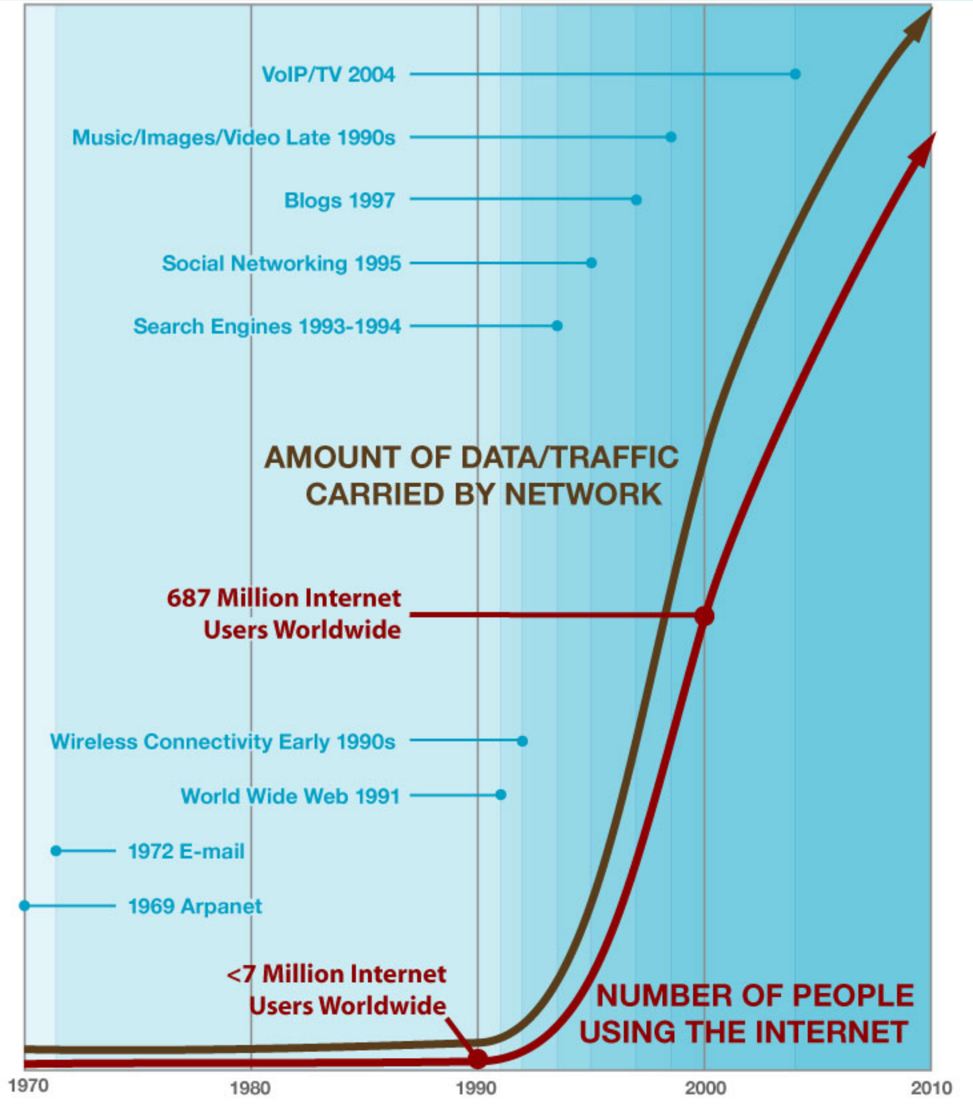
1991 World Wide Web

1972 E-mail

1969 Arpanet

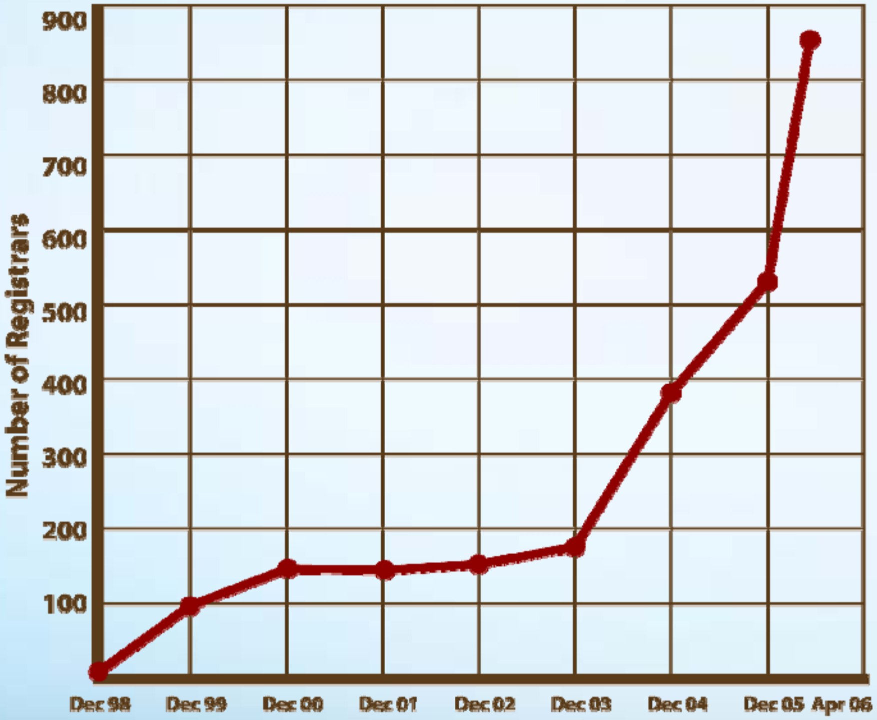
ICANN

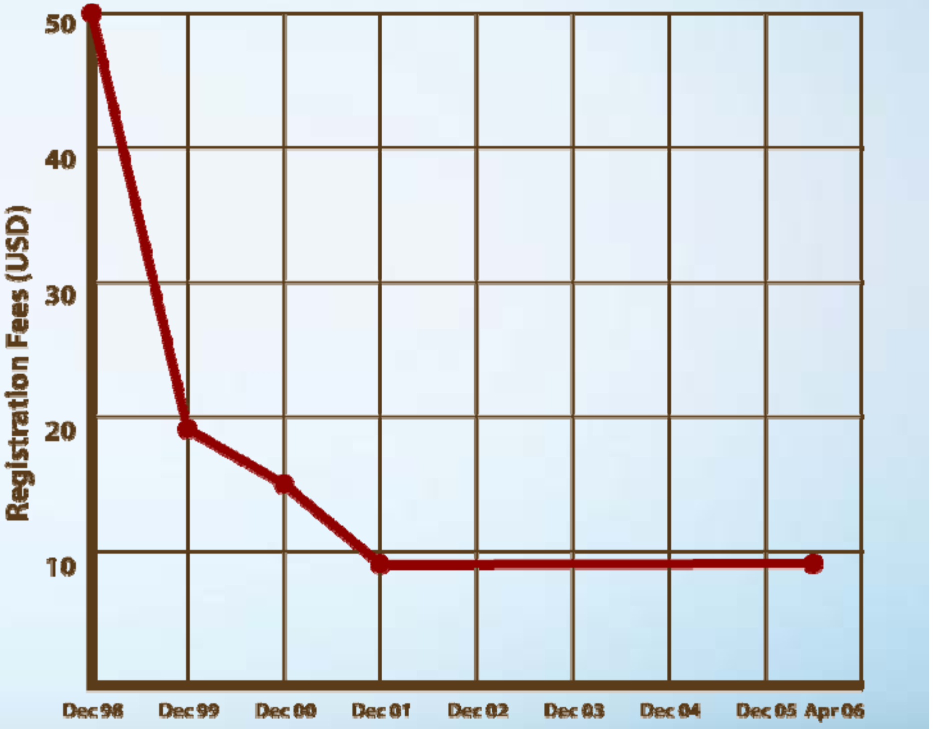
Explosion in Internet growth



Competition in the Domain Name Space

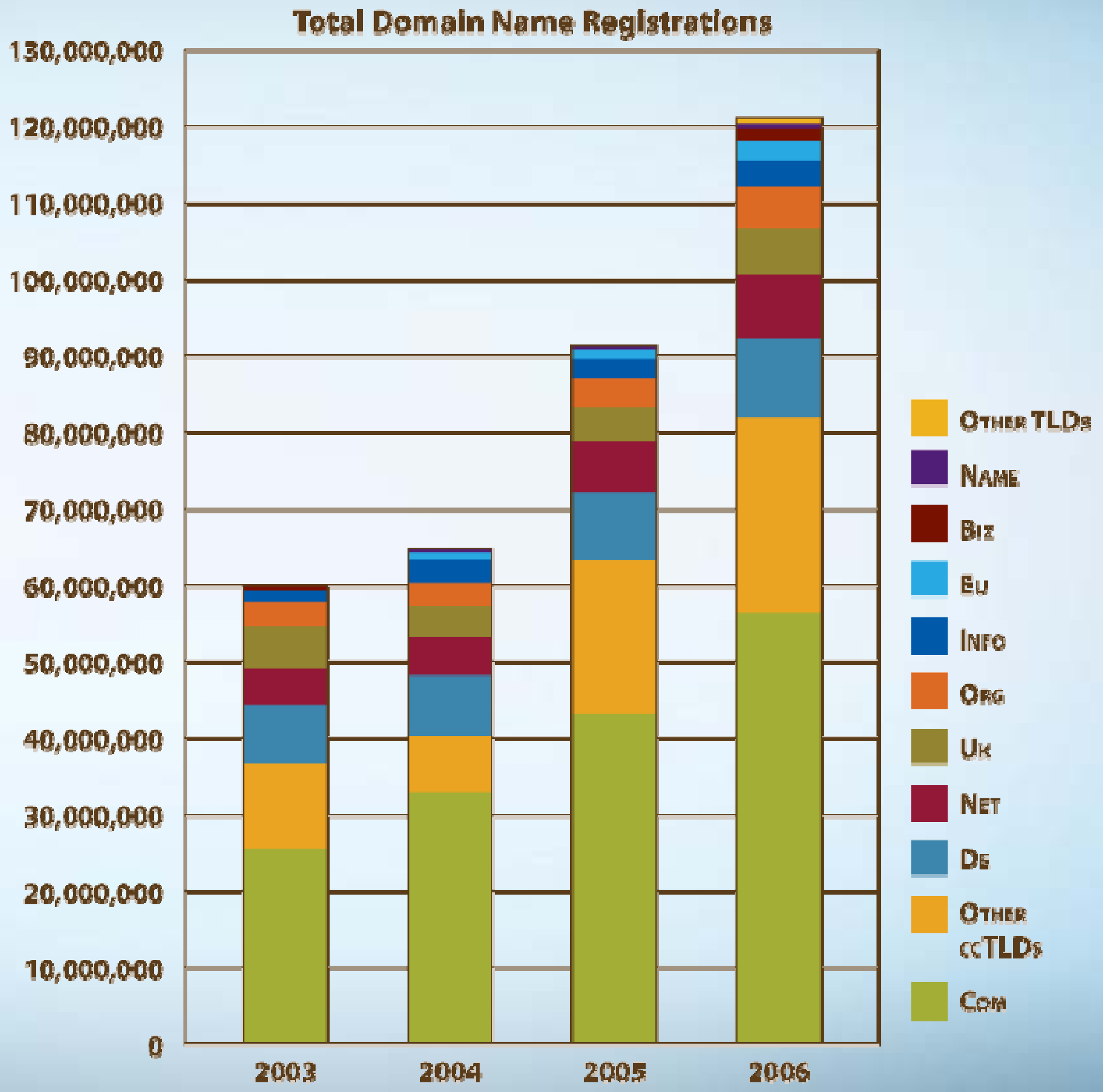
- ICANN introduced competition to the domain name space
- Registrars now have a market **and** a business
- Consumers have greater choice in price and services
- Domain name marketplace is even driving how we search – contextually as well as topically – and the scale of sites that can be searched
- Total registrars = **888** and counting





Snapshot of the domain name marketplace

More than **120 million** domain names registered globally today



The Internet ecosystem

Some organisations concerned with the Internet

Internet Governance Forum

W3C® World Wide Web consortium

IETF

Internet Architecture Board

ICANN

Internet Society™

ISO International Organization for Standardization

ICC™ International Chamber of Commerce™
The world business organization™

UNESCO
United Nations Educational, Scientific and Cultural Organization

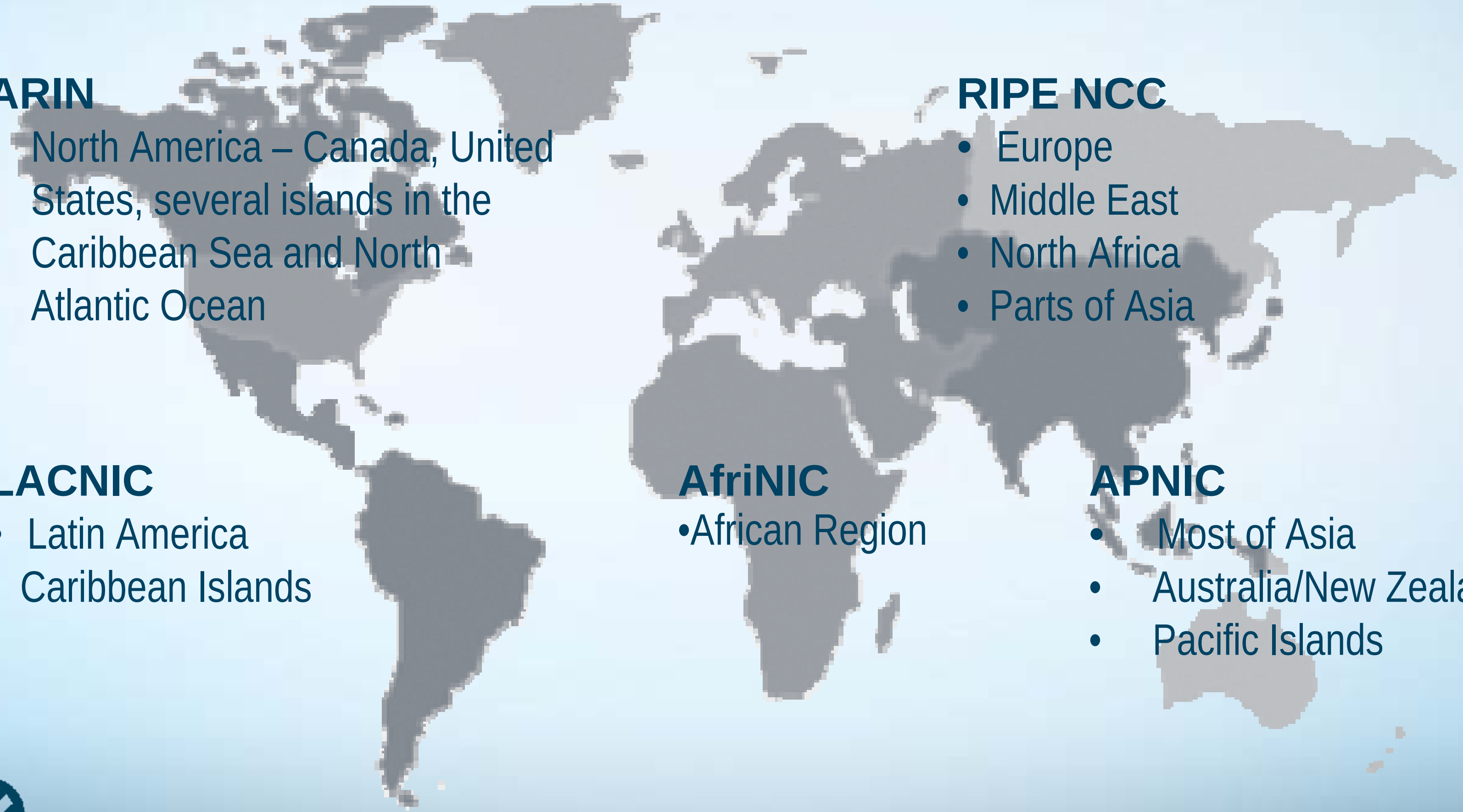
World Intellectual Property Organization WIPO

ICANN

The Internet ecosystem

Some organisations concerned with the Internet

Five Regional Internet Registries (AS and IP addresses)



ARIN

- North America – Canada, United States, several islands in the Caribbean Sea and North Atlantic Ocean

RIPE NCC

- Europe
- Middle East
- North Africa
- Parts of Asia

LACNIC

- Latin America
- Caribbean Islands

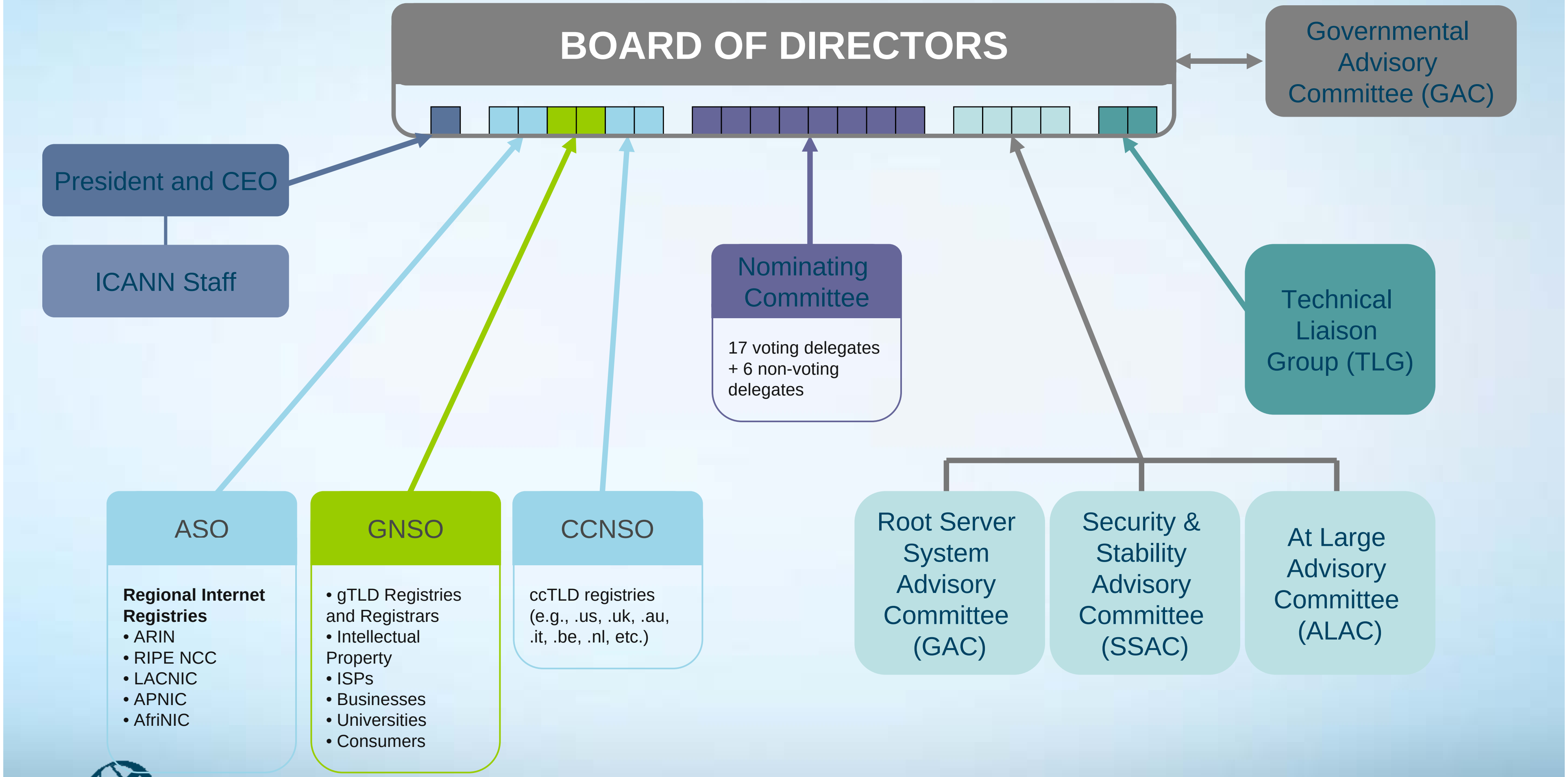
AfriNIC

•African Region

APNIC

- Most of Asia
- Australia/New Zealand
- Pacific Islands

ICANN’s community



BOARD OF DIRECTORS

Governmental Advisory Committee (GAC)

President and CEO

ICANN Staff

Nominating Committee

17 voting delegates + 6 non-voting delegates

Technical Liaison Group (TLG)

ASO

Regional Internet Registries
- ARIN
- RIPE NCC
- LACNIC
- APNIC
- AfriNIC

GNSO

- gTLD Registries and Registrars
- Intellectual Property
- ISPs
- Businesses
- Universities
- Consumers

CCNSO

ccTLD registries (e.g., .us, .uk, .au, .it, .be, .nl, etc.)

Root Server System Advisory Committee (GAC)

Security & Stability Advisory Committee (SSAC)

At Large Advisory Committee (ALAC)

What do we stand for?

- Ensuring a single, interoperable Internet
- All can express their own language and identity, **but**…
- All can access all others
- Creativity, development and growth are encouraged
- Security of the network is maintained to ensure confidence in the model
- Stability of the experience for application development and consumer experience
- Efficient deployment of resources in support of a global network
- All relevant stakeholders have a voice and role
- Encouraging innovation, particularly at the edge of the network

Internet community – a real phenomenon with world changing values

- Bottom-up technical policy-making and decision-making
- Participation open to all who wish to do so
- Legitimacy determined by open participation and the value of the contribution to the joint effort
- Consensus-based decision making
- Cooperation, coordination and consultation among participants and groups pushing initiatives forward
- Yet, **very** spirited and blunt public debate
- Private agreement or contract approach to creating and managing linkages among and to the network
- Global efficiency in the allocation of resources, such as Internet Protocol addresses

Where stakeholders find common ground

- Increasingly, ICANN finds itself one of the few forums in which these issues can be raised so that solutions can be found and implemented within the Internet community

Internet infrastructure threats

1. Physical disruption of major lines and switching centers
2. Loss of routing infrastructure continuity and/or fidelity
3. Loss of DNS service continuity and/or fidelity
4. Flooding of network or specific sites, i.e., denial of service attack

Not all Internet-based systems are Internet infrastructure…

Routing infrastructure

- Status
  - Routing information is maintained in routing registries
    - These are reasonably well protected against physical attack
  - Inputs to the routing registries can be compromised
  - False routing information can be inserted
- Potential protection
  - Secure BGP has been defined and implemented

Does not look feasible – too much hardware required

Routing security does not fall directly within anyone's charter. What is the financial sector's role in engaging ISPs?

DNS infrastructure root servers – status

- Root servers point to top level domains
  - 20 generic TLDs (gTLDs) – .com, .org, etc.
    - U.S. Government has .gov and .mil
  - 243 country codes (ccTLDs) – .de, .jp, .uk, etc.
- Root servers are heavily replicated
  - 13 independent businesses
  - Many-fold replication and distribution

ICANN

DNS infrastructure root servers – threats

Threats

- Loss of Service
  - Network outage
  - Machine or site failures
  - Overwhelming traffic (denial of service attack)
  - Business failure
- Hijacking
  - Cache poisoning
  - False registration
  - Fake zone transfer
  - Fake registrar-registry interaction
  - Private roots
- Loss of coherence
  - Unauthorized roots and TLDs
  - Private character set extensions

Countermeasures

- Excess capacity
- Distribution, replication
- Strong connectivity
- Multiplicity of businesses
- DDoS counters (long term)

- Protocol changes, DNSSEC
- Tight registrar controls
- TSIG (crypto)
- Crypto authentication
- DNSSEC

- DNSSEC; policy/political pressure
- DNSSEC; policy/political pressure

Lots of work is under way. But threats are growing and this will take more time and money than many expect

System threats

- Denial of service attacks target high-value sites
  - DNS servers are among the obvious targets
  - These will get more sophisticated
  - Action is required – see later slides
- Domain and address theft is growing
  - Spammers like to hide their identity
  - The legal framework doesn't provide protection

Address theft, per se, is not actionable(!)
Should individual sectors lobby for this (internationally)?

The denial of service problem

- Denial of service attacks are increasing
  - This will get worse – probably much worse
- Law enforcement is important but necessarily at the wrong end of the problem
- Technical changes in the Internet would help a lot

ICANN

Distributed denial of service

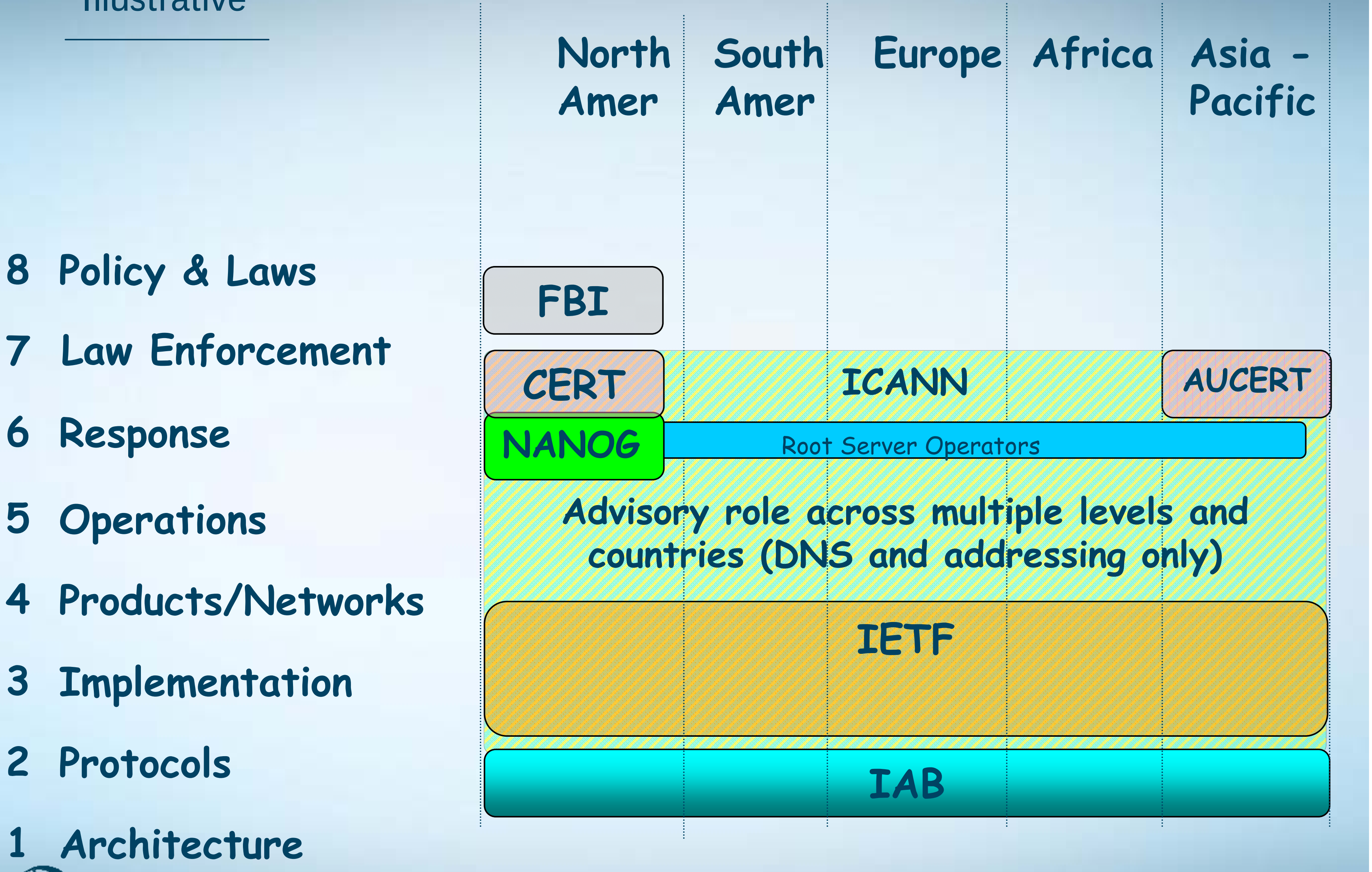
- On 6 February 2007 – most visible since 2002 attack but not as comprehensive as amplified DDoS attack on TLDs of 2006
- Six of the 13 root servers that form building blocks of the Internet were affected – two badly
- The attack highlighted the effectiveness of Anycast load balancing technology
- More analysis is needed before a full report on what happened can be drawn up – reasons behind the attack are unclear – a wake-up call
- Root server operators worked together in a fast, effective, and co-ordinated effort
- Recent SSAC recommendations for improving the security of the domain name system still need to be followed through – other measures should also be considered
- Coordination and preparation were key
- Did you notice?

ICANN

ICANN purview

- ICANN strives to achieve coherence, stability and security
- Almost all of the operational details are carried out by others, but
  - The IANA (Internet Assigned Numbers Authority) function is within ICANN
  - L root
- Join us in both dialogue and new funding mechanisms – security foundation/gold star service, etc.

Illustrative



North Amer

South Amer

Europe

Africa

Asia - Pacific

8 Policy & Laws

7 Law Enforcement

6 Response

5 Operations

4 Products/Networks

3 Implementation

2 Protocols

1 Architecture

FBI

CERT

ICANN

AUCERT

NANOG

Root Server Operators

Advisory role across multiple levels and countries (DNS and addressing only)

IETF

IAB

DDoS – some technical approaches

- Identification of sources of traffic
  - Tighten the routing security
- Refashion the protocols to know the identity of senders of traffic
- Distinguish between well managed computers on well managed networks vs others
  - “Well managed” means they aren’t zombies and their configuration is checked regularly
- Well managed networks quarantine computers which appear to be infected or misbehaving
- Well managed networks report misbehaviors and accept reports of misbehaviors
- Traffic among well managed networks gets preference

DDoS – customer approaches

- Pressure on the vendor to supply machines that are safe out of the box
- Establishment of an ethic that machines should be safe – it's the vendor's problem, not the user's

Some ICANN initiatives

- Agreement on formal relationship between Root Server Operators and ICANN
- Tightened procedures for distributing changes to the root zone (CRADA report)
- DNSSEC deployment analysis and road map
- IPv6 transition road map (re DNS)
- DNS service robustness enhancements
- Best practices for ccTLDs

Whois database

- Some businesses see a strong need for unrestricted access to Whois information to
  - Identify cybersquatters and domain infringement
  - Investigate online fraud and phishing
  - Manage domain names and intellectual property
  - Conduct e-commerce by researching other online entities
- One major hotel chain recorded 100-plus new domain names registered in its name – or a version thereof – every day
  - Confusingly similar names led to pay-per-click sites
- Full registration data would help legitimate businesses shut down fraudulent domains

Whois concerns

- ICANN’s Security and Stability Advisory Committee (SSAC) tracking correlation between email addresses placed in Whois and incidence of spam
  - Malware predators use spamming techniques
  - Spamming uses Whois
- But, on the Internet, there is never a direct route and thus never a direct cut-off to a particular problem
- A logical approach in one area of the Internet creates problems in another area

Whois policy process

- Whois issues are being addressed through the General Names Supporting Organisation’s (GNSO’s) policy development process (PDP)
- Numerous opportunities for public review and comment

Recent public comments on Whois

- Many support full Whois access –
  - Businesses and trade organisations
  - Nonprofits engaged in fighting fraud
  - Law enforcement agencies
- Opposition to Whois from other advocacy organisations, some government agencies, some Internet users

Different views of Whois

- Privacy commissioners in the European Union
- Attention in public comments to restricted access, privacy and accuracy of the data

Enforcement of existing Whois policy

- That will remain the case until the Board approves any new policy, if any

Next steps on Whois

- ICANN staff is preparing notes for the GNSO Council on the Task Force Recommendations to –
  - Identify issues for clarification
  - Identify issues for further discussion
  - Identify potential implementation issues
  - Suggest a framework for further development of the proposal

Task force recommendation (1)

- Nonbinding recommendation to GNSO Council
- Operational Point of Control (OPoC) proposal –
  - Registrants could use an OPoC in place of the current administrative and technical contact details
  - If there was an issue with the domain name, the OPoC would contact the registrant

Task force recommendation (2)

- OPoC includes –
  - Improved procedure for correcting inaccurate Whois data
- OPoC does not include –
  - Procedure for access by rights-holders, law enforcement – suggests use of best practices for dealing with requests

Next steps

- GNSO's Whois Task Force presented Final Task Force Report to GNSO Council March 2007
- Council will send its own recommendations to ICANN Board for consideration and decision.
- ICANN Board will review GNSO recommendations, 2nd/3rd quarter of 2007

New generic top-level domain timetable

- Next working group report to Lisbon meeting in late March
- Potentially GNSO Policy Development Process may be completed by July meeting in Puerto Rico
- Policy may be concluded by the end of the 3rd Quarter 2007
- Next round of new gTLDs in early 2008?

Consider the impact of –

- Unique industry TLDs
- Industry cross-certified
- DNSSEC
- Other anti-phishing tools?

Thank You

www.icann.org