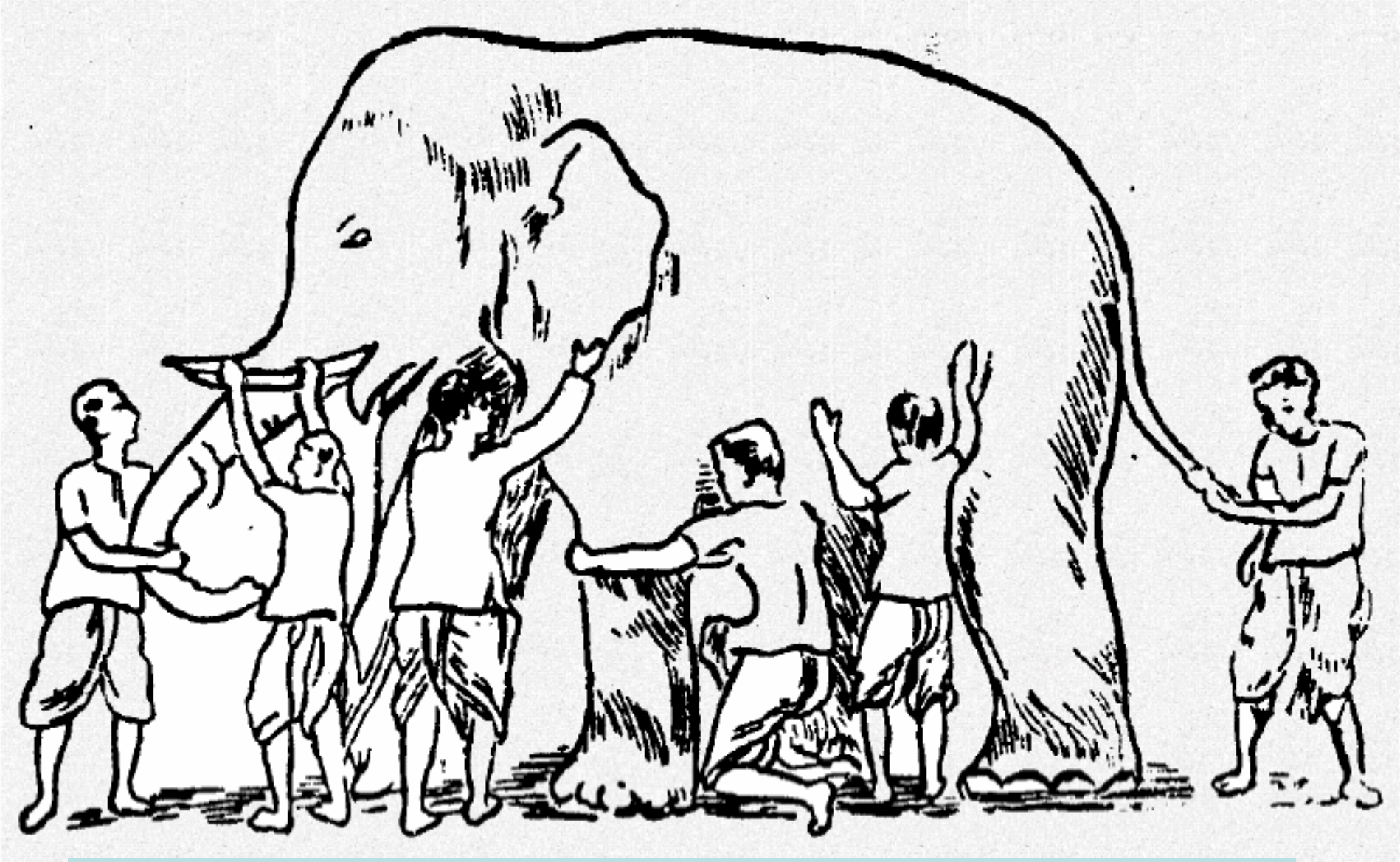
# A Methodology for Measuring the Capability to Counter Cybersecurity-related offences

Benoit MOREL

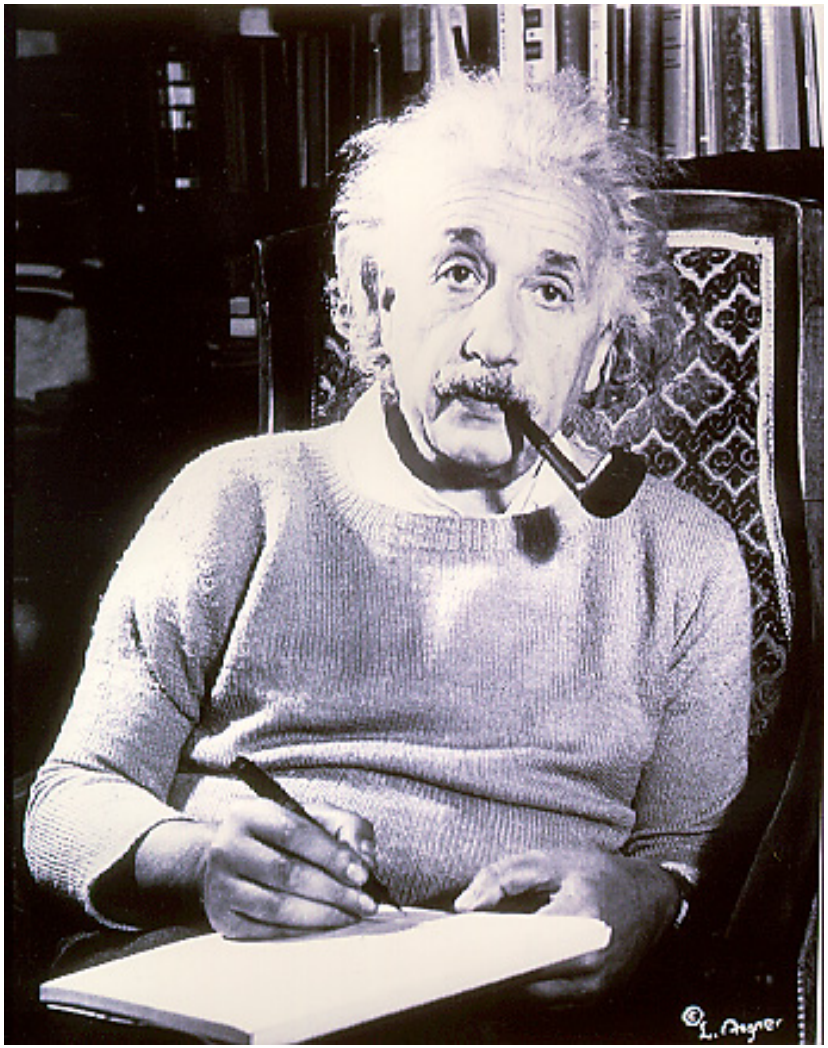
Carnegie Mellon University



# Cybersecurity: a different thing for different people

# Different levels of Cybersecurity

- Law enforcement
- Economic problem
- IT problem, i.e. rooted in the technology of computers
- National security problem

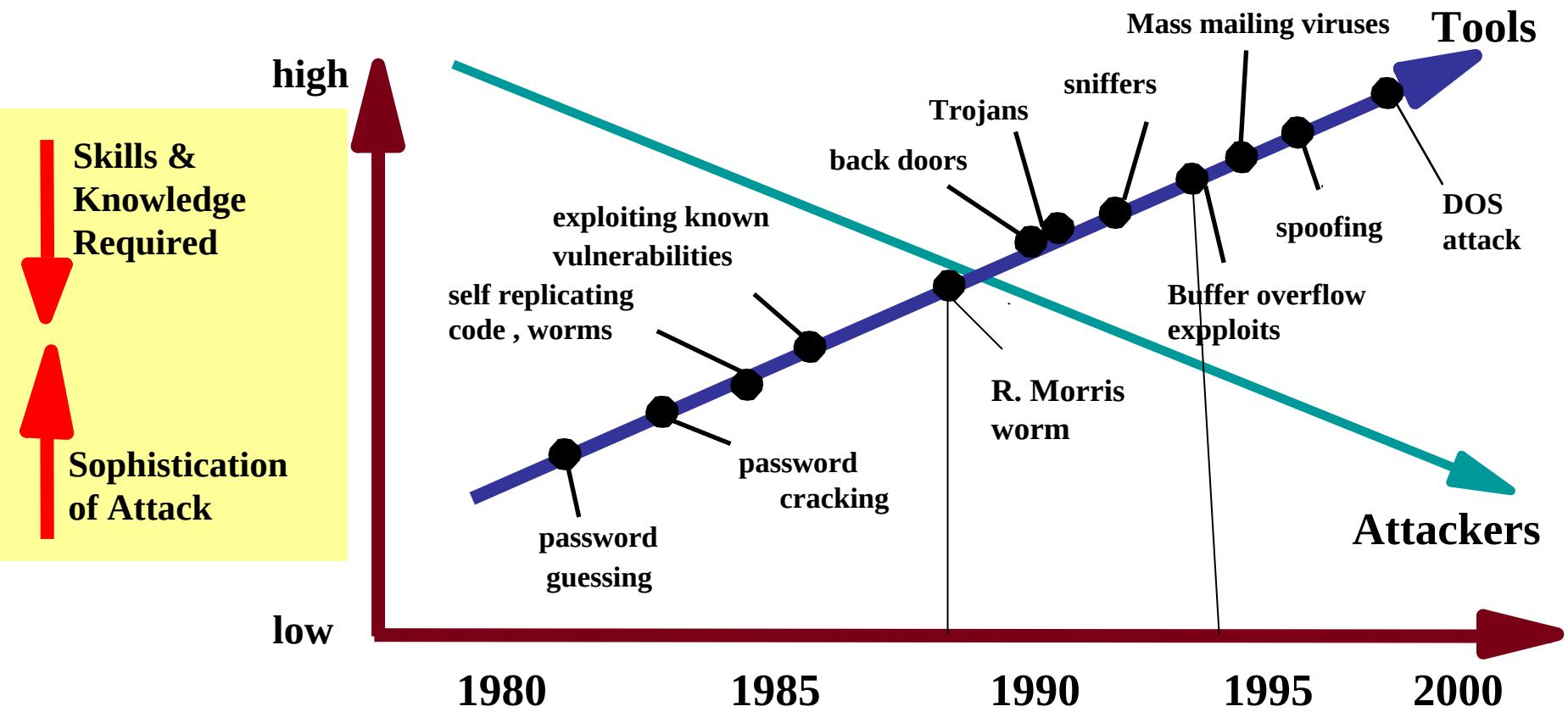


**A model must be as simple as possible, but not *simpler***

**Einstein, 1879 -1955**

# The Past

## Effort Needed to Disrupt Systems has been Decreasing → 200x



# Cyber threat environment
# *The past*

- When hacking was glamorous:
  - Virus/Worms
    - From R. Morris worm (1988), to I  love you
  - Buffer overflow vulnerability (1994, Aleph one, Dr Mudge)
  - Black hat meetings, DefCon
- Distributed Denial of Service Attack (DDOS)
- Trojans and Backdoors (back orifice, cult of the Dead Cows)
- Phishing (419)
- Multiplicity of tools (“Hacking Exposed”, G. Kurtz et al) and “script kiddies”.

# Cyber threat environment
# *The present*

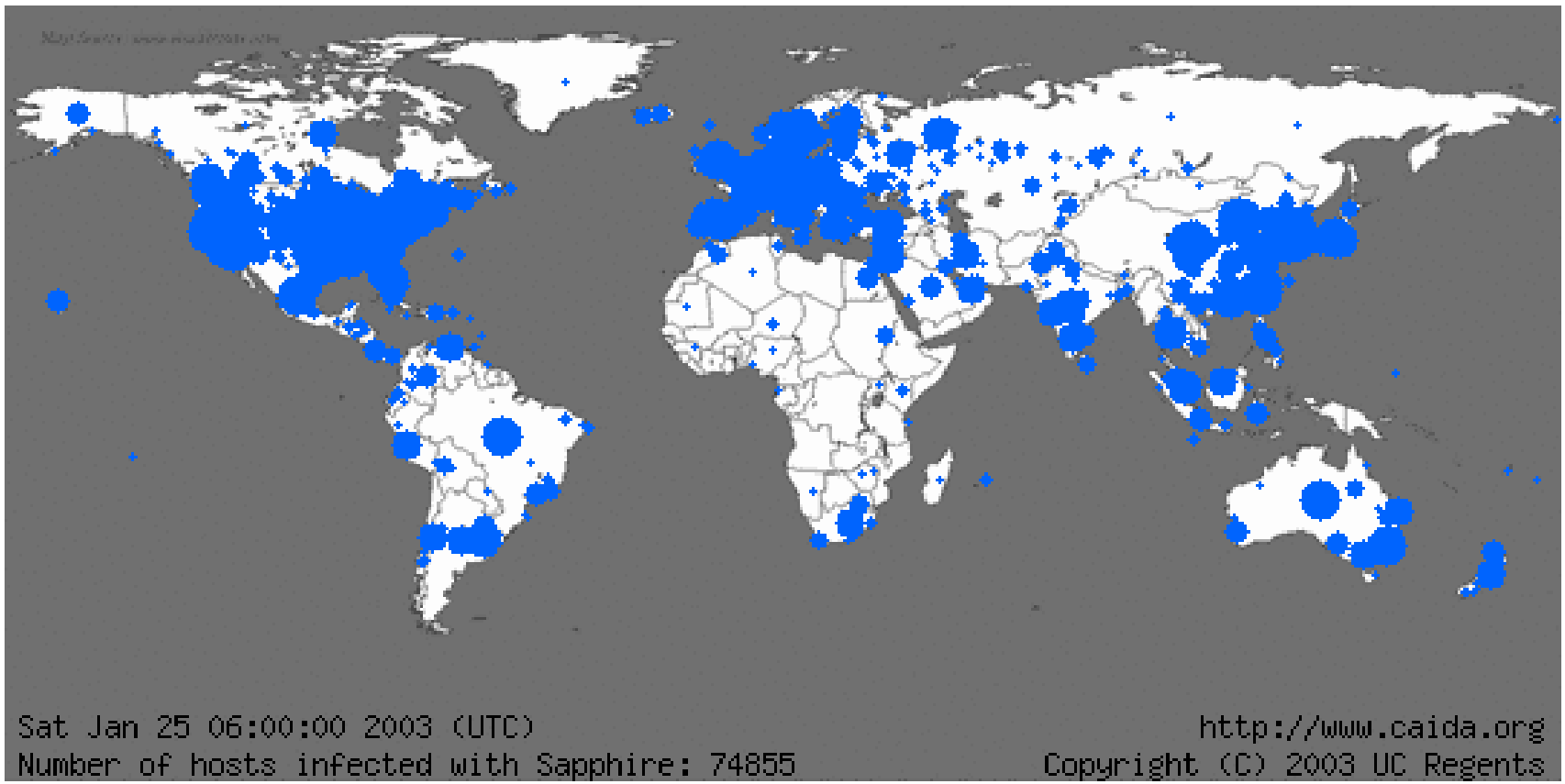
- Cybercriminals are *real* criminals
- Spam (for profit)
- Sophisticated Phishing in a variety of language

- Today's trends:
  - More ominous: more invisible attacks (key loggers,
  - Large scale: botnets
  - Flash threats (Slammer, Witty, …)

**The present**

# Impact of Slammer

- Flooded the Internet with traffic
- Slowdowns reported across the world



# No more guns blazing for silent thieves

By Daniel Thomas

Published: May 10 2006 10:03 | Last updated: May 10 2006 10:03

- Recent research by KPMG shows that in the UK  financial crime – including money laundering, payment card and online banking fraud – rose almost tenfold in one year, from £37m in 2004 to £360m last year, and figures for the US and Asia are just as bad.
- But if crooks are getting smarter, so are the banks.

# Bots

# Problems with the current system:

- All airlines rely on one of 4 Global Distribution Systems
  - If one goes down, it brings down at least 25% of the airline industry with it
  - All of the GDSs are interconnected, so problems could spread quickly from one to another
- Privacy: The GDS also works for your competition

# The Sabre Global Distribution System

- The *Sabre*® global distribution system is the world's largest electronic travel reservation system.
- The *Sabre* system is a primary component for travel and transportation information for over 50,000 travel agencies, major travel suppliers, Fortune 500 companies and travel web sites around the globe.
- The *Sabre* system provides users with schedules, availability, pricing, policies and rules, as well as reservation and ticketing capability for travel suppliers including:

- Airlines
- Car Rental Companies
- Ferry Companies
- Hotel Properties
- Rail Operations
- Tour Operators
- Event Tickets
- Cellular Phone Rentals
- Sightseeing
- Travel Insurance
- Theme Parks
- Independent Resorts
- Condos
- Campgrounds
- Charter operations
- Golf Course Tee Times

# Cyber threat environment
## *The future*

- Attacks on critical infra-structure?
- Very large scale attacks?
- E-Pearl Harbor?
- Cyber-terrorism? (Airplanes, drug manufacturing, hospital monitoring, etc…)

# Forces of change which exacerbate cybersecurity problems

- Technological changes:
  - Wireless
  - Omni-cyberization (PDA, RFID, sensors and scada)
  - VoIP
- Globalization

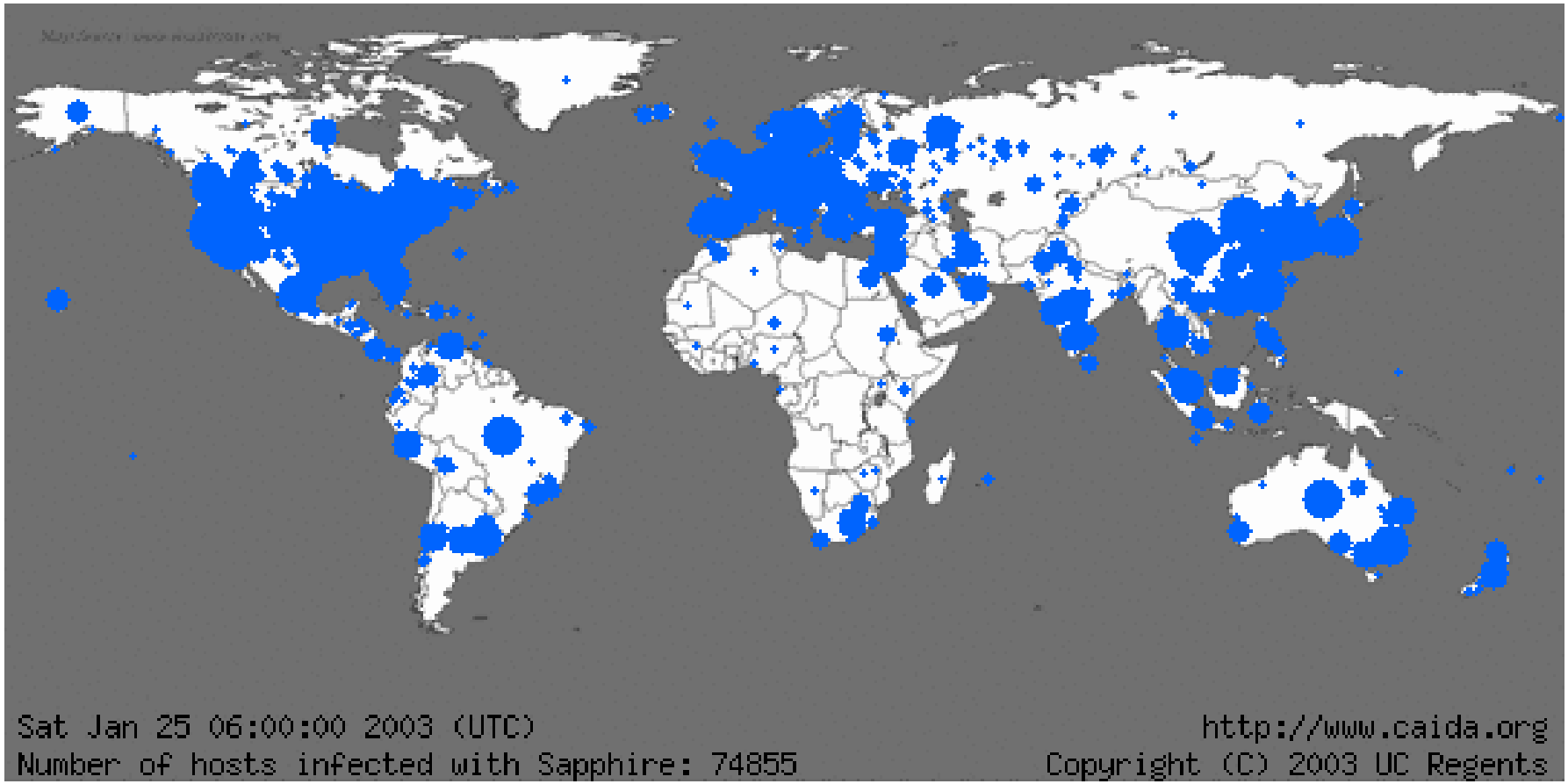
# VoIP could provoke 'electronic Pearl Harbor'

- Leaping into cheap Internet telephony before looking at the security risks could create a lot of risk for companies.

- A widespread IT security incident [will] occur in the next two years, possibly as a result of companies hastily moving to voice over Internet Protocol technology without carrying out the necessary due diligence.

- Source: David Lacey, director of information security for the Royal Mail Group, quoted in C|net news, March 17, 2005 11:17 AM

# Globalization of cyberization




- http://www.caida.org/tools/visualization/mapnet/

# Need for indicators of cyber-readiness

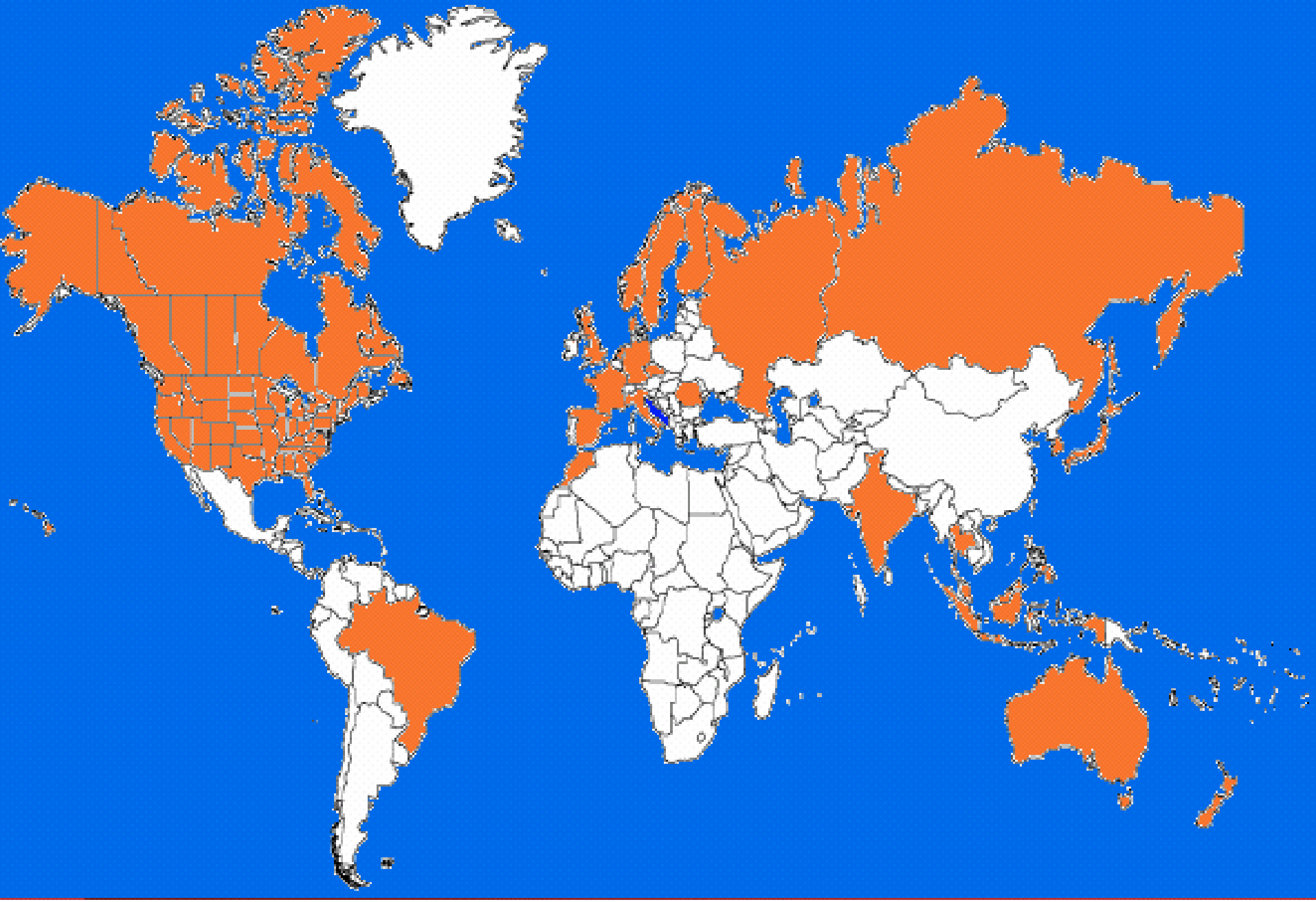
- Many new players on the internet.
- With them come potentially new threats and cyberization leads to expose assets they need to protect.
- Cyberizing today is significantly more hazardous than before
- Indicators gauging the degree of readiness would be useful to everybody.

# Candidate indicators

- Are best practices enforced?
- Is there a national CERT?
- What constitute a cybercrime in that country?
- Does a lot of malicious code originate from that country? (Virus factory…)
- Does the government put adequate resources into cybersecurity?

# Candidate indicators

- Has the nation joined the anti-spam pact?
- Number of private networks (NAT level)
- Degree of cyberization of infra-structure
- What are the ISPs?
- Does a nation belong to the 24/7 network?



**24/7 Network as of May 2003**

# Futility of indicators

- What these indicators tell us:
  - What the government cyberpolicy is
  - What is the degree of cyberization of the country

- What these indicators do not tell us:
  - Degree of expertise in the country, and how it is distributed
  - Cybercriminals are often the best experts …
  - A good cyber-defender should know more than the cyberattacker

# Diversity of situation

- Cybersecurity a concern for every nation, no exception
- Cybersecurity: each nation is a special case, no exception…

- Culture of cybersecurity a useful concept?

# “Culture of cybersecurity”

**General Assembly**

Distr.: General
31 January 2003

**Fifty-seventh session**
Agenda item 84 (*c*)

**Resolution adopted by the General Assembly**

[*on the report of the Second Committee (A/57/529/Add.3)*]

**57/239. Creation of a global culture of cybersecurity**

# Elements for creating a global culture of cybersecurity

- *Awareness* of the need for security of information systems and networks and of what they can do to enhance security;
- *Responsibility* for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;
- *Response*: Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.

- ***Ethics***. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;
- ***Democracy***. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;
- ***Risk assessment***. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk;
- ***Security design and implementation***. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;
- ***Security management***. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;
- ***Reassessment*.** Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

# The real challenge

- Cybersecurity is complex
- There is no good indicator to measure “expertise”
- Dissemination and maintenance of *technical* expertise worldwide is what matters
- Instinct is to create National CERT: is that the solution?

# The US model

- US is the state of the art in cybersecurity
- No national cybersecurity agency with clout in US
- US cyberdefense provided by a chaotic self organized system that defies all simplifications (networks of cybersec professionals, consortia, institutions (SANS, US/CERT, ….), ISAC,…

- US government as example?

# IPUTER SECURITY REPORT CARD

March 16, 2006

## GOVERNMENTWIDE GRADE 2005: D+

| | 2005 | 2004 | | 2005 | 2004 |
|---|---|---|---|---|---|
| AGENCY FOR INTERNATIONAL DEVELOPMENT | A+ | A+ | DEPARTMENT OF COMMERCE | D+ | F |
| DEPARTMENT OF LABOR | A+ | B- | DEPARTMENT OF JUSTICE | D | B- |
| SOCIAL SECURITY ADMINISTRATION | A+ | B | NUCLEAR REGULATORY COMMISSION | D- | B+ |
| OFFICE OF PERSONNEL MANAGEMENT | A+ | C- | DEPARTMENT OF TREASURY | D- | D+ |
| ENVIRONMENTAL PROTECTION AGENCY | A+ | B | DEPARTMENT OF ENERGY | F | F |
| NATIONAL SCIENCE FOUNDATION | A | C+ | DEPARTMENT OF VETERANS AFAIRS | F | F |
| GENERAL SERVICES ADMINISTRATION | A- | C+ | DEPARTMENT OF HEALTH AND HUMAN SERVICES | F | F |
| NATIONAL AERONAUTICS AND SPACE ADMINISTRATION | B- | D- | DEPARTMENT OF THE INTERIOR | F | C+ |
| SMALL BUSINESS ADMINISTRATION | C+ | D- | DEPARTMENT OF DEFENSE | F | D |
| DEPARTMENT OF TRANSPORTATION | C- | A- | DEPARTMENT OF STATE | F | D+ |
| DEPARTMENT OF EDUCATION | C- | C | DEPARTMENT OF HOMELAND SECURITY | F | F |
| HOUSING AND URBAN DEVELOPMENT | D+ | F | DEPARTMENT OF AGRICULTURE | F | F |

# National CERTs as solution!

- For developing countries, no better model
  - Advise, education must know about Private networks
  - Must know about managing a national network
  - Must be abreast of the latest vulnerability, worms, etc..
- Has to be invented
- Skill for that exists in the US (among other places)
- …but it has to be found and gathered
- Repository of knowledge: scholars, “practitioners”, Hackers, …

# The international community will eventually have to address fundamental issues

- Worldwide defense against worldwide threats: Flash threats, Botnets, etc…
- Need to revisit fundamentals of the internet like BGP, protocols

# *Interior vs. Exterior Routing Protocols*

**Interior Gateway Protocols (IGP) : inside autonomous systems**

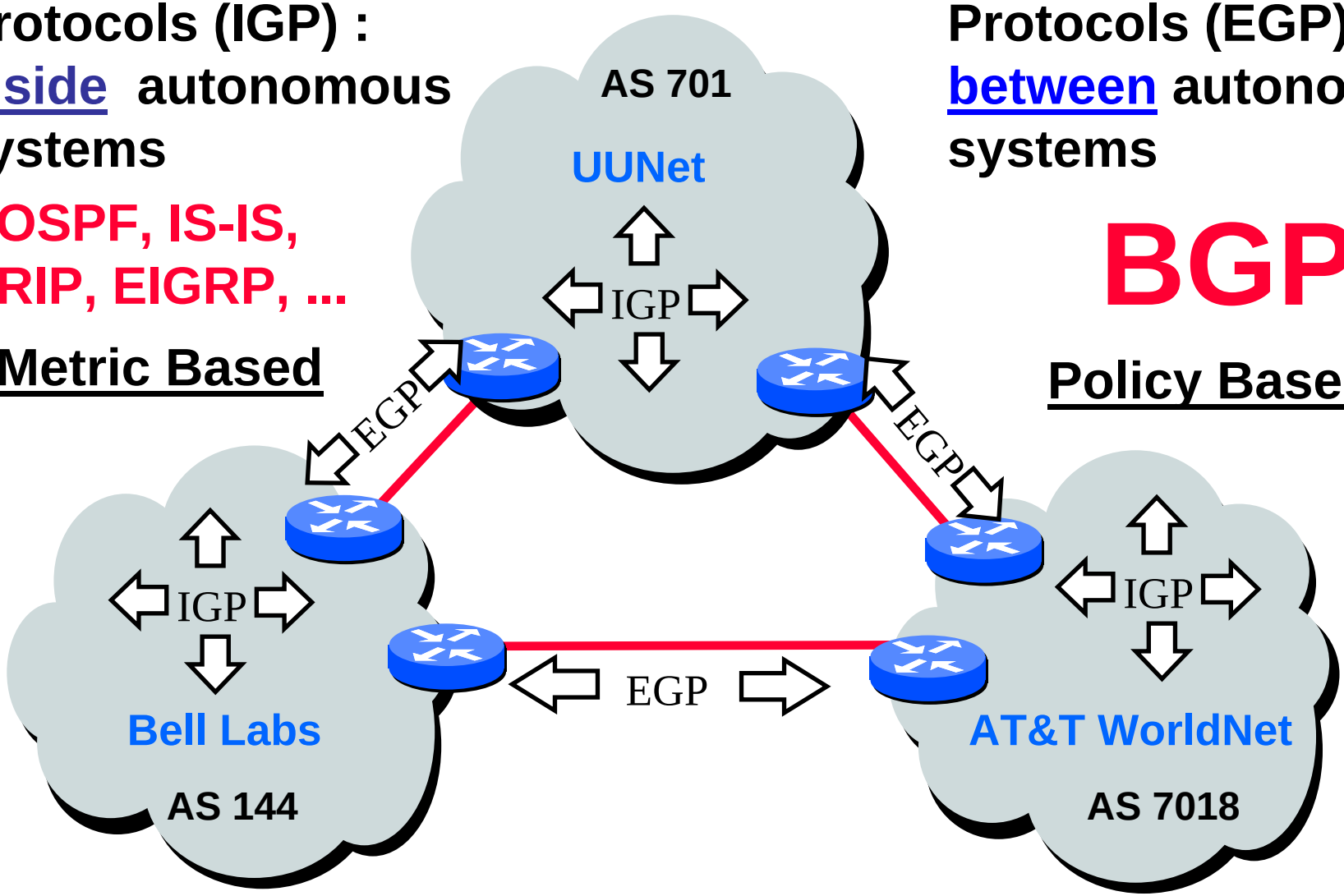
**OSPF, IS-IS, RIP, EIGRP, ...**

**Metric Based**

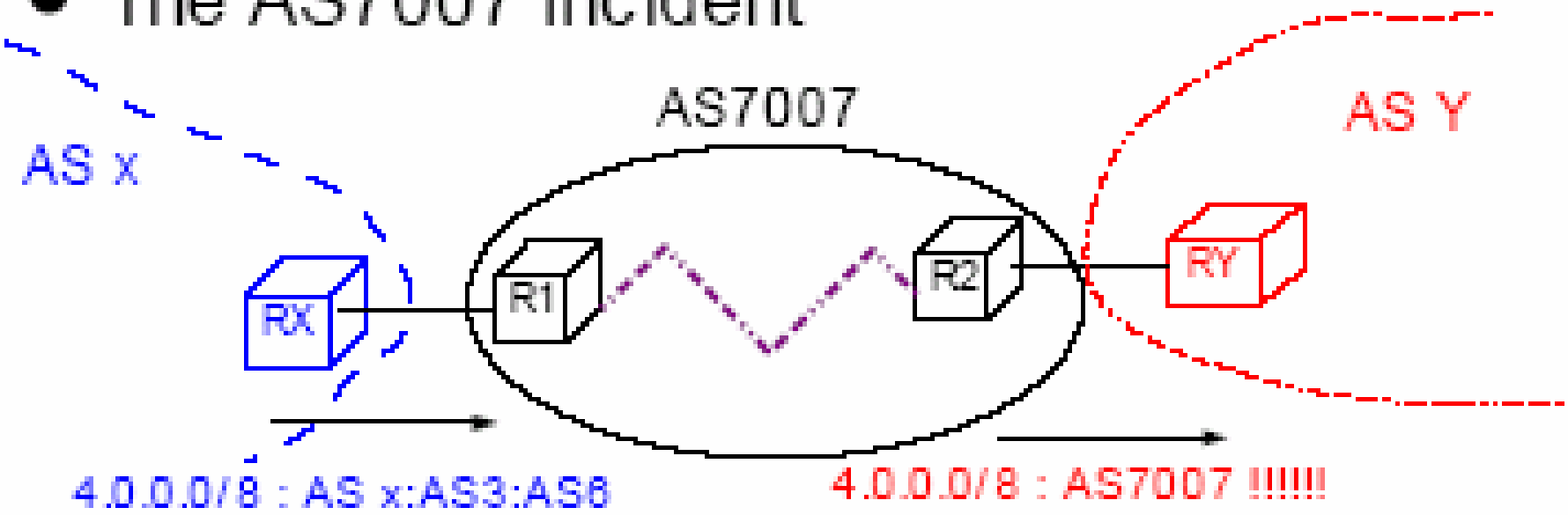
**Exterior Gateway Protocols (EGP) : between autonomous systems**

**BGP**

**Policy Based**



- The AS7007 incident




- A single configuration error in two routers
  - All routes learned from ASX on R1 were redistributed to R2 via IGP and R2 announced them to ASY
  - Consequence
    - AS7007 advertised routes that almost all IP addresses were belonging to AS7007
    - These routes were shorter than the real routes ...
  - Two hours of disruption for large parts of the Internet !

*Jon Postel*, Director of the Computer Networks Division at the Information Sciences Institute at the University of Southern California, took over stewardship of the RFCs in the early 1970's. He served as the official RFC Editor for a quarter of a century, and authored and led development of more RFCs than anyone else. He also helped develop many of the Internet protocols, including the *Domain Name System*, File Transfer Protocol, Telnet, and the *Internet Protocol* itself.

Someone had to keep track of all the protocols, the identifiers, networks and addresses and ultimately the names of all the things in the networked universe. And someone had to keep track of all the information that erupted with volcanic force from the intensity of the debates and discussions and endless invention that has continued unabated for 30 years.

That someone was Jonathan B. Postel, our Internet Assigned Numbers Authority, friend, engineer, confident, leader, icon, and now, first of the giants to depart from our midst.

# A metaphor for the Internet today?