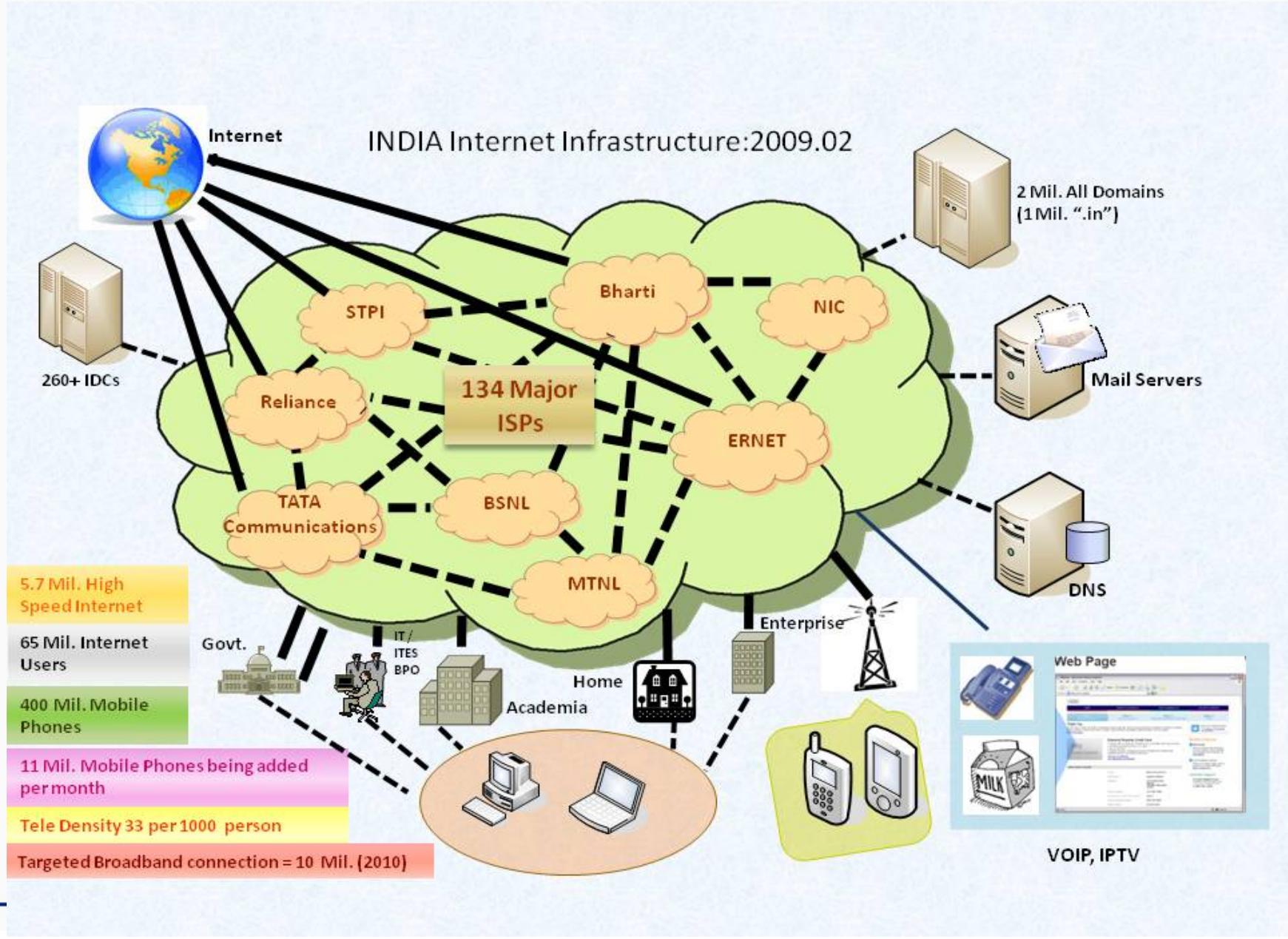
Cyber Security
&
Role of CERT-In

Dr. Gulshan Rai
Director General, CERT-IN
Govt. of India
grai@mit.gov.in

Web Evolution

Web Sites (WWW)	
1993	Web Invented and implemented 130 Nos. web sites
1994	2738 Nos.
1995	23500 Nos.
2007	550 Million Nos.
2008	850 Million Nos.
2009	1.1 Billion Nos.

Internet Infrastructure in INDIA



Innovation fostering the Growth of NGNs

- Smart devices
  - Television
  - Computers
  - PDA
  - Mobile Phone
    (Single device to provide an end-to-end, seamlessly secure access)

- Application Simplicity
  - Preference of single, simple and secure interface to access applications or content
  - Ubiquitous interface - web browser

- Flexible Infrastructure

Because of these areas of evolution, today's NGNs are defined more by the services they support than by traditional demarcation of Physical Infrastructure.

To Reap Benefits

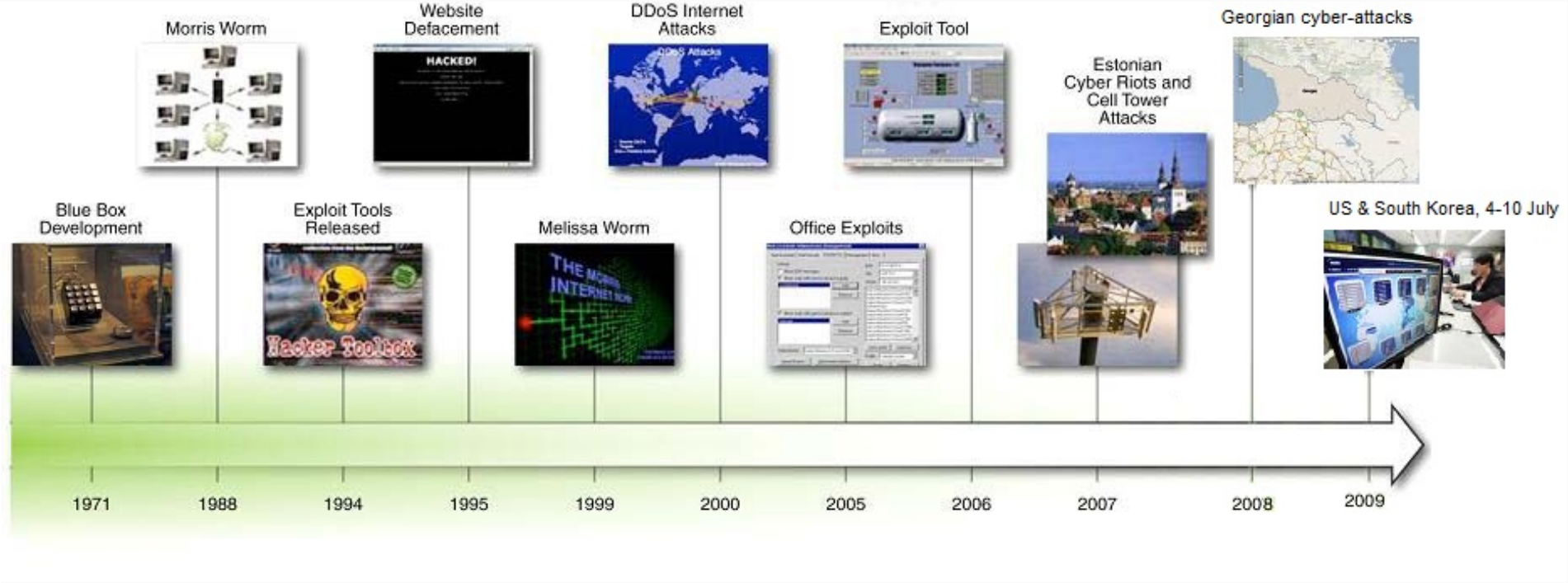
The issues concerning NGN are:

- Technology
- Risk
- Security
- Efficiency

Growing Concerns

- Computing Technology has turned against us
- Exponential growth in security incidents
  - US & South Korea, 4-10 July, 2009
  - Georgia in August 2008
  - Estonia in April 2007
- Common computing technologies and systems
- Constant probing and mapping of network systems

Rapid Development of Cyber Threats

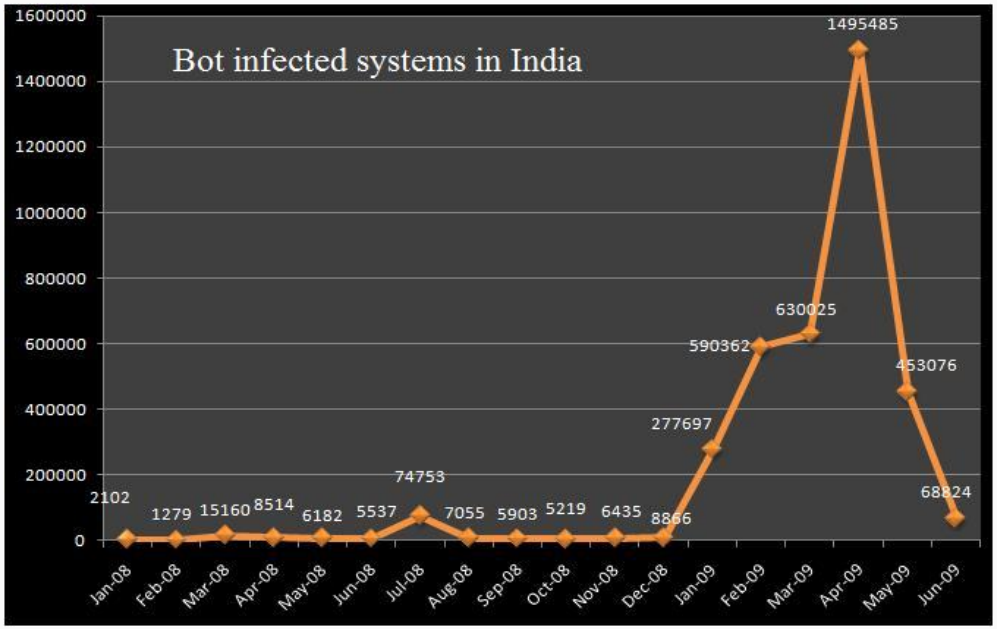


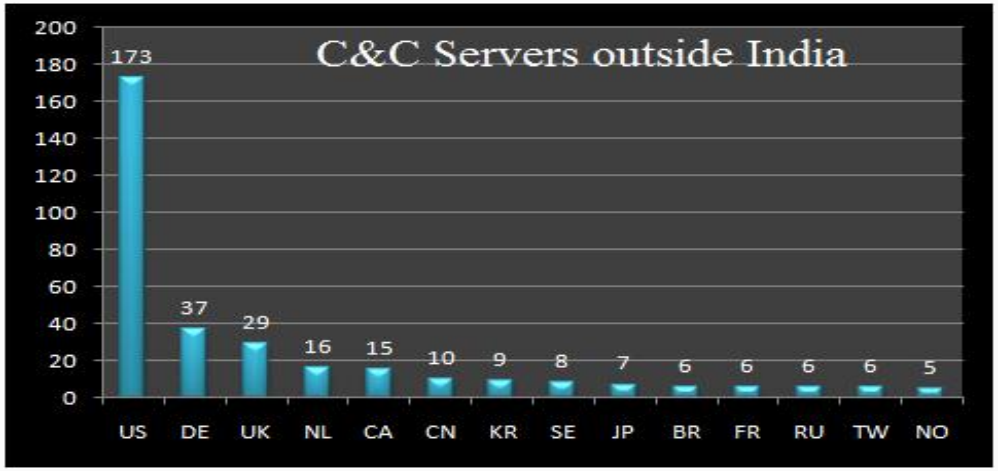
Cyber attacks being observed

- Web defacement
- Spam
- Spoofing
- Proxy Scan
- Denial of Service
- Distributed Denial of Service
- Malicious Codes
  - Virus
  - Bots
- Data Theft and Data Manipulation
  - Identity Theft
  - Financial Frauds
- Social engineering Scams

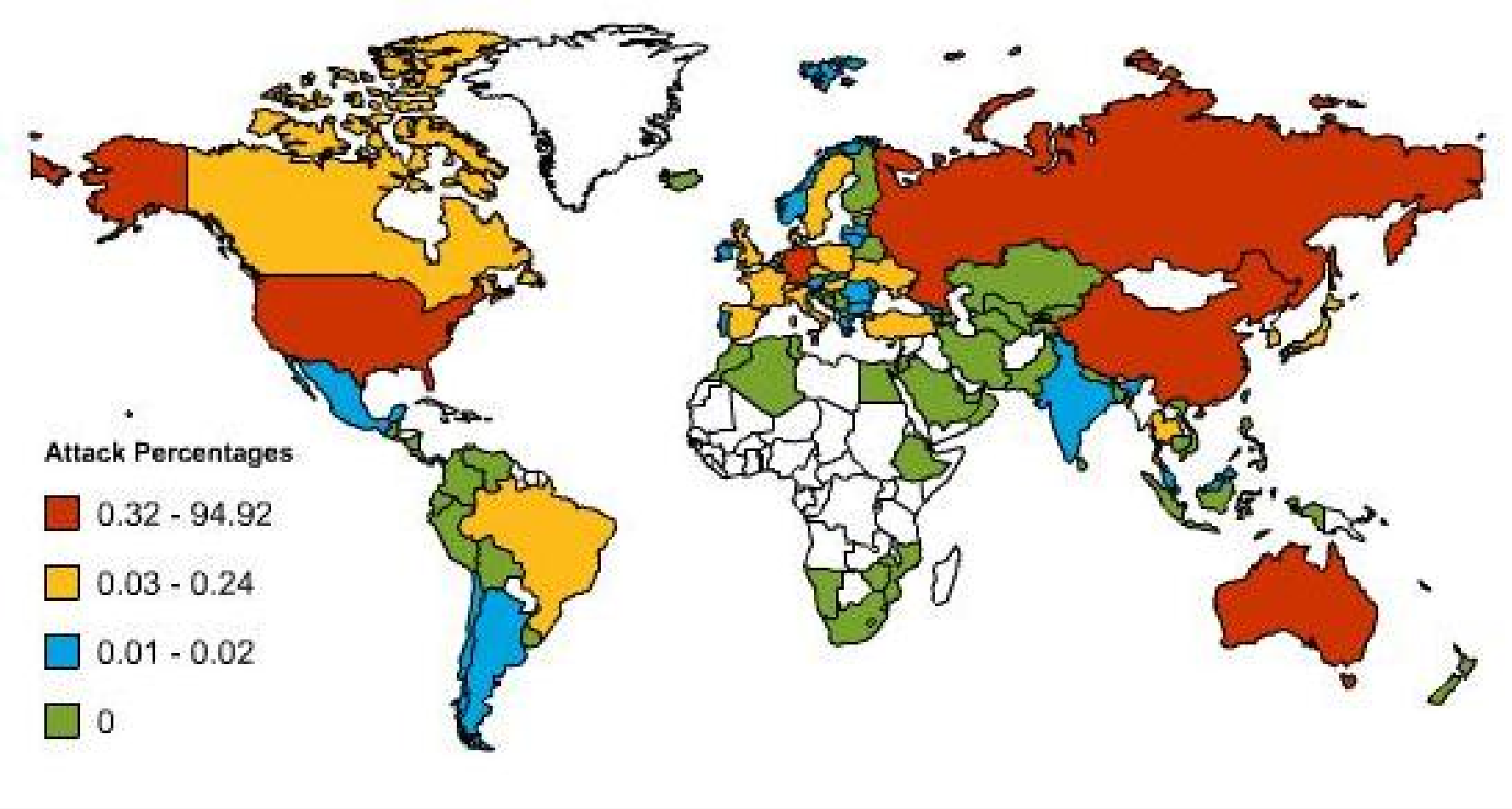
Threat elements

- Attack groups
  - Nation States
  - Organized cyber criminals
  - Independent hacker groups
- Botnets
  - DDoS
  - Spam
  - Phishing
  - Malware propagation
- Attack tool kits
  - Mpack



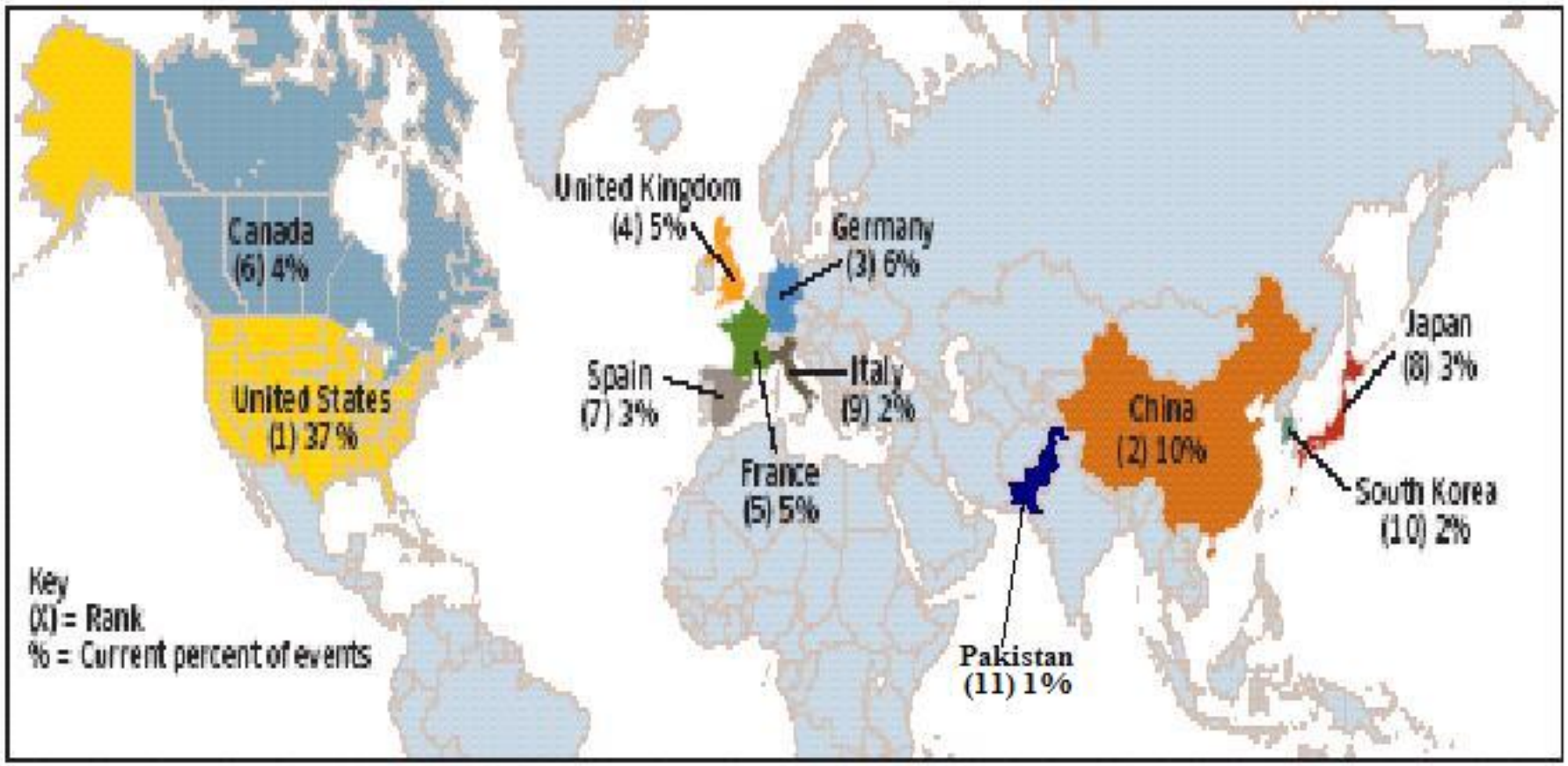


Global Attack Trend



Source: Websense

Top originating countries – Malicious code



Top originating countries

Three faces of cyber crime

- Organised Crime
- Terrorist Groups
- Nation States

Security of Information Assets

- Security of information & information assets is becoming a major area of concern
- With every new application, newer vulnerabilities crop up, posing immense challenges to those who are mandated to protect the IT assets
- Coupled with this host of legal requirements and international business compliance requirements on data protection and privacy place a huge demand .
- **There is a need to generate 'Trust & Confidence'**

Cyber Security Strategy – India

- **Security Policy, Compliance and Assurance – Legal Framework**
  - IT Act, 2000
  - IT (Amendment) Bill, 2006 – Data Protection & Computer crimes
  - Best Practice ISO 27001
  - Security Assurance Framework- IT/ITES/BPO Companies

- **Security Incident – Early Warning & Response**
  - CERT-In National Cyber Alert System
  - Information Exchange with international CERTs

- **Capacity building**
  - Skill & Competence development
  - Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
  - Training in the area of implementing information security at International organisations like CMU, USA, Cornell University, Stanford University.

- **Setting up Digital Forensics Centres**
  - Domain Specific training – Cyber Forensics

- **Research and Development**
  - Network Monitoring
  - Biometric Authentication
  - Network Security

- **International Collaboration**

Crisis Management Plan

- Crisis Management Plan for countering Cyber Attacks and Cyber Terrorism

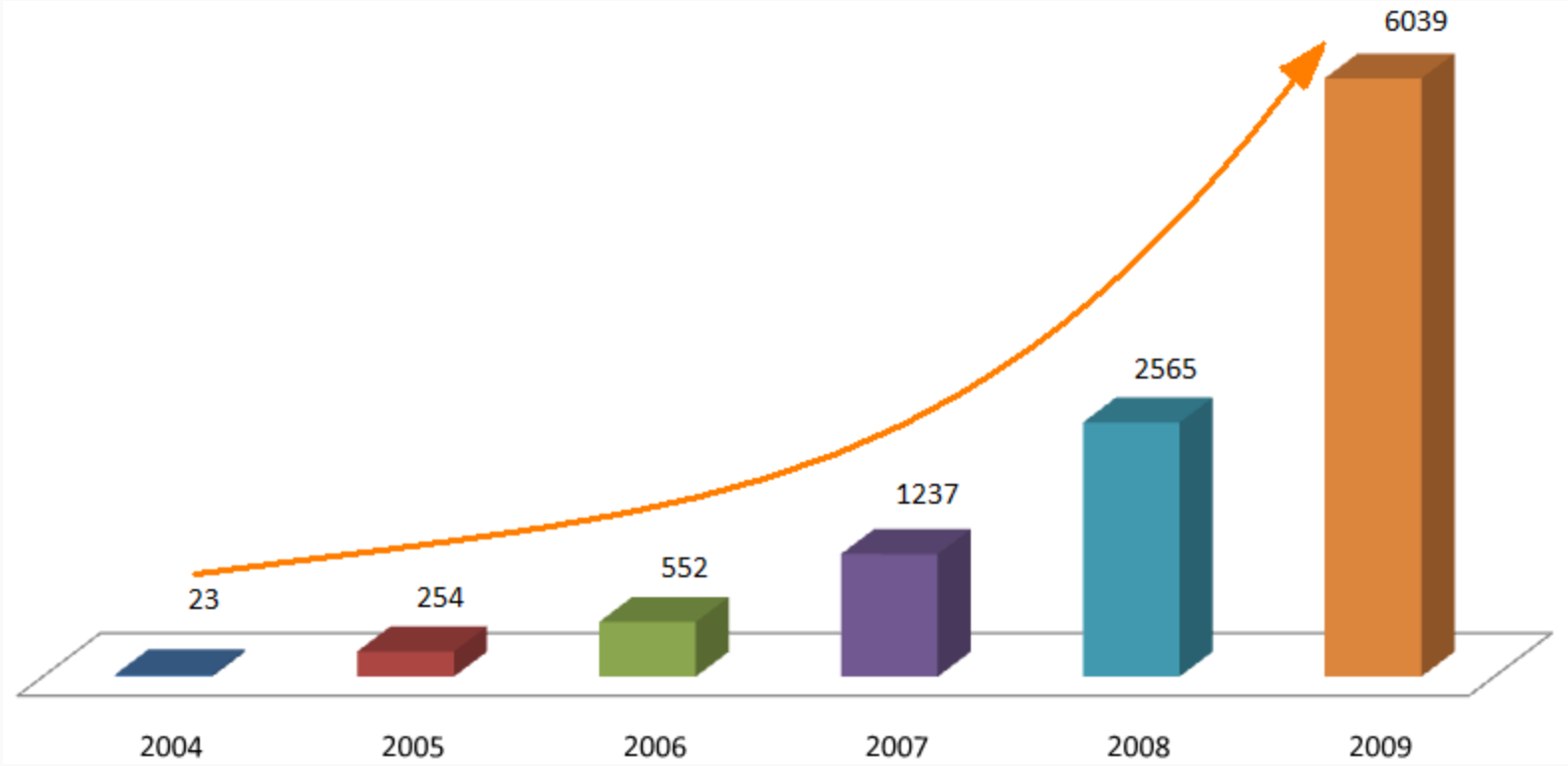
- Rapid response , remedial measures and restoration of normalcy in the emergence of a crisis
  - Containment of crisis
  - Communication to all concerned and
  - Coordination of efforts

Role of CERT-In

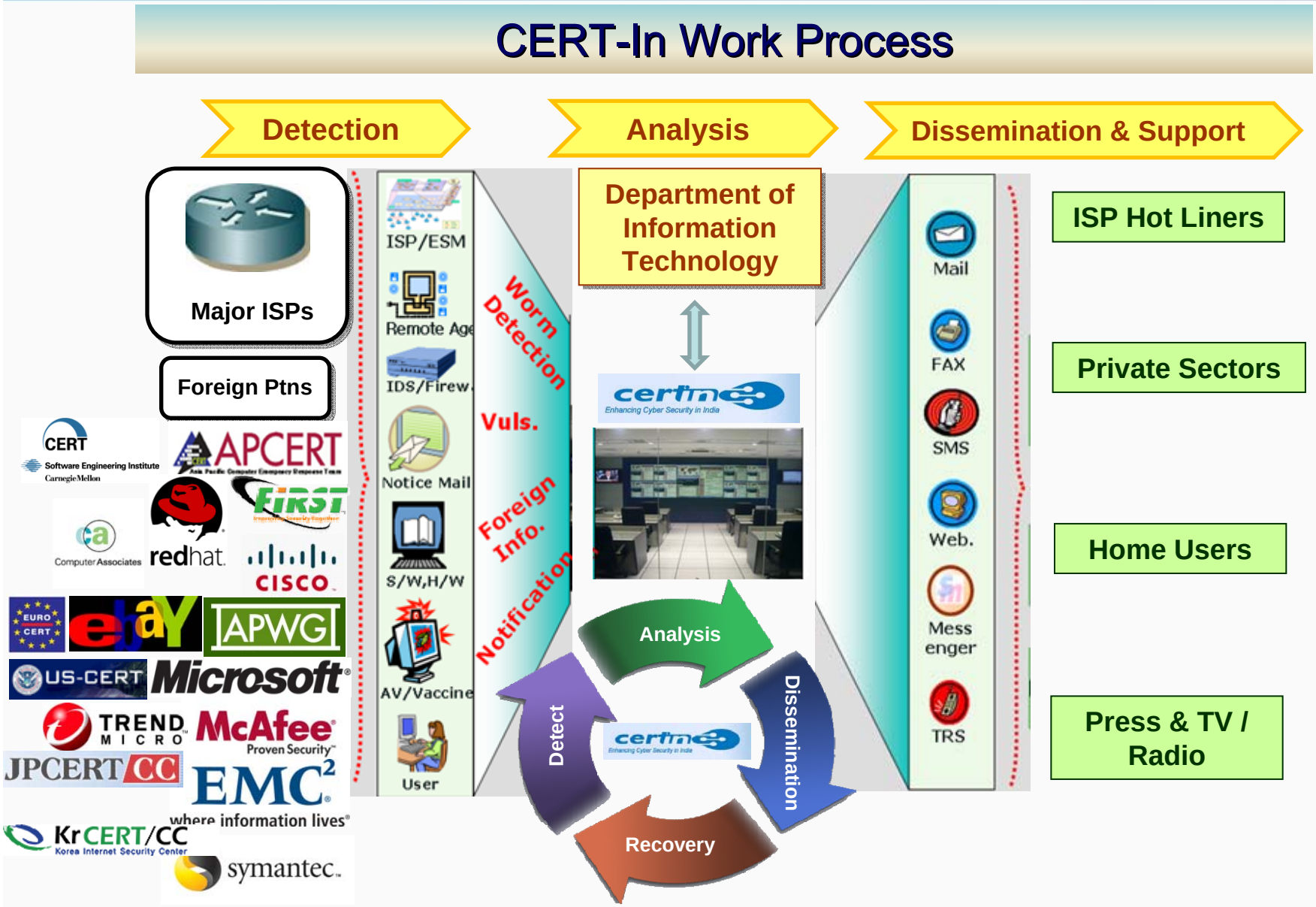
- Established in January 2004 by Department of Information Technology, Govt. of India
- Role of CERT-In
  - Computer Security Incident Response (Reactive)
  - Computer Security Incident Prevention (Proactive)
  - Security Quality Management Services
- Information Exchange
  - With sectoral CERTs (CSIRTs), CIOs of Critical Infrastructure organisations, ISPs, Vendors
- International Collaboration
  - Member of FIRST
  - Member of APCERT
  - Research Partner- APWG
  - Functional relationship with US-CERT and CERT/CC

Incidents Trend (from Jan 2004 – Aug 2009)

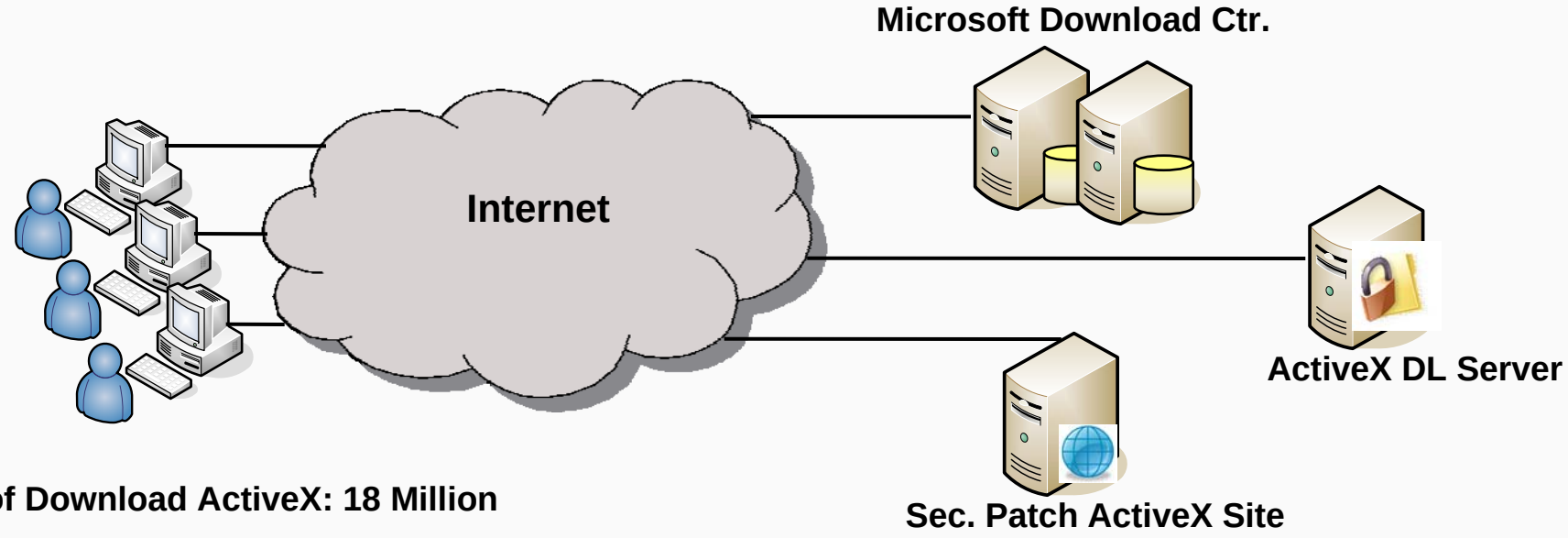
Year	2004	2005	2006	2007	2008	2009
No. of Incidents	23	254	552	1237	2565	6039



CERT-In Work Process



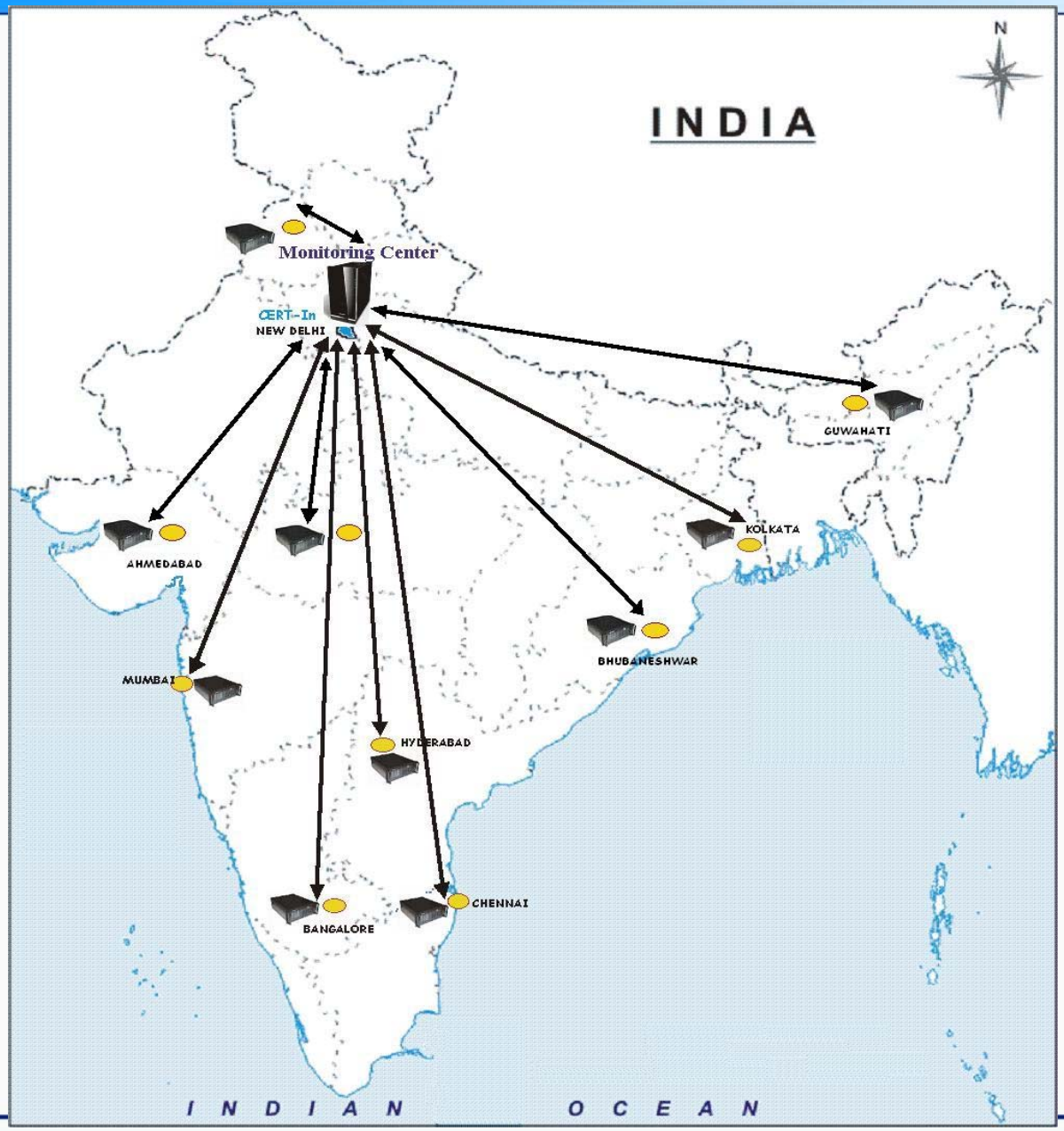
Windows Security Patch Auto Update



No. of Download ActiveX: 18 Million

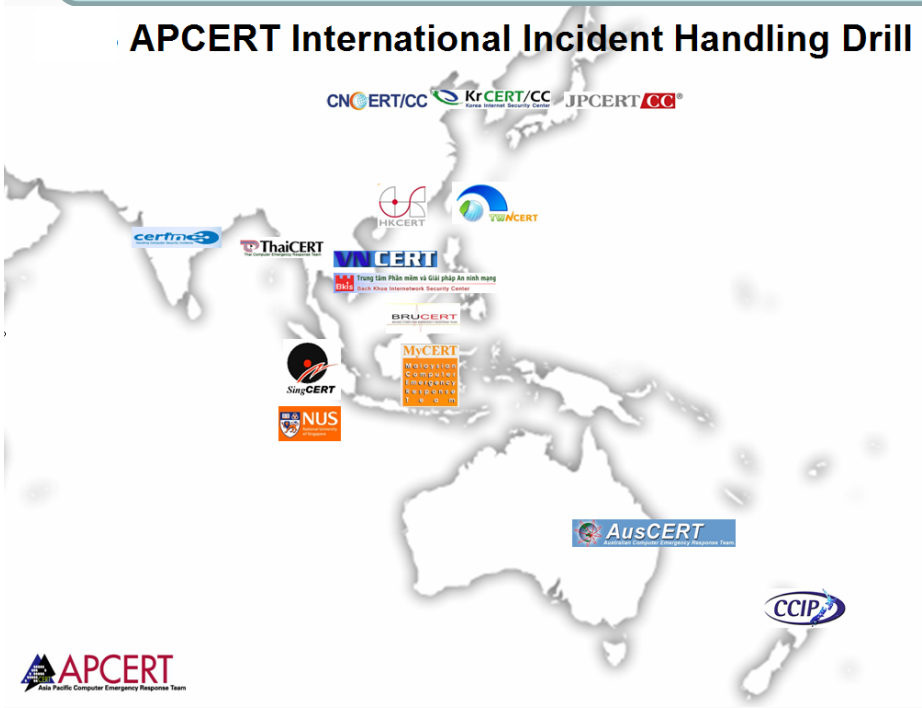
secureyourpc.in Portal

Distributed Honeypot Deployment



Int'l Co-op: Cyber Security Drills and Exercises

Joint International Incident Handling Coordination Drills



- Participated APCERT International Incident Handling Drill 2006
- Participants: 13 APCERT Members and New Zealand, Vietnam including 5 major Korean ISPs
- Scenario: Countermeasure against Malicious Code and relevant infringement as DDoS attack

- Participated APCERT International Incident Handling Drill 2007
- Participants: 13 APCERT Members + Korean ISPs
- Scenario: DDoS and Malicious Code Injection

- Participated APCERT International Incident Handling Drill 2008
- Participants: 13 APCERT Members
- Scenario: Online Underground Economy

CERT-In Activities

Activities	2003	2004	2005	2006	2007	2008	2009 (up to Aug)
E-mail messages received	-	625	1822	1948	3283	4073	5112
Incidents handled	-	23	254	552	1237	2565	6039
Security Alerts/ Incident Notes	4	20	30	48	44	49	20
Advisories	17	23	25	50	66	76	39
Vulnerability Notes	16	74	120	138	163	197	106
Security Guidelines	9	4	2	1	1	1	
White papers/Case studies	-	3	6	2	2	3	1
Trainings	1	7	6	7	6	18	12
Indian Website Defacement tracked	1687	1529	4705	5211	5863	5475	3429
Open Proxy Servers tracked	-	236	1156	1837	1805	2332	1497
Bot Infected systems tracked	-	-	-	-	25915	146891	3132618

Thank you

Incident Response Help Desk

Phone: 1800 11 4949

FAX: 1800 11 6969

e-mail: incident *at* cert-in.org.in

http://www.cert-in.org.in