# Critical Information Infrastructure Protection (CIIP)

By
S. K. Gupta, Advisor (CN&IT)
Telecom Regulatory Authority of India

# Agenda of Discussion

- Background
- Threats
- Present Status
- Challenges and Strategies

# Critical Information Infrastructure

- "Critical infrastructure means the computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters." **(Source: ITU Toolkit for Cybercrime Legislation)**

- All critical infrastructures are increasingly dependent on ICT for communication, information management and control functions.

# Security

- 'Security' refers to minimizing the vulnerabilities of assets and resources.
  - An 'asset' is anything of **value**.
  - 'Vulnerability' is any **weakness** that could be exploited to violate a system or the information it contains.
  - A 'threat' is a **potential violation** of security

# CIIP : ICT Impact

- ICT has direct impact on economic growth, social behaviour and conduction of business. As a result, it is now considered one of the core critical infrastructure.
- Monitoring and control of various core infrastructure like electricity, water supply, medical services are getting computerised, increasing their dependency on ICT.
- Protection of ICT infrastructure is vital as it has wide ramifications both direct and indirect on critical infrastructure.
- The emerging information infrastructure differ radically in terms of scale, connectivity, and dependencies from traditional structures.

# CIIP : ICT Impact

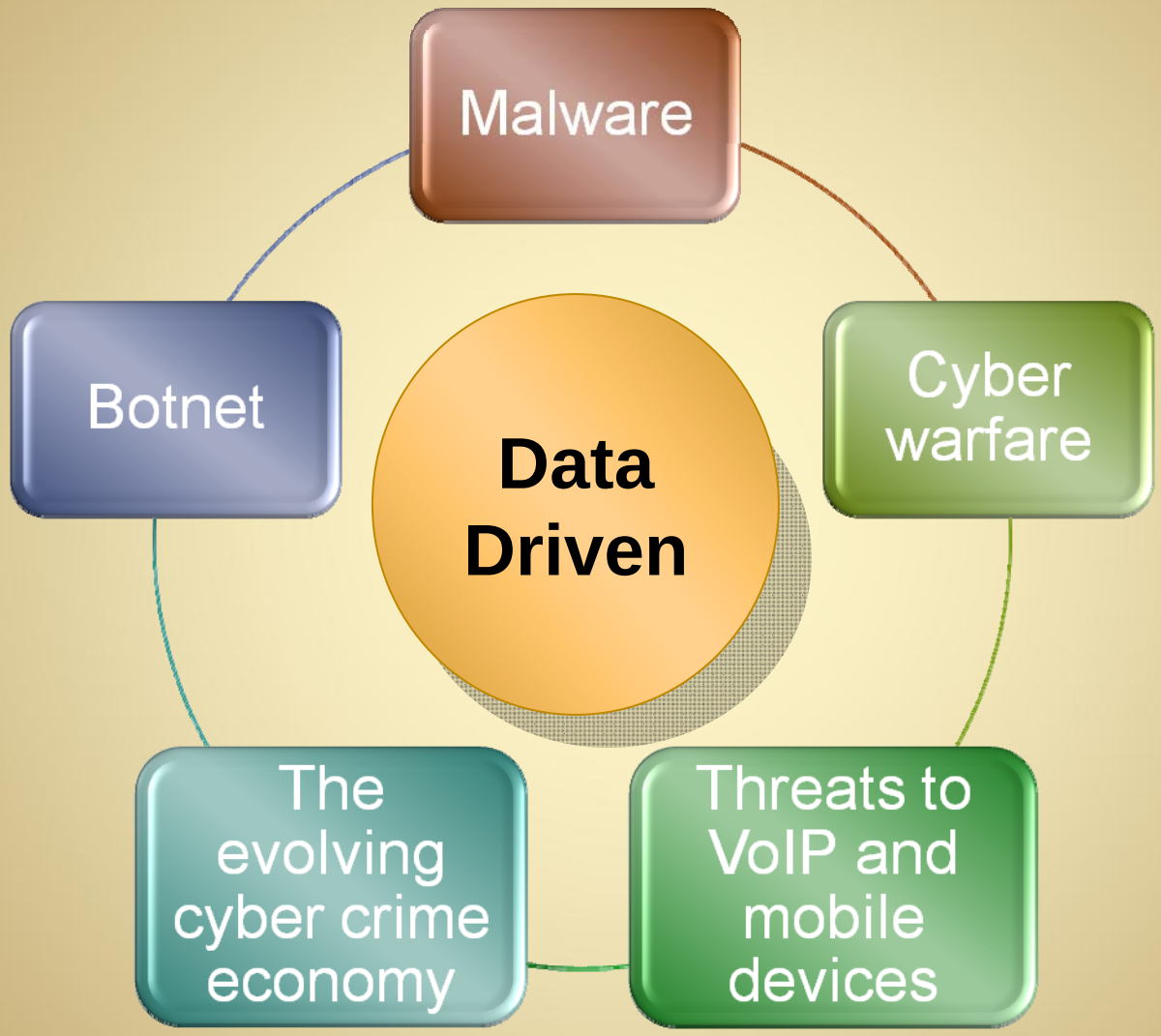
- Cyber-threats are evolving rapidly both in terms of nature and capability to cause harm.
- Threats must be managed to maximize social benefits from ICTs and to reduce risks resulting from interdependences and vulnerabilities.
- Communication systems are interconnected resulting in global interdependencies and vulnerabilities including threats to the national systems.
- Protective measures require continual technological improvements and new approaches, to minimize threats on ICT.

# CIIP: Potential of IP

| Features |
| --- |
| • IP networks are able to provide different services including triple play. |
| • IP technologies support flexibility, managed QoS, dynamic bandwidth management and support different applications. |
| • IP networks are cost effective when compared with legacy network. |
| • IP networks are resilient, robust, modular, scalable and require low capex/ opex. |

**IP based networks are becoming default choice for ICT.**

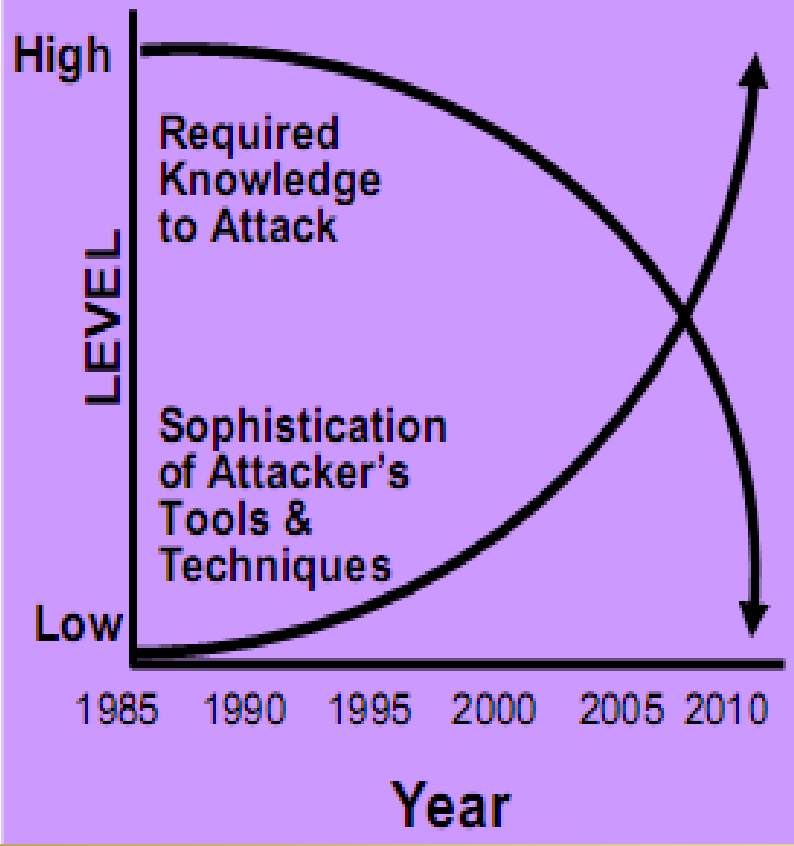
# Cyber Security : Emerging Threats




**Emerging threats …mostly data-driven!**

# Cyber Security : Emerging Threats

## Growing World-wide Cyber Threats




- The art of cyber attack is improving faster than our ability to respond.
- Emerging threats like Conficker, GhostNet etc outsmarts our defense capabilities by using sophisticated techniques.
- Cyber attackers have the strategic edge. **Cyber attacks are being considered as third greatest threat to the security after nuclear war and weapons of mass destruction (WMD).**
- A new threat **"Cybergeddon"** has been coined, in which an advanced society, that has most of its major infrastructure systems linked to or controlled by computers, is sabotaged by computer hackers with catastrophic results.

**Emerging threats …Increase with technology & Sophistications!**

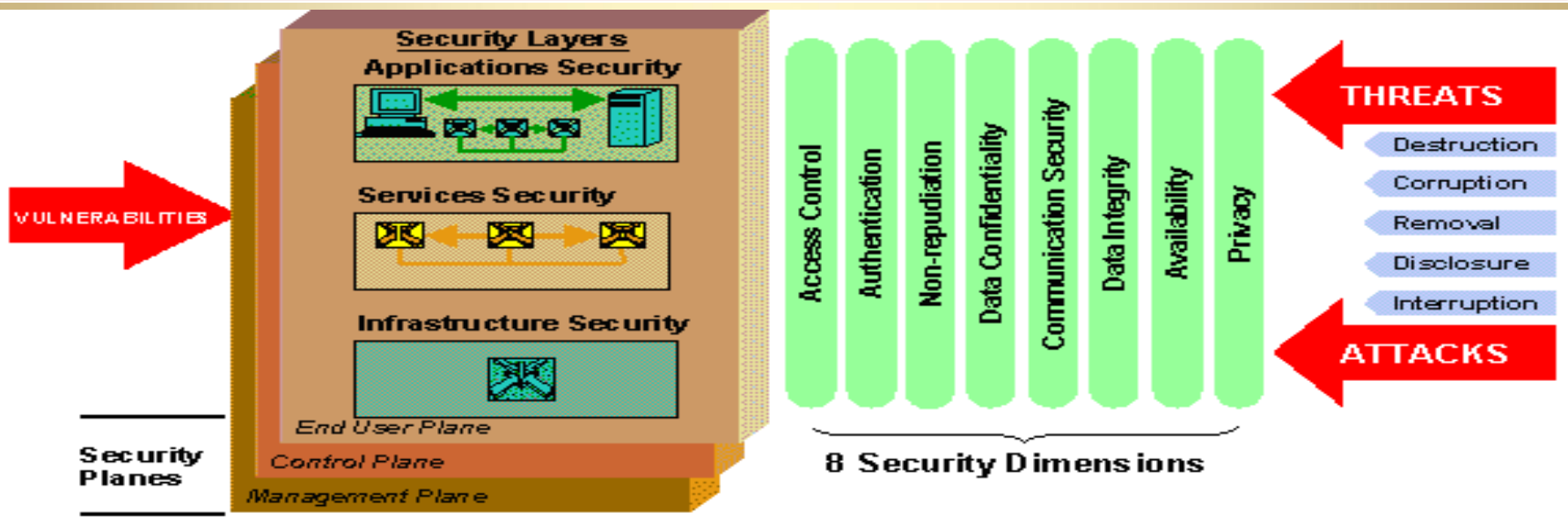
# Security Threats and Impact

| Sector/ Verticals | Threat | Impact |
|---|---|---|
| • Information and communication | • Identity theft | • Data Theft |
| • Banking & finance | • Spyware | • Industrial Espionage |
| • Emergency services | • Phishing | • System Downtime |
| • Power | • Denial of Service | • Financial Frauds |
| • Water supply networks | • Hack | • Reduced QoS |
| • Air traffic control | • Botnet | • Harassment |
| • Transportation | • Malware | • Information Loss |
| • Defense and security | • Viruses | • Compromised National Security |
| • Government | • Spam | • Defamation |
| • Food and agriculture etc | • Pop-ups etc | • Economic slowdown |

# Security Architecture : ITU-T

**Security has:**

- Three security planes (End user security, Control/Signaling security & Management Security)
- Three layers ( Infrastructure, service & application layers with each Security Layer having unique vulnerabilities, threats)
- Eight Dimensions (applies to each security perspective )




**Vulnerabilities can exist in each Layer, Plane and Dimension creating 72 Security Perspectives**

# Security Issues
## Main Areas

- Network security problems can be divided roughly into four closely interwined areas:

| Area | Characteristic |
|---|---|
| Secrecy | Keeping information out of the hands of unauthorized users |
| Authentication | Determining whom you are talking to before revealing sensitive information or entering into a business deal |
| Non-repudiation | to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is the assurance that someone cannot deny something |
| Integrity control | Modification of message in transit or concocted |

# Security Issues
# Main Threats

| Attacks on Network |
| --- |
| • Attack within subnet |
| • Broadcast storm |
| • Media Access Control (MAC) Flooding |
| • Dynamic Host Control Protocol (DHCP) DoS |
| • DHCP rogue |
| • Spanning Tree hijack |
| • Address Resolution Protocol (ARP) table poisoning |
| • IP address spoofing |

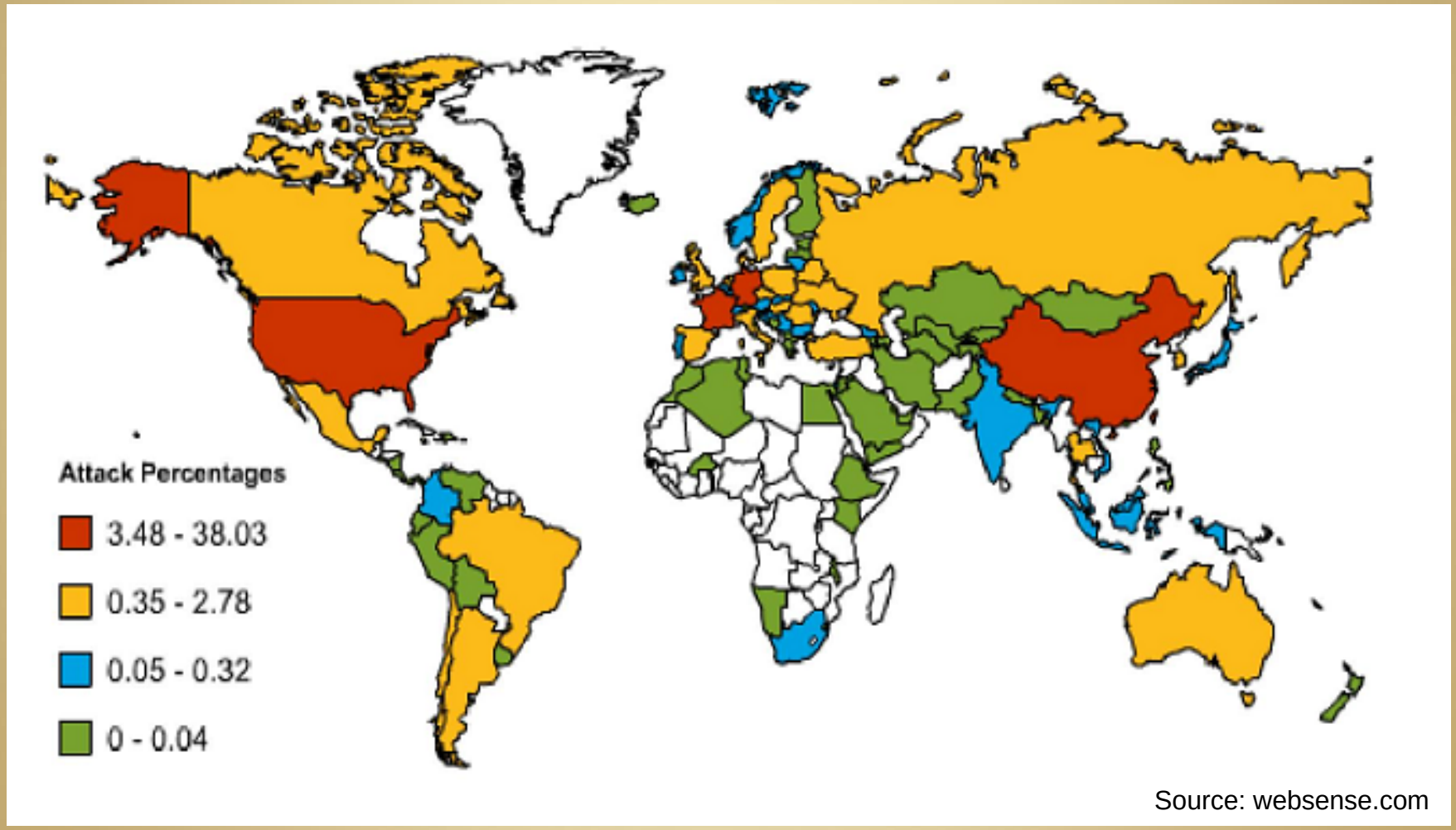
| Attacks on Services |
| --- |
| • Denial of Service (DOS) |
| • Backdoor |
| • Man in Middle |
| • Password Guessing |
| • Brute Force |
| • Dictionary |
| • Software Exploitation |

| Malicious Codes |
| --- |
| • Viruses |
| • Adware |
| • Spyware |
| • Worms |
| • Trojans |
| • Browse Hijackers |

# Types of Threats

| Type of Threats |
| --- |
| • Bot-network operators |
| • Criminal groups |
| • Foreign intelligence services |
| • Hackers |
| • Insiders |
| • Phishers |
| • Spammers |
| • Spyware/malware authors |
| • Terrorists |

# Security Issues : Global Threat Map




Source: websense.com

# Security Issues : Wireless

- Wireless IP network
  - Misuse of Wi-Fi signals- need for protections
  - Subscriber awareness issues
  - Securing subscriber devices

**Example-case India**

- **Total vulnerable Wireless networks in India : 86%**
  - **Without any encryption : 37%**
  - **With lower-level protection like Wired Equivalent Privacy (WEP) encryption : 49%**
  - **With security layers like Wi-Fi Protected Areas (WPA and WPA2) : 14%**

Source: Survey by Deloitte and Data Security Council of India (DSCI)

# Security Issues : IP Ports

- **Misuse of IP Ports**

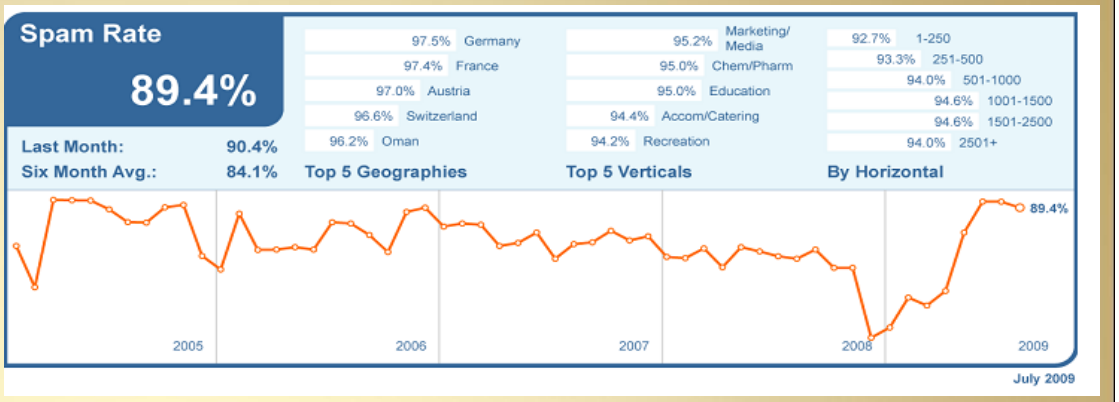
– Attacks using open IP Ports

– Misuse of application in absence of server hardening

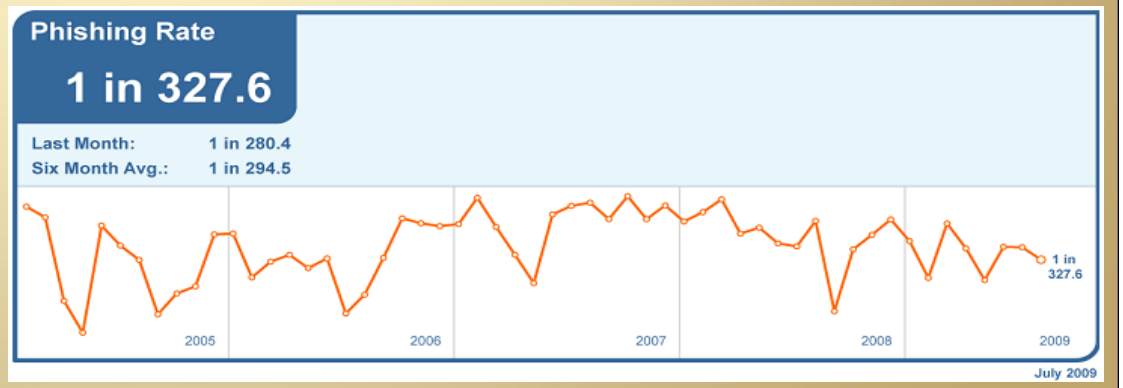
– Exploiting Hardware / Software vulnerabilities

# Security Issues : SPAM, Virus & Phishing

| Threat | Value (July 09) |
|---|---|
| Spam | 89.4% |
| Phishing – | one in 327.6 email |
| Viruses | one in 295.2 emails |
| malware | 0.03% emails |
| Malicious websites | 3,618 new sites blocked per day |
| Spam language localization | one in 20 |
| URL-shortened spam | 6.2% of all spam |





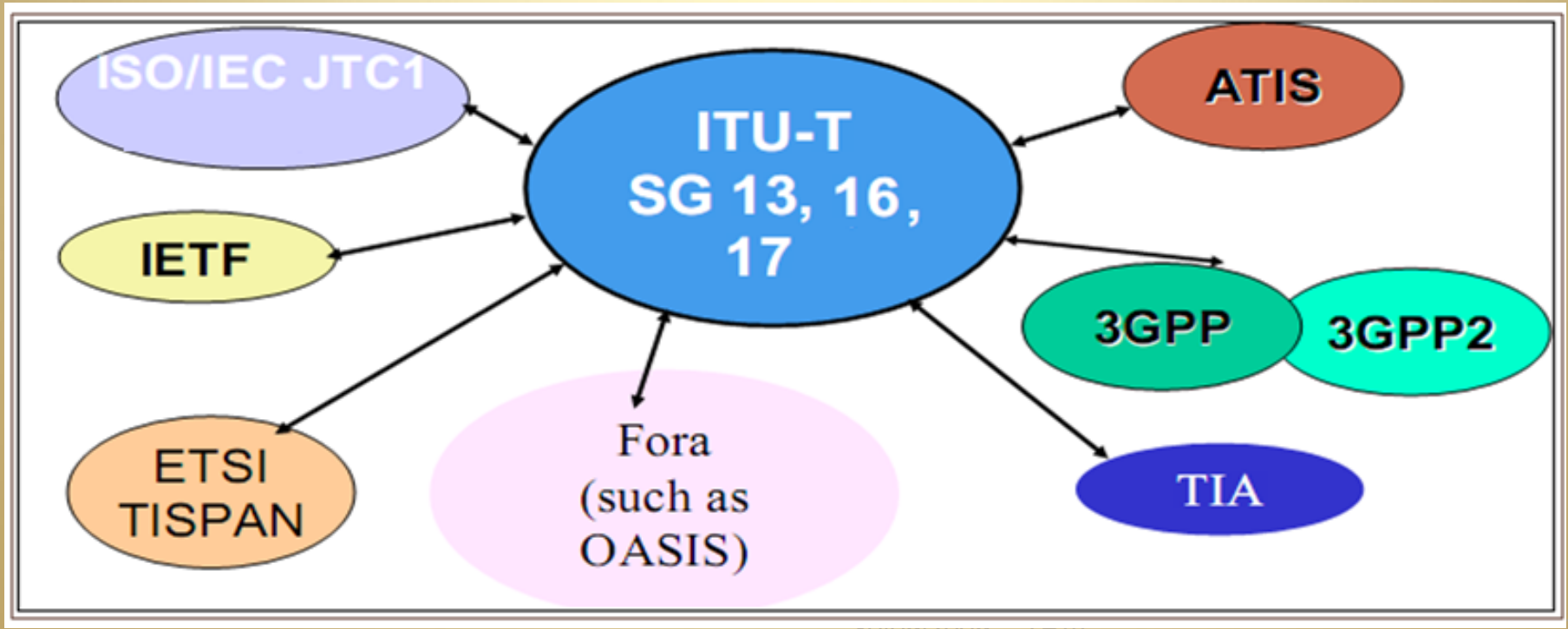



9/30/2009

Source: MessageLab

# Security Issues : NGN

| Component of NGN security |
| --- |
| • Network domain security |
| • IMS access security |
| • Application security |
| • Security of open services/ application frameworks |



# Cyber Security : Challenges

- All need to protect our critical information infrastructures, as risks are huge, especially in electronic warfare.
- The rapid growth of ICTs and societal inter-dependency have led a shift to perception of Critical Information Infrastructure threats and, as a consequence, cyber security has become international political agenda.
- It is crucial to understand the risks that accompany new technologies in order to maximize the benefits.
- Growing threats to security, at the level of the individual, the firms, government and critical infrastructures, make security everyone's responsibility.
- It is important to understand and keep up-to-date contours of fast changing challenges.

# Cyber Security : Approach and Strategies

| Approach and Strategies |
| --- |
| • Legal Measures: |
| • Technical and Procedural Measures |
| • Capacity Building |
| • International Cooperation |

# Approach and Strategies

## Legal Measure

- Adoption of appropriate legislation against the misuse of ICTs for criminal or disruptive purposes, including activities intended to affect the integrity of national critical information infrastructures.
- Threats can originate from anywhere around the globe, the challenges are inherently international in scope and require international cooperation, investigative assistance, common substantive and procedural provisions.
- There is urgent need to enhance information sharing to improve incidence response capabilities.

## Technical and Procedural Measures

- Standardization brings private sector and governments to coordinate work and promote the harmonization of security policy and standards globally.
- Various standards and security provision defined by international organizations like ITU, IEEE etc. should be implemented across all countries. These standards must provide safeguards for security and updated regularly to combat new security risk.

# Approach and Strategies: Capacity Building

- Promote cybersecurity risk awareness for all citizens;
- Build an education system that will enhance understanding of cybersecurity in information technology;
- Expand and train the workforce to protect the Nation's competitive advantage;
- Help organizations and individuals make smart technological choices as they manage risk.
- Develop skills to reduce risk and exposure from unsecure environment
- Enabling citizen through impowerment of:
  - Knowledge,
  - capabilities and
  - Decision-making.

# Way forward

| Way Forward: |
| --- |
| • Security is important, manageable but requires participation of all stakeholder and awareness in masses. |
| • Service providers must be sensitized to make a secure network for future. |
| • CIIP unit must act effectively with the help of various partners across the globe. |
| • The establishment of Public-Private Partnerships with strong mutual trust is essential for the success of the CIIP unit. |

# Thank You

S K Gupta, Advisor (Converged Network)
Telecom Regulatory Authority of India
J.L. Nehru Marg, New Delhi – 110002
Ph. +91-11- 23217914 (O)
+91-11- 23211998 (Fax)

Email: guptask61@gmail.com