


# **CYBER SECURITY STRATEGIC PLANNING FOR PAKISTAN**

Lesson # 13


# CHALLENGES

- ▶ CYBER AWARENESS
  - ▶ LACK OF CYBER AWARENESS
  - ▶ NATIONAL CYBER SECURITY FORUM
  - ▶ ABSENCE OF REGIONAL COOPERATION
  - ▶ DIGITAL RIGHTS AND OBLIGATION
  - ▶ CYBER CENSORSHIP
  - ▶ UNCHECKED HACKTIVISM
- 

# **CYBER AWARENESS**



# CYBER AWARENESS

- ▶ Cyber security has yet to blip on the national radar.
  - ▶ No political party has included it on its manifesto.
  - ▶ No legislation on cyber issues in the parliament .
  - ▶ Police department, judiciary & lawyers have little/no knowledge and experience in investigating & prosecuting digital crimes.
  - ▶ No chamber of commerce runs any cyber security course or gives advice to businesses to secure their digital enterprises.
  - ▶ No policy in preventing import of hardware with embedded technologies.
  - ▶ None of the government agency, electronic media, higher education institute has a cyber security policy.
  - ▶ Digitally advanced countries organize cyber awareness days/weeks.
- 

# **LACK OF NATIONAL CYBER POLICY**



# LACK OF NATIONAL CYBER POLICY


- ▶ National cyber mandate & division of turf among multiple stakeholders i.e. It ministry, moi, most, mod, js hq, int agencies .
- ▶ National cyber strategy – issues such as protection of critical infrastructure & response to computer emergencies.
- ▶ Cyber terrorism.
- ▶ Cyber criminal code .
- ▶ Laws to regulate online businesses .
- ▶ Cyber censorship – rules & policies .
- ▶ Foreign policy
  - how to respond diplomatically to cyber incidences .
  - policy for delegates attending the GGE conferences at the un, internet governance conferences & international seminars .
  - policy guidelines for engagement with ITU.
- Defense policy – how to react to various kinds of attacks .

# **NATIONAL CYBER SECURITY FORUM**



# NATIONAL CYBER SECURITY FORUM

Government to create a national cyber security forum and designate a lead ministry /Agency .

- ▶ Lead ministry to publish a national calendar for holding cyber security seminars .
  - ▶ Lead ministry to organize national cyber security drills more than once annually .
  - ▶ Lead ministry to run courses for parents to digitally monitor their children.
  - ▶ Universities to group together to promote cyber security education under the umbrella of the HEC .
- 



# **ABSENCE OF REGIONAL CO-OPERATION**



# ABSENCE OF REGIONAL CO-OPERATION

- ▶ Countries are cooperating jointly and en bloc in cyber security issues i.e. Asian is very active in this regard.
- ▶ There is no bilateral or regional cooperation in South Asia. SAARC can provide an important forum for cyber security .

# **DIGITAL RIGHTS AND OBLIGATIONS**



# DIGITAL RIGHTS AND OBLIGATIONS

- ▶ Is our Government aware of its national digital obligations?


In matters like enforcing un convention on right of children  
(UNRC) preventing children pornography through digital means .

- ▶ What are a citizen's digital rights?

To access all kinds of websites .

- ▶ What are the citizen's obligations?

To prevent cyber bullying/sexual harassment & reporting illegal  
activity in cyber space .




# **CYBER CENSORSHIP**



# CYBER CENSORSHIP


**Cyber censorship** is of what can be accessed, published, or viewed on the Internet. Cyber censorship can be implemented by:

- ▶ National policy for handling digital incidents e.g. The YouTube incident .
  - ▶ Stronger filters for pornographic sites .
  - ▶ Efficient mechanisms to control preventing spread of hate literature & operations of prohibited organizations .
- 

# UNCHECKED HACKTIVISM




# UNCHECKED HACKTIVISM

- ▶ Uncontrolled hacktivism now forms part of the India Pakistan rivalry.
  - ▶ Independent group of hackers with colorful names like Pakistan cyber army, Indian cyber army, Pakistan hackers club, Pakhaxors, predators PK, Hindustan hacker's organization defaces an Indian or Pakistani website.
  - ▶ Mostly the homepage is littered with poorly- worded patriotic statements and taunts that often provoke the other nation's hacking groups to retaliate.
- 



# UNCHECKED HACKTIVISM ....

- ▶ The homepage is defaced and replaced with juvenile comments. Often, these hackers block visitors' access to important information. Such acts, of course, lead to more cyber defacements, with the most "coveted" targets being government websites. A cyber-attack is usually triggered by some act of violence or aggression from the rival country. Within a span of hours, these groups of hackers locate a high-value website that doesn't have adequate cyber security in place, and gains root access to the web server by hacking into it.
- 

# Reference

KTH-SEECs Applied Information Security (AIS) Lab

