

**Website Usability
Engineering for Global Trade
3-day evaluation workshop
Russell Plus International
August 6th to August 8th.**



Masood Ur Rehman-
Research Fellow

National Security in the Cyber Age

By

Masood Ur Rehman
Research Fellow
South Asian Strategic Stability Institute



All Copyrights belong to the South
Asian Strategic Stability
Intitute(SASSI) Aug 09

Conti...

- ❑ Globalisation has made national borders irrelevant and brought about radical changes in the concept of National Security.
- ❑ Traditionally the military has been at the heart of security policy; now national security must be evaluated more in terms of Human, Economic and Cultural terms.

Conti...

- National security involves protecting the nation's infrastructure, the potency of its foreign policy and economy, the civil rights of its citizens, trade and work availability and the essentials of national sovereignty.
- National Security envisages the interrelationship of these facts with terrorism, globalisation, poverty and human trafficking and/or illegal immigration.
- Three factors in the 21st century predominate national security, the economy, the demographic movement of people and the threats and attacks by extremists.

National Security Goals of Pakistan....

- ❑ Maintenance of the integrity and security of Pakistan
- ❑ Securing the safety of its strategic assets
- ❑ Rehabilitation of the economy and restoring investor confidence
- ❑ Dealing firmly with militancy and religious extremism
- ❑ Strengthening of the Federation
- ❑ Removal of inter-provincial disharmony and restoration of national cohesion

Challenges in the Cyber age

- ❑ The information technology is a double edge sword, which can be used for destructive as well as constructive work.
- ❑ Governments and organisations face significant challenges to ensure their computer systems and websites are protected against cyber warfare attacks.
- ❑ Activity in which computers or networks are a tool, a target, or a place of criminal activity.

Challenges to E-Commerce...

- As the use of the internet continues to grow, websites are assuming greater importance as the public face of business.
- Furthermore, the revenues generated by e-commerce systems mean that organisations are becoming ever more reliant on them as core elements of their business.

Cyber Crime a Global Phenomena.

- ❑ Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever.
- ❑ Former U.S. officials say the attacks appear to have originated in China. However it can be extremely difficult to determine the true origin because it is easy to mask identities online.
- ❑ These types of attacks against the super power of time shows the level of threat, we are facing today.

Internet Fraud, Scam and Crime Statistics – 2006-2009.



Masood Ur Rehman-
Research Fellow

All Copyrights belong to the South
Asian Strategic Stability
Intitute(SASSI) Aug 09

Internet Fraud, Scam and Crime Statistics – 2006-2009.

- In 2008 according to the Annual Report there is 33.1% increase in the cyber crimes. The total dollar loss linked to online fraud was \$265 million.
- Americans reported losses of US\$240 million from global cyber-crime in 2007. A \$40 million increase from 2006. The I3C received 206,884 complaints of online fraud in 2007.
- a decrease from the previous year's 207,492 complaints and over 231,000 complaints in 2006

Tactics and Threats of Cyber Warfare.

- ❑ **Cyber Spying:**
- ❑ Cyber Spying is the act or practice of obtaining secrets, sensitive, classified information from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.
- ❑ Such activities are really a grave threat for the national security.

Tactics and threats...

❑ **Web Vandalism:**

- ❑ Attacks that deface web pages, or denial-of-service attacks. Such attacks would seriously hamper the image of respective organisations.

❑ **Propaganda:**

- ❑ Political messages can be spread through or to anyone with access to the internet or any device that receives digital transmissions from the Internet to include cell phones.
- ❑ This type of propaganda can create uncertainty in the country and would harm the national interests of the respective state.

Tactics and threats....

- ❑ **Gathering Classified Data:**
- ❑ Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world.
- ❑ **Equipment Disruption:**
- ❑ Military activities that use computers and satellites for coordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk and threatening the national security of country.

Tactics and Threats....

- ❑ **Attacking critical infrastructure:**
- ❑ Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.

Tactics and Threats....



Research Fellow

Asian Strategic Stability
Intitute(SASSI) Aug 09

Pak Cyber law.

Ordinances No..XIV of 2009.

- ❑ Pakistan in this regard have taken stringent measures to curb the cyber crimes.
- ❑ Pakistan have promulgated different laws which not only deal with crimes on Internet but also deals with all dimensions related to computer & networks.
- ❑ Ordinance for the prevention of the electronic crimes: Ordinances No..XIV of 2009.

Offences and Punishments

□ **Data Damage:**

- Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.

□ **Punishment:**

- 3 years
- 3 Lac

Criminal Access:

- Who intentionally gains unauthorized access to the whole or any part of the electronic device would be
- Punished for
- Three years imprisonment
- 3-Lac Rs Fine

Electronic Fraud:

- ❑ People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm.

- ❑ **Punishment:**
- ❑ 7 years
- ❑ 7 Lac

Electronic Forgery:

- Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not.
- **Punishment:**
- 7years
- 7 Lac

Malicious code:

- Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or device, with intent to cause harm to any electronic system or resulting in the theft or loss of data commits the offence of malicious code.
- **Punishment:**
- 5 years
- 5 Lac

Cyber Stalking:

- ❑ Whoever with intent to harass any person uses computer, computer network, internet, or any other similar means of communication to communicate obscene, vulgar, profane, or indecent language, picture or image.
- ❑ Make any suggestion or proposal of an obscene nature
- ❑ Threaten any illegal or immoral act
- ❑ Take or distribute pictures or photographs of any person without his consent or knowledge
- ❑ Punishment for this crime is 7 year imprisonment with three hundred thousand rupees fine.

Spamming:

- ❑ Whoever transmits harmful, fraudulent, misleading,
- ❑ illegal or unsolicited electronic messages in bulk to any person
- ❑ without the express permission of the recipient,
- ❑ involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.
- ❑ **Punishment:**
- ❑ 3- month
- ❑ 50,000

Spoofing:

- ❑ Whoever establishes a website, or sends an electronic message with a counterfeit source intended to be believed by the recipient or visitor or its electronic system to be an authentic source
- ❑ with intent to gain unauthorized access or obtain valuable information
- ❑ Later, Information can be used for any lawful purposes commits the offence of spoofing.
- ❑ Three years Jail with Fine.

Cyber Terrorism:

- ❑ Any person, group or organization who, with terroristic intent utilizes,
- ❑ accesses or causes to be accessed a computer, computer network or electronic system or device or by any available means,
- ❑ knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism.
- ❑ Punishment
- ❑ Whoever commits the offence of cyber terrorism and causes death of any person shall be punished with **Death Or imprisonment for life, and with fine** **Otherwise he shall be punishable with imprisonment of ten years or with fine ten million rupees.**

Options to overcome Threats to E-Commerce

- **Consumer Education**
- The government of Pakistan should aim to take more active steps in making consumers more aware of their rights.
- It also seeks to increase general awareness on unlawful business practices that have crept up in the online world.

Option....

- ❑ **Government should Introduce new legislation:**
- ❑ **Advances made by technology have made available a wide, new range of products and services.**
- ❑ **More importantly, it has also thrown up newer ways of marketing as also for collecting or making payments for the products.**
- ❑ **This introduces new risks like the risk of identities being stolen or unauthorized access to personal bank accounts among others.**
- ❑ **The Government should introduce new laws to deter such crimes from happening.**

Option....

- ❑ **Monitoring of new channels of Marketing.**
- ❑ Over the last few years, many new channels of marketing have opened up for businesses.
- ❑ As yet, these channels are not regulated. Government of Pakistan should bring all these channels within its ambit with the purpose of ensuring fair deals for the consumers.
- ❑ This should deter many fraudsters who presently conduct scams in the guise of businesses, online.

Option....

- ❑ **Increase Cooperation with Foreign Agencies:**
- ❑ Government of Pakistan should widen its role globally by increasing its collaboration with foreign agencies in tackling international issues.
- ❑ **Encourage businesses to take up self regulation**
- ❑ Seeks to put a system wherein businesses would be encouraged to take up security measures which can ensure safe and fair interaction with the company for the customer.

Conclusion

- ❑ The cyber war and cyber terrorism threats are not only real but also very dangerous and posing a real threat to the national security of a country.
- ❑ online espionage and internet-based terrorism now represent some of the gravest threats to global security.
- ❑ The digital life is an altogether different segment where traditional methods are ineffective.
- ❑ We have witnessed many of these attacks and we don't think this problem will disappear soon. Unless we take globally supported measures because it has become a global problem, and it needs global solution.