FORMULATION OF CYBER SECURITY STRATEGY FOR PAKISTAN

NEED & CHALLENGES

DR TUGHRAL YAMIN
AUTHOR OF
CYBER CBMs BETWEEN PAKISTAN & INDIA

CHALLENGES

- LACK OF CYBER AWARENESS
- NO CLEAR CUT NATIONAL CYBER POLICY
- DIGITAL RIGHTS & OBLIGATIONS
- NO NATIONAL CYBER FORUM TO SHARE BEST PRACTICES IN CYBER SECURITY
- ABSENCE OF REGIONAL COOPERATION
- UNCHECKED HACKTIVISM

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

- NATIONAL CYBER MANDATE & DIVISION OF TURF AMONG MULTICIPLE 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
- FOREIGNPOLICY
  - HOW TO RESPOND DIPLOMATICALLY TO CYBER INCIDENCES
  - POLICY FOR DELEGATES ATTENDING THE GGE CONFERENCES AT THE UN, INTERNET GOVERNANCE CONFERNENCES & INTERNATIONAL SEMINARS
  - POLICY GUIDELINES FOR ENGAGEMENT WITH ITU
- DEFENCE POLICY – HOW TO REACT TO VARIOUS KINDS OF ATTACKS

NATIONAL CYBER SECURITY FORUM

- GOVT 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 COOPERATION

- COUNTRIES ARE COOPERATING BILATERALLY AND EN BLOC IN CYBER SECURITY ISSUES I.E. ASEAN 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 & OBLIGATIONS

- IS OUR GOVT 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 HARRASMENT & REPORTING ILLICIT ACTIVITY IN CYBER SPACE

CENSORSHIP

- NATIONAL POLICY FOR HANDLING DIGITAL INCIDENTS E.G. THE YOUTUBE INCIDENT
- STRONGER FILTERS FOR PORNOGRAPHIC SITES
- EFFICIENT MECHANISMS TO CURB PREVENTING SPREAD OF HATE LITERATURE & OPERATIONS OF PROSCRIBED ORGANISATIONS

UNCHECKED HACKTIVISM

- UNCONTROLLED HACKTIVISM NOW FORMS PART OF THE INDIA PAKISTAN RIVALRY
- INDEPENDENT GROUP OF HACKERS WITH COLOURFUL NAMES LIKE PAKISTAN CYBER ARMY, INDIAN CYBER ARMY, PAKISTAN HACKERS CLUB, PAKHAXORS, PREDATORS PK, HINDUSTAN HACKERS ORGANISATION DEFACE 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.
- THESE ATTACKS HAVE BEEN OCCURRING INTERMITTENTLY SINCE THE LATE 90S, THEY SEEM TO HAVE ESCALATED SINCE THE MUMBAI TERRORIST ATTACKS IN 2008. WHILE PREVIOUSLY THESE HACKS TARGETED POPULAR BUT HARMLESS WEBSITES, THE TREND HAS GRADUALLY MOVED TO DEFACING MAJOR GOVERNMENT AND LAW ENFORCEMENT WEBSITES.
- 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.

Q&A