DEVELOPING INFORMATION SPACE CBMs FOR INDIA & PAKISTAN: PROSPECTS & PROPOSALS



The views expressed here are solely those of the presenter and do not necessarily represent those of any government, its agencies or representatives

ACKNOWLEDGEMENTS

Atlantic Council

PROBLEMS & PROSPECTS

- **INTERNATIONAL LEVEL**
  - BASED ON THEIR DIGITAL PROWESS, STATES HAVE DIFFERING PERCEPTIONS ABOUT INTERNATIONAL INFORMATION ORDER
  - UNCHECKED INFORMATION SPACE ACTIVITY CAN CAUSE WARS
  - PROSPECTS OF WARS DUE TO UNREGULATED CYBER ACTIVITY CAN BE ELIMINATED/REDUCED BY CREATING
    - INTERNATIONALLY ACCEPTABLE CYBER NORMS
    - A CYBER CBM REGIME BEFORE CONCLUDING FORMAL TREATIES & CONVENTIONS

PROBLEMS & PROSPECTS

- **REGIONAL LEVEL**
  - AS GOVERNMENT INFRASTRUCTURE BECOMES DIGITALLY LINKED AND THE MILITARY C^2 SYSTEMS COME OF AGE IN SOUTH ASIA, THE PROSPECTS OF AN UNINTENTIONAL WAR OCCURRING DUE TO MALICIOUS CYBER ACTIVITY CANNOT BE RULED OUT
  - MY RESEARCH PAPER PROPOSES A RANGE OF BILATERAL CBMs BETWEEN INDIA & PAKISTAN TO AVERT A WORST CASE SCENARIO THAT COULD BE TRIGGERED BY UNSCRUPULOUS INFO SPACE ACTIVITY

RESEARCH QUESTIONS

- WHAT IS ‘ACCEPTABLE’ BEHAVIOR IN INFO SPACE?
- WHAT ARE THE INTERNATIONAL, REGIONAL, NON-GOVERNMENTAL, PRIVATE AND PUBLIC INITIATIVES TO BRING ORDER INTO INFO SPACE?
- IS THERE A MODEL OF CBMs IN INFO SPACE?
- WHAT COULD BE A SET OF MUTUALLY ACCEPTABLE INFO SPACE CBMs BETWEEN INDIA & PAKISTAN?
- WHAT IS THE WAY FORWARD?

INFORMATION SPACE IS BECOMING AN AREA OF INCREASING THREATS AND CHALLENGES

AN OPEN, SAFE AND SECURE INFORMATION SPACE IS IN THE INTEREST OF ALL STATES

INFO SPACE CHARACTERISTICS

- NO BORDERS OR BOUNDARIES
- DIFFERING NATIONAL POLITICAL & COMMERCIAL INTERESTS / DIGITAL DIVIDE – MONOPOLY OF THE WEST OVER THE INTERNET
- NO DISTINCTION BETWEEN CYBERCRIME & CYBER ATTACKS
- ABSENCE OF CYBER NORMS
- ABSENCE OF LEGALLY BINDING INTERNATIONAL TREATIES
- LACK OF ATTRIBUTION AND PROPORTIONAL RESPONSE
- PRESENCE OF CYBER CRIMINALS & NON STATE ACTORS
- FREE SOCIAL MEDIA

SOCIAL MEDIA & RUMOR MILL

- **1938 -** PANIC CAUSED BY THE WAR OF THE WORLDS BROADCAST
- **2008 -** PANIC CAUSED BY CRANK TELEPHONE CALL
- **2012 -** ETHNIC VIOLENCE IN ASSAM
- **2012 -** YOUTUBE VIOLENCE IN PAKISTAN
- **2013 -** PANIC ON THE WALL STREET

APPLICABILITY OF LAW OF WAR ON CYBER WAR

- THE LAW OF WAR SPECIFIES THAT THE INITIAL ATTACK MUST BE ATTRIBUTED BEFORE A COUNTERATTACK IS PERMITTED
- ARTICLE 2(4) OF UN CHARTER CLEARLY PROHIBITS THE USE OF FORCE:

  "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN."
- DOES CYBER WARFARE FULFILL THE CONDITIONS OF *JUS IN BELLO* (JUSTIFICATION TO GO TO WAR) / *JUS AD BELLUM* (RIGHT CONDUCT OF WAR), UNDER THE PRINCIPLES OF PROPORTIONALITY, DISTINCTION, AND NEUTRALITY AS EXPLAINED IN INTERNATIONAL LAW?

US POSITION ON CYBER ATTACKS

- LEGAL EXPERTS IN THE US CONTEND THAT LAW OF WAR COVERS CYBERSPACE
- US GOVERNMENT RESERVES THE RIGHT TO RESPOND TO CYBER ATTACKS
- OFFICIALS DESCRIBE CYBER ATTACKS AS AN ‘EXISTENTIAL THREAT’ AND TALK OF THE POSSIBILITY OF A POTENTIAL CYBER PEARL HARBOR

SHANGHAI COOPERATION ORGANIZATION (SCO) POSITION ON CYBER WAR

- CYBER WAR IS CONFRONTATION BETWEEN TWO OR MORE STATES IN THE INFORMATION SPACE AIMED AT DAMAGING INFORMATION SYSTEMS, PROCESSES AND RESOURCES, AND UNDERMINING POLITICAL, ECONOMIC AND SOCIAL SYSTEMS, MASS BRAINWASHING TO DESTABILIZING SOCIETY AND STATE, AS WELL AS FORCING THE STATE TO TAKE DECISIONS IN THE INTEREST OF AN OPPOSING PARTY
- THE “MAIN THREATS IN THE FIELD OF ENSURING INTERNATIONAL INFORMATION SECURITY” AS “[D]ISSEMINATION OF INFORMATION HARMFUL TO SOCIAL AND POLITICAL, SOCIAL AND ECONOMIC SYSTEMS, AS WELL AS SPIRITUAL, MORAL AND CULTURAL SPHERES OF OTHER STATES.”

CYBER SECURITY

- **DEFINITION**: COLLECTION OF TOOLS, POLICIES, SECURITY CONCEPTS, SECURITY SAFEGUARDS, GUIDELINES, RISK MANAGEMENT APPROACHES, ACTIONS, TRAINING, BEST PRACTICES, ASSURANCE AND TECHNOLOGIES THAT CAN BE USED TO PROTECT THE CYBER ENVIRONMENT AND ORGANIZATION AND USER'S ASSETS
- **ASSETS**: CONNECTED COMPUTING DEVICES, PERSONNEL, INFRASTRUCTURE, APPLICATIONS, SERVICES, TELECOMMUNICATIONS SYSTEMS, AND THE TOTALITY OF TRANSMITTED AND/OR STORED INFORMATION IN THE CYBER ENVIRONMENT

SOURCE: UN ITU-T X.1205

INTERNATIONAL ORGANIZATIONS MOST ACTIVE IN CYBER SECURITY INITIATIVES

ORGANIZATIONS CONTROLLING THE INTERNET

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

UN INITIATIVES TO CREATE INFO SPACE ORDER

- THE RUSSIAN RESOLUTION OF 1998 TO THE GENERAL ASSEMBLY
- UA/RES/53/70 (4 JANUARY 1999) DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY
- GROUP OF GOVERNMENTAL EXPERTS (GGEs) ON INFORMATION SECURITY SINCE 2004
- INTERNET GOVERNANCE FORUM (IGF) 2006
- INTERNATIONAL CODE OF CONDUCT 2011

UN BODIES ON INFO SECURITY

- POLITICAL-MILITARY STREAM
  - INTERNATIONAL TELECOM UNION (ITU)
  - UN INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR)
  - COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (CTITF) WORKING GROUP
- ECONOMIC STREAM
  - UN OFFICE ON DRUG AND CRIME (UNODC)
  - UN INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI)

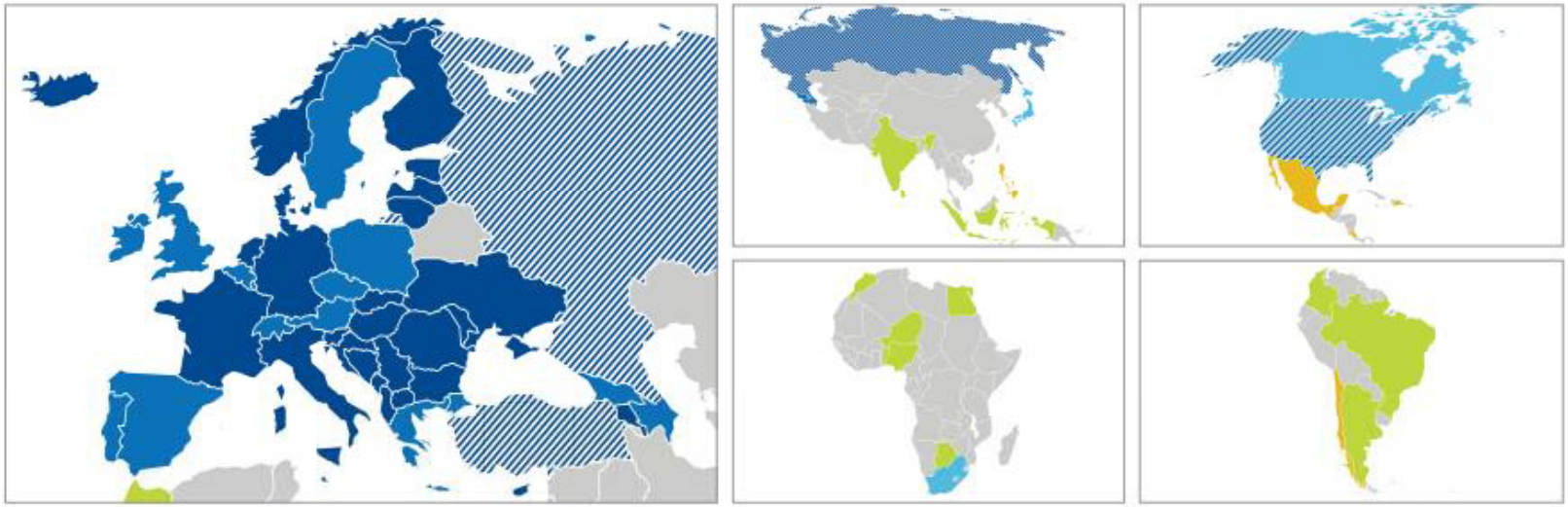
DECISIONS AT WORLD SUMMIT ON INFORMATION SOCIETY (WSIS) 2005

- UN SECRETARY GENERAL ASKED TO CREATE AN INTERNET GOVERNANCE FORUM (IGF)
- INTERNATIONAL TELECOMMUNICATIONS UNION (ITU) GIVEN THE RESPONSIBILITY FOR ACTION LINE C5 – BUILDING CONFIDENCE AND SECURITY IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTs)

LANDMARK TREATY & DOCUMENT

- COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (CEC)
  - LEGALLY BINDING INSTRUMENT
  - ENTERED INTO FORCE IN 2004
  - 39 STATE PARTIES AND 14 SIGNATORIES
  - ADDITIONAL PROTOCOL CAME INTO FORCE IN 2006
- TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE
  - ACADEMIC STUDY WRITTEN BY LEGAL EXPERTS AT THE INVITATION OF NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE
  - PUBLISHED IN MARCH 2013

Global reach of the Council of Europe Convention on Cybercrime



Countries party to the Convention

Council of Europe member states

Albania
Armenia
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Denmark
Estonia
Finland
France
Germany
Hungary
Iceland
Italy
Latvia
Lithuania
Moldova
Montenegro
Netherlands
Norway
Romania
Serbia
Slovak Republic
Slovenia
«the former Yugoslav Republic of Macedonia »
Ukraine

Non Council of Europe member states

United States*

Signatory countries

Council of Europe member states

Austria
Azerbaijan
Belgium
Czech Republic
Georgia
Greece
Ireland
Liechtenstein
Luxembourg
Malta
Poland
Portugal
Spain
Sweden
Switzerland
United Kingdom

Non Council of Europe member states

South Africa
Canada*
Japan*

Countries which did neither ratify nor sign the Convention

Council of Europe member states

Andorra
Monaco
Russia
San Marino
Turkey

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Source: Council of Europe, 9th March 2010

Countries that are known to use the Convention as a guideline for their national legislation

Non Council of Europe member states

Argentina
Botswana
Brazil
Colombia
Egypt
India
Indonesia
Morocco
Nigeria
Sri Lanka

Non Council of Europe member states invited to accede

Chile
Costa Rica
Dominican Republic
Mexico*
Philippines

* observer countries

REGIONAL INITIATIVES

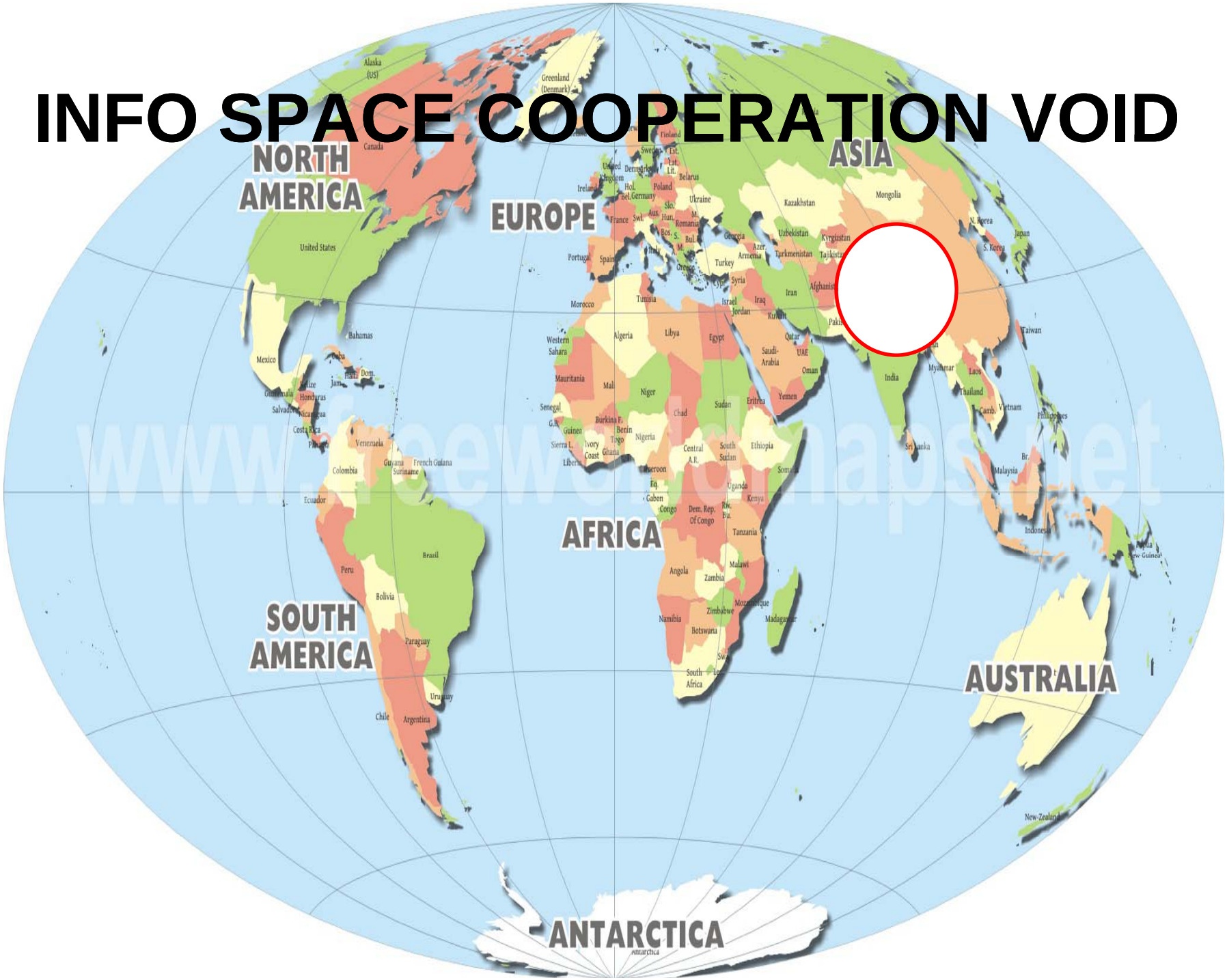
ASIA & AFRICA

- SCO
- ASEAN
- APEC
- AL
- ECOWAS
- AU
- COMESA
- SA?

EUROPE & AMERICAS

- CE
- EU
- OSCE
- OAS
- CARICOM

INFO SPACE COOPERATION VOID

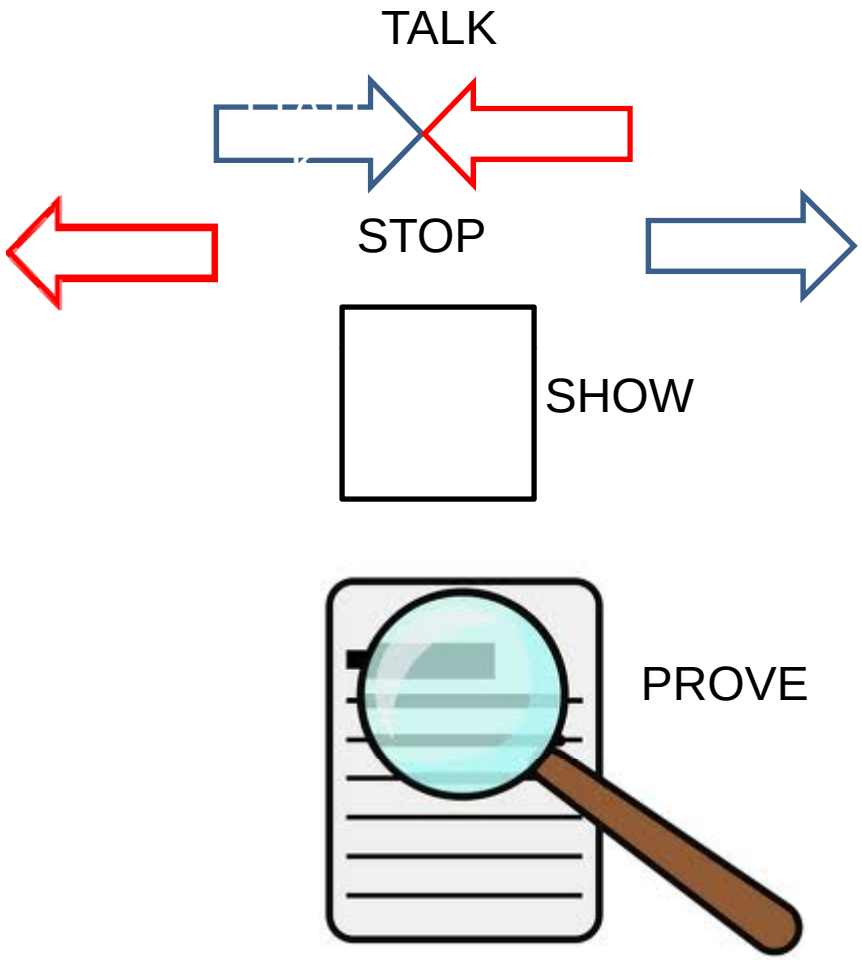


WHY INFO CBMS?

- CYBER ATTACKS CAN CAUSE LETHAL DAMAGE
- THE RESPONSE CAN BE DISPROPORTIONATE TO THE ATTACK
- THERE CAN BE A CASCADING EFFECT
- A WORSE CASE SCENARIO COULD LEAD TO AN EXCHANGE OF NUCLEAR WEAPONS

BASIC ELEMENTS OF CBMs

- COMMUNICATION
- CONSTRAINT
- TRANSPARENCY
- VERIFICATION



UN GUIDELINES ON MILITARY CBMS

- MAJOR OBJECTIVE IS TO REDUCE OR EVEN ELIMINATE THE CAUSE OF MISTRUST, FEAR, MISUNDERSTANDING AND MISCALCULATION WITH REGARD TO RELEVANT MILITARY ACTIVITIES AND INTENTIONS OF OTHER STATES, FACTORS WHICH MAY GENERATE THE PERCEPTION OF AN IMPAIRED SECURITY AND PROVIDE JUSTIFICATION FOR THE CONTINUATION OF THE GLOBAL AND REGIONAL ARMS BUILDUP
- A CENTRALLY IMPORTANT TASK OF CBMs IS TO REDUCE THE DANGERS OF MISUNDERSTANDING OR MISCALCULATION OF MILITARY ACTIVITIES, TO HELP PREVENT MILITARY CONFRONTATION AS WELL AS COVERT PREPARATIONS FOR THE COMMENCEMENT OF A WAR, TO REDUCE THE RISK OF SURPRISE ATTACKS AND OF THE OUTBREAK OF WAR BY INCIDENT; AND THEREBY, FINALLY, TO GIVE EFFECT AND CONCRETE EXPRESSION TO THE SOLEMN PLEDGE OF ALL NATIONS TO REFRAIN FROM THE THREAT OR USE OF FORCE IN ALL ITS FORMS AND TO ENHANCE SECURITY AND STABILITY

US-RUSSIA INFO CBMS

- DEEPER ENGAGEMENT THROUGH SENIOR-LEVEL DIALOGUE
- US-RUSSIA PRESIDENTIAL BILATERAL COMMISSION TO ESTABLISH A NEW WORKING GROUP TASKED TO ASSESS EMERGING THREATS TO ICTs AND PROPOSE JOINT RESPONSES TO SUCH THREATS
- ICT CBMs
  - LINKS AND INFORMATION EXCHANGES BETWEEN THE US AND RUSSIAN CERTs
  - EXCHANGE CYBER SECURITY NOTIFICATIONS THROUGH THE NUCLEAR RISK REDUCTION CENTERS
  - DIRECT CYBER HOTLINE BETWEEN THE WHITE HOUSE AND THE KREMLIN
- SHARING UNCLASSIFIED ICT STRATEGIES & OTHER RELEVANT STUDIES

INDIA-PAKISTAN MILITARY CBMs

- DGMO HOTLINE (1971)
- NON-ATTACK ON NUCLEAR FACILITIES (1988) & EXCHANGE OF LISTS OF NUCLEAR FACILITIES (1992)
- ADVANCE NOTICE OF MILITARY EXERCISES AND MANEUVERS (1991)
- PREVENTION OF AIRSPACE VIOLATIONS (1991)
- MORATORIUM ON NUCLEAR TESTING (1998)
- LINK BETWEEN THE INDIAN COAST GUARD AND THE PAKISTAN MARITIME SECURITY AGENCY (2005)
- INFORMAL CEASEFIRE ALONG LOC (2003)
- PERIODIC FLAG MEETINGS & NON DEVELOPMENT OF NEW POSTS
- BIANNUAL MEETING BETWEEN INDIAN BORDER SECURITY FORCES AND PAKISTANI RANGERS (2004)
- ADVANCE NOTICE OF BALLISTIC MISSILE TESTS (2005)

PAKISTAN'S CYBER SECURITY PLAN 2013

- **CYBER SECURITY BILL** TO PROVIDE FRAMEWORK FOR PRESERVATION, PROTECTION AND PROMOTION OF PAKISTAN'S CYBER SECURITY
- ESTABLISHMENT OF **PAKISTAN COMPUTER EMERGENCY RESPONSE TEAM (PKCERT)**
- ESTABLISHMENT OF A **CYBER SECURITY TASK FORCE** IN COLLABORATION WITH THE MOD, MINISTRY OF IT, MINISTRY OF INTERIOR, MINISTRY OF FOREIGN AFFAIRS, MINISTRY OF INFORMATION, SECURITY ORGANIZATIONS AND SECURITY PROFESSIONALS TO FORMULATE **NATIONAL CYBER SECURITY STRATEGY**
- ESTABLISHMENT OF AN **INTER SERVICES CYBER COMMAND** UNDER THE OFFICE OF THE CHAIRMAN JOINT CHIEFS OF STAFF COMMITTEE TO COORDINATE CYBER SECURITY AND CYBER DEFENSE FOR THE ARMED FORCES
- INITIATING TALKS WITHIN THE AUSPICES OF **SAARC** TO ESTABLISH ACCEPTABLE REGIONAL NORMS OF CYBER BEHAVIOR SO THAT MEMBERS DO NOT ENGAGE IN CYBER WARFARE AGAINST EACH OTHER
- CONCLUDING AN **AGREEMENT WITH INDIA NOT TO ENGAGE IN CYBER WARFARE** PATTERNED ON THE AGREEMENT NOT TO ATTACK NUCLEAR INSTALLATIONS
- ORGANIZING A **SPECIAL MEDIA WORKSHOP** TO PROMOTE AWARENESS AMONG THE PUBLIC AND EDUCATE OPINION LEADERS ON THE ISSUE OF CYBER SECURITY

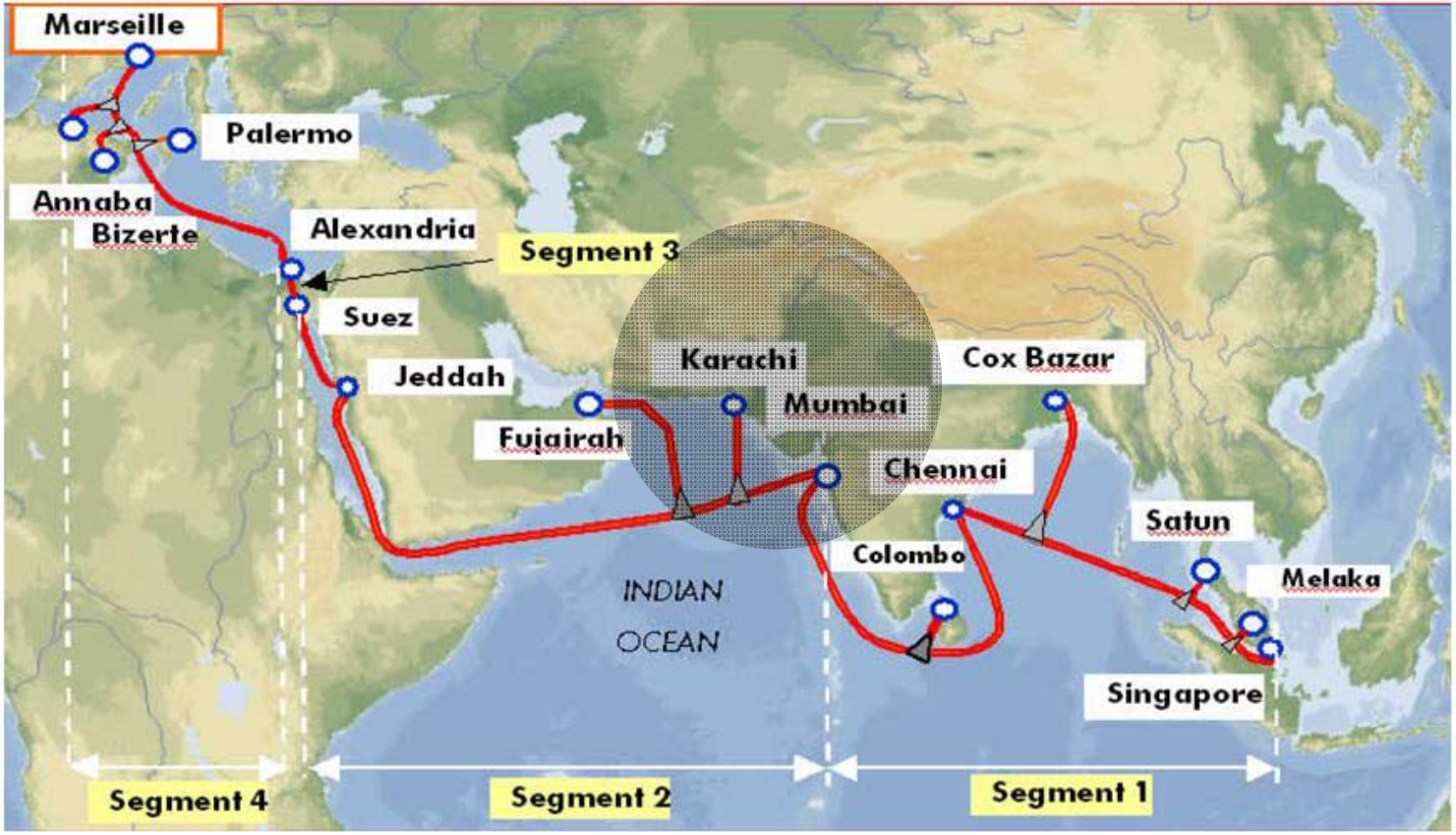
INDIA'S POSITION ON CYBER SECURITY

- IT ACT 2000
- CERT-IN 2004
- CRISIS MANAGEMENT PLAN FOR CYBER ATTACKS 2010
- NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE (NCIIPC) 2011
- GOVERNMENT-PRIVATE SECTOR CYBER SECURITY PLAN 2012
- NATIONAL CYBER SECURITY POLICY (NCSP) 2013
- NATIONAL CYBER SECURITY COORDINATOR 2013
  - NATIONAL TECHNICAL RESEARCH ORGANIZATION (NTRO)
  - HOME MINISTRIES
  - CERT
- PLANS TO HIRE 500,000 CYBER-EXPERTS

INDIA'S CYBER SECURITY COLLABORATION

- MOU BETWEEN US-CERT AND CERT-IN TO PROMOTE CLOSER COOPERATION AND TIMELY EXCHANGE OF CYBER SECURITY INFORMATION (JULY 2011)
- 2+2 MEETING WITH JAPANESE TO EXPAND CYBER COLLABORATION (OCT 2012)
- CYBER COLLABORATION WITH THE UK (FEB 2013)

PAKISTAN INDIA CYBER CONNECTIVITY



The South East Asia-Middle East-West Europe (SEA-ME-WE) 4 project is a next generation submarine cable system linking South East Asia to Europe via the Indian Sub-Continent and Middle East.

PRE-REQUISITES FOR CBMs

- RAISING AWARENESS
- CAPACITY BUILDING
  - DEVELOPING CYBER POLICIES
  - INCIDENT MANAGEMENT & RESPONSE
- IMPROVEMENT OF POLICIES
- CYBER SECURITY WORK PLAN

INFO SPACE CBMs

- INFORMATION SHARING
- JOINT EMERGENCY RESPONSES
- RESTRAINT AGREEMENTS
- RECOGNITION & RESPECT
- DEFINING RESPONSIBILITIES
- ATTRIBUTION

INFO SPACE CBMS BETWEEN INDIA & PAKISTAN

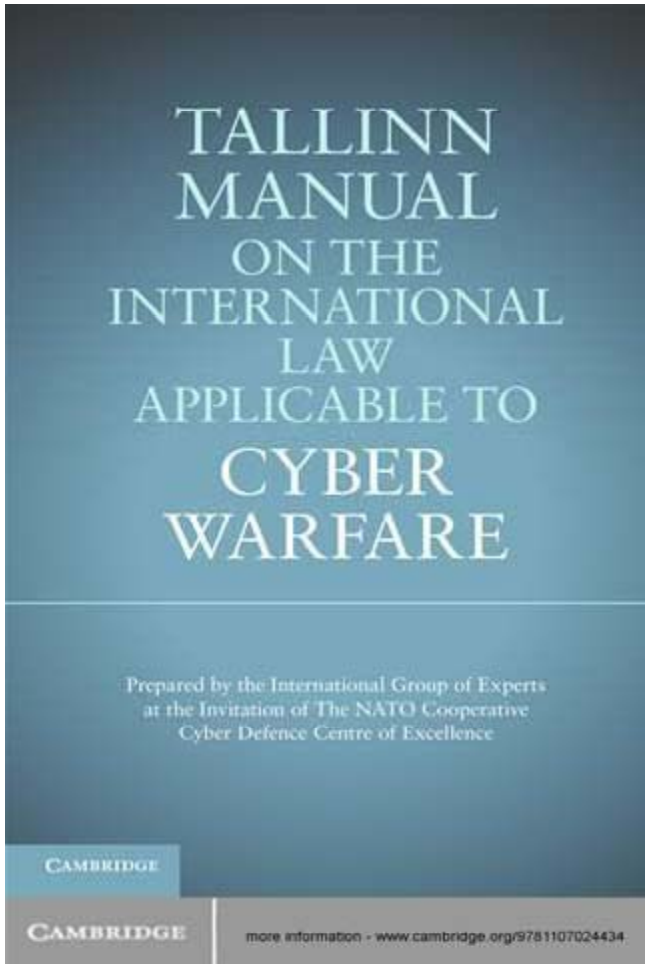
- SHARE BEST PRACTICES IN CYBER SECURITY
- HOLD JOINT TRAINING SESSIONS IN IT UNIVERSITIES ON CYBER ETHICS
- ESTABLISH JOINT FORUMS TO CURB CYBERCRIME
- CREATE A SAARC CERT
- ESTABLISH AN INFO SPACE HOTLINE
- AGREEMENT NOT TO ATTACK NATIONAL CRITICAL INFRASTRUCTURE, COMMERCIAL ENTITIES (BANKS & FINANCIAL ORGANIZATIONS), TRANSPORT SERVICES, EMERGENCY SERVICES (HOSPITALS, FIRE FIGHTING SERVICES & THE POLICE FORCE)
- REFRAIN FROM TARGETING NATIONAL/NUCLEAR COMMAND AUTHORITIES

PROPOSED BILATERAL AGREEMENTS

- AGREEMENT ON CYBERCRIME LAWS
- AGREEMENT ON NOT TO ATTACK ESSENTIAL SERVICES
- AGREEMENT ON NOT TO TARGET NATIONAL COMMAND AUTHORITIES
- AGREEMENT TO REFRAIN FROM HOSTILE PROPAGANDA

RULE 80 OF TALLINN MANUAL

"IN ORDER TO AVOID THE RELEASE OF DANGEROUS FORCES AND CONSEQUENT SEVERE LOSSES AMONG THE CIVILIAN POPULATION, PARTICULAR CARE MUST BE TAKEN DURING CYBER-ATTACKS AGAINST WORKS AND INSTALLATIONS CONTAINING DANGEROUS FORCES, NAMELY DAMS, DYKES, AND NUCLEAR ELECTRICAL GENERATING STATIONS, AS WELL AS INSTALLATIONS LOCATED IN THEIR VICINITY"



WAY FORWARD

- **PRELIMINARY ISSUES**
  - BUILD PUBLIC AWARENESS ABOUT CYBER SECURITY
  - CRAFT DOMESTIC CYBER LAWS & CYBER SECURITY POLICIES
- **PHASE I** (INFORMAL CONTACTS & CAPACITY BUILDING)
  - INITIATE CONTACTS AT THE INFORMAL LEVEL BETWEEN TECHNICAL SOCIETIES THROUGH FORUMS LIKE THE INSTITUTE OF ELECTRICAL & ELECTRONICS ENGINEERS (IEEE)
  - DEVELOP NETWORKS BETWEEN UNIVERSITIES & ACADEMIC COMMUNITIES
  - ORGANIZE REGIONAL SEMINARS
  - JOINTLY SEEK INTERNATIONAL COLLABORATION TO BUILD CAPACITIES

WAY FORWARD

- **PHASE II** (NON MILITARY FORMAL CONTACT)
  - POLICE COLLABORATION TO COMBAT TRANSNATIONAL CYBERCRIME
  - LEGAL COLLABORATION TO HARMONIZE CYBER LAWS & PROSECUTE TRANS-BORDER CRIMINALS
  - COLLABORATION BETWEEN FINANCIAL INSTITUTIONS AND INDUSTRY TO BUILD CYBER DEFENSES
  - FORM JOINT CERTs

WAY FORWARD

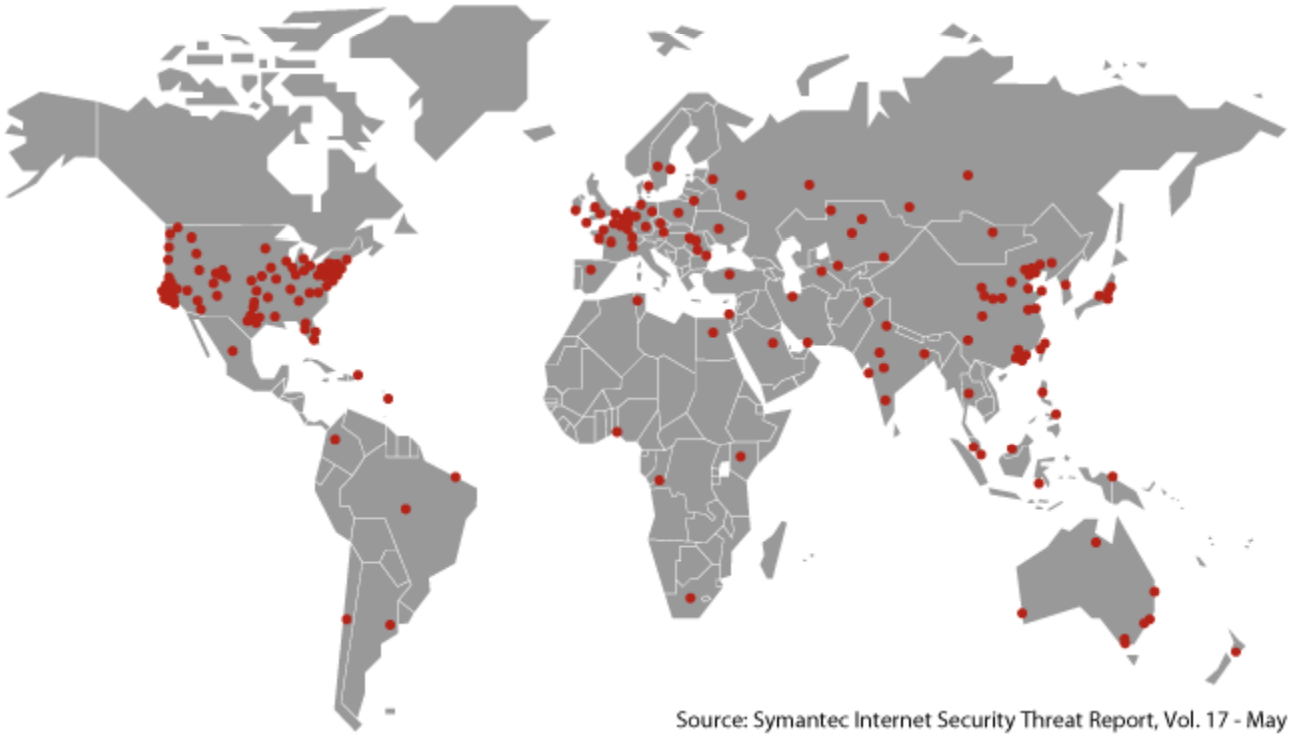
- **PHASE III** (MILITARY CYBER CBMs)
  - DEFINE REDLINES
  - DECIDE UPON DE-ESCALATORY MEASURES
  - ESTABLISH A CYBER HOTLINE
- **PHASE IV** (FORMALIZE CYBER COOPERATION)
  - BILATERAL TREATIES ON CYBERCRIME
  - BILATERAL MILITARY TREATIES

OPENING STATEMENT BY CHAIRMAN SUBCOMMITTEE ON CYBER SECURITY IN ASIA (JULY 23, 2013)

http://www.youtube.com/watch?v=l6G_s8l5Eb0


Q
&
A

Geographical Locations Of Attackers' IP Addresses

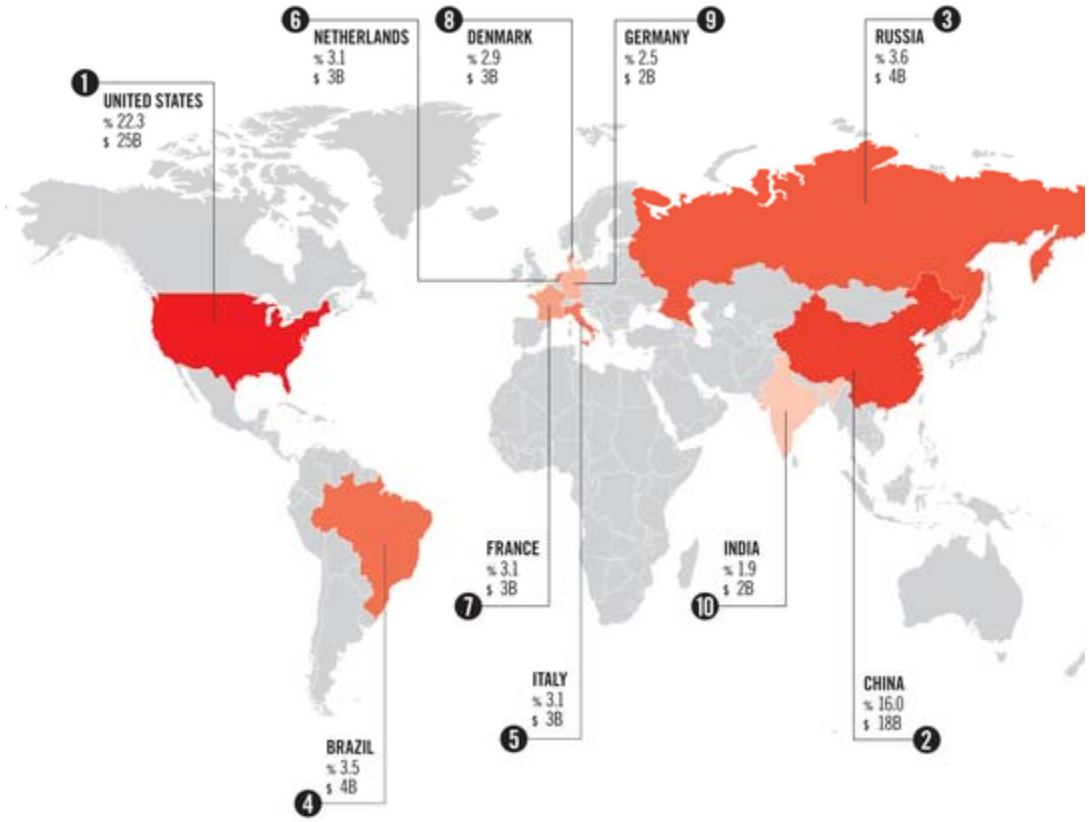


Source: Symantec Internet Security Threat Report, Vol. 17 - May 2012

ORIGIN OF HACKS

% BY COUNTRY OF ORIGIN
$ ESTIMATED COST TO GLOBAL ECONOMY

nccgroup
assure·secure·advise



CYBER WARFARE

THE DIGITAL DIVIDE