SANDIA REPORT
SAND2014-4934
Unlimited Release
Printed June 2014

Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan

Tughral Yamin
Visiting Research Fellow
Cooperative Monitoring Center

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation,
a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's
National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

SAND2014-4934
Unlimited Release
Printed June 2014

Developing Information-Space Confidence Building Measures (CBMs) between India and Pakistan

Tughral Yamin
Cooperative Monitoring Center
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1373

Abstract

The Internet has changed the world in ways hitherto unknown. The international financial system, air, land and maritime transport systems are all digitally linked. Similarly most militaries are fully or partially networked. This has not only sped up the decision making processes at all levels, it has also rendered these systems vulnerable to cyber-attacks. Cyber-warfare is now recognized as the most potent form of non-kinetic war fighting. In order to prevent large scale network-attacks, cyber-powers are simultaneously spending a lot of time, money and effort to erect redundant cyber-defenses and enhancing their offensive cyber capabilities. Difficulties in creating a stable environment in information-space stem from differing national perceptions regarding the freedom of the Internet, application of international law and problems associated with attribution. This paper discusses a range of Confidence Building Measures that can be created between India and Pakistan in information-space to control malicious cyber behavior and avert an inadvertent war.

ACKNOWLEDGMENTS

I am grateful to Sandia National Laboratories (SNL), the US Department of Energy (DOE) and Bob Swartz for providing me this wonderful opportunity to work on a project that is close to my heart. I genuinely think there is an urgent need to address this issue for the sake of peace and stability in the world in general and South Asia in particular, where my homeland is located.

I am thankful to a host of people for making my stay comfortable and for letting me devote my entire energies to single mindedly pursue my assignment. At the top of the list is of course Geoff Forden, my supervisor in Albuquerque and his team: Dave Walker, Jeff Mortimer, Chuck Skeens and Bob Finch. I would like to place on record my thanks to Karl Horak for his useful and insightful contributions on cyber security and to Feroz Hasan Khan for sharing his ideas regarding strategic stability in South Asia.

During the course of my research, I interviewed a number of people in Pakistan and in the US, which enabled me to make headway into this new field of study. This included people in the policymaking circles and cyber security establishment in Rawalpindi and Islamabad and diplomats in our permanent mission in the UN headquarters in New York. This helped me gauge, the official perspective on the subject. I was also provided commendable support by the researchers of Ahmer Bilal Soofi’s law firm on Pakistani cyber laws (or the absence of them).

I was lucky to meet with and interview William O. (Bill) Waddell, Director Mission Command and Cyber Division at the US Army War College, who patiently answered my questions and provided me vital clues to understand this complex and difficult subject.

Finally, I must thank the National University of Sciences and Technology (NUST) Islamabad for allowing me a sabbatical to engage in this interesting research work. In closing, I hope this preliminary study in cyber security would generate the necessary enthusiasm among governments, scholars and professionals to join hands in creating a safer cyberspace.

CONTENTS

1. Introduction 11
   1.1 Organization of the Paper 11
   1.2 Information-space and Information Warfare (IW) 12
   1.3 Information-Space CBMs in South Asia 20

2. INFORMATION CBMs BETWEEN INDIA AND PAKISTAN 25
   2.1 Introduction to CBMs 25
   2.2 Information CBMs 27
      2.2.1 Pre-requisites for Information CBMs 28
      2.2.2 Capacity Building. 28
      2.2.3 Raising Awareness 29
   2.3 Developing Policies and Structures. 29
      2.3.1 Establishing Incident Management and Response Systems. 30
      2.3.2 Holding Cyber Security Incident Response Workshops.[122] 30
      2.3.3 Improving Policies. 30
      2.3.4 Crafting Cyber Security Work Plan. 31

3. Suggested Information CBMs 33
   3.1 Agreement on Cybercrime Laws 34
   3.2 Agreement Not to Attack Essential Services 34
   3.3 Agreement on Not Targeting National Command Authorities 35
   3.4 Agreement to Refrain from Hostile Propaganda 35
   3.5 Joint Emergency Teams 36
   3.6 Joint Monitoring & Policing 36
   3.7 Training 36
   3.8 Information-Space Hotline 36

4. THE WAY FORWARD 39
   4.1 Roadmap for India Pakistan Information-Space CBMs 40
   4.2 Phase I (Informal Contacts and Capacity Building) 40
      4.2.1 Contacts between Technical Societies 40
      4.2.2 Contacts between Academic Communities/Universities 41
      4.2.3 Capacity Building 41
   4.2 Phase II (Non Military CBMs) 41
      4.2.1 Police Collaboration to Combat Transnational Cybercrime 41
      4.2.2 Legal Collaboration to Frame Cyber Laws 42
      4.2.3 Joint CERTs 42
   4.3 Phase III (Military Cyber CBMs) 42
      4.3.1 Define Redlines 42
      4.3.2 Decide Upon De-Escalatory Measures 42
      4.3.3 Establish Cyber Hotline 42
   4.4 Phase IV (Cyber Cooperation through Treaties) 43
      4.4.1 Bilateral Treaties on Cybercrime 43
      4.4.2 Bilateral Military Treaties 43

5. Conclusions 45

6. References 47

Appendix A: Literature Review of Existing Agreements, both Cyber and Otherwise 61
A.1 National Cyber Security Policies and Threat Assessments 61
A.2 International Law and Cyber Norms 62
A.3 CBMs in South Asia 62

Appendix B: International Initiatives to Create Cyber Norms and Behavior 65
B.1 Legality of Cyber-Attacks 66
B.2 International Initiatives 68
B.2.1 The United Nations 68
B.2.2 Other International Organizations and Forums 75
B.3 Regional Initiatives 80
B.3.1 The Shanghai Cooperation Organization (SCO) 80
B.3.2 The Commonwealth of Independent States (CIS) 82
B.3.3 The Council of Europe (CE) 82
B.3.4 The European Union (EU) 83
B.3.5 The European Telecommunications Standards Institute (ETSI) 84
B.3.6 The Organization of American States (OAS) 84
B.3.7 The Organization of Security and Cooperation in Europe (OSCE) 85
B.3.8 The Association of South East Asian Nations (ASEAN) 85
B.3.11 Organizations in Africa 86
B.3.9 Asia Pacific Economic Cooperation (APEC) 86
B.3.12 Network Operations Groups (NOG) 87
B.4 Bilateral Initiatives 87
B.4.1 US-Russian Bilateral Cyber Security Initiatives 87

Appendix C: Existing Domestic Laws and Treaties Regulating Activity in the Information Environment in South Asia 91
C.1 Cybercrime Laws in Pakistan 91
C.1.1 Cyber Security Bill 91
C.2 Cyber Law of India 93
C.2.1 Cyber Defenses of India 93
C.2.2 Foreign Collaboration 94
C.3 The SEA_ME_WE Internet Cable 94

Appendix D: A History of CBMs Between India and Pakistan 95

Appendix E: List of International and Regional Instruments and Short Names 101

Distribution 105

NOMENCLATURE

ACRS Arms Control and Regional Security

ASEAN Association of South East Asian Nations

ASEANAPOL ASEAN National Police Chiefs Conference

ARF ASEAN Regional Forum

C2 Command and Control

CTU Caribbean Telecommunications Union

CE Council of Europe

CEC Council of Europe Convention on Cybercrime

CERT Computer Emergency Response Team

CNCI Comprehensive National Cybersecurity Initiative

CS&C Office of Cybersecurity and Communication

CIS Commonwealth of Independent States

CBMs Confidence Building Measures

CW Chemical Weapons

CWC Chemical Weapon Convention

CNA Computer Network Attacks

CND Computer Network Defense

CNE Network Exploration

CNO Computer Network Operations

CSIRT Computer Security Incident Response Team

CTITF Counter-Terrorism Implementation Task Force

CYBERCOM Cyber Command

DCEO Defensive Computer Effects Operations

DR Disaster Recovery

DOE Department of Energy

DNS Domain Names System

DSB Defense Science Board

DHS Department of Homeland Security

DOD Department of Defense

DOS Denial of Service

DDoS Distributed Denial of Service

ECM Electronic Countermeasures

ENISA European Network & Information Security Agency

Europol European Police Office

ETSI European Telecommunications Standards Institute

EW Electronic Warfare

FIRST Forum of Incident Response and Security Teams

EU European Union

3GPP Third Generation Partnership Project

G8 Group of Eight

GGE Group of Government Experts

GoI Government of India

GOP Government of Pakistan

GGCL Government-to-Government Communications Link

ICANN Internet Corporation for Assigned Names and Numbers

ICC International Criminal Court

ICRC International Committee of the Red Cross

ICS Industrial Control System

ICT Information and Communications Technology

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronic Engineers

IGF Internet Governance Forum

IHL International Humanitarian Law

ISO International Organization for Standardization

ISP Internet Service Provider

IO Information Operations

IW Information Warfare

INTERPOL International Criminal Police Organization

IP Internet Protocol

ISP Internet Service Provider

IT Information Technology

ITU International Telecommunication Union

JTFCND Joint Task Force Computer Network Defense

JS Joint Staff

Ministry of Defense MoD

MilDec Military Deception

NCA National/Nuclear Command Authority

NCSA National Cyber Security Authority

NCCIC National Cybersecurity and Communications Integration Center

NICE National Initiative for Cybersecurity Education

NIPP National Infrastructure Protection Plan

NIST National Institute of Standards and Technology

NITRD Subcommittee on Networking and IT Research & Development

NRRC Nuclear Risk Reduction Center

NSA National Security Agency/Advisor

OASIS Organization of Advance Structured Information Standards

OCEO Offensive Computer Effects Operations

OP-CRC-SC Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

OPSEC Operational Security

PTA Pakistan Telecommunication Authority

P2P Peer-to-Peer

PC Personal Computer

PKI Public Key Infrastructure

PSY-OPS Psychological Operations

PPD Presidential Policy Directive

SAARC South Asian Association for Regional Cooperation

SCADA Supervisory Control and Data Acquisition

SCO Shanghai Cooperation Organization

SEA Syrian Electronic Army

SMS Short Message Service

SOP Standard Operating Procedure

TRAI Telecommunication Regulatory Authority of India

UNGA United Nations General Assembly

UNSC United Nations Security Council

UNSG United Nations Secretary General

UNIDIR United Nations Institute for Disarmament Research

UNODC United Nations Office on Drugs and Crime

USB Universal Serial Bus

USG United States Government

VGT Virtual Global Taskforce

WSIS World Summit on the Information Society

WTO World Trade Organization

WWW Worldwide Web

1. INTRODUCTION

This study looks at the problem of unchecked cyber activity both from the international as well as the regional perspective. It posits that unregulated behavior in cyberspace can lead to inadvertent wars. Since consensus is lacking on how much freedom or control should be exercised in an agreed international information order, this paper theorizes that cyber-differences can be narrowed and a relatively stable cyber-environment can be created by instituting information-space CBMs. Based on the experiences of developing CBMs in South Asia, this paper proposes a range of bilateral trust building measures in information-space to avert a war triggered by unscrupulous cyber-behavior.

The following questions formed the basis of the research:

Q.1 What is 'acceptable' behavior in information-space?

Q.2 What are the international, regional, non-governmental, private and public initiatives to bring about order in the cyberspace?

Q.3 Is there a model for CBMs in information-space?

Q.4 What could be a set of mutually acceptable information-space CBMs between India and Pakistan?

Q.5 What is the way forward?

1.1 Organization of the Paper

This paper has been organized into four parts. This first chapter discusses international initiatives to create cyber norms and behavior and includes a literature review of the relevant work. Appendix A provides an annotated listing of information-space CBMs around the world. The second chapter reviews issues relevant for information-space CBMs and possible approaches. The second chapter takes a look at what general principles might be useful for creating information-space CBMs between India and Pakistan. Appendix B discusses existing national cyber-security measures in Pakistan and India while Appendix C reviews the history of existing confidence building measures. The third chapter suggests possible information-space

CBMs between Pakistan and India and presents a menu of these confidence building measures. Chapter Four outlines a map of how these CBMs might be implemented taking into account the realities of the Indian-Pakistani relations. Overarching conclusions are presented in Chapter 5.

1.2 Information-space and Information Warfare (IW)

Human beings are social animals. They communicate with each other in complex ways, using a variety of spoken and written languages. Homo sapiens have the distinct honor of inventing the sign language and the braille for those amongst them without the natural ability to see or hear. There are thousands of languages and dialects in the world. Over the millennia some of these have died out, a few have been revived and newer ones have emerged including computer languages. An elaborate system of encryption ranging from simple codes and cyphers to exotic algorithms has been developed to keep the content of the messages secret. The Oxford dictionary defines communication as "imparting or exchanging of information or news." Means of communication collectively form the integrated management backbone for all kinds of human undertakings extending from family matters to corporate and government dealings, as well as interstate relationships. Different kinds of agents, instruments and methods are used to pass information. These range from primitive means such as the word of mouth, drumbeats, smoke signals, bugles, messengers, carrier pigeons, and semaphore to the more sophisticated ones like modern computer networks. The area, where information resides, is the information-space. In the Internet lexicon terms like cyberspace and information-space are used interchangeably.[1] For most people cyberspace signifies the world of computer networks. The *Bing Dictionary* describes **cyberspace** as the "imagined place where electronic data goes," or the "the notional realm in which electronic information exists or is exchanged." Others have defined cyberspace in similar terms e.g.

> The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify, and exchange data using computer networks. [2]
>
> A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.[3]

Ronald Reagan once famously said “information is the oxygen of the modern age.”[4] The internet provides the digital oxygen to the contemporary information system. The worldwide web has converted the planet into a virtual global village. The international financial system, air, land and maritime transport structures are all digitally connected and controlled by computer networks. Like the commercial sector, most defense organizations are also fully or partially networked. Digital connectivity has not only sped up the decision making processes, it has also rendered these systems vulnerable to cyber-attacks. Cyber warfare has evolved into what some feel is the most potent form of non-kinetic war fighting. As nations upgrade their net-centric capabilities, they constantly fret about imminent cyber-attacks of 9/11 proportions.[5] As a result they are investing a lot of time, money and effort into developing cyber defenses to protect critical infrastructure like the national command and control (C2) systems. At the same time technologically advanced countries are enhancing their offensive capabilities to launch cyber-attacks against hostile computer networks. Some fear an all pervasive cyber surveillance campaign is in the works. The prospects have become so frightening that countries like Iran, China, Saudi Arabia and Russia are actually working on creating their own Internets.[6]

The Internet is the glue of modern management systems. It holds governments, defense organizations, and financial services together. The airlines, maritime industry, railways, and the road traffic system, to mention a few, are controlled by computer networks. The waterways, logistics services, emergency services, energy management systems, electrical grids and industrial units are operated by SCADA (supervisory control and data acquisition) type of industrial control system (ICS).[7] All these are high-payoff cyber-targets. Cyber-attacks directed against individual PCs or large networks take place singly or as a large well-coordinated operation. The cumulative effects of these attacks can range from minor breakdowns—such as interrupted routine—to major disruptions such as complete system breakdowns. The aftermath can range from mildly chaotic to absolutely devastating. An element of fear can cause unintended panic and mayhem.

Cyberspace or “Cyberia,”[8] instead of becoming an area of cooperation has turned out to be the fifth dimension of war fighting.[9] The fourth being outer space. The devastating effects of cyber-attacks have significantly altered the landscape of modern warfare.[10] In the US cyber annals the roots of cyber conflict have been traced back to events taking place in 1986.[11] Things haven’t stabilized since then. Digitally advanced nations are involved in a bitterly intense competition to dominate cyberspace through the unbridled use of Information Warfare (IW) weapons. Many consider Information Operations (IO) now form an essential part of all military planning and training. A 2011 survey commissioned by the UN Institute for Disarmament Research (UNIDIR) found that 33 states, including China, Russia and the US, have included cyber warfare in their military planning and organization. At least 12 countries including India have either established or are in the process of establishing military cyber warfare organizations.[12]

In order to understand the cyber-language, some of the more commonly used terms are defined as under. Cyber-warfare with both its offensive and defensive facets has been variously defined as:

> [A]ctions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.[13]
>
> [D]eliberate attempt to disable or destroy another country's computer networks.[14]
>
> [D]efending information and computer networks, deterring information attacks, as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary, or even dominating information on the battlefield.[15]

Cyber-attacks are "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[16] **Cyber exploitation** and **cyber espionage** are long-term cyber offensive actions to obtain "information resident on or transiting through an adversary's computer systems or networks," without disturbing "the normal functioning of a computer system or network," and without arousing suspicion. Cyber threats include "external threat actors, insider threats, supply chain vulnerabilities," and threats to the defense establishment.[17] Information Operations (**IO**) is described as the: "Integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." It is meant "to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting [one's] own."[18] The five forms of IO are electronic warfare (EW), computer network operations (CNO), including computer network attacks (CNA), psychological operations (psy-ops), military deception (MilDec) and operational security (Opsec). Computer network warfare is defined as the employment of complete range of CNO to deny the adversaries the use of its computers, information systems, and networks, while ensuring the effective use of one’s own computers, information systems, and networks. These operations include not only CNA but also Computer Network Exploration (CNE), and Computer Network Defense (CND).[19] A combination of these five, along with related supporting capabilities, are used to influence, disrupt, corrupt or usurp adversarial human and automated decision making processes, while protecting one’s own.[20]

As cyber-attacks become increasingly commonplace, new concepts of **cyber security** are also emerging. This defensive mechanism is described as:

> The 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.[21]
>
> One way to ensure cyber-security is by instituting effective local and international laws to check illicit cyber activity. Countries with economies heavily dependent on e-commerce have devised laws to deal with cybercrimes. Federal and state governments in the US have improved cyber security through regulations and collaborative efforts with the private-sector. These cyber regulations are governed by the Comprehensive National Cyber Security Initiative (CNCSI).[22] The purpose of these regulations is to protect companies, organizations and the government from malicious software or malware,[23] such as viruses, worms, Trojan horses, spam emails, scareware, phishing, spear phishing, denial of service (DOS) or distributed denial of service (DDoS) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks.[24] An innocuous Universal Serial Bus (USB) thumb drive might introduce a deadly virus into a computer system.[25] Similarly Peer-to-Peer (P2P) applications, such as those used to share music files, can also introduce security risks that may put information or personal computers (PC) in jeopardy.[26] Numerous measures are available to prevent cyber-attacks. These include firewalls, anti-virus software, intrusion detection and prevention systems, encryption and login passwords.[27]

As what some consider an Internet superpower,[28] the US vigorously pursues its commercial, political, and security. In order to give policy guidelines on cyber affairs, the US State Department has created an office of the Coordinator for Cyber Issues. Its mission is to “promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.”[29] The technical side of the cyber security is handled by the Department of Homeland Security (DHS) and the Department of Defense (DOD). The Office of Cybersecurity and Communications (CS&C) within the National Protection and Programs Directorate is responsible for the security and reliability of the national cyber and communications infrastructure. It works to prevent and minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national point of cyber and communications incident integration.[30]

The US cyber planners have two kinds of cyber threats in mind. Firstly, those aimed against critical government, military and civilian infrastructure, such as electricity and water supply, transportation and communication networks, and financial services. They point towards the 17-fold increase in intrusions into the country’s vital infrastructure and highlight the fact that the ICS running the chemical, electrical, water and transport sectors have all been probed by hackers.[31] The second area of their concern is the large-scale theft/destruction of valuable government, military, private sector and allied country secrets by state-sponsored hackers and criminals. Open sources indicate widespread hacking activity in the private sector, e.g. in August 2012, hackers attacked the networks of Saudi Aramco, destroying data on some 30,000 of the company’s computers.[32] In July 2013, federal prosecutors in New York indicted a group of Russian and Ukrainian hackers for stealing and selling 160 million credit card numbers from more than a dozen companies, causing hundreds of millions of dollars in losses. This has been described as the largest hacking and data breach case in the US.[33] The volume of global online crime is estimated to be between US $110 to 500 billion.[6]

While governments are anxious about rampant theft and crime in cyberspace, some are not averse to buying tantalizing cyber ware from the open market for exactly the same purpose. Coding flaws in software like Microsoft Windows known as “zero day exploits” are being freely sold to the highest bidder by clandestine companies. These open market resources add to a country’s potential to launch effective cyber-attacks, e.g. in June 2013, South Korea blamed the North for attacking 69 websites, including the presidential office and media companies.[34]

In 1998, the Pentagon created a Joint Task Force Computer Network Defense (JTFCND).[35] The task force was subsequently upgraded to a cyber-command (CYBERCOM). The CYBERCOM, which became fully operational on October 31, 2010, now controls all cyberspace operations, organizes existing cyber resources and synchronizes defense of military networks.[36] The commanding general of the CYBERCOM also heads the National Security Agency (NSA). The CYBERCOM is mandated to protect the national security systems from infiltration and disruption. Despite budget cuts and looming 'sequestration,'[37] the US CYBERCOM intends to maintain its cyber capabilities and towards that end, it intends to quadruple its size by hiring a large number of information technology (IT) specialists over the next four years.

As the revolution in military IT affairs took place, the Chinese People's Liberation Army (PLA) has reportedly studied the emerging trends and developed indigenous IW concepts to suit their military strategy.[38] Sweeping reforms were carried out to establish a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the entire electromagnetic spectrum. Their overarching cyber policy is believed by some to have been guided by the doctrine of fighting "Local War under Informationized Conditions."[39] Informatization requires the armed forces to be more "dynamic, flexible, effective, creative and forward looking."[40] Some analysts believe that this policy provides the operational framework to the highly trained PLA units engaging in offensive IOs.[41] The acquired cyber skills are reportedly being sharpened by conducting cyber drills.[42] The PLA's General Staff Department (GSD) 4th Department is believed by some independent analysts to be responsible for Electronic Countermeasures (ECM), while CND and intelligence gathering responsibilities likely belong to the GSD 3rd Department (Signals Intelligence).[39] Reportedly the 2nd Bureau of GSD 3rd Department, which have become commonly referred to as Unit 61398 in the media, poses an Advanced Persistent Threat1 (APT1) to US computer networks.[43] Western media claims that the Chinese cyber-attacks have expanded beyond the government targets to energy sector corporations,[44] universities,[45] and influential newspapers like the *New York Times*.[46]

The US and China have reportedly started broaching the subject of cyber-security in high-level talks.[47] Progress seems slow to outside observers but there are indications that they may cooperate at least in fighting cybercrime.[48] It has been suggested that they could begin by jointly tackling common threats like 'spam' or unsolicited bulk electronic messages sent indiscriminately.[49] In a summit meeting held in the first week of June 2013 the Chinese and the US Presidents are reported to have agreed that "their two countries needed to develop better military-to-military relations and improve cyber security cooperation."[50] Cyber security was reportedly again on the top of the agenda, when top Chinese and American cabinet level officials met during the annual Strategic and Economic Dialogue in July 2013 in Washington DC.

The Russians want tighter controls over the Internet.[51] They are also busy improving their cyber capabilities. In February this year, the Russian Defense Minister Sergei Shoigu reportedly instructed the General Staff to complete proposals to set up an army cyber command by the end of 2013.[52] However, since the US and Russia have a long standing tradition of concluding bilateral nuclear arms limitation and reduction treaties dating back to the Cold War, they appear to some outside observers more confident in matters concerning cyber cooperation. After their meeting on the sidelines of the G8 summit in Ireland on June 15, 2013, the presidents of Russia and the US announced 'landmark steps' to improve cyber-security, including establishing a communications link to exchange information about computer incidents of national security concern. In a joint statement they pledged to create information sharing mechanisms like secure communication channels between national Computer Emergency Response Teams (CERTs). In order to promptly exchange information related to Information and Communications Technologies (ICT) with the aim of reducing tension, the two presidents agreed to authorize the use of the existing direct communications link between their Nuclear Risk Reduction Centers (NRRCs) to resolve cyber tensions,[53] and to establish a direct communication link between high-level cyber officials. Furthermore, a bilateral working group was constituted for consultations on cyber-security related issues. This cyber group was tasked to "assess emerging threats, elaborate, propose and coordinate concrete joint measures to address such threats as well as strengthen confidence."[54]

Cyber-attacks can pose a major decision making dilemma for the victim, in case of a complete breakdown in communication. The US stance to handle such a situation is quite clear. The *International Strategy for Cyber Space* (2011), unambiguously states that the USG reserves the right to "respond to hostile acts in cyberspace," as it "would to any other threat."[55] The Pentagon's Defense Science Board (DSB) believes that China and Russia can develop capabilities to launch an 'existential cyber-attack':

> capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc.[56]

Senior US security managers feel that a ‘cyber Pearl Harbor’ is a distinct possibility.[57] A 2011 Pentagon report to the Congress, describes a hostile cyber-attack as one directed against the economy, government or military, requiring a response using electronic or conventional military options.[58] The officials do not rule out the threat of use of nuclear weapons to deter cyber-attacks.[59] The Pentagon has reportedly updated the rules of military engagement for cyber warfare for the first time in seven years, and developed emergency procedures to guide rapid responses to attacks having serious national security or economic consequences.[60]

US policymakers remain alert to the possibility of hostile cyber-attacks. The Fact Sheet issued by the White House regarding the Nuclear Weapon Employment Strategy has codified “an alternative approach to hedging against technical or geopolitical risk, which will lead to more effective management of the nuclear weapons stockpile.”[61]

How would countries, with less developed cyber policies, react to cyber-attacks is largely unknown. What for instance would they do in case their C2 systems are knocked out? How long would they take to respond? Would they take it as a signal to automatically launch their nuclear tipped missiles? How would the launch orders be passed? Would combatant commanders be allowed to launch nuclear weapons as per their own discretion? How would the unsuspecting population be informed about the impending nuclear holocaust? Would the emergency services be ready to handle the situation? What would be the alternate lines of communication to speak with the adversary to get out of a potentially no-win situation?

It seems possible that fallback options would be limited and unpredictable owing to the fog of war. If irrational or erratic cyber behavior goes unregulated, military and non-military cyber-attacks may become an uncontrollable phenomenon in times to come. The confusion in information-space is likely to be exacerbated because of the activities of non-state actors. Not only is there a need to develop reliable measures to protect the national C2 systems but also to develop a code of conduct among nations to reduce cyber risks. A robust national and international regulatory mechanism can be bolstered through mutually agreed CBMs. This would reduce ambiguity, eradicate doubt and suspicion and improve international cooperation. Such arrangements should increase stability in inter-state relations in military as well as civilian areas, reduce the possibility of cyber conflict and create mechanisms to prevent situations of tension.[63]

1.3 Information-Space CBMs in South Asia

Despite the tremendous potential of growth and progress, South Asia remains a potential conflict zone. The root of disharmony lies in the hasty partition of the South Asian subcontinent in 1947.[64] Intractable issues like the dispute over Kashmir bedevil the relations of the two countries. Since 1998, South Asia has become a veritable nuclear battlefield. Over the years, both India and Pakistan have entered into treaties, agreements and understandings to defuse tensions and prevent wars. One early model of successful negotiations to resolve the issue of the division of water resources was the Indus Basin Treaty of 1960.[65] The fragile stability in the region is maintained through an extensive CBM regime. CBMs are a step below formal treaty agreements. These are important means to reduce the risk of conventional and nuclear wars.[66] India-Pakistan CBMs have been developed both in military and non-military spheres.[67] In order to improve the existing mechanism a structured dialogue process was initiated after the meeting of Prime Ministers Nawaz Sharif and I.K. Gujral on the sidelines of the 9th summit of South Asian Association for Regional Cooperation (SAARC) held in Malé, the capital of Maldives in 1997. Since then, this process has survived a number of crises and continues to sputter along. It broadly covers eight areas,[68] namely Peace and Security including CBMs, Jammu and Kashmir, Siachen, Wullar Barrage Project/Tulbul Navigation Project, Sir Creek, Terrorism and Drug Trafficking, Economic and Commercial, Cooperation and Promotion of Friendly Exchanges in various fields.[69] The leaders, officials and experts of the two countries regularly meet to improve and add to the existing basket of CBM's.[70] The 7th round of expert-level talks on nuclear CBM's was held in New Delhi in December 2012.[71] Information-space CBMs were not on the agenda.

This is worrisome since international fears about cyberspace rivalry in the region are steadily gaining currency. In a recent statement by subcommittee Chairman Steve Chabot (Subcommittee on Asia and the Pacific, Committee on Foreign Affairs) warned that Asia was fast becoming "the cyber security battleground."[72] The solution that he offered was paradoxical. He began by showing the resolve to strengthen the weakest link in the cyber chain by engaging "allies around the world to promote the preservation of global network functionality, in addition to establishing confidence building measures that foster trust and reliability with nations that have become Wild West havens for cyber criminals." He ended up suggesting an alliance between India and US from the "threats emanating from Pakistan." While it is possible to draw too much from these statements, they were met with what might be considered predictable reactions from the Indian media.[73] Surely, if Pakistan is the weakest link then it ought to be strengthened and integrated rather than be isolated and sidelined. Cyber mistrust exists in South Asia and it is likely to aggravate if international cyber battle lines are drawn in the region.

South Asia took most readily to the Internet revolution by adopting a wide array of commercially available ICTs for managing businesses and private affairs. Unfortunately, the region did not do enough to improve the regional cyber security environment. Most of its public and private concerns are now digitally linked to the international system and the militaries are in the process of establishing networked C2 systems. The Indian armed forces have reportedly invested heavily in developing net-centric capabilities since the 1980s,[74] and are now lobbying for a separate cyber-command.[75] Pakistan is reported to have tested its fully automated Strategic Command & Control Support System (SCCSS) in November 2012,[76] and its nuclear safety regime caters to cyber threats.[77] The potential of cyber warfare remains because a growing community of cyber warriors in India and Pakistan are actively engaged in defacing government websites,[78] in a spirit of patriotic 'hacktivism' that reportedly is without formal sanction.[79] Needless to say, this kind of unregulated behavior can cause unnecessary tensions in an already fragile relationship.

Even before the dawn of the digital age both India and Pakistan were aware of the pitfalls of unrestrained information-space activity. The need to curb hostile propaganda was recorded in the first government level negotiations between the two states. Article C (8) of the Liaquat-

Nehru Agreement of 1950 made it incumbent upon the two governments to “Not permit propaganda in either country directed against the territorial integrity of the other or purporting to incite war between them and shall take prompt and effective action against any individual or organization guilty of such propaganda.”[80] As part of the Tashkent (1965) and Simla (1972) Agreements both countries “agreed to ‘discourage’ and ‘prevent’ any hostile propaganda directed against each other and ‘encourage’ the dissemination of such information as would promote the bilateral friendly relations.”[81] Since no monitoring or enforcement mechanisms were enacted, hostile propaganda never ceased. In fact it has increased disproportionately during times of tension, making the situation more combustible.[82]

There are a number of examples to substantiate this theory. For instance in the first 12 hours after Mumbai attacks on November 26, 2008, “the volume of information and misinformation” is reported to have grown exponentially – “much of it drawn from social media messages.”[83] Two days later, the two countries almost went to war, when the Pakistani President received a telephone call purportedly from India’s External Affairs Minister warning him that his country was about to launch a military response.[84] Pakistan took immediate defensive measures. The air force was placed on high alert and all important countries of the world were informed about these developments.[83] The US Secretary of State immediately placed a call on her Indian counterpart, whose delayed response caused panic at her end. [85][86] She then undertook a visit to South Asia to advise India to exercise restraint.[85, p. 271]

Another incident that raised tensions between India and Pakistan was the outbreak of ethnic violence in the North Eastern Indian state of Assam in July and August of 2012. Clashes between the indigenous Bodo tribes and Muslim migrants from Bangladesh resulted in killing, violence and internal displacement. Troops were called in to maintain law and order. A rumor soon started making the rounds that Bodos living elsewhere in India would be killed after the Muslim holy month of Ramzan, coinciding August 20. This hate campaign was fuelled by sending bulk SMS and MMS over the cellphones and through indiscriminate use of social media platforms like the Facebook. As the rumor mill spun out of control the Bodos fled *en masse* for their native homes, choking the local transport system.[87] The Indian government reacted by ordering the telecom services to limit the use of SMS to five per person and the transmission of data beyond 20 KB was banned for 15 days.[88] Indian businesses rely heavily on cellphone advertisements and suffered massive losses. On the international front, India quickly accused Pakistan for sponsoring the unrest.[89] The Government of Pakistan (GOP) asked India to come up with credible proof.[90] Eventually, tensions eased and things returned to business as usual, if only for a brief period.

Almost a month later violence broke out in Pakistan over a sacrilegious movie clip uploaded on YouTube. Twenty people died and public and private property worth millions of rupees was damaged. Police had a hard time restraining the crowds from storming the US embassy. The repercussions were so severe that President Obama and Secretary Clinton had to make public announcements that the USG had nothing to do with the blasphemous movie.[91] The Pakistani government banned YouTube, while the ban continues to this day.[92] It has yet to be determined if the movie was uploaded on purpose to provoke religious sentiments and to incite anti US feelings.

It is not only countries like India or Pakistan that are wracked by spasmodic alarm and anxiety, when unsubstantiated rumors maliciously or inadvertently go viral. On April 23, 2013, a message on the Associated Press Twitter account claimed that two explosions had shaken the White House. Within seven minutes, the Dow Jones Industrial Average dropped by 150 points destroying billions of dollars in value. The tweet was quickly exposed as bogus, the result of hacking by a group identifying itself as the Syrian Electronic Army (SEA). The Dow recovered immediately but the lesson was clear – A single tweet can cause major economic disruption.[93] This was not the last of the shenanigans of the SEA. On August 15, 2013, the *Washington Post* reported that it had been hacked by none other than the dreaded SEA.[94]

These incidents reminds one of the nationwide panic caused in the US after the radio broadcast of H.G. Wells famous fantasy *The War of the Worlds* in 1938.[95] The power of the social media to perpetuate the rumors is unlimited. If the content is malicious the rumor mill can cause mayhem. A scare can be created about a nuclear attack causing panic in the public or false reports generated to undermine launch notification or nuclear accident agreements can trigger unexpected responses at the decision making levels. Therefore, there is an urgent need to develop an agreed framework for building confidence and trust in information-space. A cyber-hotline could be a good way of mitigating disasters created by the malicious spread of dubious information. The US and the Russian Federation are actively considering upgrading their NRRC communication link,[96] for cooperating on matters related to cyber security.[97] Similar options are on the table to reduce Sino-US cyber tensions.[98] The suggestion that Pakistan and India establish their own NRRC has been suggested in the past.[99]

2. INFORMATION CBMS BETWEEN INDIA AND PAKISTAN

2.1 Introduction to CBMs

CBMs are time honored diplomatic tools to build trust and prevent wars. The peace treaty of Hudaybiyah is the earliest documented CBM in Islamic history. The pact was signed between the Muslim pilgrims from Medina and the tribesmen of Quraiysh on the outskirts of Mecca in 6th Al Hijra (628 CE). Although some of the clauses of the treaty appeared highly unfavorable for the Muslims, the agreement to co-exist peacefully for 10 years, gave them time to establish their state and spread their religion in Arabia.[100]

In pre-World War I Europe, it was customary to invite observers from different states (friendly and not so friendly) to witness annual military maneuvers as a means to instill confidence and trust among nations. Most contemporary military CBMs include: communication links like hotlines and regional communication centers; mechanisms to ease border tensions; exchange of military data like troop locations, movements and exercises, military budgets, weapon systems information (conventional, nuclear, chemical and biological); weapon test notifications; demilitarized or thin-out zones and goodwill visits etc.[101] Non-military CBMs cover political, economic, environmental, social and cultural fields.[102]

According to Norwegian political scientists Johan Jørgen Holst and Karen Alette Melander “confidence-building involves the communication of credible evidence of the absence of feared threats by reducing uncertainties and by constraining opportunities for exerting pressure through military activities.”[103] This concept was further refined as “arrangements designed to enhance such assurance of mind and belief in the trust worthiness of states and the fact they create.”[104] CBMs became part of modern diplomacy at the Helsinki Conference on Security and Cooperation in Europe (CSCE). The Helsinki Final Act 1975 described CBMs as means to eliminate the causes of tensions, to promote confidence and contribute to stability and security and to reduce the danger of armed conflict arising from misunderstanding or miscalculation. CBMs are also referred to as Conflict Avoidance Measures, Trust Building Measures, Conflict Resolution Measures, Confidence and Security Building Measures and Confidence Building and Security Measures, and Tension Reduction Measures.

The concept of CBMs was formalized through UN Resolution 33/91 B of December 16, 1978.[105] The UN *Comprehensive Study on Confidence Building Measures* declares that the main purpose of these measures is to “eliminate the sources of tension by peaceful means and thereby to contribute to the strengthening of peace and security in the world.” The study recognized that “Confidence, like security, is a result of many factors, both military and non-military.” It further stated that “the final objective of CBMs is to strengthen international peace and security and to contribute to the development of confidence, better understanding and more stable relations between nations, thereby creating and improving the conditions for fruitful international cooperation.”[106] The primary tools for managing successful CBMs are “communication, constraint, transparency, and verification measures.” Together these make the behavior of states more predictable.[107]

Contemporary CBMs are the legacy of the Cold War and were used extensively to stabilize the East-West relationship.[108] The famous hotline between the White House and the Kremlin was established after the 1962 Cuban Missile Crisis “to reduce the danger of an accident, miscalculation or a surprise attack, and especially an incident that might trigger a nuclear war.”[109] Initially only teletypewriters were deployed at both terminals. In the 1970s, the hotline was upgraded to a telephonic link.[110] The Nuclear Risk Reduction Center (NRRC) began operations on April 1, 1988 through a digitally linked direct government-to-government communications link (GGCL). It is a round-the-clock watch center staffed by members of various government agencies. Its expanded role includes the operation of additional international communications links, which allows the US to implement 13 different nuclear, chemical, and conventional arms control treaties and security-building agreements. The NRRC contributes to bilateral and multilateral transparency and mutual understanding through timely and accurate information exchanges.[111]

The hotline was followed by the arms control talks between the US and the former USSR. The CBMs negotiations were codified in the Helsinki Final Act of 1975.[112] These new generation measures were classified as Confidence and Security Building Measures (CSBMs). The same model was adopted for the Middle East Arms Control and Regional Security (ACRS) working group that was active in the early 1990s.[113] Typically the CBMs include Transparency, Information Exchange Measures, Observation and Verification Measures, and Constraint Measures.[114] In the early 1980s, the UNDC developed a set of guidelines for

CBMs, which was presented at a special UNGA session devoted to disarmament. A couple of these guidelines are reproduced below:

> 1.2.5 A 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.
>
> 1.2.6 A centrally important task of confidence-building measures 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.[115]

Military and non-military CBMs have been introduced in a number of global conflict zones in the Middle East, Europe, the Korean peninsula and South Asia. Appendix D: A History of CBMs Between India and Pakistan, reviews the history of confidence building measures between India and Pakistan.

2.2 Information CBMs

The first mention of information security CBMs was made at the 2005 WSIS summit held in Tunis. It was agreed there that it was essential to strengthen the "trust framework, including information security and network security, authentication, privacy and consumer protection, as a prerequisite for the development of the Information Society and for building confidence among users of ICTs." In order to do so it was considered appropriate that a global culture of cyber-security should be promoted through "cooperation with all stakeholders and international expert bodies." It was understood that developing a cyber-security culture would require "the protection of data and privacy, while enhancing access and trade." These conflicting requirements would require taking into account "the level of social and economic development of each country and respect the development-oriented aspects of the Information Society." The WSIS resolved to support the activities of the UN "to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights.” It recognized spam as “a significant and growing problem for users, networks and the Internet as a whole,” and therefore it needed to be dealt with at “appropriate national and international levels.” Last but not least the WSIS emphasized that “Confidence and security” were “among the main pillars of the Information Society.”[116]

2.2.1 Pre-requisites for Information CBMs

A necessary precondition for developing cyberspace CBMs is to have good national cyber security policies and practices, particularly for the protection of critical infrastructure.[117] Since all countries and most businesses are digitally linked to each other, their mutual interdependence has increased manifold. Axiomatically, therefore, the national cyber practices and policies have regional and international implications. Poor national cyber security practices will most likely weaken collective cyber defenses. In this regard it is in the interest of governments, businesses as well as individual users with greater capacity to assist governments, business and users in countries with lesser capacity. Such measures will improve the confidence and trust among nations and will also strengthen global cyber security. Shoring up the cyber defenses cannot be done by governments alone and expertise available in the private sector, as well as in the academic circles, civil society and users can be helpful. This mutual collaboration requires a number of structural changes.

2.2.2 Capacity Building.

As discussed earlier, a lot of guidance is available on cyber capacity building in the form of the UN resolutions on the Creation of a Global Culture of Cybersecurity (57/239, 58/199, 64/211), the OECD Guidelines for the Security of Information Systems and Networks, as well as the work of the ITU and other intergovernmental agencies, as well as businesses and non-governmental bodies. The key characteristics of this exercise includes stocktaking of the public key infrastructure (PKI);[118] investigating threats and vulnerabilities; identifying stakeholders and their responsibilities; raising national awareness; developing public and private cooperation; putting in place national policies and strategies, developing appropriate organizational structures;

developing appropriate legal frameworks especially to facilitate law enforcement cooperation across jurisdictions on cybercrime; and perhaps most importantly developing a national incident response and management capacity. In each of these fields international cooperation, linkages and networks are important. Clearly, the plan to develop capacity building mechanisms has to be seen from basic design questions through to the implementation stage.[119]

2.2.3 Raising Awareness

Many governments are blissfully ignorant of emerging cyber threats. The first step, therefore, is to raise awareness among official quarters regarding this sensitive topic. Policymakers need to understand how dependent their countries have become on ICTs and the vulnerabilities this reliance has created. This ignorance void can be covered through dialogue between states at the diplomatic, operational and technical levels, and between the public and private sectors on cyber security issues. This can be supplemented by launching initiatives to raise awareness among businesses and individual users to create good online security practices. This can be done for instance by observing annual Cyber Security Awareness Days.[120] This event can help promote secure online practices. Effective partnerships can be established with the industry to address cyber security issues through the development and promotion of good practices guidelines. National Cyber Security Awareness Weeks can also be observed to help users and small businesses to understand cyber security risks, and develop effective cyber security practices.

2.3 Developing Policies and Structures.

Countries without robust cyber security structures are the weak links in the international system. Therefore, it is important to develop sound national cyber security policies. The policies would be based on available cyber ideologies and the prevailing cyber philosophy of the country. This will help form cyber crisis management responses. A well-defined strategy would help the government to streamline and coordinate cyber security approaches. Improved coordination within governments on cyber security issues is a key ingredient in managing coordinated responses. Improved government coordination on cyber security issues would strengthen its capacity to prevent, manage and react to cyber crises. This is also important to harmonize crisis communications measures with other governments. Improved government cyber activity is thus critical in the development of a number of measures between governments.

2.3.1 Establishing Incident Management and Response Systems.

A key element of national cyber security strategy is the creation of national capacity to manage and respond to incidents. A crisis management plan and cyber exercises to test the plan are critical corollaries, vital for improving the national cyber security potential. The plan would be based on a cyber defence design taking into account the data security standards; the mechanism for Cyber Event Detection; Incident Response; Internal Investigation; Third-party Forensic Investigation; Law Enforcement; Customer Notification; and a Containment and Remediation Plan.[121] National incident response capacity is an essential part of the international incident response network. Countries also need to think about their capacity to protect and defend key government networks. The national cyber incident response system requires two bodies i.e. national and organizational CERTs and a Cyber Security Operations Centre for protecting the Government's critical infrastructure.

2.3.2 *Holding Cyber Security Incident Response Workshops.[122]*

Workshops aimed at developing the national and organizational capacities to respond to cyber emergencies can be useful. The objectives of such workshops could include topics such as the essential elements of national cyber defenses; information sharing methods in case of an incident; identifying best practice; and prioritizing capacity building activities for those countries with less mature frameworks and mechanisms. A number of practical scenarios can be discussed at such forums based on the level of willingness of the countries. Challenge could include the information sharing mechanism before an incident occurs and improving preparedness and prevention. Such workshops can become important platforms to understand the capabilities and responsibilities of the countries through face-to-face discussions in an atmosphere of confidence and trust.

2.3.3 Improving Policies.

Developing good cyber security is an ongoing process. These policies and practices need to be constantly improved and the capabilities of the CERTs and Cyber Security Operations Centre upgraded to stand up to emerging challenges. In undertaking this work the governments will have find out areas of common interest in the realm of cyber security. In this respect, it would be worthwhile, to encourage the governments to issue Cyberspace White Papers laying down a framework for maximizing opportunities and minimizing the risks of the digital age.[123] The policies outlined in the White Paper should support the development of long-term trust and confidence in the online world and contribute to the development of international norms of behavior in cyberspace.

2.3.4 Crafting Cyber Security Work Plan.

Last but not least there is a need to develop national cyber security work plans. These work plans should not only provide users a guideline to enforce cyber security measures in government and organizations' offices,[124] but also seriously consider ways and means for peaceful collaboration with other nations in cyberspace.

3. SUGGESTED INFORMATION CBMS

Keeping in mind the basic building blocks of CBMs i.e. communication, constraint, verification and monitoring, countries genuinely interested in establishing confidence and trust in information-space should consider the following:

1. Information Sharing. Sharing information can go a long way in reducing suspicion and mistrust. Non-classified portions of the national cyber security policies; national organizations, programs, or relevant cyber security strategies and standard cyber terminology; emergency response SOPs; and methods of communicating cyber incidents can be conveniently exchanged. A still better way of sharing information can be with regards best practices. This can be done by organizing regional seminars and exchanging visits of experts.

2. Joint Emergency Response Systems. Battling cyber threats jointly can increase the sense of participation in a common cause. A number of countries are already pooling their expertise and resources in regional CERTs and developing joint strategies to respond to ICT emergencies. Emergency drills could be organized to sharpen the skills of first responders.

3. Restraint Agreements. A path breaking form of information-space CBM can be an agreement enjoining upon interested parties to refrain from directing malicious cyber activities against critical infrastructure vital to the wellbeing of civilians, such as telecommunications, energy, transportation and financial systems. Experts are of the opinion that adversaries like the "US and China are *both* increasingly vulnerable to each other in strategic domains – nuclear, space, and cyberspace – where great harm can be done." [125] Commonsense therefore demands that countries should exercise mutual restraint in these fields.

4. Means of Recognition and Respect. Cyber bullying has become a common phenomenon in modern societies.[126] Online hate crime is rife.[127] Cyber intimidation and coercion is now considered part of cyber-terrorism.[128] Such obnoxious behavior can only be controlled by developing an acceptable code of conduct in cyberspace. Unwarranted propaganda and hacktivism can increase mistrust and sour relations. One way to improve trust and confidence is to enter into agreements to recognize and respect national cyber jurisdictions.[129]

5. Defining Responsibilities. If governments are held responsible for the cyber misdeeds of companies and organizations located on their sovereign territories, a lot of irresponsible activity can be curtailed. This can in the long run engender trust. It is therefore important to lay down

precisely the responsibilities of the governments and their national organizations to behave in cyber-space in accordance with the international and national legislations.[130]

6. Means of Attribution. One major problem associated with cyber-attacks is that of 'attribution.' It is very difficult to assign responsibility to the perpetrator of a malicious activity either technically or at a human level. [131] Yet it is not entirely impossible to investigate cyber-attacks forensically and assign responsibility.[132] One way of making attribution easier is by declaring the geographic location of known IP addresses. Exchanging such information on regular basis can become the bedrock of information-space CBMs.

Given their wide experience in negotiating and practicing CBMs, India and Pakistan can find areas of building trust in the information-space as well. Pakistan and India can choose from a host of bilateral agreements on cyber security, some of which are fairly benign.

Following are some of the recommended CBMs:

3.1 Agreement on Cybercrime Laws

Cybercrime is one area where both countries can collaborate without agitating the domestic hawks. An agreement to jointly tackle cybercrime can cover a broad range of issues like harmonizing laws covering cybercrime such as online theft. Social issues like child pornography and human trafficking already find mention in law manuals.[133] An international conference was held in Vienna in September-October 1999, where it was agreed to show zero tolerance towards child pornography on the Internet and to criminalize this activity at the worldwide level.[134] An Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OP-CRC-CPC) was enacted by the UN in 2000.[135] The two countries can expand on the existing statutes and develop laws to curb this nefarious activity, involving regional and international rings.

3.2 Agreement Not to Attack Essential Services

Drawing inspiration from the IHL, Rule 80 of the *Tallinn Manual* recommends that:

> 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.[136]

This humanitarian tenet has actually been practiced in the South Asian wars fought between 1947 and 1971, where India and Pakistan had both avoided bombing essential services like dams, dykes and electrical works. This spirit can be extended into the cyberspace. The essential services not to be subjected to cyber-attacks could be expanded to include financial institutions, industrial units, water and sewerage systems, nuclear power plants, health and emergency services. The critical C2 systems can in fact be declared as a cyber-attack exclusion zone.[137]

3.3 Agreement on Not Targeting National Command Authorities

Cyber-attacks against national/nuclear command authorities (NCAs) can leave individual commanders and weapon handlers with no choice but to make independent decisions with regards conventional as well as nuclear weapons. Such a worst case scenario could have apocalyptic consequences. Fortunately both countries have a CBM, pledging not to attack each other's facilities. Article 1 (i) of this 1988 agreement can be amended by including the cyber dimension through an amendment or an Additional Protocol.[138]

3.4 Agreement to Refrain from Hostile Propaganda

Social media has made the spreading of rumors and fanning hatred much easier than through state controlled media. The governments of Pakistan and India need to seriously study this issue and come up with imaginative ways of curbing uncontrolled activity in this domain. Hostile media effect is a subject of serious study. Case studies indicate that perception management by media can aggravate an already tense situation.[139] There have been agreements between Pakistan and India in the past to cease hostile propaganda against each other e.g. in the fall of 1974, the foreign secretaries of India and Pakistan had exchanged letters agreeing to a cessation of hostile propaganda through radio broadcasts. This agreement came into force on October 21, 1974.[140] Although this was never followed in letter and spirit, this concept can be extended to the social media, to avoid toxic fallouts from instances like a potentially damaging video clip going viral.

3.5 Joint Emergency Teams

Both India and Pakistan can become part of joint teams to handle computer emergencies and monitor criminal and terrorist activity in cyberspace. This can be done at the bilateral level or within the framework of regional organizations like the SAARC or SCO. Both countries are members of the SAARC and have observer status in the SCO. Whereas, SAARC has become a moribund organization, a victim of irreconcilable issues between India and Pakistan, SCO is not only very active in security and counter terrorism issues; it is the only regional association which has an agreement on cyber security. Creating a joint CERT within SCO and SAARC is worth exploring.

3.6 Joint Monitoring & Policing

The two countries can set up a joint cell to monitor illicit activity in cyber space and share vital information. Forming a cyber-police force on the pattern of Interpol, Europol and ASEANAAPOL can be put on the information-space CBM's menu.

3.7 Training

There is a lot of scope for building trust by sharing common experiences at professional forums. Regional seminars and meets of technical people and cyber security experts can be organized to share best practices and common experiences in dealing with computer emergencies.[141] Exchanging IT students for fellowships or regular degrees can be another way of reducing mistrust.

3.8 Information-Space Hotline

Hotlines between the national computer emergency response centers will not only enhance reaction times to respond to emergencies but also strengthen the belief in each other's dependability.

These and other meaningful suggestions can be considered in creating a credible cyber security CBM regime between India and Pakistan.

4. THE WAY FORWARD

It has been suggested in this paper that before formal laws governing cyber activity are formalized, information-space CBMs should be considered. According UN policy guidelines, the ultimate goal of CBMs is to strengthen international peace and security.[142] Peace in cyberspace can be greatly facilitated by instituting internationally recognized cyber code of conduct. This will help reduce tensions, enhance transparency and make state behavior predictable.[143] Imaginative CBMs can precede complex negotiations on treaty agreements and longwinded ratification procedures. CBMs can sometimes even be installed unilaterally. Of course, a well prepared package of CBMs with consensus can set into motion a genuine peace process.

Currently, most activities in cyberspace take place amidst a deep feeling of distrust and high secrecy cyber military applications. Wide disparities of views among states, insufficient research on important regulatory issues and lack of a common vision about the future of cyberspace makes cooperation in this area a complicated issue. Some crucial issues may not lend themselves to a CBM negotiation on broad principles at all. Differences exist on common definitions on cyber warfare, lack of agreement on what constitutes an armed attack or what responses would be justified, and what should be the rules of engagement in cyberspace. It will take a long time before these basic issues are resolved.

At the present juncture there is no movement either on the part of India or Pakistan to broaching the subject of cyber security. The issue of collaborating or building cyber CBMs is nowhere on the horizon. Once the governments recognize that there is a need to include this on the negotiation agenda, the process will start and then problems of structure and content will follow. Contributions from outside, including state parties, international and regional organizations, academic community and dedicated NGOs would help shape the proceedings. Local experts can contribute by taking stock of the existing situation and making independent assessment of how new ideas can be incorporated. For the moment this project may sound ambitious but then this may just be the right time to initiate it before things begin to heat up. Clearly, only genuine negotiations based on common interests will help carry forward the process.[144] Professional groups can help set the agenda for the negotiation, by pressing for more transparency in the official doctrines and recommending better mechanisms of international cooperation and crisis management. UN urges cooperation among governments on the subject of cyber security and the USG is willing to "build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and sustain the law of cyberspace."[145] Well-reflected inputs from published material like the *Tallinn Manual* on the applicability of international law in cyber warfare will prove useful.

Preliminary regional endeavors are already under way, and their dynamics should be used. If a regional approach prevails, some coordinating mechanism should be developed to avoid contrasting or setting contradictory standards. A new forum for cyber security can also be considered outside the existing ones.[146] The political implications and acceptance potential of any of these options have to be weighed carefully, and international experts could be invited to provide their inputs.

4.1 Roadmap for India Pakistan Information-Space CBMs

Before earnest negotiations are undertaken, there is a requirement that the two governments start cooperating by building awareness at public and private levels on the necessity and virtues of cyber-security. Simultaneously there is a need to craft robust domestic cyber laws and wholesome cyber security policies. The suggested approach for establishing sustainable cyber-contacts should progress through a carefully calibrated process from informal to formal stages. It is reiterated that unnecessary media hype and undue publicity can be fatal for any meaningful dialogue in South Asia and hence should be avoided. The following roadmap is suggested.

4.2 Phase I (Informal Contacts and Capacity Building)

4.2.1 Contacts between Technical Societies

The first step in initiating cyber-contacts should be between technical societies working on cyber security issues. These societies should be encouraged to form a regional hub to set semi-official cyber ground rules in South Asia. The governments could patronize these societies and offer them guidance by arranging local and international workshops. The IEEE is one international forum with presence both in India and Pakistan. In Pakistan IEEE sections are located in Islamabad, Lahore and Karachi.[147] Peshawar subsection also appears in the IEEE map. The Islamabad section has a Computer Society Chapter.[148] The IEEE regularly organizes international technical conferences through its computer society.[149] A SAARC IEEE could have a meaningful cyber presence in the region.

4.2.2 Contacts between Academic Communities/Universities

Another informal forum for exchange on cyber information could be the universities. In this regard it would be useful to organize regional seminars to share best practices and showcase the latest trends in cyber security. Universities can play an important role in building capacities through cross pollination of ideas i.e. through exchange of students and by developing courses that could be useful for cyber security professionals. NUST School of Electrical Engineering & Computer Sciences (SEECS)[150] and FAST National University of Computers and Emerging Sciences[151] are two world class schools of computer sciences in Pakistan with the potential of contributing towards developing a common cyber security culture in South Asia.

4.2.3 Capacity Building

Professional organizations can help build national capacities in drafting cyber laws, improving the quality of cyber policing through improved cyber forensics, investigation and prosecution methods. The national parliamentarian training services,[152] bar associations,[153] police training academies,[154] and judicial academies[155] can provide good forums for cyber capacity building. The telecommunication authorities of both countries also need to be trained to handle emergencies like politically motivated unrest spread through rumor mongering on the social media. So far the telecom agencies in South Asia namely, the Telecommunication Regulatory Authority of India,[156] and Pakistan Telecommunication Authority (PTA),[157] have both reacted to inflammatory texting or objectionable video clips by shutting down mobile texting services, laying down restrictions on the content of the text,[158] and banning video sharing and social media sites.[159]

4.2 Phase II (Non Military CBMs)

4.2.1 Police Collaboration to Combat Transnational Cybercrime

Collaboration between the police forces can be an ideal way of creating CBMs at the official level. Cybercrime is a trans-border phenomenon. Regional and international police forces are collaborating to fight it and have successfully established joint monitoring and reporting centers. Collaborations among Interpol, Europol and ASEANAPOL can provide useful examples of joint cyber policing in South Asia.[160]

4.2.2 Legal Collaboration to Frame Cyber Laws

Neither Pakistan nor India is a signatory to the CEC. They can accede to this agreement and also come up with bilateral agreements to harmonize local laws to jointly prosecute transnational cybercrime. The two countries can mutually organize seminars and training sessions to build capacities for lawyers and legislators to frame cyber laws.

4.2.3 Joint CERTs

Pakistan and India can combine forces to respond to computer emergencies by forming joint CERTs bilaterally or within the forum of SAARC or the SCO. A joint CERT would be an excellent CBM.

4.3 Phase III (Military Cyber CBMs)

4.3.1 Define Redlines

Military information-space CBMs can be a hard sell. One way to proceed in this regard could be by setting redlines, which could prompt a response. One way to do so can be by identifying no-go areas, where no cyber operations should be permitted.

4.3.2 Decide Upon De-Escalatory Measures

Keeping various scenarios in mind necessary de-escalatory measures could be worked out in advance before a situation gets out of control.

4.3.3 Establish Cyber Hotline

A dedicated hotline linking professionals and policy planners would help first responders to react immediately and the political leadership to undertake de-escalatory measures quickly.

4.4 Phase IV (Cyber Cooperation through Treaties)

4.4.1 Bilateral Treaties on Cybercrime

The next step to CBMs is concluding regular treaties. Bilateral treaties criminalizing cybercrime would help both countries to efficiently combat cybercrime and increase trust in each other.

4.4.2 Bilateral Military Treaties

Areas can be selected, where the two countries would find it agreeable to collaborate. Binding agreements not to attack each other's national C2 centers could be a major coup, if it can be brokered.

5. CONCLUSIONS

Information based CBMs have yet to be accepted as a means to establishing trust in conflict zones. Yet this is exactly the area, where the nations need to make progress. This is indeed a complex issue involving integration of high technology with low technology, understanding the implications of international law, seeing cybercrime and cyber military attacks as overlapping activities and building a common perception about Internet governance. Of course these ideas have be synchronized with other issues like national security exceptions, human rights and privacy policies, which need careful study.[161] Since cyberspace is becoming more dangerous by the day, there is a dire need to institute international and regional measures to create a healthy respect for national sovereignty in cyberspace.

CBMs between India and Pakistan have a checkered history. Yet in times of crises these have proven extremely useful in preventing wars and facilitating conflict resolution. The first step towards conflict resolution is removal of mistrust and suspicion. Only then, can the dialogue process begin. It is a hard task to popularize the concept of CBMs between the two countries without removing suspicions and misunderstanding among people about the implied objectives and application of such measures.

In order to institutionalize the process of information based CBMs, it is necessary to create basic awareness among governments, organizations and the common man to embrace this concept. Currently, there is little knowledge at policy making circles about the vulnerabilities associated with ICT tools used for governance and management. This awareness can be created with the assistance of international organizations and local NGOs. Workshops, seminars, track II and track III efforts will help.

Multiple factors should be kept in mind, while formulating information-space CBMs. First, the process should be kept out of the media glare. Second, it should begin informally and should steadily progress upto official levels. Thirdly, a regional approach may help and facilitate India and Pakistan move out of the vicious circle of bilateral animosity. SAARC needs to be resuscitated. It can draw some inspiration from ASEAN by constructively keeping a low-key approach to contentious issues.[162] Balance between military and non-military CBMs is essential for creating conditions for peace. Non-military CBMs such as collaboration between the police forces, the legal, technical and academic communities can certainly make things easier for sustaining the dialogue process between the antagonistic parties.

It would be foolish to expect miracles from information-space CBMs overnight. It has taken a considerable amount of time for CBMs to work out in other areas. However, one cannot help but repeat that the need for India and Pakistan to begin negotiating cyber security CBMs is both immediate and vital.

6. REFERENCES

[1] "Timothy L. Thomas, Cyber Silhouettes: Shadows over Information Operations (Fort Leavenworth: Foreign Military Studies, 2005), 13." .

[2] "Michael N. Schmitt ed., Tallinn Manual on the International Law Applicable to Cyber Warfare (New York: Cambridge University Press, 2013), 258." .

[3] "The National Military Strategy for Cyberspace Operations (U), US JS Publication, 2006, http://www.dod.mil/pubs /foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (accessed October 3, 2012). Ronald Reagan Quotes, http://thinkexist.com/quotation/information_is_the_oxygen_of_the_modern_age-it /224364.html (accessed July 4, 2013)." .

[4] "Ronald Reagan Quotes, http://thinkexist.com/quotation/information_is_the_oxygen_of_the_modern_age-it /224364.html (accessed July 4, 2013)." .

[5] "David Garret Jr, 'Cyber Attack is imminent, says DHS Secretary Napolitano,' January 25, 2013, examiner.com, http://www.examiner.com/article/cyber-attack-is-imminent-says-dhs-secretary-napolitano (accessed January 26, 2013).".

[6] "Adam Segal, 'Defending an Open, Global, Secure and Resilient Internet,' CFR Independent Task Force Report No. 70, (June 2013): xi, http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836 (accessed August 15, 2013).".

[7] "Supervisory Control and Data Acquisition (SCADA) Systems, Office of the Manager National Communications System, 2004, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf (accessed April 22, 2013)." .

[8] "Douglas Rushkof, Cyberia: Life in the Trenches of Cyberspace (Manchester: Clinamen Press Ltd, 2002)." .

[9] "Chris Hardy, 'Cyber-space now seen as "fifth dimension of warfare",' Public Service Europe, February 9, 2012, http://www.publicserviceeurope.com/article/1485/cyber-space-now-seen-as-fifth-dimension-of-warfare (accessed June 22, 2013).".

[10] "Dr. Dan Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem,' Information Resources Management College/National Defense University, http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl %20Final.doc (accessed June 15, 2013).".

[11] "Jason Healy ed., A Fierce Domain: Conflict in Cyber Space, 1986 to 2012 (Washington DC: CCSA Publication in partnership with the Atlantic Council, 2013)." .

[12] "James A. Lewis and Katrina Timlin, Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011, http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf (accessed January 12, 2013)." .

[13] "Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and what to do about it (New York: HarperCollins Publishers, 2010), 6." .

[14] "Tom Gjelten, 'Extending the Law of War into Cyberspace,' NPR.COM (September 22, 2010), http://www.npr.org /templates/story/story.php?storyId=130023318 (accessed October 3, 2012).".

[15] "Steven A. Hildreth, Cyberwarfare, Congressional Research Service (June 15, 2001), 16, http://www.fas.org/irp /crs/RL30735.pdf (accessed September 19, 2012)." .

[16] "William A. Owens, Kenneth W. Dam and Herbert S. Lin eds., 'Technology, Policy Law and Ethics regarding U.S. Acquisition and use of Cyberattack Capabilities,' Committee on Offensive Information Warfare, National Research Council (Washington DC: The National Academies, 2009), 10, www.nap.edu (accessed June 15, 2013).".

[17] "US Department of Defense Strategy for Operating in Cyberspace (July 2011), 3, http://www.defense.gov/news /d20110714cyber.pdf (accessed September 24, 2012)." .

[18] "Information Operations, US JS Joint Publication (November 27, 2012), 3-13, http://www.dtic.mil/doctrine/new _pubs/jp3_13.pdf (accessed January 12, 2013)." .

[19] "Jeffrey Carr, Inside Cyber Warfare: Mapping the Cyber Underworld (Sebastopol, CA: O'Reilly Media Inc., 2010), 176." .

[20] "Information Operations, US JS Joint Publication, 3-13." .

[21] "Cybersecurity Information Exchange (CYBEX), UN ITU-T X.1205, (4/2011), http://www.ietf.org/mail-archive /web/mile/current/pdfUoI7Qb1eMb.pdf (accessed June 8, 2013)." .

[22] "US Homeland Security: Cyber Laws & Regulations, http://www.dhs.gov/cybersecurity-laws-regulations (accessed July 4, 2013)." .

[23] "Defining Malware: FAQ, http://technet.microsoft.com/en-us/library/dd632948.aspx (accessed August 14, 2013)." .

[24] "Detailed definitions are given in 'Cyber-Crime: A Growing Challenge for Governments,' Issues Monitor, July 2011, Vol. 8, KPMG International: 2, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications /Documents /cyber-crime.pdf (accessed October 3, 2012).".

[25] "Dave Jevans, 'Little thumb drives now a big security threat,' USA Today, June 15 2013, http://www.usatoday .com /story/cybertruth/2013/06/15/why-thumb-drives-have-become-a-major-security-risk/2426129/ (accessed June 15, 2013).".

[26] "Security Tip (ST05-007): Risks of File-Sharing Technology, US-CERT, February 13, 2013, http://www.us-cert .gov/ncas/tips/ST05-007 (accessed February 14, 2013)." .

[27] "Written testimony of US DHS Secretary Janet Napolitano for a Senate Committee on Homeland Security and Governmental Affairs hearing titled 'Homeland Threats and Agency Responses,' http://www.dhs.gov/news/2012 /09/19/written-testimony-secretary-napolitano-senate-committee-homeland-security-and (accessed July 5, 2013).".

[28] "'Online US is still a Superpower,' June 15, 2013, http://www.eurotopics.net/en/home/presseschau/archiv/article /ARTICLE125313-Online-US-is-still-a-superpower (accessed June 15, 2013).".

[29] "The US State Department: Office of the Coordinator for Cyber Issues, http://www.state.gov/s/cyberissues/ (accessed June 30, 2013)." .

[30] "Office of Cybersecurity and Communications, http://www.dhs.gov/office-cybersecurity-and-communications (accessed July 4, 2013)." .

[31] "'Cyber Threat Source Descriptions,' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (accessed July 3, 2013).".

[32] "Adam Segal, 'What to read on Cyber Security,' Foreign Affairs (November 13, 2012), http://www.foreignaffairs.com/features/readinglists/what-to-read-on-cybersecurity# (accessed January 12, 2013).".

[33] "Nathaniel Popper and Somini Sengupta, 'U.S. Says Ring Stole 160 Million Credit Card Numbers,' New York Times, July 25, 2013, http://dealbook.nytimes.com/2013/07/25/arrests-

planned-in-hacking-of-financial-companies/?nl=todaysheadlines &emc=edit_th_20130726&_r=0 (accessed July 26, 2013).”.

[34] “‘South Korea blames North Korea for cyberattack,’ Dawn, July 16, 2013, http://dawn.com/news/1029460 /south-korea-blames-north-korea-for-cyberattack (accessed July 16, 2013).”.

[35] “Jason Healy, ‘The Future of US Cyber Command,’ The National Interest, July 3, 2013, http://nationalinterest.org /commentary/the-future-us-cyber-command-8688?page=1 (accessed July 5, 2013).”.

[36] “US Army Cyber Command/2nd Army, http://www.arcyber.army.mil/ (accessed June 13, 2013).” .

[37] “The Sequester, http://www.whitehouse.gov/issues/sequester (accessed April 25, 2013).” .

[38] “Timothy L. Thomas, Cyber Bytes (Fort Leavenworth: Foreign Military Studies Office, 2004) and Decoding the Virtual Dragon (Fort Leavenworth: Foreign Military Studies Office, 2007).” .

[39] “Bryan Krekel, Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Report prepared for US-China Economic and Security Review Commission, Northrop Grumman Corporation Information Systems Sector 7575, Colshire Drive McLean, VA 22102 October 9, 2009, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf (accessed June 19, 2013).” .

[40] “Timothy L. Thomas, The Dragon’s Quantum Leap: Transforming from a Mechanized to an Informatized Force (Ft Leavenworth, KS: FMSO, 2009), 39.” .

[41] “Pierluigi Paganini, China vs US, Cyber Superpowers Compared, Infosec Institute Resources, http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/ (accessed June 13, 2013).” .

[42] “‘Cyber war games in China raise concerns in Western media,’ http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130611000105&cid=1101 (accessed July 4, 2013).”.

[43] “‘APT1: Exposing one of China’s Cyber Espionage Units,’ Mandiant Report, www.mandiant.com (accessed June 17, 2013).”.

[44] “David E. Sanger and Nicole Perlroth, ‘Cyberattacks against U.S. Corporations are on the Rise,’ New York Times, May 12, 2013, http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html ?pagewanted=all&_r=0 (accessed June 20, 2013).”.

[45] R. Pérez-peña, “Universities Face a Rising Barrage of Cyberattacks,” *The New York Times*, 16-Jul-2013.

[46] N. Perlroth, “Chinese Hackers Infiltrate New York Times Computers,” *The New York Times*, 30-Jan-2013.

[47] “US, China aligned on N Korea, climate and cybercrime | News | DW.DE | 09.06.2013,” *DW.DE*. [Online]. Available: http://www.dw.de/us-china-aligned-on-n-korea-climate-and-cybercrime/a-16868686. [Accessed: 27-Nov-2013].

[48] “‘China, US Agree to Combat Cyber Crime,’ Beijing International, http://www.ebeijing.gov.cn /BeijingInformation/BeijingNewsUpdate/t1138000.htm (accessed April 25, 2013).”.

[49] “Dragan Stojanovski, ‘Preventing a U.S.-China Cyber War,’ EastWest Institute, http://www.ewi.info/preventing-us-china-cyber-war (accessed June 6, 2013).”.

[50] “‘Obama, Xi Discuss Military-to-Military Relations,’ Cybersecurity, http://www.defense.gov/news/newsarticle .aspx?id=120243 (accessed June 13, 2013).”.

[51] A. E. Kramer, “N.S.A. Leaks Revive Push in Russia to Control Net,” *The New York Times*, 14-Jul-2013.

[52] “Andrei Lvov, ‘Russian Army developing Cyberattack Defences,’ February 27, 2013, Russia beyond the Headline, http://rbth.ru/politics/2013/02/27/russian_army_developing_cyberattack_defenses_23313.html (accessed April 25, 2013).”.

[53] “NRRC: Confidence Building through Information Exchange, http://www.state.gov/t/avc/nrrc/ (accessed June 23, 2013).” .

[54] “‘Cybersecurity high on Agenda of Obama-Putin Meeting,’ Ria Novosti, http://en.ria.ru/russia/20130618 /181726010/Cybersecurity-High-on-Agenda-of-Obama-Putin-Meeting.html (accessed June 17, 2013).”.

[55] “International Strategy for Cyberspace: Prosperity Security and Openness in a Networked World, The White House, (May 2011): 14, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed June 8, 2013).” .

[56] “Geoffrey Ingersoll, ‘Defense Science Board Warns of “Existential Cyber Attack”,’ Business Insider, March 6, 2013, http://www.businessinsider.com/cyber-exploits-turn-weapons-on-us-2013-3 (accessed June 20, 2013) and http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf (accessed October 10, 2013).”.

[57] E. Bumiller and T. Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.,” *The New York Times*, 11-Oct-2012.

[58] D. Alexander, “U.S. reserves right to meet cyber attack with force,” *Reuters*, Washington, 16-Nov-2011.

[59] R. A. Clarke and S. Andreasen, “Cyberwar’s threat does not justify a new policy of nuclear deterrence,” *The Washington Post*, 14-Jun-2013.

[60] “Michael Richardson, ‘When Cyber Attacks Could Lead to War,’ The Strait Times, July 1, 2013, http://www.iseas.edu.sg/ISEAS/upload/files/mr1july13.pdf (accessed July 5, 2013); Thom Shanker, ‘Pentagon is Updating Conflict Rules in Cyberspace,’ New York Times, June 27, 2013, http://www.nytimes.com/2013/06/28/us /pentagon-is-updating-conflict-rules-in-cyberspace.html?ref=cyberwarfare& _r=0 (accessed July 4, 2013).”.

[61] “FACT SHEET: Nuclear Weapons Employment Strategy of the United States, The White House Office of the Press Secretary, June 19, 2013, http://m.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states (accessed June 20, 2013).” .

[62] “Charles Perrow, The Next Catastrophe: Reducing our Vulnerabilities to Natural, Industrial, and Terrorist Disaster, (NJ: Princeton University Press, 2007), 248; Healy, A Fierce Domain, 3.” .

[63] “James Andrew Lewis, ‘Confidence Building Measures and International Agreements in Cyber Security,’ Disarmament Forum, http://unidir.org/pdf/articles/pdf-art3168.pdf (accessed January 7, 2013).”.

[64] S. Wolpert, *Shameful Flight: The Last Years of the British Empire in India*. Oxford University Press, USA, 2006.

[65] “Dennis Kux India-Pakistan Negotiations: Is Past Still Prologue? (Washington DC: USIP, 2006), 13; Arshad H. Abbasi, Indus Basin Treaty, Pildat Report (2012), http://www.pildat.org/publications/publication/FP /IndusWaterTreatybetweenPakistanAndIndia_PakIndiaDialogueIII.pdf (accessed January 12, 2013).” .

[66] A. Z. Hilali, “Confidence-and Security-Building Measures for India and Pakistan,” *Altern. Glob. Local Polit.*, vol. 30, no. 2, pp. 191–222, 2005.

[67] “Saman Zulfqar, ‘Efficacy of Confidence Building Measures (CBMs) in India-Pakistan Relations,’ IPRI Journal , XIII, no. 1 (Winter 2013): 106-116, http://ipripak.org/journal/winter%202013/std2.pdf (accessed June 21, 2013).”.

[68] S. Padder, “The Composite Dialogue between India and Pakistan: Structure, Process and Agency,” *Heidelb. Pap. South Asian Comp. Polit.*, vol. 65, no. Februa, 2012.

[69] “Samarjit Ghosh, ‘Indo-Pak Composite Dialogue - 2008: Review,’ IPCS Special Report 65, February 2009, http://ipcs.org/pdf_file/issue/SR65-Samarjit-Final.pdf (accessed February 25, 2013).”.

[70] “South Asia Confidence-Building Measures (CBM) Timeline, Stimson Center, http://www.stimson.org/data-sets /south-asia-confidence-building-measures-cbm-timeline/ (accessed January 12, 2013).” .

[71] “‘India, Pak Review Implementation, Strengthening of Nuclear CBMs,’ Zee News, December 28, 2012, http://zeenews.india.com/news/nation/india-pak-review-implementation-strengthening-of-nuclear-cbms _819426 .html (accessed January 7, 2013).”.

[72] “Steve Chabot (R-OH), ‘Asia: The Cyber Security Battleground,’ Opening Statement, US Congress Committee on Foreign Affairs, Subcommittee on Asia and the Pacific, July 23, 2013, http://docs.house.gov/meetings/FA/FA05 /20130723/101186/HHRG-113-FA05-20130723-SD001.pdf (accessed July 31, 2013).”.

[73] S. Mehdudia, “Congressional committee calls for strong India-U.S. ties on cyber security,” *The Hindu*, New Delhi, 30-Jul-2013.

[74] “Network Warfare: Armed Forces and NCW, Defence and Security of India DSI, http://defencesecurityindia.com /armed-forces-and-ncw/ (accessed June 12, 2013).” .

[75] “‘India’s Forces to Seek Three New Commands from PM,’ Defence.now, October 20, 2012, http://www.defencenow.com/news/979/indias-forces-to-seek-three-new-commands-from-pm.html (accessed February 14, 2013).”.

[76] “‘Pakistan Tests Medium Range Missile,’ ISPR Press Release, November 28, 2012, http://www.ispr.gov.pk/front /main.asp?o=t-press_release&id=2208 (accessed January 7, 2012).”.

[77] “Pakistan’s nuclear facilities ‘safe and secure’: Masood, The News, July 02, 2013, http://www.thenews.com.pk /Todays-News-13-23837-Pakistans-nuclear-facilities-safe-and-secure-Masood (accessed July 10, 2013).”.

[78] “Muhammad Yusha, ‘India - Pakistan’s Cyber War: CBI Website Still Not Restored,’ Pakistan Spectator: Candid Blog, December 22, 2010, http://www.pkhope.com/india-pakistans-cyber-war-cbi-website-still-not-restored/; ‘India links Pakistan to a terror cyber attack,’ August 28, 2012, http://tacstrat.com/content/index.php/2012/08/28/india-links-pakistan-to-a-terror-cyber-attack/ (accessed January 22, 2013).”.

[79] "'Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose.' Definition posted by Margret Rouse, http://searchsecurity.techtarget.com/definition/hacktivism (accessed June 20, 2013).".

[80] "Agreement between the Governments of India and Pakistan regarding Security and Rights of Minorities (Nehru-Liaquat Agreement 1950), Indian Treaty Series, http://www.commonlii.org/in/other/treaties/INTSer/1950/9.html (accessed February 25, 2013)." .

[81] M. Ahmar, *The challenge of confidence-building measures in South Asia*. New Delhi, India: Har-Anand, 2001.

[82] "Beena Sarwar, 'LOC Tensions: Need Facts not Hype,' January 14, 2013, https://beenasarwar.wordpress.com /2013/01/14/loc-tensions-need-facts-not-hype/ (accessed July 1, 2013).".

[83] P. Nayak, M. Krepon, and Henry L. Stimson Center, *The unfinished crisis US crisis management after the 2008 Mumbai attacks*. Washington, DC: Henry L. Stimson Center, 2012.

[84] "'Hoax call pushed Pakistan to brink of war with India,'" *The Economic Times*. [Online]. Available: http://articles.economictimes.indiatimes.com/2008-12-06/news/28394766_1_india-and-pakistan-mumbai-attacks-mumbai-killings. [Accessed: 27-Nov-2013].

[85] *By Condoleezza Rice:No Higher Honor: A Memoir of My Years in Washington [Hardcover]*. Hardcover.

[86] "Post-26/11, Mukherjee's words rattled Pakistan: Condoleezza Rice," *The Times Of India*. [Online]. Available: http://articles.timesofindia.indiatimes.com/2011-10-28/us/30332002_1_pranab-mukherjee-mumbai-attacks-external-affairs-minister. [Accessed: 27-Nov-2013].

[87] "Assam violence: Where it all began - India - dna." [Online]. Available: http://www.dnaindia.com/india/slideshow-assam-violence-where-it-all-began-1735032. [Accessed: 27-Nov-2013].

[88] "5 Sms Per Day Limit Comes Into Effect- Latest Update," *The Times of India*. [Online]. Available: http://timesofindia.indiatimes.com/topic/5-Sms-Per-Day-Limit-Comes-Into-Effect. [Accessed: 27-Nov-2013].

[89] "India accuses Pakistan of using social media to stir tensions," 20-Aug-2012. [Online]. Available: http://www.abc.net.au/am/content/2012/s3571168.htm. [Accessed: 27-Nov-2013].

[90] "Pakistan seeks proof of messages," *BBC*, 20-Aug-2012.

[91] "Violent protests against video rock Pakistan." [Online]. Available: http://www.aljazeera.com/news/asia/2012/09/20129219618263113.html. [Accessed: 27-Nov-2013].

[92] "Pakistan Demands Filters Before Lifting YouTube Ban," *RadioFreeEurope/RadioLiberty*, 13-Jun-2013.

[93] "Anders Fogh Rasmussen, 'NATO's Next War – in Cyberspace,' The Wall Street Journal, June 2, 2013, wsj.com (accessed June 8, 2013).".

[94] Andrea Peterson, "The Post just got hacked by the Syrian Electronic Army. Here's who they are.," *Washington Post*. [Online]. Available: http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are/. [Accessed: 27-Nov-2013].

[95] “Radio Listeners in Panic, Taking War Drama as Fact; Many Flee Homes to Escape ‘Gas Raid From Mars,’” *The New York Times*, 31-Oct-1938.

[96] “Agreement between the United States of America and the Union of Soviet Socialist Republics on the Establishment of Nuclear Risk Reduction Centers (and Protocols Thereto), Bureau of Arms Control, Verification and Compliance, The US Department of State, http://www.state.gov/t/isn/5179.htm (accessed June 15, 2013). Ellen Nakashima, ‘In U.S.-Russia deal, nuclear communication system may be used for cybersecurity,’ Washington Post, April 26, 2012, http://articles.washingtonpost.com/2012-04-26/world/35453448_1_cyberspace-cybersecurity-russia-and-china (accessed February 25, 2013).”.

[97] “In U.S.-Russia deal, nuclear communication system may be used for cybersecurity,” *Washington Post*. [Online]. Available: http://articles.washingtonpost.com/2012-04-26/world/35453448_1_cyberspace-cybersecurity-russia-and-china. [Accessed: 27-Nov-2013].

[98] “Adam Segal, ‘US-China Cyber Hotline,’ The Diplomat, December 1, 2011, http://thediplomat.com/china-power /us-china-cyber-hotline/ (accessed February 25, 2013).”.

[99] “Rafi uz Zaman Khan, Nuclear Risk Reduction Centers, Stimson Center, October 15, 2003, http://www.stimson.org /images/uploads/research-pdfs/rafikhan.pdf (accessed June 15, 2013).” .

[100] M. Lings, *Muhammad: his life based on the earliest sources*. Rochester, Vt.: Inner Traditions, 2006.

[101] “Confidence-Building Measures | Topics | The Stimson Center | Pragmatic Steps for Global Security.” [Online]. Available: http://www.stimson.org/topics/confidence-building-measures/. [Accessed: 28-Nov-2013].

[102] “OSCE Guide on Non-Military CBMs (Vienna: OSCE Secretariat, 2012), 9, http://www.osce.org/cpc/91082 (accessed July 4, 2013).” .

[103] J. J. rgen Holst and K. A. Melander, “European security and confidence-building measures,” *Survival*, vol. 19, no. 4, pp. 146–154, 1977.

[104] J. J. rgen Holst, “Confidence-building measures a conceptual framework,” *Survival*, vol. 25, no. 1, pp. 2–15, 1983.

[105] “Relationship between Disarmament and International Security, Department of Political and Security Council Affairs United Nations Centre for Disarmament Report of the Secretary-General, 1982, http://www.un.org /disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/SS-8.pdf (accessed April 22, 2013).” .

[106] “Comprehensive Study on CBMs, Department of Political and Security Council Affairs UN Centre for Disarmament Report of the Secretary-General, 1982, http://www.un.org/disarmament/HomePage/ODAPublications /DisarmamentStudySeries/PDF/SS-7.pdf (accessed April 22, 2013).” .

[107] “Confidence-Building and Nuclear Risk-Reduction Measures in South Asia | Research Pages | The Stimson Center | Pragmatic Steps for Global Security.” [Online]. Available: http://www.stimson.org/research-pages/confidence-building-measures-in-south-asia-/. [Accessed: 28-Nov-2013].

[108] 269th Plenary Meeting the OSCE Forum for Security Co-operation in Istanbul, “Vienna Document of the Negotiations on Confidence- and Security-Building Measures,” 16-Nov-1999. [Online]. Available: http://www.osce.org/fsc/41276. [Accessed: 28-Nov-2013].

[109] K. Davenport, “Hotline Agreements | Arms Control Association,” Nov-2012. [Online]. Available: http://www.armscontrol.org/factsheets/Hotlines. [Accessed: 28-Nov-2013].

[110] “Cold War hotline recalled,” *BBC*, 07-Jun-2003.

[111] B. of P. A. Department Of State. The Office of Website Management, “Welcome to the Nuclear Risk Reduction Center (NRRC),” 25-Jul-2008. [Online]. Available: http://www.state.gov/t/avc/nrrc/. [Accessed: 28-Nov-2013].

[112] “Helsinki Final Act - Summits / Ministerial Councils.” [Online]. Available: http://www.osce.org/mc/39501. [Accessed: 28-Nov-2013].

[113] E. Landau, “Assessing the Relevance of Nuclear CBMs to a WMD Arms Control Process in the Middle East Today,” 05-Nov-2012. [Online]. Available: http://www.nonproliferation.eu/documents/backgroundpapers/landau.pdf. [Accessed: 28-Nov-2013].

[114] “UNODA - Confidence Building.” [Online]. Available: http://www.un.org/disarmament/convarms/infoCBM/. [Accessed: 28-Nov-2013].

[115] “Special Report of the Disarmament Commission to the UNGA at its 3rd Special Session devoted to Disarmament, UN Document A/S/-15/3 (May 28, 1988): 31, http://www.un.org/ga/search/view_doc.asp?symbol =A/S-15/3(SUPP) &Lang=E (accessed August 7, 2012).” .

[116] World Summit on the Information Society Geneva, “WSIS: Declaration of Principles.” [Online]. Available: http://www.itu.int/wsis/docs/geneva/official/dop.html. [Accessed: 28-Nov-2013].

[117] National Institute of Standards and Technology (NIST), “Federal Register | Developing a Framework To Improve Critical Infrastructure Cybersecurity.” [Online]. Available: https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity. [Accessed: 28-Nov-2013].

[118] PKI (Public Key Infrastructure), “What is PKI (public key infrastructure)? - Definition from WhatIs.com.” [Online]. Available: http://searchsecurity.techtarget.com/definition/PKI. [Accessed: 28-Nov-2013].

[119] O. M. School and U. of Oxford, “The Global Cyber Security Capacity Centre,” *The Oxford Martin School*. [Online]. Available: http://www.oxfordmartin.ox.ac.uk/institutes/cybersecurity. [Accessed: 28-Nov-2013].

[120] Department of Energy, “AwarenessDayChecklist_12a_currentDOEOCIOlogo.pdf.” [Online]. Available: http://energy.gov/sites/prod/files/AwarenessDayChecklist_12a_currentDOEOCIOlogo.pdf. [Accessed: 28-Nov-2013].

[121] “Cyber Crisis Management: A New Philosophy and Approach to Incident Response | Enterprise Risk Management Initiative (ERM) | North Carolina State College of Management.” [Online]. Available: http://www.poole.ncsu.edu/erm/index.php/articles/entry/Cyber-Crisis-Management/. [Accessed: 28-Nov-2013].

[122] 13 February 2004, “IPSC: PECO Workshop ‘Cybersecurity and Incident Response,’” *Times Higher Education*. [Online]. Available: http://www.timeshighereducation.co.uk/news/ipsc-peco-workshop-cybersecurity-and-incident-response/182893.article. [Accessed: 28-Nov-2013].

[123] “Calls for incoming government to develop another cyber security white paper,” 29-Jul-2013. [Online]. Available: http://www.abc.net.au/worldtoday/content/2013/s3813166.htm. [Accessed: 28-Nov-2013].

[124] “Cyber Security Planning Guide, DHS, http://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity %20Planning%20Guide_1.pdf (accessed July 30, 2013).” .

[125] D. Gompert and P. Saunders, “Paradox of Power: Chapter Six.” [Online]. Available: http://www.ndu.edu/press/paradox-of-power-ch6.html. [Accessed: 28-Nov-2013].

[126] J. Bolton and S. Graeve, *No room for bullies: from the classroom to cyberspace*. Boys Town, Neb.: Boys Town Press, 2005.

[127] “What We Investigate,” *FBI*. [Online]. Available: http://www.fbi.gov/albuquerque/about-us/what-we-investigate/priorities. [Accessed: 28-Nov-2013].

[128] “Dorothy E. Denning, ‘Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, US House of Representatives,’ in Edward V. Linden ed., Focus on Terrorism, Vol. 9, (New York: Nova Science Publishers, 2007), 72-75.”.

[129] W. E. A. of Swiggart, Agin, and LLC, “Jurisdiction in Cyberspace,” *Findlaw*. [Online]. Available: http://corporate.findlaw.com/law-library/jurisdiction-in-cyberspace.html. [Accessed: 28-Nov-2013].

[130] Government Accountability Office, “CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented (GAO-13-187).” [Online]. Available: http://www.gao.gov/assets/660/652170.pdf. [Accessed: 28-Nov-2013].

[131] “W. Earl Bobert, ‘A Survey of Challenges in Attribution,’ Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, 43, http://www.nap.edu/catalog /12997.html (accessed July 30, 2013).”.

[132] “‘Testifying before Senate Judiciary on Attribution and Cybersecurity,’ May 8, 2013, http://www.skatingonstilts .com/skating-on-stilts/2013/05/stewart-baker-cybersecurity-senate-judiciary-committee-testimony.html (accessed July 30, 2013).”.

[133] “Bernadette H. Schell, Miguel Vargas Martin, Patrick C.K. Hung and Luis Rueda, ‘Cyber Child Pornography: A Review Paper of the Social and Legal Issues and Remedies – and a Proposed Technological Solution,’ A Project of the University of Ontario Institute of Technology, Canada and University of Concepcion, Chile, May 9, 2006, http://faculty.uml.edu/jbyrne/44.203/schell_etal_avb_2007.pdf (accessed September 24, 2012).”.

[134] “International Conference on Combating Child Pornography on the Internet, Vienna, 29 September – 1 October 1999, http://textus.diplomacy.edu/thina/txGetXDoc.asp?IDconv=3193 (accessed May 1, 2013). Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UN 2000, http://treaties.un.org/doc/source/RecentTexts/iv-11c_eng.htm (accessed May 1, 2013).” .

[135] “Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UN 2000, http://treaties.un.org/doc/source/RecentTexts/iv-11c_eng.htm (accessed May 1, 2013).” .

[136] “Schmitt, Tallinn Manual, 223.” .

[137] “Ibid, 199.” .

[138] “Discussion with Brigadier Feroz Hassan Khan, leading South Asian nuclear security expert, July 24, 2013.” .

[139] “Robert P. Vallone, Lee Ross and Mark R. Lepper, ‘The Hostile Media Phenomenon: Biased Perception and Perceptions of Media Bias in Coverage of the Beirut Massacre,’ Journal of Personality and Social Psychology, Vol. 49, No. 3 (1985): 577-585, http://www.ssc.wisc.edu/~jpiliavi/965/hwang.pdf (accessed September 19, 2012).”.

[140] “Peter Lyon, Conflict between India and Pakistan: An Encyclopedia, (Santa Barbara, Cal: ABC-CLIO Inc, 2008), 195.” .

[141] “The Role of CBMs in Assuring Cyber Stability, UNIDIR Cyber Security Conference 2012 (CS12): 2, http://www.unidir.org/files/publications/pdfs/the-role-of-cbms-in-assuring-cyber-stability-en-384.pdf (accessed August 7, 2013).” .

[142] “UNGA Resolution 41/60C, Considerations of Guidelines for Confidence-Building Measures (December 3, 1986), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/41/60&Lang=E&Area =RESOLUTION (accessed September 25, 2012).” .

[143] “Ben Basely Walker, ‘Transparency and Confidence Building Measures in Cyber Space: Towards Norms and Behaviors,’ UNIDIR Disarmament Forum - Confronting Cyber Conflict (4/2011): 31-40.”.

[144] “David Churchman, Negotiations: Process, Tactics and Theory (New York: University Press of America, 1995), 1.” .

[145] “International Strategy for Cyberspace, 8.” .

[146] “Henning Wegener, ‘Harnessing the Perils in Cyberspace: Who is in Charge?’ UNIDIR Disarmament Forum (3/2007): 45-52, http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf (accessed January 12, 2013).”.

[147] “IEEE Karachi Section, http://ewh.ieee.org/r10/karachi/ (accessed August 7, 2013).” .

[148] “IEEE Islamabad Section, http://ewh.ieee.org/r10/islamabad/societies.htm (accessed August 7, 2013).” .

[149] “Institute of Electrical and Electronic Engineers (IEEE) Computer Society, http://www.ieee-security.org/ (accessed July 4, 2013).” .

[150] “NUST SEECS, http://seecs.nust.edu.pk/ (accessed August 7, 2013).” .

[151] “FAST-NU for Computer and Emerging Sciences, http://nu.edu.pk/ (accessed August 7, 2013).” .

[152] “Pakistan Institute of Parliamentary Services (PIPS), http://www.pips.org.pk/ (accessed August 7, 2013).” .

[153] “‘Bar Council offers to assist in drafting Cyber Laws,’ The Strait Times, January 24, 1997: 7, http://news.google.com/newspapers?nid=1309&dat=19970124&id=rvxOAAAAIBAJ&sjid=PRUEAAAAIBAJ&pg=3656,3382675 (accessed October 3, 2013).”.

[154] “National Police Academy, Government of Pakistan, http://www.npa.gov.pk/ (accessed August 7, 2013).” .

[155] “Federal Judicial Academy, Government of Pakistan, http://www.fja.gov.pk/ (accessed August 7, 2013).” .

[156] “Telecommunication Regulatory Authority of India, http://www.trai.gov.in/ (accessed September 19, 2012).” .

[157] “Pakistan Telecommunication Authority (PTA), http://www.pta.gov.pk/ (accessed September 15, 2012).” .

[158] "Leslie Horn, 'Dirty Texting Banned by Pakistan Telecom Authority,' PCMag.com, http://www.pcmag.com /article2/0,2817,2396659,00.asp (accessed May 1, 2013).".

[159] "'First Facebook, now Pakistan bans YouTube over "un-Islamic" content,' MailOnline, May 21, 2010, http://www.dailymail.co.uk/news/article-1279889/YouTube-Facebook-banned-Pakistan.html (accessed August 7, 2013).".

[160] "'International Cooperation with ASEANAPOL bolsters Security Landscape, INTERPOL Chief tells Police Meeting,' INTERPOL: Connecting Police for a Safer World, February 20, 2013, http://www.interpol.int/News-and-media/News-media-releases/2013/PR019 (accessed April 25, 2013).".

[161] "Abraham D. Sofaer, David Clark, Whitfield Diffie, 'Cyber Security and International Agreements,' Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for US Policy, http://www.nap.edu/catalog/12997.html (accessed June 8, 2013).".

[162] "Prashanth Parameswaran, 'ASEAN at a Crossroads,' The Diplomat, November 27, 2012, http://thediplomat.com/asean-beat/2012/11/27/asean-at-a-crossroads/ (accessed January 12, 2013).".

[163] US Joint Staff, "National Military Strategy for Cyberspace Operations (NMS-CO)." 2006.

[164] "The Comprehensive National Cybersecurity Initiative | The White House." [Online]. Available: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative. [Accessed: 27-Nov-2013].

[165] "Cyberspace Policy Review | The White House." [Online]. Available: http://www.whitehouse.gov/cyberreview/documents/. [Accessed: 27-Nov-2013].

[166] "Foreign Policy Cyber Security | The White House." [Online]. Available: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity. [Accessed: 27-Nov-2013].

[167] T. L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations*. Foreign Military Studies Office.

[168] T. L. THOMAS, F. M. S. O. F. LAVENFORTH, and J. W. KIPP, *DRAGON BYTES.CHINESE INFORMATION-WAR THEORY AND PRACTICE*. FOREIGN MILITARY STUDIES OFFICE.

[169] "Amir Lupovici, 'Cyber Warfare and Deterrence: Trends and Challenges in Research,' Military and Strategic Affairs, Vol. 3, No. 3 (December 2011), 49-62.".

[170] "Shmuel Even and David Siman-Tov, 'Cyber Warfare: Concepts and Strategic Trends,' The Institute for National Security Studies, Memorandum 117 (May 2012), http://www.inss.org.il (accessed January 24, 2013).".

[171] E. Amoroso, *Cyber Attacks: Protecting National Infrastructure*, 1 edition. Butterworth-Heinemann, 2010.

[172] C. Perrow, *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton, N.J.: Princeton University Press, 2007.

[173] "Dr Detlev Wolter, 'Looking towards the future of cyber security: what does a stable cyber environment look like?' UNIDIR Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability, Geneva, 8-9 November 2012, http://www.unidir.ch/pdf/conferences/pdf-conf1920.pdf (accessed January 24, 2013).".

[174] "UNIDIR : Conference - Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability." [Online]. Available: http://www.unidir.org/programmes/emerging-security-threats/cyber-security-conference-

2012-the-role-of-confidence-building-measures-in-assuring-cyber-stability. [Accessed: 27-Nov-2013].

[175] “CBMs in Cyber Space: What should be India’s Approach? | Institute for Defence Studies and Analyses.” [Online]. Available: http://idsa.in/idsacomments/CBMsinCyberspace_ArvindGupta_270612. [Accessed: 27-Nov-2013].

[176] “Mathias Miellmonka, Cyber CSBMs: Perspective of the German MoD, http://www.unidir.ch/pdf/conferences /pdf-conf1926.pdf (accessed January 24, 2013).” .

[177] “John B. Sheldon PhD, ‘Cyber Incident Information Sharing: A First Step towards Confidence Building?’ http://www.unidir.ch/pdf/conferences/pdf-conf1929.pdf (accessed January 24, 2013).”.

[178] “Dave Clemente, ‘Building Coherence and Understanding Foundational Work,’ Chatham House, http://www.unidir.ch/pdf/conferences/pdf-conf1930.pdf (accessed January 24, 2013).”.

[179] “Kwon Haeryong, ‘The ARF perspective on TCBMs: Future Work,’ http://www.unidir.ch/pdf/conferences/pdf-conf1912.pdf (accessed January 24, 2013).”.

[180] M. N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge [etc.]: Cambridge University Press, 2013.

[181] “Harold Hongju Koh, ‘International Law in Cyber Space,’ Harvard International Law Journal, September 18, 2012, http://www.harvardilj.org/2012/12/online_54_koh/ (accessed June 28, 2013).”.

[182] “Michael N. Schmitt, ‘International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed,’ 54 Harvard International Law Journal, online 13 (2012), http://www.harvardilj.org/2012/online-articles-online_54 _schmitt/ (accessed January 24, 2012).”.

[183] “See for instance Eric A. Fischer, ‘Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions,’ CRS, November 9, 2012, http://www.fas.org/sgp/crs/natsec/R42114.pdf; ‘Global Cyber Law Data Base,’ http://cyberlawsdb.com/main/, ‘Cyber Laws of USA,’http://cyberlawsusa.com/(accessed January 24, 2013).”.

[184] E. Gelbstein, *Information Insecurity: A Survival Guide to the Uncharted Territorities of Cyber Threats and Cyber Security*, vol. 1. United Nations Publications, 2002.

[185] “Ahmed Kamal, The Law of Cyber-Space, (New York: UNITAR, 2007), http://www.un.int/kamal /thelawofcyberspace/The%20Law %20of%20Cyber-Space.pdf (accessed January 16, 2013).” .

[186] O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, “The Law of Cyber-Attack,” *Calif. Law Rev.*, vol. 100, no. 4, 2012.

[187] “Nils Melser, ‘Cyber warfare and International Law,’ Ideas for Peace and Security, 2011, pdf-1-92-905-011-L-en.pdf (accessed January 24, 2013).”.

[188] M. Waxman, “Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4),” *Yale J. Int. Law*, vol. 36, 2011.

[189] “Louise Arimatsu, ‘The legal application of the prohibition of the threat or use of force in cyberspace: A starting point?’ http://www.unidir.ch/pdf/conferences/pdf-conf1934.pdf (accessed January 24, 2013).”.

[190] T. Maurer, *Cyber norm emergence at the United Nations*. September, 2011.

[191] M. Ahmar and Workshop on Internal and External Dynamics of South Asian Security, Eds., *Internal and external dynamics of South Asian security*. Karachi: Fazleesons, 1998.

[192] "Naeem Ahmad Salik, 'CBMs –Past, Present and Future,' Pakistan Defense Review (1998): 70-73.".

[193] Z. N. Jaspal, "Nuclear CBMs between India and Pakistan: Utilitarian Approach - How to build Confidence about our Nuclear Intentions." [Online]. Available: http://www.defencejournal.com/2004-5/gpa.asp. [Accessed: 28-Nov-2013].

[194] M. Lodhi, "CBMs need a bold approach," *Khaleej Times,* 14-Jan-2012. [Online]. Available: http://www.khaleejtimes.com/displayarticle.asp?xfile=data/opinion/2012/January/opinion_January49.xml&section=opinion&col=. [Accessed: 28-Nov-2013].

[195] "Kanti Bajpai, 'CBMs: Contexts, Achievements, Functions,' in Dipanker Banerjee ed., Confidence Building Measures in South Asia (Colombo: Regional Centre of Strategic Studies, 1999).".

[196] "Toby Dalton, Beyond Incrementalism: Rethinking Approaches to CBMs and Stability in South Asia, (Stimson Center, January 30, 2013), http://www.stimson.org/summaries/toby-dalton-on-beyond-incrementalism-rethinking-approaches-to-cbms-and-stability-in-south-asia/ (accessed July 4, 2013)." .

APPENDIX A: LITERATURE REVIEW OF EXISTING AGREEMENTS, BOTH CYBER AND OTHERWISE

This research covered diverse areas ranging from cyber security to international law and CBMs and multiple sources of information and subject experts were consulted. Some of these books and papers are listed in the appendices. See **Error! Not a valid bookmark self-reference.** and

Appendix C: Existing Domestic Laws and Treaties Regulating Activity in the Information Environment in South Asia for a compendium of international organizations and initiatives to improve cyber-security and national efforts in India and Pakistan. The following sections review some important aspects of policies, threat assessments, and legal aspects. The final segment of this section reviews

A.1 National Cyber Security Policies and Threat Assessments

A number of US cyber policy documents are available online e.g. the 2006 Joint Staff National Military Strategy for Cyberspace Operations (NMS-CO),[163] the Comprehensive National Cybersecurity Initiative (CNCI) of 2008 and 2010,[164] the Cyberspace Policy Review (May 2009),[165] and the International Strategy for Cyber Space (2011). According to the US National Security Council (NSC) key documents guiding their policies on cyber security are the Draft National Strategy for Trusted Identities in Cyberspace, the CNCI, the Cyberspace Policy Reviews and supporting documents, the National Initiative for Cybersecurity Education and the Cybersecurtiy R&D.[166]

Timothy Thomas's book *Cyber Silhouettes* is used as a standard textbook on IOs in US military colleges and provides interesting insights into how cyber threats are assessed.[167] Thomas has also written extensively about the evolution and formulation of Chinese strategic cyber thought. His books have been published by the Foreign Military Studies Office (FMSO) Fort Leavenworth.[168]

The concepts of cyber war have been elaborated in papers written by experts like Amir Lupovici,[169] and Shmuel Even and David Siman-Tov.[170] *Cyber Attacks* by Edward Amoroso provides guidelines in protecting national infrastructures from cyber-attacks.[171] Similar solutions are given in Charles Perrow's book *The Next Catastrophe*.[172]

Papers read out at the UNIDIR conference held in Geneva in November 2012 give the national point of views on cyber security and stability of countries like Germany,[173] Canada, India, and Russia.[174] Indian point of view is also available at the IDSA website.[175] The aforementioned paper indicates that Indian policymakers are in favor of cyber CBMs. A range of cyber CBMs are given in papers authored by Mathias Mielmonka of the German MoD,[176] John B. Sheldon of Canada Centre for Global Security Studies, University of Toronto,[177] Dave Clemente of Chatham House,[178] and Kwon Haeryong, the Ambassador of Republic of Korea to the Conference on Disarmament Permanent Mission.[179]

A.2 International Law and Cyber Norms

The applicability of international law is comprehensively covered in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[180] and US Department of State's legal advisor Harold Koh's speech on "International Law in Cyber Space."[181] A critical analysis of the two documents by Michael N. Schmitt makes for an interesting reading.[182] The need to revise federal laws to provide cyber security has been covered in some detail by Eric A. Fischer.[183]

Ambassador Ahmed Kamal, a Pakistani diplomat has produced two monographs regarding developing international cyber norms and laws. The first one, which he co-authored with Eduardo Gelbstein, is titled ***Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*.**[184] A sequel to this book is ***The Law of Cyber-Space: An Invitation to the Table of Negotiations*.**[185] Other works that provide important pointers in this respect are "The Law of Cyber-Attack,"[186] "Cyberwarfare and International Law,"[187] "Cyberattacks and the Use of Force: Back to the Future of Article 2(4),"[188] "The legal application of the prohibition of the threat or use of force in cyberspace: A starting point?"[189] A good idea of how the various bodies within the UN are shaping international cyber norms can be obtained from an article that Tim Maurer wrote for the Belfer Center in 2011.[190]

A.3 CBMs in South Asia

A number of papers and books were consulted to understand the nature of CBMs in South Asia. South Asian scholars have written substantially on this topic e.g. Moonis Ahmer,[191] Feroz Hasan Khan,[41] Naeem Salik,[192] Zafar Nawaz Jaspal,[193] Maleeha Lodhi,[194] Kanti Bajpai and Dipanker Banerjee.[195] Another paper that provided useful inputs was one written by Toby Dalton of the Stimson Center.[196] So far there has been work on developing info based CBMs between India and Pakistan. In this regard it is hoped that this paper will prove to be a catalyst for more work on this subject.

APPENDIX B: INTERNATIONAL INITIATIVES TO CREATE CYBER NORMS AND BEHAVIOR

Human society is governed by a host of rules and regulations. Informally these consist of accepted customs and traditions based on social, moral and ethical codes. At spiritual and official levels there are canons, commandments, decrees, dogmas, doctrines, laws, regulations, rules and tenets formally enshrined in religious scriptures, penal codes and state constitutions. At the interstate level activities are regulated and governed by a comprehensive set of international laws and conventions. Irrespective of the fact that at times countries tend to violate these edicts and even get away with it, standardized conventional norms and behavior lie at the heart of international relations. In order to make all transactions legitimate and acceptable, a host of international laws and conventions have been created. This urge to regulate all human activity extends into the realm ICT.

Arguably the modern information age began with the advent of the electrical telegraph in 1837. The first electronic language was the Morse code – a simple method of dots and dashes, to relay instant information. The first trans-Atlantic telegraphic message was conveyed in 1858. The transatlantic telegraph cables have since been replaced by transatlantic telecommunications cables. Telegraph was followed by more novel and secure methods to carry sound as well as image in real time through line, wireless and satellites. The development in technology was complemented by laws to control and regulate these new media of transmitting information. Whereas stringent censorship rules were invoked by governments during times of war and internal strife to protect or isolate their citizens from hostile propaganda, clear cut laws were also developed at the national and international levels to regulate the use of telegraphy and telephony, radio, print and electronic media. Unregulated use of these media, it was feared, could spell chaos and anarchy. Although the Internet has allowed boundless to access and transmit information, no international law has so far been created to regulate cyber activity. Paradoxically, notwithstanding the inherent dangers of cyber terrorism, the digitally advanced countries feel that unfettered access to Internet is good for commerce and therefore, it should be left as it is.

B.1 Legality of Cyber-Attacks

An unprotected information-space is open invitation for not only criminals and ideologues but also for nation states to launch cyber-attacks on the sly, without any a formal declaration of war. There has been a debate within the legal community, whether IW operations are covered by the classic definition of Law of War aka Law of Armed Conflict or the International Humanitarian Law (IHL). Unfortunately “the existing legal norms do not offer a clear and comprehensive framework within which states can shape policy responses to the threat of hostile cyber operations.” The argument revolves around a number of issues like what justifies the use of force, how to determine the attribution of the attack and what should be the proportionality of response? Since all cyber-attacks are not state sponsored and are in certain instances the handiwork of sundry freelancers and loose cannons, criminals and terrorists, hence it is legally not possible to pin the blame on a state party. Not at least in the short term. The law of war specifies that the initial attack must be attributed before a counterattack is permitted. Article 2(4) of the UN Charter explicitly states that “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 United Nations.” This, however, does not deny them the right of self-defense under the provisions of *jus in bello* (the international law governing the resort to force by States) and *jus ad bellum* (international law regulating the conduct of armed conflict), under the principles of proportionality, distinction, and neutrality. This begs the question, whether cyber warfare fulfills these conditions. One school of thought believes that cyberspace remains outside the jurisdiction of International Law, while the other is convinced that this is not the case. One strong proponent of the opposing school of thought is Harold Koh, the legal expert of the US State Department. Koh has built an impressive case of justifying that cyber-attacks and cyber counter attacks are governed by international law by answering a set of ten frequently asked questions. The International Group of Experts hired to draft the *Tallinn Manual* for NATO’s Cooperative Cyber Defense Center of Excellence also concur with Koh’s version that force can be used in cyberspace under the internationally accepted principles of *jus ad bellum* and *jus ad bello*.

Opinion is also divided about the lethality of cyber weapons. Lethal literally means an activity causing death. High profile cyber-attacks have incapacitated government servers in Georgia, halted banking operations in Estonia and interrupted and delayed Iranian nuclear program, without killing anyone. Therefore, anonymous cyber-attackers do not fit the conventional description of a combatant or someone guilty of war crimes. Deaths in combat can be justified and crimes against humanity like genocide can be persecuted under the Rome statute by the International Criminal Court (ICC). In the absence of death and destruction and lack of proof with regards attribution, a physical response is difficult to justify. The situation may change if there are casualties as a direct or indirect consequence of a cyber-attack. One can argue that a lethal assault supported by computer technology can be construed as an act of war.

Cyber-attacks are generally aimed against computer systems. It is, however, impossible to separate cybercrime from state sponsored cyber-attacks. Both are overlapping activities because states, criminals and non-state actors all use the same toolkit. Cybercrime broadly refers to illegal activities on computer networks directed against individuals, organizations and governments. It can cause huge losses to common citizens and businesses and can cripple governments and nations. This poses serious challenges to domestic and international law enforcement agencies. The existing laws are not strong enough to seriously curb criminal activity in cyberspace. The threat is enormous and requires unified international legislation and enforcement mechanisms. General countermeasures have been adopted by some governments and organizations to prevent criminal activity in cyber space. This includes legislation and technical measures to track down online crimes, Internet content control, using public or private proxy and computer forensics, encryption and plausible deniability etc. The problem is that each country follows its own set of rules and regulations for dealing with cybercrimes. These laws need to be harmonized into an international regime and relevant provisions and clauses are incorporated into domestic legal codes.

Although governments are actively focusing on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges i.e. cyberspace has no political borders and the methods of the cyber-criminal community are continuously evolving, making it more challenging and difficult for governments and companies to keep pace with them. Some 82 countries have signed and/or ratified one of the binding cybercrime instruments. Some countries are members of more than one such instrument. The Council of Europe (CE) Cybercrime Convention (CEC) has the largest number of signatures or ratifications/accessions i.e. 48 countries, including five non-member states. Other instruments have smaller geographic scope e.g. the League of Arab States Convention (18 countries or territories), the Commonwealth of Independent States (CIS) Agreement (10 countries), and the SCO Agreement (6 countries). If signed or ratified by all member states of the African Union (AU), the Draft AU Convention could have up to 54 countries or territories. The list of major international and regional instruments on cyber security is given towards the end of this paper.

B.2 International Initiatives

Legal difficulties like affixing culpability and differentiating between cybercrime and cyber-attacks notwithstanding, a number of international and regional instruments have been formulated to promote cyber security and prevent counter cybercrime. These include binding and non-binding instruments. A table listing these instruments on cyber security is given towards the end of this study. Five groups active in creating cyber norms are the Council of Europe (CE) and the European Union (EU), the Commonwealth of Independent States (CIS) and the Shanghai Cooperation Organization (SCO), intergovernmental African organizations, the League of Arab States, and the United Nations (UN). These initiatives are no doubt motivated by international obligations from not interfering “in any form or for any reason whatsoever in the internal and external affairs of other States.” However, the cooperation in cyber security is proceeding at a slow pace. Some of the international initiatives in developing cyber norms are listed below:

B.2.1 The United Nations

Under Article 11 of its Charter, the UN General Assembly (UNGA) has the mandate to consider general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments, and makes recommendations to the member states or to the UN Security Council (UNSC). Discussions and decisions at the UNGA on disarmament and international security issues have led to significant developments. The Disarmament and International Security Committee aka the First Committee and the UN Disarmament Commission (UNDC) are two subsidiary bodies dedicated to disarmament issues. Two more bodies namely the UN Institute for Disarmament Research (UNIDIR) and the Advisory Board on Disarmament Matters also deal with disarmament issues. Additionally, the UNGA receives inputs from a number of reporting mechanisms and Groups of

Government Experts (GGEs). The 1st Committee explicitly deals with disarmament, global challenges and threats to peace that affect the international community and seeks solutions to the challenges in the international security regime.

B.2.1.1 UNGA Resolutions on Cyber Security

The Assembly is only empowered to make non-binding recommendations on international issues within its competence. It has nonetheless, initiated a number of political, economic, humanitarian, social and legal action, affecting the lives of millions of people throughout the world. With reference to international security, the UNGA has passed a number of resolutions on cyber security. There is no evidence to suggest that the subject has been raised within the UNSC – the highest body within the global organization. The Russian Federation first introduced a draft resolution on information security in the First Committee in 1998. This resolution was based on the agenda item "Developments in Telecommunications and Information in the context of International Security" and was adopted without a vote as UNGA Resolution 53/70 (June 30-July 2, 1999). Since then there have been three annual reports on the subject (2010, 2011 and 2012) incorporating the views of the member states have been published. Two related resolutions were passed by the Second Committee, on the "Creation of a Global Culture of Cyber-Security and the Protection of Critical Informational Infrastructures," and "Creation of a Global Culture of Cyber-Security and Taking Stock of National Efforts to Protect Critical Information Infrastructures." The 2nd Committee essentially deals with global economic and financial issues.

In August 1999, the UNIDIR organized an international meeting of experts in Geneva to consider the security implications of emerging IT. Its conclusions were included in UNGA Resolution 57/53, which called upon member states to further consider and discuss information security issues and provide relevant inputs. The resolution also called for a new study of international informational security issues, but there was little action on it. Similar exhortations in subsequent UNGA sessions failed to produce any meaningful progress.

B.2.1.2 The UN Group of Governmental Experts (GGEs) on Information Security

In 2004, the UNGA first formed a 15 member GGE to examine existing and potential threats from the cyber-sphere and suggest possible cooperative measures to address them. This

Group could not come to an agreement on matters like the impact of developments in ICT on national security and military affairs issues and the question whether the discussion should address issues of information content or focus only on information infrastructures. There was particular disagreement regarding the claim that trans-border information content should be controlled as a matter of national security. Other areas of disagreement arose on proposals for capacity-building and technology transfer to developing countries.

In July 2010, the second GGE, which included cyber security specialists from major cyber-powers like the US, China, and Russia, submitted a set of recommendations for "building the international framework for security and stability that these new technologies require." In the foreword to the 2010 GGE Report, the UN Secretary General (UNSG) highlighted the need for further dialogue on the issue of information security and the need to develop 'common perspectives.' The Report itself stressed on the need for dialogue to discuss norms pertaining to state use of ICT, to reduce collective risk and protect critical national and international infrastructure; confidence-building, stability and risk reduction measures to address the implications of state use of ICT, including exchanges of national views on the use of ICT in conflict; information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; identification of measures to support capacity-building in less developed countries; and finding possibilities to elaborate common terms and definitions relevant to UNGA Resolution 64/25. The Report had also recommended the need to find possibilities to elaborate common terms and definitions. These recommendations represent progress in cyber security issues and could become the basis of a multilateral treaty under the auspices of the UN, which Russia has been advocating.

The inputs of the member states were included in the UNGA resolution 66/24, which called for the formation of a new GGE in 2012. The new GGE was asked to continue studying existing and potential threats in the sphere of information security and possible cooperative measures to address them, taking into account the assessments and recommendations contained in the last report. This GGE was tasked to report to the 68th session of the UNGA scheduled in September 2013. The third GGE has met thrice so far – once in 2012 and twice in 2013. Members include Argentina, Australia (Chair), Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK and USA.

The GGE meeting held in June 2013 agreed that CBMs, such as “high-level communication and timely information sharing, can enhance trust and assurance among states and help reduce the risk of conflict by increasing predictability and reducing misperception.” The Group agreed on the “vital importance of capacity-building to enhance global cooperation in securing cyberspace” and the requirement of an open and accessible cyberspace. It was thought that a combination of all these efforts would support a more secure cyberspace. Most importantly the Group affirmed that “international law, especially the UN Charter, applies in cyberspace.”

B.2.1.3 International Code of Conduct on Information Security

On September 12, 2011 China, Russia, Tajikistan and Uzbekistan proposed an international code of conduct on information security to the UNSG. The document discussed security challenges posed to the international community in cyberspace and recommended responsibilities of states in protecting information and cyber-networks, calling upon states to respect domestic laws and sovereignty. It also called for a multilateral approach within the framework of the UN to establish international norms and settle disputes concerning cyberspace. The proposal was discussed within the First Committee but drew criticism from some who saw it as an exercise in undermining efforts to keep the Internet free from external interference. The proposal favored states voluntarily pledging not to use ICTs including networks “to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies.”

The issue was brought directly in front of the UNGA, on September 21, 2011 by the President of Kazakhstan Nursultan Nazarbayev, who stressed the need for an information and cyber-security pact to deter frequent attacks by hackers against governments, businesses and other institutions. He underlined the need for “an international legal framework of the global information-space” based on the nine elements of a global culture of cyber security, which the Assembly had adopted in 2002.

B.2.1.4 UN Bodies on Cyber Security

The issue of developing cyber security norms at the UN broadly falls into two areas i.e. cyber warfare and cybercrime. The first one concerns the political-military stream and the other one the economic stream. The organizational platforms dealing with the political-military issues are the International Telecommunication Union (ITU), UNIDIR and Counter-Terrorism Implementation Task Force (CTITF) Working Group. The organizations tackling cybercrimes are the UN Office on Drug and Crime (UNODC) and the UN Interregional Crime and Justice Research Institute (UNICRI). UNIDIR not only organizes conferences and participates in others; it also produces documents on disarmament.

B.2.1.5 UN ICT Task Force (TF) and the Global Alliance for ICT and Development (GAID)

The UN ICT TF was set up in November 2001 to build broad-based partnerships, find the means to spread the benefits of the digital revolution in information and communication technologies and avert the prospect of a two-tiered World Information Society. The TF included multiple stake holders from the public and private sectors, civil society and the scientific community, and leaders of the developing and transition economies as well as the most technologically advanced economies. The UN ICT TF organized the World Summit on Information Society (WSIS) in 2005 but these two are separate processes. While, the WSIS could issue documents in the name of the global community, the ICT TF acted as a catalyst inside and outside the UN for ideas and partnerships for the Information Society It lacked the democratic legitimacy of WSIS. The mandate of the ICT TF ended in December 2005. The GAID can be considered, to some extent, as a successor to the UN ICT TF, but its composition is different. While the TF was composed of a limited number of persons selected by the UNSG, the GAID is an informal and open platform for all stakeholders interested in the Information Society.

B.2.1.6 ICT4Peace Project

This project was launched in 2004 after the publication of a book by the UN ICT TF on the practice and theory of ICT in the conflict cycle and peace building and the approval of paragraph 36 of the Tunis Commitment of the WSIS in 2005. ICT4Peace is primarily concerned with improving crisis information management by the international community through better use of ICT. It also advocates the use of ICTs in helping countries in conflict zones to achieve the

UN Millennium Development Goals (MDG). Since 2006 the ICT4Peace project is serving as the hub for research, advocacy and networking on the use of ICT to prevent, respond to and recover from conflict. Besides NGOs such as the ICT4Peace, individual researchers like the Estonian scientist Eneken Tikk, have also provided rules of conduct in cyber space.

B.2.17 ITU

This Geneva based organization is a member of the UN Development Group (UNDG). It was originally founded as the International Telegraph Union and is now a specialized UN agency on ICT issues. It is active in areas such as broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting and next-generation networks. It coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecom infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. It has 193 Member States and around 700 Sector Members and Associates.

As a result of the Tunis WSIS of 2005, the ITU became the lead agency in coordinating international efforts as the sole facilitator of Action Line C5 i.e. “Building Confidence and Security in the use of ICTs.” This was followed up by a UNGA resolution formalizing its role. In order to fulfill its mission the ITU has prepared an elaborate Global Cybersecurity Agenda (GCA). It has also revised and updated a 24 year old global telecommunications treaty. The new treaty was signed at an international conference in Dubai in December 2012. This treaty facilitates interconnection and interoperability of an efficient IT system and endorses information access to people with disability, assistance to developing countries in telecom development policies, and emphasize the right to freedom of expression over the ICT systems. It also aims to cut down e-waste, makes mobile roaming charges transparent to people, consistent number of users across the globe for the access of emergency services. Some issues, however, remain unresolved such as: network security, principles associated with unbiased sharing or access to other countries network, language barriers in the context of freedom of expression as outlined in the treaty. Some countries have rejected the proposed treaty because of objections against centralizing the global governance model of regulations on Internet access and the available online content. This is symbolic of sharp differences of opinion on Internet governance between the developed countries and the developing world. Some countries want more national oversights, while some of those in the former category want the Internet to be a free domain governed by voluntary standards set by the industry.

The terms of the new treaty gives the ITU an explicit role in regulating online content, specifically, spam and cyber security. This also extends the treaty's regulatory umbrella to Internet Service Providers (ISP). The ITU will meet again in 2014, when it may consider amending its constitution to formally assert jurisdiction over the technical side of the Web. ITU has a number of cooperative agreements with other groups like Association of South East Asian Nations (ASEAN) and the Caribbean Community (CARICOM). The ITU has a joint project with the CARICOM and the Caribbean Telecommunications Union (CTU) known as Harmonization of ICT Policies, Legislation and Regulatory Policies in the Caribbean. Under the auspices of this project model legislative texts were prepared on Cybercrime/e-Crimes and Electronic Evidence in 2010.

B.2.1.8 Internet Governance Forum (IGF)

There is no central authority controlling the Internet. It is a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body with each constituent network setting and enforcing its own policies. Its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for public good. Internet governance includes the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

The IGF was established at the Tunis summit of the WSIS as a multi-stakeholder forum for policy dialogue on issues of Internet governance. It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process. The establishment of the IGF was formally announced by the UNSG in

July 2006. It has since then been holding its annual sessions regularly. Its mission is to carry out non-binding conversation among stakeholders about the future of Internet governance. The term ‘Internet governance’ has been broadened beyond narrow technical concerns to include a wider range of Internet-related policy issues. The UN has also constituted a committee to update worldwide rules governing the Internet. The basic issue remains a tussle between the US and the Russian Federation about the extent of governmental controls over online content. In April 2013 the second-in-command at the US DHS Jane Holl Lute was hired to write the Internet laws for the UN.

B.2.2 Other International Organizations and Forums

B.2.2.1 ICANN, IETF, and SWIFT

The interoperability part of the Internet and several key technical and policy aspects of the underlying core infrastructure and the principal namespaces are administered by the Internet Corporation for Assigned Names and Numbers (ICANN), headquartered in Los Angeles, California. This body oversees the assignment of globally unique identifiers on the Internet, including Domain Names System (DNS), Internet Protocol (IP) addresses, application port numbers in the transport protocols, and many other parameters. This seeks to create a globally unified namespace to ensure the global reach of the Internet. The ICANN is governed by an international board of directors drawn from across the Internet’s technical, business, academic, and other non-commercial communities. However, the National Telecommunications and Information Administration, an agency of the US Department of Commerce, continues to have final approval over changes to the DNS root zone. This authority over the root zone file makes ICANN one of a few bodies with global, centralized influence over the otherwise distributed Internet. The technical underpinning and standardization of the Internet’s core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise. SWIFT connects the international banking system and all international banking transactions are conducted through it.

B.2.2.2 The IEEE and NIST

The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest organization for the advancement of technology. It develops technical standards through its Standards Association, in conjunction with the US National Institute of Standards and Technology (NIST).

B.2.2.3 The IEC and the ISO

The International Electrotechnical Commission (IEC) prepares and publishes international standards and provides conformity assessments for government, business, and society for all electrical, electronic and related technologies. World Trade Organization (WTO) agreements permit use of these standards in international trade. Its membership includes national committees from over 70 nations, comprising representatives from each country's public and private sectors. The International Organization for Standardization (ISO) and the IEC have set up a Joint Technical Committee (ISO/IEC JTC 1). Its purpose is to develop, maintain, promote, and facilitate standards in the fields of IT and ICT. It has developed information security standards for all types of organizations, including commercial enterprises, government agencies, and not-for-profit organizations. Tens or hundreds of thousands of organizations worldwide use the standards developed by it.

The ISO/IEC 27001:2005 or the "Information technology - Security techniques - Code of practice for information security management" is the internationally-accepted standard of good practice for information security. The landmark ISO/IEC 27032:2012 provides guidance for improving the state of cyber security, in particular with respect to information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the cyberspace and provides a framework to stakeholders to collaborate on resolving cyber security issues.

B.2.2.4 Organization for the Advancement of Structured Information Standards (OASIS)

This is another international, non-profit consortium that drives the development of e-business and web services standards through 70 technical committees. It has done much of its work pursuant to UN request that led ultimately to an important, widely implemented standard, ISO 15000.

B.2.2.5 Organization of Economic Cooperation and Development (OECD)

The OECD has seriously considered cyber threats to international economy. It has constituted an anti-spam task force, which submitted a detailed report, with several background papers on spam problems in developing countries, best practices for Internet Service Providers (ISPs), e-mail marketers etc. It has also commissioned works on the information economy, and the future of the Internet economy. In 2002, the OECD adopted the Guidelines for the Security of Information Systems and Networks. This established a framework of principles that apply to all participants to enhance the security of information systems and networks in order to foster economic prosperity and social development. In 2012, these Guidelines were comprehensively reviewed. After the adoption of the Guidelines, the OECD monitored their implementation and organized events to share experience and best practices by governments, with the business community and civil society.

B.2.2.6 Virtual Global Task Force (VGT)

The VGT combats online sexual exploitation of children. Twelve police organizations are members of the VGT. These include the Australian National Police, National Child Exploitation Coordination Centre (NCECC) – a national program of the Royal Canadian Mounted Police's Canadian Police Centre for Missing and Exploited Children (CPCMEC), European Police (Europol), International Criminal Police Organization (Interpol), Italian postal and telecommunication police service, Dutch National Police, New Zealand Police, Indonesian National Police, Korean National Police Agency Cyber Terror Response Center, Ministry of the Interior for the United Arab Emirates, Child Exploitation and online Protection Centre UK, DHS and US Immigration and Enforcement.

B.2.2.7 Interpol

Under an ambitious plan, the Interpol is setting up a Global Complex for Innovation in Singapore. This state of the art facility is expected to be complete by 2014. It is meant to complement the work of its General Secretariat in Lyon, France, and in Buenos Aires, Argentina and enhance its presence in Asia. It would provide cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships. The Complex will have Digital Crime Centre and a forensic laboratory to support digital crime investigations. It will provide research facilities to test protocols, tools and services and to analyze trends of cyber-attacks and will develop practical solutions in collaboration with police, research laboratories, academia and the public and private sectors. It will addresses issues such as Internet security governance, capacity building and training, research into training and methodology and the transfer of this research into police activities on the ground. It will provide classrooms, field and online training programs for National Central Bureaus; Anti-corruption training, particularly in sport. It will set quality standards and provide and accreditation. It will also provide operational and investigative support.

B.2.2.8 World Federation of Scientists (WFS) and the Information Security Permanent Monitoring Panel (PMP)

Founded in 1973, the WFS is a voluntary organization of more than 10,000 scientists from 110 countries. It promotes international collaboration in science and technology between scientists and researchers. One of its principal aims is to mitigate planetary emergencies. The WFS has identified the threats emanating from cyberspace as a major indicator of the fragility of modern, integrated societies and of undoubted relevance to the functioning and security of the world system. As of today, information security is an important priority for the WFS. In this regard, it advocates unified effort by the entire international community to ensure cyber security. The Information Security PMP was established in 2001 to examine emerging threat to the functioning of ICT systems and it has made appropriate recommendations in this regard.

The Erice Declaration on Principles for Cyber Stability and Cyber Peace was drafted by the PMP and was adopted by the Plenary of the WFS on the occasion of the 42nd Session of the International Seminars on Planetary Emergencies in Erice (Sicily) on August 20, 2009. The Declaration has urged a common code for cyber conduct.

B.2.2.9 London Conference on Cyber Space

A number of international seminars have been convened on the subject of cyber security. A number of good suggestions have come out of these. One such seminar was held in London in November 2011. Hosted by the UK Foreign Office with support from Chatham House and the International Chamber of Commerce, it brought together internet experts and cyber security practitioners from governments, the private-sector, and NGOs from around the world. Speakers included William Hague, British Foreign Secretary; Joe Biden, US Vice-President; Jimmy Wales, Co-founder Wikipedia; and Carl Bildt, the Swedish Foreign Minister. It discussed issues ranging from potential cyber-attacks on intelligence information and infrastructure to intellectual property rights and copyright infringement, the evolving cyber security vulnerabilities of governments, businesses, and individuals require a comprehensive dialogue on how to create a safe online environment while utilizing the Internet's full potential for economic growth and as a forum for the exchange of information.

B.2.2.10 FIRST and CERT

The Forum of Incident Response and Security Teams (FIRST) was formed in 1990 to respond to incidents like the worm attack against the computer systems in 1989. It is now a reputable international confederation coordinating the operations of 276 CERTs (Computer Emergency Readiness Teams) across 60 nations. It cooperatively handles computer security incidents and promotes accident prevention programs. Bringing together the educational, government, military and commercial sectors, it provides access to best practices and tools, and to trusted communication with member teams. Among other things it aims to counteract challenges arising from issues like language, time zones and international standards. Such initiatives, while originating from a very specific need, contribute greatly to the internationalization of best practices of cyber security. This is of special relevance for states with less capacity in cyber security. It is imperative that the international security community looks to mechanisms such as these and ensures that the governmental action at the multinational level is harmonized with the services of operators and other stakeholders, such as private businesses relying on cyberspace infrastructure. CERT India (CERT-In) is listed as a member of the FIRST.

CERTs are also known as Computer Security Incident Response Team (CSIRT, pronounced "see-sirt"), CIRC (Computer Incident Response Capability), CIRT (Computer Incident Response Team), IRC (Incident Response Center or Incident Response Capability), IRT (Incident Response Team), SERT (Security Emergency Response Team) and SIRT (Security Incident Response Team). A CSIRT typically receives reports of security breaches, conduct analyses of the reports and responds to the senders. These teams work either as part of an established group or an ad hoc assembly within the parent organization, such as a government, a corporation, a university or a research network. National CSIRTs are units designated to oversee incident handling for an entire country. These gather periodically throughout the year for proactive tasks such as Disaster Recovery (DR) testing, and in the event of a security breach. External CSIRTs provide paid services on either an on-going or as-needed basis.

B.3 Regional Initiatives

At the regional level, important initiatives have been undertaken by groups like the Shanghai Cooperation Organization (SCO), the Commonwealth of Independent States (CIS), the European Union (EU), the Council of Europe (CE), the G8 Group of States, Asian Pacific Economic Cooperation (APEC), Organization of American States (OAS), ASEAN, the League of Arab States, the African Union (AU) and Network Operations Groups (NOG). No initiative has been taken in South Asia within the framework of either the South Asian Association for Regional Cooperation (SAARC) or at the bilateral level.

B.3.1 The Shanghai Cooperation Organization (SCO)

SCO is a Eurasian security organization, which was founded in Shanghai in 2001. Besides Russia and China, it includes four former Soviet Central Asian Republics as permanent members. India, Pakistan, Mongolia and Iran have observer status and there are two dialogue partners – Belarus and Sri Lanka. The President of Afghanistan was invited to attend the 2012 summit meetings. As leaders of the SCO, Russia and China have used this platform to actively pursue their cyber security agenda.

International information security figures prominently on the SCO's agenda. The SCO is seriously concerned about what some perceive as threats arising from cyber space and the West dominance of the Internet. These concerns were highlighted in the declaration of the heads of states after their meeting in Shanghai in June 2006. It was stated that:

> [A] real danger is currently appearing of ICT being used for purposes capable of bringing serious harm to the security of people, society, and the state in the destruction of foundational principles of equality and mutual respect, non-interference in internal affairs of sovereign states, peaceful regulation of conflicts, non-use of force, and observation of human rights. In this regard the threat of ICT being used in criminal, terrorist, and military-political goals incompatible with the maintenance of international security may be realized in both the civil and military realms and may lead to serious political and socio-economic consequences in individual countries, regions, and the world as a whole, and to the destabilization of the public life of states.

The 2008 SCO Agreement in the Field of International Information Security underlined the ‘digital gap’ between states. It feared that the more developed parties were monopolizing the production of software/hardware, creating dependence on these products from the less developed states whose chances of participating in international IT collaborations were dwindling. SCO member states believe that the current conventions lack adequate codes of conduct in communications between different countries, omitting a broad spectrum of cyber security abuses, which could escalate into cyber-conflict.

On June 15, 2009 the landmark SCO Agreement on Cooperation in the Field of International Information Security was signed in Yekaterinburg. The Yekaterinburg Declaration stressed the significance of ensuring international information security as one of the key elements of the common system of international security. The Agreement defined cyber war as 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. It clearly described cyber warfare as dissemination of information “harmful to the spiritual, moral and cultural spheres of other states” and considers it a “security threat.” The SCO accord identified ‘information war,’ in part, as an effort by a state to undermine another’s “political, economic, and social systems.” SCO presents itself as a possible center of gravity in international legal action on cyber-attacks. In 2009 another agreement was concluded among the Governments of the SCO member states on Cooperation in the Field of Ensuring International Information Security with the ASEAN. On September 12, 2011 Russia and China used the forum of the SCO to present an international code of conduct for Internet to the UNGA.

B.3.2 The Commonwealth of Independent States (CIS)

The CIS was founded after the breakup of the Soviet Union in 1991. Its member states are the former Soviet Republics of Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan. Turkmenistan and Ukraine are the unofficial members. Georgia left the CIS in 2009, after the Georgia-Russia crisis. Cyber-security is an important issue for the CIS. An Agreement on Establishment of the Regional Commonwealth in the field of Communications (RCC) was signed by CIS members in 1992. The RCC's mission is to carry out cooperation between the member states in the field of telecommunication and postal communication. Ukraine, Georgia and Turkmenistan are also official members of the RCC. RCC participants determine collaboration around information security and trans-border information exchange between member states. In 1998, the Information Security Commission of the Coordination Council of the CIS member states was established within the RCC. The commission is responsible for developing cooperative proposals on information security matters and for harmonizing national legislation systems accordingly. In 2000 the CIS concluded agreement among themselves on Cooperation in Combating Offences related to Computer Information.

B.3.3 The Council of Europe (CE)

The 2001 CE Convention on Cybercrime (CEC) – aka the Budapest Convention on Cybercrime or just the Budapest Convention – remains to date, the only binding international legal device. It has the widest possible outreach. It is the first international treaty seeking to address computer and Internet crimes by harmonizing national laws, improving investigative techniques and increasing international cooperation. It provides an effective platform to expand the outreach of the municipal procedural law powers for investigating and prosecuting cyber offences. It deals particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network security. Its main objective is to pursue a common criminal policy aimed at the protecting the society against cybercrime by adopting appropriate legislation and fostering international cooperation. The Convention has accomplished three key goals i.e. establishment of a specific list of domestic criminal offenses and conduct that are prohibited; it has adopted a set of procedural tools and powers to properly and effectively investigate crimes. Lastly, it has established strong mechanisms for fostering international cooperation.

Not all 41 member states of the CE have either signed or ratified the Convention. Signatories include non-European countries from Asia, Africa, Oceania, North and South America. 12 countries have signed but not ratified. 39 have signed and ratified. The US ratified the Convention in August 2006. India and Pakistan are not members of the Convention. The Convention not only requires that parties adopt legislative and other measures to establish criminal offences under its domestic law but also to criminalize the willful infringement of copyright and related rights when done on a commercial scale and by means of a computer system. In addition, parties are also required to ensure that all the listed offenses are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

The CEC sets out mechanisms by which parties are obligated to assist each other in investigating cybercrimes and other crimes involving electronic evidence. It provides them the widest possible base to co-operate with each other for the purposes of investigating, collecting evidence and proceeding against criminal offences related to computer systems and data. This cooperation is, however, contingent on the basis of uniform or reciprocal legislation and domestic laws. The CEC, thus far represents the most substantive, and broadly subscribed multilateral agreement on cybercrime in existence today. In March 2012, the Council adopted an Internet governance strategy.

B.3.4 The European Union (EU)

In June 2010, EU’s law enforcement agency, the European Police Office (Europol) created the EU Cybercrime Task Force. The task force comprises an expert group of representatives from Europol, Euro Just (the EU judicial cooperation body) and the European Commission (EC). Europol provides the EU members with investigative and analytical support on cybercrime, and facilitates cross-border cooperation and information exchange. At the NATO summit of November 2010, the EU, NATO and the US, approved plans for a coordinated approach to tackle cybercrime in member states. Following a feasibility study conducted by Rand Corporation Europe, the EC decided to establish a European Cybercrime Centre (EC3) at Europol. The EC3 was operationalized in January 2013. This Centre is the focal point in the EU's fight against cybercrime, and contributes to faster reactions in the event of online crimes. It supports Member States and the EU's institutions in building operational and analytical capacity for investigations and cooperation with international partners. The Schengen Information System and the Europol Information System, with in-built safeguards to protect privacy and personal data in line with the Charter of Fundamental Rights exchange cross border information. The EU finds these mechanisms quite adequate. The EU has also established the European Network and Information Security Agency (ENISA) to advance the functioning of the internal market. ENISA serves as the center of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. It also facilitates contacts between the European institutions, the Member States and private business and industry actors.

EU has produced a number of legislations and policy directives on issues e.g. EU Directive on e-Commerce, EU Decision on Fraud and Counterfeiting, EU Directive on Data Protection, EU Decision on Attacks against Information Systems, EU Directive on Data Retention, EU Directive Proposal on Attacks against Information Systems, and EU Directive on Child Exploitation.

B.3.5 The European Telecommunications Standards Institute (ETSI)

This is a non-profit, private entity with over 700 members from 62 countries that produces through member-controlled committees globally applicable standards for ICT, including the mobile Internet standards developed by its Third Generation Partnership Project (3GPP).

B.3.6 The Organization of American States (OAS)

The OAS is committed to support member states in fighting cybercrime through the Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program. It is also cooperating with national and regional entities from the public and private sectors on policy and technical issues, to build and strengthen cyber-security capacity of member states through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to ICT. In April 2004 the OAS approved a resolution stating that member states should evaluate the advisability of implementing the principles of the CE's Convention on Cybercrime and should consider the possibility of acceding to that convention. The OAS also adopted a Comprehensive Inter-American Cyber-security Strategy, which aimed at, among other things, adopting cybercrime policies and legislation designed to protect Internet users and prevent/deter criminal misuse of computers and computer networks, while respecting the privacy and individual rights of Internet users.

B.3.7 The Organization of Security and Cooperation in Europe (OSCE)

The OSCE has produced a draft code of conduct on cyber security. In 2011 the 56 participating nations of the OSCE, including the US voted on a resolution to improve cyber security cooperation. The proposal called for participants to exchange information about the way they intend to deploy cyber technology during military conflicts. It also requested debates on international legal standards and codes of conduct for operating in cyberspace. A draft of proposed CBMs floated by the OSCE was circulated among the member states in November 7, 2012 included six proposals concerning national and transnational ICT security. Most of the suggested CBMs are voluntary and therefore difficult to enforce.

B.3.8 The Association of South East Asian Nations (ASEAN)

ASEAN member states cooperate and share best practices on ICT and business processes at the forum of Telecommunications and Information Technology Ministers Meeting (TELMIN). It has prepared an ASEAN ICT Masterplan 2015 (AIM2015) and adopted "Connected ASEAN – Enabling Aspirations." The purpose is to reiterate its commitments to promote ICT-driven economic transformation through people engagement and empowerment, innovation, infrastructure development, human capital development and to bridge the Digital Divide. ASEAN is engaging with China, Japan, the Republic of Korea, the EU and the ITU to implement their respective annual ICT work plans and joint activities. The AIM2015 envisions creating a global ICT hub. The ASEAN Chiefs of Police (ASEANAPOL) meet regularly to discuss issues like cybercrime laws. They also want to establish a partnership with the Interpol's Global Complex (IGC) in Singapore, to enable it respond effectively against challenges presented by cybercrime.

ASEAN has created a number of cyber networks with other countries. In 2009, the ASEAN-China Coordination Framework for Network and Information Security Emergency Responses was signed. Japan not only supports the implementation of AIM2015, it also wants to share its experience on the utilization of ICT in disaster management with ASEAN. In a June this year, in a meeting with senior officials of the ASEAN on Transnational Crime, the US had proposed a Cybercrime Capacity-Building initiative focusing on the requirements and models for national hi-tech crime investigative units and digital forensics programs. On July 1, US Secretary of State John Kerry met with his ASEAN counterparts on the margins of the ASEAN Regional Forum (ARF) meeting and discussed with them issues including cyber security. The ARF has also held Cyber Security workshops in collaboration with Australia.

B.3.11 Organizations in Africa

A number of African groups have come up with directives, legal frameworks and model bills concerning cyber security. ECOWAS (the Economic Community of West African States) has produced a number of legislations including Supplementary Act on Electronic Transactions, Supplementary Act on Personal Data Protection and the Directive on Fighting Cybercrime. In 2011, the African Union (AU) and the Economic Commission for Africa (ECA) produced a *Draft Convention on the Establishment of a Legal Framework for Cyber Security*. The purpose was to harmonize African cyber legislations on e-commerce organization, personal data protection, cyber security promotion and cybercrime control. Among other things the draft convention sought to establish a common language on matters pertaining to cyber security and encouraging governments to establish National Cyber Security Authorities (NCSAs) and CERTs. In 2011 another African group, the COMESA came up with the Cybersecurity Draft Model Bill.

B.3.9 Asia Pacific Economic Cooperation (APEC)

In 2002, the APEC adopted a strategy outlining six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education. It also recommended that member states adopt legislation and policies criminalizing cybercrime. To supplement the APEC Cybersecurity Strategy, the APEC Telecommunications and Information Working Group (APEC TEL) adopted the Strategy to Ensure a Trusted, Secure and Sustainable Online Environment in 2005. The aim of this strategy is to encourage APEC economies to take action for the security of information systems and networks.

B.3.10 The League of Arab States

The League of Arab States came into being after the Arab-Israel war of 1967. It has come a long way since then. Like many other regional groupings, it is concerned about cyber security, especially after the Flame virus attack that hit the Middle East in 2012. In this regard it has prepared two legislations i.e. the Model Arab Law on Combating Offences related to IT Systems (2004) and the Arab Convention on Combating IT Offences (2010).

B.3.12 Network Operations Groups (NOG)

The NOGs provide regional forums to engineers and operators to meet, network, develop business and technology relationships, discuss job opportunities, share best practices and keep the Internet working. The North American Network Operations Group came into existence in 1994. It now attracts participants from Europe and Asia also. It holds three meetings in a year.

B.4 Bilateral Initiatives

B.4.1 US-Russian Bilateral Cyber Security Initiatives

As mentioned in the introductory section, at a meeting held between the US and the Russian President Presidents in June 2013, new initiatives on cyber security were discussed to extend "traditional transparency and confidence-building measures to reduce the mutual danger we face from cyber threats." These initiatives involve 'Deeper Engagement through Senior-Level Dialogue' and 'ICT CBMs**.'** The existing US-Russia Presidential Bilateral Commission has been tasked to establish a working group to assess emerging threats to ICTs and propose joint responses to such threats. The new CBMs are “designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship.” These CBMs seek to strengthen US-Russian relations in cyberspace, expand a shared understanding of cyber threats that appear to originate in each other’s territories, and prevent escalation of cyber security incidents. The CBMs adopted are as under:

- Links and Information Exchanges between the US and Russian CERTs. This CBM aims to increase information sharing on “technical information about malware or other malicious threats” in order to facilitate “proactive mitigation of threats.”

- Exchange of Cyber Security Notifications. This measure will permit communications and “formal inquiries about cyber security incidents of national concern.” Such information exchanges and inquiries will flow through the existing NRRC, established in 1987 between the US and the former USSR, to facilitate reduction of “misperception and escalation from ICT security incidents.”

- Cyber Hotline between the White House and the Kremlin. To provide a secure means to “manage a crisis situation arising from an ICT security incident.” The direct cyber hotline will be integrated into the existing Direct Secure Communication System that the two countries maintain.

On June 21, the US and Russia announced a joint cyber-security agreement, which had taken two years in the making. A joint statement announced the creation of a cyber-hotline and the formation of a bilateral working group. The group will focus on the threat from cyber-attacks to international security, consider emerging threats, and will act to coordinate a collaborative response. The White House also indicated that to “create predictability and understanding in the political military environment,” the two militaries have “shared unclassified ICT strategies and other relevant studies” to understand “one another’s perspectives.” These steps are important for cyber security because the two countries are applying approaches used in arms control contexts e.g. CBMs and hotline communications, to cyber security challenges. This strategy dovetails with needs for better “situational awareness” and transparency through increased information exchange and for stronger, more effective cooperation among key countries through functional collaboration at the technical level and political interactions among high-level officials. However, independent experts in the US are wary that these “iCBMs” would be a panacea for all cyber security problems. American interest of course that the Internet remains free and open and unfettered by oppressive international laws.

Differing national perceptions have created a lot of ambiguity about what should constitute an acceptable cyber code of conduct. Various ideas have been floated about common management of information-space. One proposal gives a technical checklist of ten points to achieve a quasi-global regulatory mechanism short of an international treaty. It argues that cyber CBMs could be a ‘stopgap measure,’ since many countries “view a treaty as unverifiable, unenforceable and impractical.” In order to create robust CBMs it suggests setting up “bodies to share information and best practices, like the Common Assurance Maturity Model (CAMM)* and the Cloud Security Alliance (CSA).”[£] It also highlights the need to “improve communication between the various communities, from policy-makers to technological experts to business leaders both at national and international levels.” The checklist favors enhancement “in attribution capabilities by investing in new technologies, and establishing rules and standards;” and advises that the adoption of the “Dutch model of a third party cyber-exchange for improved private-public partnership on internet security.”[€] In the end it evinces hope that despite practical hurdles in transparency, both for private companies and for governments, ways could be found to establish assurance and trust “through the use of security mechanisms and processes.”

APPENDIX C: EXISTING DOMESTIC LAWS AND TREATIES REGULATING ACTIVITY IN THE INFORMATION ENVIRONMENT IN SOUTH ASIA

As mentioned in the Introduction, one important tool to ensure cyber security is an effective legal system to prevent and prosecute illegitimate cyber activity. This area seems to be extremely patchy in South Asia. South Asian states have no game plan to jointly combat cybercrime. In this Appendix, I have made an effort to describe the existing rules and regulations in Pakistan and India on the subject of cyber security.

C.1 Cybercrime Laws in Pakistan

Due to the mushrooming growth of electronic commerce and massive internet usage, Pakistan has experienced a spurt of cybercrimes but there is no official database for it. Reports posted on the Internet and the national media indicate a rise in crime such as identity thefts and illicit use of credit cards; and harassment and blackmailing on the social media. Pakistan currently has no cybercrime laws. The Prevention of Electronic Crimes Ordinance 2009 lapsed without being made into a law, and since then no legal regime has been created to replace it. Criminal activity online is presently being dealt with through an amalgamation of certain administrative measures and legal provisions borrowed from different pieces of legislation. Some provisions of Pakistan Penal Code 1860 & Electronic Transactions Ordinance 2002 are used for investigating complaints relating to illegal cyber activity, e.g. S. 483 (counterfeiting a trademark or property mark), 420 (cheating), 468 (forgery) and 471 (using forged document) of Pakistan Penal Code 1860 have been used to press charges in cases of illicit cyber activity. These laws are given in Appendix D. Cyber complaints are dealt with by the National Response Centre for Cyber Crimes (NR3C) working under the auspices of Federal Investigation Agency (FIA). Among other things it also acts a CERT.

C.1.1 Cyber Security Bill

Pakistan does not have a national cyber security policy. This indicates a serious capacity deficit at the policy planning levels. On June 24, 2013 the Chairman Senate Standing Committee on Defence Senator Mushahid Hussain Sayed announced that a Cyber Security Strategy bill was being prepared in collaboration with Pakistan Information Security Association (PISA). He demanded that sufficient funds should be allocated to execute a Cyber Security Strategy. He also suggested the formation of a Cyber Security task force within the Ministry of IT, to propose counter measures. His proposal was unanimously adopted.

In a follow up seminar held on July 8th, matters related to cyber security and their impact on sectors such as: the national defence, security, intelligence, diplomacy, nuclear and missile program, economy, energy, education, civil aviation as well as industrial and manufacturing units in the private and public sector were discussed. Three fundamental elements were highlighted: A. The ability to defend digital infrastructure must have the ability to resist attacks, cyber penetration and disruption. B. The ability not only to defend against emerging cyber threats from state sponsored as well as other sources and the ability to retaliate regionally, at least. C. The ability to recover quickly from cyber incidents caused by cyber aggression, accidents or natural disasters. The senator informed the audience that there plans to earmark a focal ministry or division to exclusively handle cyber security issues, introduce laws for data protection and extending an invitation to industry experts to join hands with Parliamentarians in this regard. A cyber security Action Plan was announced for:

1. Introducing legislation to preserve, protect and promote Pakistan’s cyber security. The drafting for the Cyber Security bill has already been initiated.

2. Establishing Pakistan Computer Emergency Response Team (PKCERT).

3. Establishing 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 from the private sector to formulate a Cyber Security Strategy for Pakistan.

4. Establishing an Inter-Services Cyber Command under the office of the Chairman, Joint Chiefs of Staff Committee to coordinate cyber security and cyber defence for Pakistan’s Armed Forces.

5. Initiating talks within the framework of SAARC, among the 8-member states particularly India to establish acceptable norms of cyber behavior so that they do not engage in cyber warfare against each other.

6. Concluding an agreement with India not to engage in cyber warfare patterned on the agreement not to attack nuclear installations.

7. Organizing a special media workshop to promote awareness among the public and educate opinion leaders on the issue of cyber security.

C.2 Cyber Law of India

India enacted its IT Act in June 2000. Spread over 32 pages it provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce," which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. It refers to the UN GA resolution A/RES/51/162, dated the 30th January, 1997 adopting the Model Law on Electronic Commerce adopted by the UN Commission on International Trade Law. Its principal aim is to promote efficient delivery of Government services by means of reliable electronic records. The Indian justice system allows cybercrimes to be tried under this Act. These crimes include theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.

C.2.1 Cyber Defenses of India

CERT-In was established in 2004. The Crisis Management Plan for Cyber Attacks was issued in 2010. The National Critical Information Infrastructure Protection Centre (NCIIPC) was created to protect energy, transport, banking, telecom, defense, space and other sensitive areas from cyber-attacks, in 2011. A government-private sector plan was started in October 2012 to strengthen the country's cyber security capabilities. Indian cyber security planners are presently looking for ways to make up for the deficiency of 500,000 cyber-experts. By February 2013, NCIIPC had finalized the national cyber security policy focusing on domestic security solutions reducing dependence on foreign technology. The National Cyber Security Policy 2013 (NCSP-2013) was published On July 2, 2013. Later, a decision was taken to establish the office of the National Cyber Security Coordinator to coordinate the work of agencies like the National Technical Research Organization (NTRO), the home ministries and the CERT. In May 2013, a full time Cyber Security Coordinator was appointed.

C.2.2 *Foreign Collaboration*

India is actively collaborating with countries other than Pakistan in cyber security matters. In July 2011, it signed a Memorandum of Understanding (MOU) with the US to promote closer cooperation and timely exchange of cyber security information between CERT-In and US-CERT. In October 2012 the Foreign and Defense Secretaries of India and Japan met at the "2+2" in Tokyo to decide among other things an expansion in cyber security collaboration. During his visit to New Delhi in February 2013, the British Prime Minister promised greater collaboration with India in fighting cyber-attacks. A large amount of UK data is on Indian databases. Britain strongly feels that it needs to partner with India in cybercrime and security related matters, to fight cyber criminals and protect itself from states like China. The British are offering the Indians police training exchanges and research into cyber security and a joint task force to share information. Cyber cooperation also includes regular meetings between leaders in cyber security research in academic institutions and industry.

C.3 The SEA_ME_WE Internet Cable

Currently the only cyber sharing that India does with Pakistan is the SEA-ME-WE (South East Asia-Middle East- West Asia) submarine Internet cable. This optical fiber cable was laid by an international telecom consortium under an agreement signed on March 27, 2004. It links South East Asia to Europe via the Indian Sub-Continent and Middle East with terminal stations in Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi Arabia, Egypt, Italy, Tunisia, Algeria and France. It is now being upgraded by a group of French and Japanese companies at the cost of US $500 million. The total length of the SEA-ME-WE 4 submarine cable system spans approximately 20,000 kilometers.

APPENDIX D: A HISTORY OF CBMS BETWEEN INDIA AND PAKISTAN

Despite deep rooted mistrust, India and Pakistan have over the years concluded a number of agreements to keep the affairs of the state moving in a mutually beneficial direction. These efforts to seek peaceful solutions to pressing problems make up for a set of practical CBMs. Some of the early agreements between India and Pakistan included matters such as transfer of official assets (1948), prevention of exodus of refugees (1948), protection of right of minorities (1950), maintenance of places of worship (1953 and 1955) and resolution of some unsettled territorial claims (1958, 1959, 1960 and 1963). Many consider the supply of water from the upper (India) to the lower riparian (Pakistan) to be a major source of friction. Tensions mounted in 1950 and 1951, when India blocked Pakistan's share of water, resulting in military mobilization. Three successive agreements were made to allow unimpeded water supply to Pakistan till 1957, and from 1959 to 1960. In September 1960, the World Bank brokered Indus Waters Treaty was concluded.

Pakistan and India formally ended wars through the Karachi Agreement (1949), Tashkent agreement (1966), and the Simla Agreement (1972). The Rann of Kutch territorial dispute that preceded the 1965 War was resolved through a UN sponsored Boundary Tribunal in 1968. Both states had pre-agreed to accept its recommendations and the border was demarcated accordingly. Both states also twice accepted UN intervention to monitor the ceasefire along the LOC. The UN Military Observer Group in India and Pakistan (UNMOGIP) still has a presence in the disputed territory of Jammu and Kashmir.

Although India and Pakistan have maintained diplomatic relations even during times of war, both sides realize the importance of direct communication between civil and military officials. In November 1990 it was agreed to establish a hotline between the offices of the two prime ministers. There is little evidence to suggest that this channel has been frequently used. During the Kargil war Prime Ministers Nawaz Sharif and Vajpayee spoke on the telephone but this conversation only served to heighten the predicament. Indian external affairs secretary J.N. Dixit recalls talking to his Pakistani counterpart Shahiryar M. Khan over the telephone in March 1993. Instead of using the ministry's phone Pakistani foreign minister Sartaj Aziz flew to New Delhi in an abortive attempt to defuse the situation, during the 1999 Kargil crisis. In 2004 there were media reports that India and Pakistan had agreed to set up a hotline between their foreign ministries to reduce the threat of accidental nuclear war but since then there has been little to indicate that this channel has been operationalized. A proposed counter terrorism hotline between the interior ministries also remains stalled, but media reports indicate that it may still be on the cards. Telephonic conversation has its limitations and diplomats prefer to directly talk to one another or communicate through carefully formal diplomatic communiques and non-papers. After the infamous prank call by someone purporting to be the Indian foreign minister threating the President of Pakistan with dire consequences, there is a requirement for additional identification filters and protocols.

One of the most dependable communication links India and Pakistan is the DGMO hotline. This direct link was established after the 1971 war and is now routinely used every week. Flag meetings between Sector Commanders at battalion and brigade level are organized to sort out problems in their areas on case to case basis through prior arrangements. As of 2004, there is a system of biannual meetings between the heads of the Indian border security forces and Pakistani Rangers. The Indian Coast Guard (ICG) and the Pakistan Maritime Security Agency (MSA) have a hotline since 2006.

To begin with military CBMs were mainly about maintaining peace along the LOC and reducing the chances of a conventional war. In the 1980s, the South Asian adversaries intensified their efforts to acquire nuclear weapons. During this time India made repeated attempts to launch decapitating air strikes against Pakistani uranium enrichment facilities in Kahuta. The matter came to a head during Exercise Brasstacks in 1986-87, when 400,000 Indian troops began military drills perilously close to the Pakistani border in the Sindh. The aim was to trigger a conventional war and simultaneously strike Kahuta. The two sides realized that the time had come to craft a new set of CBMs to prevent a nuclear war. After the exercise terminated and the forces pulled back to their peace locations, the political leadership of the two countries concluded the first nuclear CBM titled, the Prohibition of Attack against Nuclear Facilities. This bilateral agreement was signed on December 31, 1988, ratified in 1991 and implemented in January 1992. To make the process more transparent, both parties are required to annually exchange lists of the location of all their nuclear-related facilities. This ritual is being faithfully complied with, despite periods of tension. Since 1991, there has been an agreement to send advance notices of military exercises and maneuvers and prevent airspace violations.

India and Pakistan are both signatories to the Chemical Weapon Convention (CWC). On August 19, 1992 the two countries also signed a bilateral agreement on chemical weapons (CW). After the nuclear tests of 1998, both countries placed a voluntary moratorium on further nuclear testing. In the September 1998 session of the UNGA the prime ministers of India and Pakistan pledged abstinence from further testing. In February 1999, they met in Lahore, Pakistan, and agreed to: a Joint Statement by the Prime Ministers; a Memorandum of Understanding (MOU) by the Foreign Secretaries; and the Lahore Declaration itself. The major concerns identified in Lahore were about nuclear safety and security. In the joint statement by the prime ministers it was recognized that: “the nuclear dimension of the security environment of the two countries added to their responsibility of the avoidance of conflict between the two countries.” The MOU aimed at nuclear risk reduction and improving nuclear security and prevent an accidental nuclear exchange. It called for the creation of communication mechanisms similar in some aspects to those required by the Convention on Early Notification of a Nuclear Accident. Specifically, the two sides committed to exchange information on their nuclear doctrines and security concepts; prevent accidental nuclear crises; work on measures to improve control over their nuclear weapons; review existing CBMs and emergency communications (hotlines) arrangements; and strengthen unilateral moratoriums on nuclear testing by making their commitments binding, barring of course extraordinary events jeopardizing supreme national interests. The Kargil conflict that followed three months later disrupted the Lahore process. There have been no major clashes along the Line of Control (LoC) after 1999. An informal ceasefire was put in place in 2003, which barring occasional violations is still holding out.

In November 2005 Pakistan and India signed the ballistic missile advance notification agreement. Under this accord, the country’s defense ministries are obligated to provide their counterparts at least 72 hours of notice before conducting a ballistic missile flight test. They are not to allow trajectories of tested missiles to approach or land close either to their accepted borders or the LOC. They are not to allow tested missiles to fly closer than 40 kilometers from these boundaries or land closer than 70 kilometers away. This warning does not extend to cruise missiles.

On substantial issues India and Pakistan have not moved from their entrenched positions during the past few years. In the bargain, despite active Track I (formal) and Track II (informal) negotiations, opportunities have been missed to pluck ‘low hanging fruits’ like Siachen and Sir

Creek. Impartial third party studies have also failed to break the proverbial ice on issues like the demilitarization of the Siachen glacier. The slow process of the composite dialogue process notwithstanding, optimists keep floating new ideas on CBMs. However, no one has yet broached the issue of CBMs in information-space.

Although CBMs lack the binding nature of treaty obligations but the inherent flexibility of these agreements give them a chance of success in the long run. There are several phases in the lifecycle of a CBM. In the preparatory phase, the parties concerned prepare grounds for the negotiations by seeking commonality of interests. The negotiation phase is a very delicate one and requires tact and patience from all those involved. Once the differences have been ironed out and broad consensus obtained on substantial issues, the next phase is that of implementation. If CBMs successfully survive this phase, the next one is to improve, strengthen and possibly upgrade these to the status of treaties and formal accords.

The success and failure of CBMs depends on the seriousness of purpose displayed by the stakeholders, the quality of negotiations, and the sincerity with which these are implemented. The chances of a CBM negotiation succeeding depends in the first instance upon the commitment and sincerity of the governments; the charisma of the leadership and the negotiating skills of the interlocutors to steer through road bumps and hurdles. Openness to new ideas and an attitude of give and take is always helpful in nudging things forward. Having subject specialists with specific skillsets on the negotiating teams is always helpful in fine tuning a CBM. The domestic media may help by building a favorable public opinion and by desisting from creating a hype and raising unrealistic expectations. CBMs on delicate issues are best negotiated out of the media glare. The failed Agra summit between India and Pakistan is just one example. Finally, the chances of CBMs surviving and standing the test of time, is based on the premise that these are realistic in approach, simple and practical to enforce and easy to monitor and verify. Prolonged periods of non-use can render even the most promising of CBMs ineffective.

Some South Asia watchers are of the opinion that India and Pakistan have just been reactive and not proactive in formulating CBMs. This observation may not be germane to South Asia alone. It has happened elsewhere too e.g. the Kremlin-White House hotline resulted from the 1962 Cuban missile crisis and the Stockholm agreement of 1986 was the result of large scale military exercises that preceded it. However, the East-West relationship moved on from being reactionary to proactive. The entire range of arms control initiatives both the strategic arms limitation talks (SALT) and the strategic arms reduction talks (START) were forward looking measures aimed to prevent a nuclear arms race. Perhaps there is something to learn from there.

APPENDIX E: LIST OF INTERNATIONAL AND REGIONAL INSTRUMENTS AND SHORT NAMES

	ASSOCIATION/YEAR	INSTRUMENT	SHORT NAME
1	AU 2012	Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa	Draft AU Convention
2	COMESA 2011	Cybersecurity Draft Model Bill.	COMESA Draft Model Bill
3	The Commonwealth 2002	(i) Computer and Computer Related Crimes Bill and (ii) Model Law on Electronic Evidence	Commonwealth Model Law
4	CIS 2001	Agreement on Cooperation in Combating Offences related to Computer Information	CIS Agreement
5	CE 2001	Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems	CE Cybercrime Convention/Protocol
6	CE 2007	Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse	CE Child Protection Convention.
7	ECOWAS 2009	Draft Directive on Fighting Cybercrime within ECOWAS	ECOWAS Draft Directive.
8	EU 2000	Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the	EU Directive on e-Commerce

		Internal Market	
9	EU 2001	Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment	EU Decision on Fraud and Counterfeiting
10	EU 2002	Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector	EU Directive on Data Protection.
11	EU 2005	Council Framework Decision 2005/222/JHA on attacks against information systems	EU Decision on Attacks against Information Systems
12	EU 2006	Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks	EU Directive on Data Retention
13	EU 2010	Proposal COM(2010) 517 final for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA	EU Directive Proposal on Attacks against Information Systems.
14	EU 2011	Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA	EU Directive on Child Exploitation

15	ITU/CARICOM/Caribbean Telecommunications Union (CTU) 2010	Model Legislative Texts on Cybercrime/e-Crimes and Electronic Evidence	ITU/CARICOM/CTU Model Legislative Texts
16	League of Arab States, 2010	Arab Convention on Combating Information Technology Offences	League of Arab States Convention
17	League of Arab States, 2004	Model Arab Law on Combating Offences related to Information Technology Systems	League of Arab States Model Law
18	SCO 2010	Agreement on Cooperation in the Field of International Information Security	SCO Agreement
19	UN 2000	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography	UN OP-CRC-SC

DISTRIBUTION

10 Prof. Tughral Yamin
House No. 108, Street 10, F11/1,
Islamabad, Pakistan

4 Dr. Robert Swartz
Office of Nonproliferation and International Security
National Nuclear Security Administration
US Department of Energy
1000 Independence Ave SW
Washington, DC 20585

1	MS1371	Karl Horak	6832
5	MS1373	Kent Biringer	6821
1	MS1373	Tom Ciccateri	6821
1	MS1373	Robert Finch	6821
10	MS1373	Geoffrey Forden	6821
1	MS1373	Amir Mohagheghi	6821
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories