Cyberspace CBMs
between Pakistan and India

Cyberspace CBMs
between Pakistan and India

Dr Tughral Yamin

NUST
Publishing

National University of Sciences and Technology, Islamabad

ISBN 978-969-8535-21-6

First Published 2014
by
NUST Publishing
National University of Sciences and Technology,
Islamabad

Dr Tughral Yamin

Cyberspace CBMs
between Pakistan and India

Title design and book layout
Mahtab Ahmad Wasil

Printed by
NUST Press, Islamabad

email: np@nust.edu.pk
Phone: 051-90851683

Contents

Dedicated to my mother
Safia Yamin,
who taught me to read and write.

ACRONYMS & ABBREVIATIONS

ACRS	Arms Control and Regional Security
ASEAN	Association of South East Asian Nations
Aseanapol	ASEAN Police
ARF	ASEAN Regional Forum
C2	Command and Control
CBMs	Confidence Building Measures
CE	Council of Europe
CEC	Convention on Cybercrime
CERT	Computer Emergency Response Team
CIS	Commonwealth of Independent States
CNA	Computer Network Attacks
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CNE	Computer Network Exploration
CNO	Computer Network Operations
CS&C	Office of Cybersecurity and Communication
CSIRT	Computer Security Incident Response Team
CTITF	Counter-Terrorism Implementation Task Force
CTU	Caribbean Telecommunications Union
CW	Chemical Weapons
CWC	Chemical Weapon Convention
CYBERCOM	Cyber Command
DCEO	Defensive Computer Effects Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOS	Denial of Service
DR	Disaster Recovery
DSB	Defense Science Board
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
MoD	Ministry of Defense
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	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
PC	Personal Computer
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PPD	Presidential Policy Directive
PSY-OPS	Psychological Operations
PTA	Pakistan Telecommunication Authority
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organization
SEA	Syrian Electronic Army
SMS	Short Message Service
TRAI	Telecommunication Regulatory Authority of India
UNGA	United Nations General Assembly
UNIDIR	United Nations Institute for Disarmament Research
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
UNSG	United Nations Secretary General
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

FOREWORD

This book is about Confidence Building Measures (CBMs) of a different kind. Traditional CBMs have always been part and parcel of statecraft. Modern CBMs owe their genesis to the Cold War. During the East-West Conflict CBMs were used as ingenuous tools to reduce tensions and eliminate chances of physical conflict. For hostile states, caught in a bind like India and Pakistan, CBMs provide a compromise solution. Practically speaking, CBMs are self-regulating norms of behavior – bilateral as well as unilateral, a notch below legally binding treaties. With traditional fields of CBMs becoming saturated, policy planners and strategists are now exploring new areas for confidence building. Of late, information technology (IT) has emerged as a new sphere of conflict and cooperation. In this Orwellian age of "Big Brother is watching", countries are becoming increasingly wary of friends and foes. Their confidence has been shaken because they are not quickly able to ascertain the identity of the cyber attacker. The problem of attribution makes it very difficult to blame a single individual, state or non-state party for cyber attacks. The crime scene is not restricted to a lone computer system. The trail of a cyber-attack goes cold as viruses, zombies and Trojan Horses infect the systems in debilitating ways making the command and control (C2) systems go haywire. The targets includes not only commercial entities but also conventional and strategic military forces. It is extremely difficult to collect forensic evidence from cyber space because there are no established norms in this lawless and borderless territory.

For a layman it is difficult to combine policy with technology. It takes a great deal of imagination to do so. Dr Tughral Yamin has has done it with considerable ease and confidence. He has built up his case for CBMs in cyber space between India and Pakistan from multiple angles i.e. from the perspective of inter-

national law, existing regional and international treaties on cyber security, national points of view on the subject and existing models of cooperation in cyber space. He has written in a simple and straight forward manner and has parsed an extremely complex notion into simple and understandable concepts. His basic thesis is that, whereas countries are cooperating in cyber space to combat a common enemy, South Asia represents a gaping hole, where there is a complete absence of cooperation and absolutely no sharing of best practices. He suggests a bottom up approach. His formula is that cooperation should begin from the lowest level. The universities can organize seminars, for experts to exchange ideas, businesses can study joint mechanisms to ward off commercial thefts, police forces and law ministries can harmonize laws to track down and persecute cyber criminals and IT ministries can collaborate to form a SAARC CERT (Computer Emergency Response Team) before moving on to military CBMs.

I feel this book should be a must read for all those, who have genuine interest in cyber security, particularly at the government level.

Professor Dr Pervez Iqbal Cheema
Dean FCS, NDU
Islamabad
April 2014

ACKNOWLEDGEMENTS

I am grateful to Sandia National Laboratories (SNL) and the US Department of Energy (DOE) for providing me the resources to work on a project close to my heart i.e. cyber security cooperation in South Asia.

I am thankful to Bob Swartz in Washington DC and my hosts in Albuquerque NM, Geoff Forden and his team for making my stay comfortable. I would like to place on record my gratitude to Karl Horak for his useful and insightful contributions on cyber security and to Brigadier 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 headquarter in New York. This helped me gauge, the official perspective on the subject. I also received commendable support from Jamal Aziz and the researchers at Ahmer Bilal Soofi's law firm on Pakistani cyber laws (or the sheer absence of them).

I was lucky to 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, my profound thanks to National University of Sciences and Technology (NUST) Islamabad for allowing me a sabbatical to engage in this interesting research work and for publishing the result of my labors. Last but not least, my thanks to young Uzair Shaikh for combing through the final draft to remove typographical errors.

I certainly hope this preliminary study in cyber security would

generate enthusiasm among governments, scholars and professionals to join hands in creating a safer cyberspace.

Dr Tughral Yamin
Islamabad
April 2014

Chapter 1

INTRODUCTION

Information Space and Information Warfare (IW)

As social animals, human beings communicate with one another in complex ways, using a variety of spoken and written languages. The sign language and Braille is used by those, who cannot 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 revived and newer ones have emerged like the computer language. An elaborate system of encryption ranging from simple codes and ciphers 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 include primitive means like the word of mouth, drumbeats, smoke signals, bugles, messengers, carrier pigeons, semaphore and 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 notional realm in which electronic information exists or is exchanged." Others have defined cyberspace in similar terms:

---

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

> The environment formed by physical and non-physical components, characterized by the use of computers and electromagnetic 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 modern age."[4] Internet provides the digital oxygen to the contemporary information system. The worldwide web (www) 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 of the defense organizations are also fully or partially networked. Digital connectivity has not only speeded up the decision making processes, it has also rendered these systems vulnerable to cyber-attacks. Cyber warfare has evolved into most potent form of non-kinetic war fighting. As nations upgrade their net-centric capabilities, they 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 C2 systems. At the same time technologically advanced countries are enhancing

---

[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).

[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).

their offensive capabilities to launch cyber-attacks against hostile computer networks. An all-pervasive cyber surveillance campaign is in the works. The prospects are so frightening that countries like Iran, China, Saudi Arabia and Russia are actually working to create their own Internets.[6]

Internet is the glue of modern management system. It holds together governments, defense organizations and financial services. Airlines, maritime industry, railways and the road traffic systems are all controlled by computer networks. The waterways, logistics services, emergency services, energy management systems, electricity grids and industrial units are operated by SCADA (supervisory control and data acquisition) type of industrial control system (ICS).[7] All these are lucrative cyber-targets. Cyber-attacks directed against individual PCs or large networks take place singly or as a large well-coordinated operation. Their cumulative effects can range from minor to major disruptions including interrupted routines to complete breakdown of systems. 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 into the fifth dimension of war-fighting,[9] the fourth being outer space. The devastating effects of cyber-attacks

---

[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).

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 unbridled use of Information Warfare (IW) weapons. Information Operations (IO) now form the 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 one must understand some commonly used terms e.g. cyber-warfare with both its offensive and defensive facets is 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

---

[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] Read 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.

> 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.[17] Cyber threats include "external threat actors, insider threats, supply chain vulnerabilities," and threats to the defense establishment.[18] 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

---

[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] Ibid, 11.

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

human and automated decision-making while protecting [one's] own."[19] 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 adversaries the use of its computers, information systems, and networks, while ensuring the effective use of own computers, information systems, and networks. These operations include not only CNA but also Computer Network Exploration (CNE), and Computer Network Defense (CND).[20] A combination of these five alongwith related supporting capabilities are used to influence, disrupt, corrupt or usurp adversarial human and automated decision-making processes, while protecting one's own.[21]

As cyber-attacks become increasingly commonplace, new concepts of cybersecurity are also emerging. The defensive mechanism to protect against cyber-attacks 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.[22]

Cyber laws can be effectively used to check illicit cyber activity. Advance countries with economies heavily dependent on e-commerce have devised laws to deal with cybercrimes. The federal

---

[19] *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).

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

[21] *Information Operations*, US JS Joint Publication, 3-13.

[22] 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).

and state governments usually involve the private sector to fine tune these laws. The cyber regulations in the US are governed by the Comprehensive National Cyber Security Initiative (CNCSI).[23] The purpose of these regulations is to protect companies, organizations and the government from malicious software or malware,[24] 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.[25] An innocuous Universal Serial Bus (USB) thumb drive can introduce a deadly virus into a computer system.[26] 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.[27] Numerous measures are available to prevent cyber-attacks. These include firewalls, anti-virus software, intrusion detection and prevention systems, encryption and login passwords.[28]

---

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

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

[25] 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).

[26] 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).

[27] 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).

[28] 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).

As an Internet superpower,[29] the US vigorously pursues its commercial, political, as well as military interests in cyberspace. Its actions are driven by creeping worries that it hold on Internet leadership may be loosening.[30] 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."[31] 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.[32]

The US cyber planners contend with two kinds of cyber threats. 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

---

[29] "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).

[30] Segal, "Defending an Open, Global, Secure and Resilient Internet," *CFR Independent Task Force Report No. 70, 5.*

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

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

running the chemical, electrical, water and transport sectors have all been probed by hackers.[33] The second area of concern is the large-scale theft/destruction of valuable government, military, private sector and allied countries secrets by state-sponsored hackers and criminals. Widespread hacking activity has been reported in the private sector e.g. in August 2012, hackers attacked the networks of Saudi Aramco, destroying data on 30,000 company computers.[34] 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 history.[35] The volume of global online crime is estimated to be between US $110 to 500 billion.[36]

While governments are anxious about rampant theft and crime in cyberspace, they 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 days" are being freely sold to the highest bidder by clandestine companies. Big buyers include American NSA, Iranian Revolutionary Guards and agencies from South Africa to South Korea. Israel, Britain, Russia, India and Brazil are known to be some of the biggest spenders in the field. The list also includes North Korea, some Middle Eastern intelligence services and countries in the Asian

---

[33] "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).

[34] 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).

[35] 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).

[36] Segal, "Defending an Open, Global, Secure and Resilient Internet," *CFR Independent Task Force Report* No. 70, 17.

Pacific, including Malaysia and Singapore.[37] These open market resources have increased the frequency of cyber attacks e.g. in June 2013, South Korea blamed North Korea for attacking 69 websites, including the presidential office and media companies.[38]

The cyber warfare revolution was triggered by the spectacular use of cutting edge technology by the US military in the first Gulf War. Soon after the War, the US DOD raised cyber and IW units.[39] In 1998, the Pentagon created a Joint Task Force Computer Network Defense (JTFCND).[40] The task force was subsequently upgraded to a cyber-command (CYBERCOM). The CYBERCOM became fully operational on October 31, 2010 and now controls all cyberspace operations, organizes existing cyber resources and synchronizes defense of military networks.[41] The commanding general of this organization 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,'[42] the US CYBERCOM intends to maintain its cyber dominance and towards that end, it intends to quadruple its size by hiring 4,000 information technol-

---

[37] Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *New York Times*, July 13, 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=all&_r=0 (accessed July 13, 2013).

[38] "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).

[39] Choe Sang-Hun, "South Korea blames North for June Cyber Attacks," *New York Times*, July 16, 2013, http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?src=recg&gwh=C1CC11FC0E8EA71B45CA3AD0DC6D7098 (accessed July 16, 2013).

[40] 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).

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

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

ogy (IT) specialists over the next four years. This will happen at an additional cost of US $23 billion.[43] The NSA collects and analyzes huge troves of foreign communications and foreign signals intelligence to monitor and thwart worldwide threats.[44] The NSA also wants more money to deploy a "Star Wars" kind of cyber defense but cyber leaks about the magnitude of internal electronic surveillance has created caution within the US government to support such programs.[45] The scale of NSA global surveillance outreach has also sent shock waves around the world,[46] alarming both allies,[47] and competitors.[48]

As revolution in military IT affairs took place, the Chinese

---

[43] Elisabeth Bumiller, "Pentagon Expanding Cybersecurity Force to Protect Networks against Attacks," *New York Times*, January 27, 2013, http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=0 (accessed February 14, 2013).

[44] Ellen Nakashima, "Bush Order Expands Network Monitoring Intelligence Agencies to Track Intrusions, *Washington Post*, January 26, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html (accessed July 1, 2013).

[45] David E. Sanger, "N.S.A. Leaks Make Plan for Cyber defense Unlikely," *New York Times*, August 12, 3013, http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html?src=recg (accessed August 13, 2013).

[46] Gabriel Rodriguez, "Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview with the Man who Leaked PRISM," *Politics*, http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism (accessed June 20 2013).

[47] "U.S. needs to deal with E.U. concerns about NSA spying," *Washington Post*, July 5, 2013, http://articles.washingtonpost.com/2013-07-05/opinions/40390110_1_nsa-national-security-agency-e-u (accessed July 9, 2013).

[48] Howard La Franchi, "US-China Cybersecurity Talks: Will Snowden leaks thwart US goals? Topping the US agenda for Strategic and Economic Talks with China this Week is Cybersecurity: But since Obama and Xi met in California, Edward Snowden spilled the beans on US spying," *Christian Science Monitor*, http://www.csmonitor.com/USA/Foreign-Policy/2013/0709/US-China-cybersecurity-talks-Will-Snowden-leaks-thwart-US-goals (accessed July 10, 2013).

People's Liberation Army (PLA) seriously studied the emerging trends and developed indigenous IW concepts to suit their military strategy.[49] Sweeping reforms were carried out to establish a fully networked architecture capable of coordinating military operations on land, air, sea, space and across the entire electromagnetic spectrum. Their overarching cyber policy was guided by the doctrine of fighting "Local War under Informationized Conditions."[50] Informatization requires the armed forces to be more "dynamic", flexible, effective, creative and forward-looking."[51] This policy provides the operational framework to highly trained PLA units engaged in offensive IOs[52] and cyber drills.[53] China's cyber army is estimated to have more than 100,000 people, with an annual budget of over US $2.71 million.[54] PLA's General Staff Department's (GSD), 4th Department, is responsible for Electronic Countermeasures (ECM), while CND and intelligence gathering responsibilities belong to the 3rd Department (Signals Intelli-

---

[49] Read about the evolution of Chinese IW in Timothy L. Thomas, *Cyber Bytes* (Fort Leavenworth: Foreign Military Studies Office, 2004) and *Decoding the Virtual Dragon* (Fort Leavenworth: Foreign Military Studies Office, 2007).

[50] 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).

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

[52] 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)

[53] "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).

[54] Jeff Goldman, "Taiwan Says China's Cyber Army Now Numbers 100, 000," May 1, 2013, http://www.esecurityplanet.com/hackers/taiwan-says-chinas-cyber-army-now-numbers-100000.html (accessed June 30, 2013).

gence).[55] US blames the 2nd Bureau of the 3rd Department, commonly known as Unit 61398, as the Advanced Persistent Threat 1 (APT1) to their computer networks.[56] Western media claims that the Chinese cyber-attacks have expanded beyond government targets to energy sector corporations,[57] universities,[58] and influential newspapers like the *New York Times*.[59]

In order to cool down cyber tempers, the US and China have started broaching the subject in high-level talks.[60] Due to differing perceptions, progress is slow but there are indications that they may cooperate at least in fighting cybercrime.[61] It has been suggested that they could begin by jointly tackling common threats like spam or unsolicited bulk electronic messages sent indiscrimi-

---

[55] Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare.*

[56] APT is the name given to cyber espionage with state backing and is considered one of the top threats in cyber space.Read "APT1: Exposing one of China's Cyber Espionage Units," *Mandiant Report*, www.mandiant.com (accessed June 17, 2013).

[57] 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).

[58] Richard Pérez-Peña, "Universities Face a Rising Barrage of Cyberattacks," *New York Times*, July 16, 2013, http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=1&_r=0&nl=todaysheadlines&emc=edit_th_20130717 (accessed July 16, 2013).

[59] Nicole Perlroth, "Hackers in China Attacked The Times for Last 4 Months," *New York Times*, January 30, 2013, http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0 (accessed February 14, 2013).

[60] "Diplomacy: US, China aligned on North Korea, Climate and Cybercrime," *Deutschewelle*,http://www.dw.de/us-china-aligned-on-n-korea-climate-and-cybercrime/a-16868686 (accessed June 15, 2013).

[61] "China, US Agree to Combat Cyber Crime," *Beijing International,* http://www.ebeijing.gov.cn /BeijingInformation/BeijingNewsUpdate/t1138000.htm (accessed April 25, 2013).

nately.[62] In a summit meeting held in June 2013, Chinese and US Presidents agreed that "their two countries needed to develop better military-to-military relations and improve cyber security cooperation."[63] Cyber security was 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 meeting began on an unfavorable note as accusations were traded about intellectual property theft and large scale digital surveillance. This was in stark contrast to the serious and meaningful meeting held between Chinese and the US cyber experts, two days ahead of the Strategic Dialogue. Many regard this meeting as real progress.[64]

While the US and China vie for cyber dominance, the Russians are not far behind. To offset the pervasive US digital surveillance, the Russians want tighter controls over the Internet.[65] They are also busy improving their cyber capabilities. In February 2013, the Russian Defense Minister instructed the General Staff to complete proposals to set up an army cyber command by the end of the year.[66] On the positive side, since the US and Russia have a long standing tradition of concluding bilateral nuclear

---

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

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

[64] David E. Sanger, "Differences on Cybertheft Complicate China Talks," *New York Times*, July 10, 2013, http://www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html?cid=nlc-dailybrief-daily_news_brief-link3-20130711 (accessed July 11, 2013).

[65] Andrew E. Kramer, "NSA Leaks Revive Push in Russia to Control Net, *New York Times*, July 14, 2013, http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?src=recg&gwh=32551918C3F6092B12097F447F3343BB (accessed July 16, 2013).

[66] 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).

arms limitation and reduction treaties dating back to the Cold War, they appear less hesitant 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 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,[67] 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."[68] Despite this promising beginning the cyber relations between the two countries are currently stalled on account of the asylum that the Russians have granted to the American cyber defector.[69]

Cyber-attacks can pose a major decision-making dilemma, in case of 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

---

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

[68] "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).

[69] "Obama cancels Moscow summit with Putin in showdown over Snowden," *New York Times*, August 7, 2013, http://www.nydailynews.com/news/politics/obama-cancels-moscow-summit-putin-showdown-snowden-article-1.1419848 (accessed August 7, 2013).

reserves the right to "respond to hostile acts in cyberspace," as it "would to any other threat."[70] The Pentagon's Defense Science Board (DSB) believes that China and Russia can develop capabilities to launch an 'existential cyber-attack' which can cause:

> 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.[71]

Senior US security managers feel that a 'cyber Pearl Harbor' is a distinct possibility.[72] The 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.[73] Government officials do not rule out the threat of use of nuclear weapons to deter cyber-attacks.[74] Under the US Constitution, it is the prerogative of the

---

[70] I*nternational 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).

[71] 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).

[72] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.,"*New York Times*, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html ?pagewanted=all (accessed January 12, 2013).

[73] David Alexander, "U.S. reserves right to meet cyber attack with force," *Reuters*, November 15, 2011, http://www.reuters.com/article /2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116(accessed June 28, 2013).

[74] Richard A. Clarke and Steven Andreasen, "Cyberwar's threat does not justify a new policy of nuclear deterrence," *Washington Pos*t, June 14, 2013, http://www.washingtonpost.com/opinions/cyberwars-threat-does-not-justify-a-new-policy-of-nuclear-deterrence/2013/06/14/91c01bb6-d50e-11e2-a73e-826d299ff459_story.html (accessed June 15, 2013).

president, as commander in chief of the armed forces, to decide if a cyber-attack is considered sufficiently serious to be declared a hostile act, and thus an act of war. However, it is a moot point as to what kind of cyber-attack could prompt such a response and what might be its form and intensity? The Pentagon has recently updated the rules of military engagement for cyber warfare, and developed emergency procedures to guide rapid responses to attacks having serious national security or economic consequences.[75]

The top secret US President Policy Directive (PDP) 20 signed in October 2012 addresses issues like responses to a cyber-attack.[76] It explains that the use of cyber weapons would need presidential approval, in case of likelihood of causing significant damage i.e. "loss of life, serious levels of retaliation, damage to property, adverse foreign policy consequences or economic impact on the country." Under PDP 20 the Defensive Cyber Effects Operations (DCEO) and the Offensive Cyber Effects Operations (OCEO) are intended to advance US national objectives globally "with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."[77] The US policymakers remain alert to the possibility of hostile cyber-attacks. The Fact Sheet issued by the White House regarding the Nuclear Weapon

---

[75] 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).

[76] "Obama tells intelligence chiefs to draw up cyber target list – full document text: Eighteen-page presidential memo reveals how Barack Obama has ordered intelligence officials to draw up a list of potential overseas targets for US cyber attacks," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/interactive /2013/jun/07/obama-cyber-directive-full-text (accessed June 8, 2013).

[77] "Taking the Mystery out of Cyberwar," *Washington Post*, http://www.washingtonpost.com/opinions/cyberwar-the-white-house-is-thinking-ahead/2013/06/16/b4a0ab00-d4fa-11e2-a73e-826d299ff459_story.html (accessed June 17, 2013).

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."[78] Technical risk, in other words, may be construed as a cyber-attack.

The urge to react strongly against a cyber-attack is not new. In early 1998, during a buildup of forces to mount a three-day bombing campaign in the Middle East, the US DOD discovered that intruders had broken into numerous secure computers and had obtained root access, allowing them to potentially steal and alter information or damage their networks. The Iraqi government was suspected of sponsoring this subversive activity. When the case was presented to President Clinton, both cyber and kinetic countermeasures were considered. An armed response was finally ruled out after it was discovered that a couple of American teenagers and their Israeli mentor were responsible for the mischief.[79]

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 at 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 is reasonable to assume 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

---

[78] 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).

[79] 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.

times to come. The confusion in information space is likely to be exacerbated because of the activities of the 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.[80]

Information Space CBMs in South Asia

Despite 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.[81] 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 understanding 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.[82] 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.[83] India-Pakistan

[80] 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).

[81] Read Stanley Wolpert, *Shameful Flight: The Last Years of the British Empire in India* (USA: Oxford University Press, 2006).

[82] Dennis Kux *India-Pakistan Negotiations*: Is Past Still Prologue? (Washington DC: USIP, 2006), 13;

[83] A.Z. Hilali, "Confidence- and Security-Building Measures for India and Pakistan," *Alternatives: Global, Local, Political,* Vol. 30, No.2, (April 30 2005): 191-222.

CBMs have been developed both in military and non-military spheres.[84] 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 Male, 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,[85] 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.[86] The leaders, officials and experts of the two countries regularly meet to improve and add to the existing basket of CBMs.[87] The 7th round of expert-level talks on nuclear CBMs was held in New Delhi in December 2012.[88] Information space CBMs were not on the menu.

This is worrisome, since international fears about cyberspace rivalry in the region are steadily gaining currency. In a recent statement the US Foreign Affairs Sub-committee on Asia and the

---

[84] 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).

[85] Sajad Padder, "The Composite Dialogue between India and Pakistan: Structure, Process and Agency," *Heidelberg Papers in South Asian and Comparative Politics*, Vol. 65 (February 2012): 1, http://www.ub.uni-heidelberg.de/archiv/13143 (accessed May 1, 2013).

[86] 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).

[87] 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).

[88] "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).

Pacific warned that Asia was fast becoming "the cyber security battleground." 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."[89] Indians noted with satisfaction the strong pitch the senator had made for the India-US cyber security partnership.[90] strangely there was studied silence from the Pakistani side. Surely, if Pakistan is the weakest link than 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 Internet revolution by adopting a wide array of commercially available ICT for managing businesses and private affairs but unfortunately did not do enough to improve the regional cybersecurity 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 been investing heavily in developing net-centric capabilities since 1980s.[91]

---

[89] 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).

[90] Sujay Mehdudia, "Congressional committee calls for strong India-U.S. ties on cyber security," The Hindu, July 30, 2013, http://www.thehindu.com/news/national/congressional-committee-calls-for-strong-indiaus-ties-on-cyber-security /article4970604.ece (accessed August 1, 2013).

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

they are now lobbying for a separate cyber-command.[92] Pakistan has a fully automated Strategic Command & Control Support System (SCCSS) since November 2012.[93] Its nuclear safety regime explicitly caters to cyber threats.[94] Cyber security measures, not withstanding, a growing community of cyber warriors in India and Pakistan is actively engaged in defacing government websites,[95] in the spirit of patriotic 'hacktivism' without formal sanction.[96] 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

---

[92] "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).

[93] "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).

[94] "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).

[95] 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).

[96] "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).

propaganda."[97] 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."[98] Since no monitoring or enforcement mechanisms were enforced, hostile propaganda never ceased. In fact it has increased disproportionately during times of tension, making the situation more combustible.[99]

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" grew exponentially – "much of it drawn from social media messages."[100] Two days later, the two countries almost went to war, when 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.[101] Pakistan took immediate defensive measures. The air force was placed on high alert and all important countries of the world were informed about

---

[97] 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).

[98] Moonis Ahmar ed., *The Challenges of Confidence Building in South Asia* (New Delhi: Har-Anand Publications, 2001), 317.

[99] 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).

[100] Polly Nayak and Michael Kreppon, *The Unfinished Crisis: US Crisis Management after the 2008 Mumbai Attacks* (Washington DC: Stimson Center, 2012), 6, http://www.stimson.org/images/uploads/research-pdfs/Mumbai-Final_1.pdf (accessed February 14, 2013).

[101] "Hoax call pushed Pakistan to brink of war with India," *Economic Times,* December 6, 2008, http://articles.economictimes.indiatimes.com/2008-12-06/news/28394766_1_india-and-pakistan-mumbai-attacks-mumbai-killings (accessed October 3, 2012).

these developments.[102] A very flustered US Secretary of State immediately placed a call on her Indian counterpart. A much delayed response caused panic at her end.[103] She then undertook a visit to South Asia to advise India to exercise restraint.[104] According to American diplomats in New Delhi one senior official of the Indian Ministry of External Affairs (MEA) confirmed that the call had indeed been made. There were subsequent denials and the entire affair was dismissed as a prank.[105]

Another incident that raised the level of vitriol 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 started making rounds that Bodos living elsewhere in India would be killed after the Muslim holy month of Ramzan, ended on August 20. This hate campaign was fuelled by bulk SMS and MMS over cell phones 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

---

[102] Nayak and Kreppon, *The Unfinished Crisis*, 12-13, http://www.stimson.org/images/uploads/research-pdfs/Mumbai-Final_1.pdf (accessed February 14, 2013).

[103] Condoleezza Rice, *No Higher Honor: A Memoir of my Years in Washington* (New York: Broadway Paperbacks, 2011), 720. "Post-26/11, Mukherjee's words rattled Pakistan: Condoleezza Rice," *The Times of India*, October 28, 2011, http://articles.timesofindia.indiatimes.com/2011-10-28/us/30332002_1_pranab-mukherjee-mumbai-attacks-external-affairs-minister (accessed June 10, 2013).

[104] Rice, *No Higher Honor*, 271.

[105] Dean Nelson, "WikiLeaks: hoax phone call brought India and Pakistan to brink of war," *The Telegraph*, 23 March 2011, http://www.telegraph.co.uk/news/worldnews/wikileaks/8401391/WikiLeaks-hoax-phone-call-brought-India-and-Pakistan-to-brink-of-war.html (accessed March 2, 2013).

local transport system.[106] 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.[107] The Indian businesses rely heavily on cell phone advertisements and suffered massive losses. On the international front, India quickly accused Pakistan of sponsoring the unrest.[108] The Government of Pakistan (GOP) asked India to come up with credible proof.[109] The matter rested there and after the customary period of mutual indignation it was business as usual.

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.[110] Pakistani government banned YouTube. The ban

---

[106] Maleeva Rebello, "Assam violence: Where it all began," September 1, 2012, http://www.dnaindia.com/india /1735111/report-assam-violence-where-it-all-began (accessed June 10, 2013).

[107] "5 SMS per day limit comes into effect," *The Times of India*, August 18, 2012, http://articles.timesofindia .indiatimes.com/2012-08-18/telecom/33260957_1_smses-and-mmses-bulk-messages-ban-period (accessed June 10, 2013).

[108] Michael Edward, "India accuses Pakistan of using social media to stir tensions," August 20, 2012, http://www.abc.net.au/am/content/2012/s3571168.htm (accessed June 10, 2013).

[109] "Pakistan seeks proof of India exodus messages," *BBC News*, August 20, 2012, http://www.bbc.co.uk/news /world-asia-india-19314937(accessed June 10, 2013).

[110] "Violent protests against video rock Pakistan," *Al Jazeera*, September 22, 2012, http://www.aljazeera.com /news/asia/2012/09/20129219618263113.html (accessed May 1, 2013)

continues to date.[111] It has yet to be determined if the movie was uploaded on purpose to provoke religious sentiments and 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.[112] This was not the last shenanigans of the SEA. On August 15, 2013, the *Washington Post* reported that it had been hacked by none other than the dreaded SEA.[113]

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.[114] 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 gener-

---

[111] Abubakar Siddique, "Pakistan Demands Filters Before Lifting YouTube Ban," *Radio Free Europe Radio Liberty,* June 13, 2013, http://www.rferl.org/content/gandhara-pakistan-youtube-ban/25016243.html (accessed June 15, 2013).

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

[113] Andrea Peterson, "The Post just got hacked by the Syrian Electronic Army. Here's who they are," *Washington Post*, August 15, 2013, 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 August 16, 2013).

[114] "Radio Listeners in Panic, Taking War Drama as Fact: Many Flee Homes to Escape 'Gas Raid From Mars' – Phone Calls Swamp Police at Broadcast of Wells Fantasy," *New York Times*, October 31, 1938, http://www.war-of-the-worlds.org/Radio/Newspapers/Oct31/NYT.html (accessed January 12, 2013).

ated 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,[115] for cooperating on matters related to cyber security.[116] Similar options are on the table to reduce Sino-US cyber tensions.[117] The suggestion that Pakistan and India establish their own NRRC has been suggested in the past.[118]

Thesis and Research Proposal

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; it theorizes that cyber-differences can be narrowed and a relatively stable cyber environment can be created by instituting an information space CBM regime. Based on the experiences of

---

[115] 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).

[116] 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).

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

[118] 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).

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 research: What is acceptable behavior in information-space? What are the international, regional, non-governmental, private and public initiatives to bring about order in cyberspace? Is there a model for CBMs in information space? What could be a set of mutually acceptable information-space CBMs between India and Pakistan? What is the way forward?

Literature Review

This research covered diverse areas ranging from cyber security to international law and CBMs. Therefore multiple sources of information and subject matter experts were consulted. Some of these books and papers are listed below:

National Cyber Security Policies and Threat Assessments. A number of US cyber policy documents are available online e.g. the National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive 23, Cybersecurity Policy (January 2008) and the 2006 Joint Staff National Military Strategy for Cyberspace Operations (NMS-CO),[119] the Comprehensive National Cybersecurity Initiative (CNCI) of 2008 and 2010,[120] the Cyberspace Policy Review (May 2009),[121] the Presidential Pol-

[119] National Military Strategy for Cyberspace Operations (NMS-CO), US Joint Staff Publication 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf

[120] US NSC's Comprehensive National Cybersecurity Initiative (CNCI), http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed June 20, 2013).

[121] Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

icy Directive (PPD) 20 on US Cyber Operations Policy,[122] 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.[123]

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.[124] 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.[125] Some thought-provoking information about the future of cyber war is available in Defense Advance Research Projects Agency (DARPA)'s Foundational CyberWarfare Plan-X: The Roadmap for Future Cyber War.[126]

The concepts of cyber war have been elaborated in papers written by experts like Amir Lupovici,[127] and Shmuel Even and

---

[122] PPD 20: US Cyber Operations, http://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf (accessed June 20, 2013).

[123] "Cyber Security," NSC, http://www.whitehouse.gov/cybersecurity (accessed July 10, 2013).

[124] Thomas, *Cyber Silhouettes.*

[125] Thomas, *Dragon Byte and Decoding the Virtual Giant and The Dragon's Quantum Leap.*

[126] "DARPA's Foundational CyberWarfare Plan-X: The Roadmap for Future CyberWar."http://cyberarms.wordpress.com/2012/12/01/darpas-foundational-cyberwarfare-plan-x-the-roadmap-for-future-cyberwar/ (accessed January 24, 2013).

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

David Siman-Tov.[128] *Cyber Attacks* by Edward Amoroso provides guidelines in protecting national infrastructures from cyber-attacks.[129] Similar solutions are given in Charles Perrow's book The *Next Catastrophe*.[130]

Papers read out at the UNIDIR conference held in Geneva in November 2012 give the national points of view on cyber security and stability of countries like Germany[131], Canada,[132] India,[133] and Russia[134]. Indian point of view is also available at the IDSA website.[135] 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

---

[128] 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).

[129] Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Burlington MA: El SevierInc, 2011),

[130] Perrow, *The Next Catastrophe*.

[131] 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).

[132] Roger Hurwitz, "Cross-domain threat assessment in international security: the need for cyberstability," Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability, UNIDIR, Geneva, Nov. 8-9, 2012, http://www.unidir.ch/pdf/conferences/pdf-conf1927.pdf (accessed January 24, 2013).

[133] Amandeep Gill, "What does a stable cyber environment look like?"UNIDIR Cyber Security Conference, November 8-9, 2012, Geneva, http://www.unidir.ch/pdf/conferences/pdf-conf1921.pdf (accessed January 24, 2013).

[134] Sergey Fedosov, "What does a Stable Cyber Environment look like?" http://www.unidir.ch/pdf/conferences/pdf-conf1922.pdf (accessed January 24, 2013).

[135] Arvind Gupta, "CBMs in Cyber Space: What should be India's Approach?" *IDSA*, June 27, 2012, http://idsa.in/idsacomments/CBMsinCyberspace_ArvindGupta_270612 (accessed January 22, 2013).

MoD,[136] John B. Sheldon of Canada Centre for Global Security Studies, University of Toronto,[137] Dave Clemente of Chatham House,[138] and Kwon Haeryong, the Ambassador of Republic of Korea to the Conference on Disarmament Permanent Mission.[139]

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,[140] and US Department of State's legal advisor Harold Koh's speech on "International Law in Cyber Space."[141] A critical analysis of the two documents by Michael N. Schmitt makes for an interesting reading.[142] The need to revise federal laws to provide cyber security has been covered in some detail by Eric A. Fischer.[143]

---

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

[137] 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).

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

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

[140] Schmitt ed.,*Tallinn Manual*.

[141] 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).

[142] 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).

[143] 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).

Pakistani diplomat ambassador Ahmed Kamal 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.*[144] A sequel to this book is *The Law of Cyber-Space: An Invitation to the Table of Negotiations*.[145] Other works that provide important pointers in this respect are *The Law of Cyber-Attack*,[146] *Cyberwarfare and International Law*,[147] "*Cyberattacks and the Use of Force: Back to the Future of Article* 2(4),"[148] and "The legal application of the prohibition of the threat or use of force in cyberspace: A starting point?"[149] An idea about how 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.[150]

---

[144] Eduardo Gelbstein & Ahmed Kamal, *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security UN ICT Task Force* (New York: UNITAR, 2002), http://www.un.int/kamal/publications/Information_Insecurity_Second_Edition_PDF.pdf (accessed January 12, 2013).

[145] 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).

[146] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel "The Law of Cyber-Attack," *California Law Review*, 2012, LawOfCyberAttack.pdf (accessed January 24, 2013).

[147] 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).

[148] Mathew C. Waxman, "Cyberattacks and the Use of Force: Back to the Future of Article 2(4)," http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf

[149] 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).

[150] Tim Maurer, Cyber Norm Emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-security, Discussion Paper #2011-11, Belfer Center for Science and International Affairs, http://belfercenter.org (accessed June 15, 2013).

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,[151] Feroz Hasan Khan,[152] Naeem Salik,[153] Zafar Nawaz Jaspal,[154] Maleeha Lodhi,[155] Kanti Bajpai and Dipanker Banerjee.[156] Another paper that provided useful inputs was one written by Toby Dalton of the Stimson Center.[157] So far no work has been done in developing info-based CBMs between India and Pakistan. It is hoped that this endeavor will prove to be a catalyst for more work on this subject.

---

[151] Moonis Ahmer ed., *Internal and External Dynamics of South Asian Security* (Karachi: Fazleesons, 1997).

[152] Feroz Hassan Khan, "Prospects for Indian and Pakistani Arms Control and Confidence-Building Measures," *Naval War College Review*, Vol. 63, No. 3 (Summer 2010): 105-121.

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

[154] Zafar Nawaz Jaspal, "Nuclear CBMs between India and Pakistan: Utilitarian Approach - How to build Confidence about our Nuclear Intentions," Defence Journal, Vol.7, No. 10 (May 2004), http://www.defencejournal.com/2004-5/gpa.asp (accessed July 4, 2013).

[155] Maleeha Lodhi, "CBMs need a bold approach," *Khaleej Times*, January 14, 2012, http://www.khaleejtimes.com/displayarticle.asp?xfile=data/opinion/2012/January/opinion_January49.xml&section=opinion&col= (accessed January 12, 2013).

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

[157] 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).

Organization of the Book

This work has been organized into four parts. The first section discusses international initiatives to create cyber norms and behavior. The section takes stock of the existing domestic and international cyber laws and treaties. The third portion studies existing models of CBMs in information space and the final portion suggests a menu of info-based CBMs that can be developed between India and Pakistan. The last section recommends a way forward.

Chapter 2

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 temporal 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. The urge to regulate all human activity extends into the realm of ICT as well.

Arguably the modern information age began with the advent of the electrical telegraph in 1837.[1] 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.[2] The transatlantic telegraph cables have since been replaced by 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 satellite. The

---

[1] Read Tom Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century On-line Pioneers* (New York: Walker & Company, 2007).

[2] *Ocean Telegraphy: The Twenty Fifth Anniversary* (New York: March 10, 1879), 6, http://books.google.com /books?id=dGfJTRgzexYC&pg=PA4&lpg=PA4&dq=telegraphy+across+the+oceans&source=bl&ots=xR-CGvtuNp&sig=JagB_PmdIOxnz09fGxH5V429EY0&hl=en&sa=X&ei=G8bRUc2RfqiMigLUq4DYAg&ved=0CGIQ6AEwBw#v=onepage&q=telegraphy%20across%20the%20oceans&f=false (accessed July 1, 2013).

development in technology was complemented by laws to control and regulate the new media of transmitting information. Stringent censorship rules were invoked by governments during times of war and internal strife to protect and 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. The Internet has allowed boundless access to transmit information but 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.

Legality of Cyber-Attacks

Unprotected information space is an open invitation for not only criminals and ideologues but also for nation states to launch cyber-attacks on the sly, without any 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).[3] 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."[4] The argument revolves around a number of issues like what justi-

[3] Bryan W. Ellis, "The International Legal Implications and Limitations of Information Warfare: What Are Our Options?"*US Army War College* (April 10, 2001), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA389043 (accessed August 7, 2012). For details about IHL visit International Society of the Red Cross (ICRC) website http://www.icrc.org/eng/war-and-law/index.jsp (accessed June 8, 2013).

[4] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy, National Research Council of the National Academies, Washington D.C., (2010): 152, www.nap.edu (accessed June 15, 2013)

fies 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.[5] 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),[6] under the principles of proportionality, distinction, and

[5] Dmitar Kostadinov, "The Attribution Problem in Cyber Attacks," February 1, 2013, *Infosec Institute*, http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/ (accessed February 14, 2013).

[6] Jus in bello & Jus ad bellum, http://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/index.jsp (accessed June 15, 2013). For detailed comments on the legality of cyber war see Richard W. Aldrich, "The International Legal Implications of Information Warfare," *Airpower Journal* (Fall 1996), http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf; Dimitrios Delibasis, "State Use of Force in Cyberspace for Self Defence: A New Challenge for a New Century," *Peace Conflict Development: An Interdisciplinary Journal* (February 2006): 8; Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkley Journal of International Law,* 192 (2009): 27, http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil(accessed April 22, 2013); David Willson, "A Global Problem: Cyberspace Threats Demand an International Approach, *ISSA Journal* (August 2009), http://www.issa.org/Library/Journals/2009/August?Wilson-A%20Global%20Problem.pdf (accessed August 7, 2013); William Yurcik, "Information Warfare: Legal and Ethical Challenges of the Next Global Battleground," Proceedings of the 2ndAnnual Ethics and Technology Conference (June 6-7, 1997), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.15.2345 (accessed September 25, 2012).

neutrality.[7] 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, Harold Koh, the legal expert of the US State Department, 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.[8] The International Group of Experts hired to draft the Tallinn Manual for NATO's Cooperative Cyber Defense Center of Excellence also concurs with Koh's version that force can be used in cyberspace under the internationally accepted principles of jus ad bellum and jus ad bello.[9]

Opinion is also divided about the lethality of cyber weapons.[10] 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

---

[7] Nils Melzer, "Cyberwarfare and International Law," *Cyberwarfare and International Law 2011*, UNIDIR Resources, http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (accessed April 25, 2013).

[8] Harold Hongju Koh, "International Law in Cyberspace," September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (accessed September 24, 2012).

[9] Michael N. Schmidt ed., *Tallinn Manual on the International Law applicable on Cyber Operations* (New York: Cambridge University Press, 2013), 9.

[10] For different opinions on the lethality of cyber-attacks read Stuart Casey-Maslen, "Non-kinetic-energy weapons termed 'non-lethal:' A Preliminary Assessment under International Humanitarian Law and International Human Rights Law," October 2010, http://www.geneva-academy.ch/docs/projets/Non-Kinetic-EnergyOctober2010.pdf (accessed January 12, 2013); and David A. Fulghum, "Cyber Attacks no longer Non-kinetic," September 28, 2010, http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%253A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%253Acc9234ab-f505-41d5-895a-8580f4bf4222 (accessed January 22, 2013).

Iranian nuclear program,[11] 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).[12] In the absence of death and destruction and lack of proof with regards to 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. So far, this line of thinking has not been pursued against deadly predator strikes in Pakistan using computer networks in Nevada.[13]

The use of remotely controlled surveillance planes has been justified by users as legitimate intelligence gathering exercise, and Airspace violations, by remotely controlled plans have been regretted as inadvertent. A case in point is the US drone that was brought down by the Iranians. On 4th December 2011, Iran announced that it had forced a Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) to land on its territory. The Americans claimed it had crashed, while on a recon mission. Iranians said that they had jammed both satellite and land control signals to the UAV, and followed it up by a spoofing attack. The false GPS data fed to the UAV led it into believing that it was landing

---

[11] For a detailed account of the stuxnet attack on Iran read Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," http://www.jonrlindsay.com/research/papers (accessed June 8, 2013).

[12] Rome Statute of the International Criminal Court, http://untreaty.un.org/cod/icc/statute/romefra.htm (accessed April 25, 2013).

[13] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber Attack," *California Law Review*, (2012): 11, http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberattack.pdf (accessed June 8, 2013)

at its home-base in Afghanistan.[14] Technology was used by both parties but since there were no human casualties, the reaction on both sides remained muted. However, things can get serious, if the country being spied upon retaliates against the infringement of its sovereign airspace with disproportionate physical means.

Cyber-attacks are not purely national campaigns. It is, impossible to separate cyber-crime from state sponsored cyber-attacks. Both are overlapping activities because states, criminals and non-state actors all use the same toolkit.

Cyber-crime 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. These include 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 cyber-crimes. These laws need to be harmonized into an international regime and relevant provisions and clauses incorporated into domestic legal codes.[15]

---

[14] Scott Peterson, "Exclusive: Iran hijacked US drone, says Iranian engineer (video)," *Christian Science Monitor,* December 15, 2011, http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video (accessed May 1, 2013); Barbara Starr, "Drone that crashed in Iran was on CIA recon mission, officials say," CNN, December 7, 2011, http://www.cnn.com/2011/12/06/world/meast/us-iran-drone/index .html (accessed May1, 2013).

[15] K. Prasad, Cyber-terrorism: Addressing the Challenges for Establishing an International Legal Framework. Originally published in the Proceedings of the 3rdAustralian Counter Terrorism Conference, December 2012, o.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act (accessed June 15, 2013).

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 eighty two 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 ratifications/accessions i.e. forty eight 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.[16] The list of major international and regional instruments on cyber security has been included in this book.

INTERNATIONAL INITIATIVES

Legal difficulties like affixing culpability and differentiating between cyber-crime and cyber-attacks, notwithstanding a number of international and regional instruments have been formulated to promote cyber security and prevent counter cyber-crime. 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 CE and the European Union (EU), the CIS and the SCO, intergovernmental African organizations, the League of Arab States, and the

[16] Comprehensive Study on Cybercrime, Draft February 2013, UN, 2013, http://www.unodc.org/documents /organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed April 25, 2013).

UN.[17] 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."[18] However, the cooperation in cyber security is proceeding at a slow pace. Some of the international initiatives in developing cyber norms are listed below:

The UN

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 num-

[17] "Comprehensive Study on Cybercrime: Draft," UN Office on Drug & Crime (UNODC), February 2013, http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY _210213.pdf (accessed July 4, 2013).

[18] UNGA Resolution 2131 (XX), *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty* (December 29, 1965), http://www.un-documents .net/a20r2131.htm (accessed April 24, 2013); UNGA Resolution 36/103, *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States,* (December 9, 1981), http://www.un.org/documents /ga/res/36/a36r103.htm (accessed September 24, 2012). Also refer to the Corfu Channel Case (UK & Ireland vs. Albania), *ICJ Reports* 1949, http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=cd&case=1; and the case Against Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. USA), *ICJ Reports* 1986, http://www.icj-cij.org/docket/files/70/6503.pdf (accessed September 19, 2012).

ber of reporting mechanisms and Groups of Government Experts (GGEs).[19] 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.[20]

UNGA Resolutions on Cyber Security

The UNGA is empowered only 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.[21] 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.[22] 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).[23] Since then three annual reports on the subject (2010, 2011 and 2012) incorporating the views of the member

---

[19] UNGA, http://www.nti.org/treaties-and-regimes/united-nations-general-assembly/ (accessed August 7, 2012).

[20] Disarmament and International Security: First Committee, http://www.un.org/en/ga/first/ (accessed June 20, 2013).

[21] Functions and Powers of the General Assembly, http://www.un.org/en/ga/about/background.shtml (accessed January 12, 2013).

[22] Developments in the Field of Information and Telecommunications in the Context of International Security, *UNODA*, http://www.un.org/disarmament/topics/informationsecurity/ (accessed April 25, 2013).

[23] UNGA Resolutions adopted in the 53rd session, http://www.un.org/depts/dhl/resguide/r53.htm (accessed June 15, 2013. Also see Jody R. Westby ed., *International Guide to Cyber Security* (Chicago: American Bar Association, 2004), 84.

states have been published. Two related resolutions were passed by the Second Committee,[24] on the "Creation of a Global Culture of Cyber-Security and the Protection of Critical Informational Infrastructures,"[25] and "Creation of a Global Culture of Cyber-Security and Taking Stock of National Efforts to Protect Critical Information Infrastructures."[26] 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.[27] 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.[28] The resolution also called for a new study of international informational security issues but there was little action on it.[29] Similar exhortations in subsequent UNGA sessions failed to produce any

[24] For an explanation on the 2nd Committee read UNGA: Economic and Financial – The Second Committee, http://www.un.org/en/ga/second/index.shtml (accessed April 25, 2013).

[25] UNGA Resolution 58/199, (December 23, 2003), *UN Documentation Research Guide*, http://www.un.org/depts /dhl/resguide/r58.htm (accessed April 22, 2013).

[26] UNGA Resolution 64/211 (March 17, 2010), http://www.un.org/en/ga/64/resolutions.shtml (accessed April 25, 2013).

[27] *Disarmament Resolutions and Decision of the Fifty-Fifth Session of the United Nations General Assembly* (Department for Disarmament Affairs,2000), 4; UNGA Resolution 57/53 (December 30, 2002), The United Nations Disarmament Yearbook, Vol. 37, Part I (2012): 3 & 4, http://www.un.org/disarmament/HomePage /ODAPublications/Yearbook/2012/YB2012-Part-I.pdf (accessed April 25, 2013).

[28] UNGA Resolution 57/53 (December 30, 2002), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/57 /53&Lang =E (accessed April 25, 2013).

[29] Ibid.

meaningful progress.[30]

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

In 2004, the UNGA 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 specifically, there was 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

[30] UNGA Resolution 58/32 (December 18, 2003), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES /58/32&Lang=E (accessed September 24, 2012); UNGA Resolution 59/61(December 16, 2004), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/59/61&Lang=E (accessed October 3, 2012) ; UNGA Resolution 60/45 (December 8, 2005), http://www.un.org/disarmament/HomePage/ODAPublications /ResolutionsDecisions/PDF/ResDes2005.pdf (accessed January 12, 2013); UNGA Resolution 61/54 (December 19, 2006), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/61/54&Lang=E (accessed February 14, 2013); UNGA Resolution 62/17 (January 8, 2008), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/62/17 &Lang=E (September 15, 2012); UNGA Resolution 63/37 (January 9, 2002), http://www.un.org/ga/search/view _doc.asp?symbol=A/RES/63/37&Lang=E (accessed June 15, 2013); UNGA Resolution 64/25(January 14, 2010), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/64/25 (accessed August 7, 2012). Also see Sean Kanuck, "Sovereign Discourse on Cyber Conflict under International Law," https://www.law.upenn.edu/institutes /cerl/conferences/cyberwar/papers/reading/Kanuck.pdf (accessed September 19, 2012).

countries.[31]

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."[32] 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 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.[33] The Report had also recommended the need to find possibilities to elaborate common terms and defi-

---

[31] Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security, *UNODA*, June 2013, http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf (accessed July 4, 2013);Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *UN Document A/60/202*, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05 /453/63/PDF/N0545363.pdf?OpenElement (accessed October 3, 2012).

[32] Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Document A/65/201 (July 30, 2010), http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf (accessed August 7, 2012).

[33] "Developments in the Field of Information and Telecommunications in the Context of International Security," *UNODA*, http://www.un.org/disarmament/topics/informationsecurity/ (accessed January 12, 2013).

nitions.[34] These recommendations represent progress in overcoming a long impasse between the US and Russia on cyber security issues and could become the basis of a multilateral treaty under the auspices of the UN, as Russia has been advocating.[35]

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.[36] The third GGE has met thrice – 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.[37] According to the available literature on the subject, countries like Germany and India are favorably inclined towards information space CBMs.[38]

---

[34] Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security, *UNODA*.

[35] John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks," *New York Times*, July 16, 2010, http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1 (accessed February 14, 2013). The draft Russian Convention on Information Security (2011) is available at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

[36] UNGA 66/24, *Developments in the Field of Information and Telecommunications in the Context of International Security*(December 13, 2011), http://www.un.org/ga/search/view_doc.asp?symbol=%20A/RES/66/24 (accessed April 22, 2013).

[37] "Developments in the Field of Information and Telecommunications in the Context of International Security," *UNODA*.

[38] "Challenges in Cyber Security: Risks, Strategies and Confidence Building," *Conference Report German Ministry of Foreign Affairs*, December 13 and 14, 2011, Berlin, http://www.auswaertiges-amt.de/DE/Aussenpolitik /Friedenspolitik/Abruestung/Projekte/Cybersicherheit.html; Arvind Gupta, "CBMs in Cyber Space: What should be India's Approach?" Institute for Defence Studies and Analysis (IDSA), June 27, 2012, http://www.idsa.in /idsacomments/CBMsinCyberspace_ArvindGupta_270612 (accessed October 3, 2012).

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."[39]

International Code of Conduct on Information Security

On September 12, 2011 China, Russia, Tajikistan and Uzbekistan proposed to the UNSG an international code of conduct on information security. 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 sharp criticism from US officials, who saw it as an exercise in undermining their efforts to keep the Internet free from external interference.[40] 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 informa-

[39] Jen Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," *US Department of State,* June 7, 2013, http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm (accessed June 8, 2013).

[40] Timothy Farnsworth, "China and Russia Submit Cyber Proposal," *Arms Control Association*, http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal (accessed August 7, 2012).

tion weapons or related technologies."[41]

The issue was brought directly before 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 cybersecurity, which the Assembly had adopted in 2002.[42]

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).[43] UNIDIR organizes con-

---

[41] 66th Session of the UN, Item 93 of the Provisional Agenda, Developments in the Field of Information and Telecommunication in the Context of International Security, Letter dated 12 September 2011from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, A/66/359, http://cs.brown.edu/courses/csci1800/sources /2012_UN_Russia_and_China_Code_o _Conduct.pdf (accessed April 25, 2013).

[42] "At UN, Kazakhstan calls for global cybersecurity treaty to deter hackers," *UN News Center,* September 21, 2011, http://www.un.org/apps/news/story.asp?NewsID=39652&Cr=cyber#.UgK8sZI4vwY (accessed September 24, 2012).

[43] Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security," Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf (accessed April 25, 2013).

ferences and also produces documents on disarmament.[44]

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 stakeholders 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 were 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 is to some extent, 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 open platform for all stakeholders interested in the Information Society.[45]

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 an NGO

---

[44] Read for instance Kirstin Vignard, *Confronting Cyberconflict*, 2011, UNIDIR Disarmament Forum, http://unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf (accessed September 24, 2012).

[45] What was the UN ICT Task Force?http://www.itu.int/wsis/basic/faqs_answer.asp?lang=en&faq_id=88 (accessed September 25, 2013).

concerned with improving crisis information management by the international community through better use of ICT. It advocates the use of ICT in helping countries in conflict zones to achieve the UN Millennium Development Goals (MDG). Since 2006 it has served as the hub for research, advocacy and networking on the use of ICT to prevent, respond to and recover from conflict.[46] Besides NGOs, individual researchers like the Estonian scientist Eneken Tikk, have also provided rules of conduct in cyber space.[47]

ITU

This Geneva-based organization is a member of the UN Development Group (UNDG). Originally founded as the International Telegraph Union it is now a specialized UN agency on ICT issues.[48] 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.[49]

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

---

[46] ICT4Peace Project, http://ict4peace.org/whoweare/ict4peace-history#sthash.2rxeSuHR.dpuf. (accessed August 7, 2012).

[47] Eneken Tikk, "Ten Rules for Cyber Security", *Survival*, Vol.53, No.3, June-July 2011, http://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-june-july-2011-bad3/53-3-12-tikk-4349 (accessed September 15, 2012).

[48] ITU, http://www.itu.int/en/Pages/default.aspx (accessed April 25, 2013).

[49] UN Development Group, http://www.undg.org/index.cfm?P=13 (accessed September 15, 2012).

in the use of ICTs."[50] This was followed by a UNGA resolution formalizing its role.[51] In order to fulfill its mission, the ITU prepared an elaborate Global Cybersecurity Agenda (GCA).[52] It 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 emphasizes 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 networks of other countries, language barriers in the context of freedom of expression as outlined in the treaty. The US, UK, Australia and a few other major countries have rejected the treaty because of objections against centralizing the global governance model of regulations on Internet access and the available online content.[53] This is symbolic of sharp differences of opinion on Internet governance between the developed countries and the developing world. Countries like Russia and China want more national oversights, while those in the former category want the Internet to be a free domain governed by voluntary standards set by the industry. It is widely believed that the Internet is controlled by

---

[50] Security in the use of ICTs, http://files.wcitleaks.org/public/WCIT12%20-%20ITRs%20and%20security.pdf (accessed June 18, 2013).

[51] UNG.A. Resolution 60/252 (April 27, 2006), http://www.itu.int/wsis/docs background/resolutions/60-252.pdf (accessed October 3, 2012).

[52] Dr Hamadoun I. Touré, *The Quest for Cyber Peace*, ITU and PMP on Information Security World Federation of Scientists, January 2011, http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf (accessed October 3, 2012).

[53] Anitha Nagaraj, Global Telecom Treaty 2012 signed in the ITU world conference, Center for Information and Communication Science (CICS), June 21, 2013, http://cicsworld.centerforics.org/blog/2013/01/3/global-telecom-treaty-2012-signed-in-the-itu-world-conference/ (accessed June 21, 2013).

the US, and that it draws the major advantages from its use. China and Russia would like to have a greater control over online content and users, which they sometime see as threats to their national policies. They are also concerned about legitimate problems like spam. The terms of the new treaty gives the ITU an explicit role in regulating online content, specifically spam and cybersecurity. This also extends the treaty's regulatory umbrella to Internet Service Providers (ISP). The ITU is considering amending its constitution to formally assert jurisdiction over the technical side of the Web.[54] ITU has a number of cooperative agreements with other groups like the Association of South East Asian Nations (ASEAN) and the Caribbean Community (CARICOM). It has a joint project with the CARICOM and the Caribbean Telecommunications Union (CTU) known as the 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. [55]

Internet Governance Forum (IGF)

There is no central authority controlling the Internet. It is a globally distributed network comprising many voluntarily interconnected autonomous networks, and 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 drawn from civil society, the private sector, governments, the academic and research communities and national and

---

[54] "Who rules the Internet? The U.N. agency that oversees phone, radio and satellite communications last week stopped short of fragmenting the Internet into national fiefdoms," *Los Angeles Times*, December 16, 2012, http://articles.latimes.com/2012/dec/16/opinion/la-ed-itu-united-nations-internet-20121216 (accessed June 20, 2013).

[55] Cybercrimes/e-crimes: Model Policy Guidelines and Legislative Texts, HIPCAR, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf (accessed on June 15, 2013).

international organizations. They all work cooperatively to create shared policies and standards to 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.[56] The establishment of the IGF was formally announced by the UNSG in July 2006. It has since 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.[57] In April 2013, the second-in-command at the US DHS Jane Holl Lute was hired to write the Internet laws for the UN.[58]

---

[56] Internet Governance Forum (IGF), http://www.intgovforum.org/cms/ (accessed June 21, 2013).

[57] S.E. Jones, "United Nations set to Define New Worldwide Rules for the Internet: New Rules to Define Internet Use between Countries," November 6, 2012, http://voices.yahoo.com/united-nations-set-define-worldwide-rules-for-11894888.html (accessed June 20, 2013).

[58] "Homeland Security top officer to work on UN's new global Internet rules," http://rt.com/usa/cyber-lute-un-internet-572/ (accessed June 20, 2013).
overnance Forum (IGF), http://www.intgovforum.org/cms/ (accessed June 21, 2013).

Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF) and Society for Worldwide Interbank Financial Telecommunication (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 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. ICANN seeks to create a globally unified namespace to ensure the global reach of the Internet, and 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 the 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.[59] Another example of digital monopoly by the advanced countries over the Internet is SWIFT which is located in La Hulpe, Belgium.[60] This society connects the international banking system and all international banking transactions are conducted through it.

[59] Internet Corporation for Assigned Names and Numbers (ICANN), http://www.icann.org/ (accessed June 21, 2013).

[60] The Swift Codes, http://www.theswiftcodes.com/ (accessed January 12, 2013).

The Institute of Electrical and Electronics Engineers (IEEE) and NIST

The IEEE is the world's largest organization for the advancement of technology.[61] It develops technical standards through its Standards Association, in conjunction with the US National Institute of Standards and Technology (NIST).[62]

International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO)

The 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.[63] ISO/IEC JTC 1 is the Joint Technical Committee 1 of the ISO and the IEC, with the objective of developing, maintaining, promoting, and facilitating 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.[64]

The ISO/IEC 27001:2005 or the "Information technology - Se-

---

[61] Institute of Electrical and Electronics Engineers, http://www.ieee.org/index.html (accessed September 24, 2012).

[62] National Institute of Standards and Technology (NIST) http://www.nist.gov/index.html (accessed September 19, 2012).

[63] International Electrotechnical Commission (IEC) http://www.iec.ch/index.htm (accessed August 7, 2012).

[64] ISO/IEC JTC 1 Information Technology, http://www.iso.org/iso/standards_development/technical_committees /list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020 (accessed September 19, 2012).

curity techniques - Code of practice for information security management" is the internationally-accepted standard of good practice for information security.[65] 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 for stakeholders to collaborate on resolving cyber security issues.[66]

Organization for the Advancement of Structured Information Standards (OASIS)

OASIS 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.[67]

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

[65] ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management, http://www.iso27001security.com/html/27002.html (accessed August 14, 2013).

[66] ISO/IEC 27032:2012 Information technology – Security Techniques – Guidelines for Cybersecurity, http://www.iso.org/iso/catalogue_detail?csnumber=44375 (accessed September 15, 2012).

[67] Organization for the Advanced Structured Information Standards (OASIS), https://www.oasis-open.org/ (accessed January 12, 2013).

Service Providers (ISPs) and e-mail marketers etc.[68] It has also commissioned works on the information economy,[69] and the future of the Internet economy.[70] In 2002, the OECD adopted the Guidelines for the Security of Information Systems and Networks. This established a framework of principles 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.[71] 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.[72]

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) program of the Canadian Police Centre for Missing and Exploited Children (CPCMEC), European Police (Europol), International Criminal Police Organization (Interpol), Italian postal and telecommunication police service, Dutch Na-

---

[68] Report of the OECD Task Force on Spam: Anti-spam Toolkit of Recommended Policies and Measures, April 12, 2006, http://www.oecd.org/internet/consumer/36494147.pdf (accessed June 17, 2013).

[69] Information Economy, http://www.oecd.org/sti/ieconomy/informationeconomy.htm (accessed June 18, 2013).

[70] OECD Seoul Declaration for the Future of the Internet Economy, OECD Ministerial Meeting on the Future of Internet Economy, South Korea, June 17-18, 2008, http://www.oecd.org/futureinternet/ (accessed June 18, 2013).

[71] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm (accessed April 25, 2013).

[72] The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, JT00196105, December 16, 2005, http://www.oecd.org/internet/ieconomy/35884541.pdf (accessed September 24, 2012).

tional Police, New Zealand Police, Indonesian National Police, Korean National Police Agency Cyber Terror Response Center, Ministry of the Interior of UAE, Child Exploitation and online Protection Centre UK, DHS and US Immigration and Enforcement.[73]

Interpol

Under an ambitious plan, the Interpol has set up a Global Complex for Innovation in Singapore. This state-of-the-art facility 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. Additionally it will provide research facilities to test protocols, tools and services to analyze trends of cyber-attacks; develop practical solutions in collaboration with police, research laboratories, academia and the public and private sectors; address issues such as Internet security governance, capacity building and training, research into training and methodology and transfer the findings into police activities on ground; provide classrooms, field and online training programs for National Central Bureaus; Anti-corruption training, particularly in sport; set quality standards and provide and accreditation. It will also provide operational and investigative support.[74]

---

[73] Virtual Global Task Force, http://www.virtualglobaltaskforce.com/ (accessed July 4, 2013).

[74] Connecting Police for a Safer World, *Interpol*, http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation (accessed February 14, 2013).

World Federation of Scientists (WFS), 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. 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.[75] 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.[76]

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.[77]

---

[75] World Federation of Scientists Permanent Monitoring Panel on Information Security, http://www.unibw.de /infosecur/publications/papers_supporting/infosecur/documents/supporting_documents/westby_cyberspace_security_presentation_2003 (accessed June 8, 2013).

[76] "Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar - Report & Recommendations," World Federation of Scientists Permanent Monitoring Panel (PMP) on Information Security, August 2003, http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (accessed September 19, 2012).

[77] Reprinted in "The Quest for Cyber Peace" www.itu.int/S-GEN/WFS,01-2011-PDF-E, 110, http://pdf.ebooks6.com/The-QuesT-for-cyber-peace--ITU-Committed-to-connecting-the-world-download-w67356.pdf (accessed September 15, 2012)

London Conference on Cyber Space

Several international seminars have been convened on cyber security, which have brought to fore a number of good suggestions. 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 like William Hague, British Foreign Secretary; Joe Biden, US Vice-President; Jimmy Wales, Co-founder Wikipedia; and Carl Bildt, the Swedish Foreign Minister 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.[78]

Forum of Incident Response and Security Teams (FIRST) & CERTs

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 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

[78] The London Conference, *Chatham House*, http://www.chathamhouse.org/research/security/current-projects/london-conference (accessed October 3, 2012)

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.[79]

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 as 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 regular or need basis.[80]

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

[79] FIRST is the global Forum for Incident Response and Security Teams, http://www.first.org/ (accessed July 4, 2013).

[80] Stan Gibilisco, "Computer Security Incident Response Team (CSIRT)," August 2012, http://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT (accessed August 7, 2012).

Pacific Economic Cooperation (APEC), Organization of American States (OAS), ASEAN, the League of Arab States, the African Union (AU) and Network Operations Groups (NOG). Surprisingly, no initiative has been taken in South Asia within the framework of South Asian Association for Regional Cooperation (SAARC) or at any other bilateral level.

SCO

This Eurasian security organization, 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.[81] The President of Afghanistan was invited to attend the 2012 summit meetings.[82] 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 agenda. The organization is seriously concerned about threats arising from the 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

[81] SCO official website, http://www.sectsco.org/ (accessed September 19, 2012).

[82] Official Website of Beijing SCO Summit 2012, http://www.scosummit2012.org/english/2012-04/28/c_131558560.htm (accessed April 25, 2013).

> 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.[83]

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. Russia's SCO National Coordinator, Ambassador Barsky has described the Council of Europe (CE) Convention on Cybercrime as less than satisfactory.[84]

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.[85] 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

---

[83] Declaration of the Heads of the SCO Member States on International Information Security (Non official translation from the Russian Text), June 15, 2006, http://www.fidh.org/Declaration-of-the-Heads-of-the (accessed June 15, 2013).

[84] Alica Kizekova, "The Shanghai Cooperation Organisation: Challenges in Cyberspace," S. Rajaratnam School of International Studies, NTU, February 22, 2012, http://www.rsis.edu.sg/publications/Perspective/RSIS0332012.pdf (accessed September 25, 2012).

[85] Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security, signed in Yekaterinburg on June 15, 2009, http://www.fmprc.gov.cn/eng/wjdt/2649/t569701.htm (accessed June 15, 2013).

decisions in the interest of an opposing party.[86] It clearly described cyberwarfare 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."[87] SCO presents itself as a possible center of gravity in international legal action on cyber-attacks.[88] In 2009 another agreement was concluded among the governments of SCO member states on Cooperation in the Field of Ensuring International Information Security and ASEAN.[89] The US is wary that other countries may use the SCO Accord template to crack-down on domestic dissent.[90] On September12, 2011 Russia and

---

[86] Annex I to the Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security, June 16, 2009, based on an unofficial translation reproduced in *International Information Security: The Diplomacy of Peace: Compilation of Publications and Documents* (Moscow 2009): 202-203.

[87] Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security, 61st Plenary Meeting, cited by Jason Healey, "The Five Futures of Cyber Conflict and Cooperation," *Georgetown Journal for International Affairs*, http://journal.georgetown.edu/wp-content/uploads/cyber-Healy.pdf (accessed October 3, 2012); SCO – Cooperation on Security, January 22, 2013, http://www.infosco.eu/index.php/aboutsco/activities (accessed February 14, 2013).

[88] Oona A. Hathaway et al., "The Law of Cyber Attack," *California Law Review*, (2012): 54.

[89] "Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation," *Ministry of Foreign Affairs People's Republic of China,* http://www.fmprc.gov.cn/eng/wjdt/2649/t569701.htm (accessed January 12, 2013). Pliny Han ed., Full Text: The Internet in China, Xinhuanet, June 8, 2010, http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm (accessed September 19, 2012).

[90] Julie Boland, *Ten Years of the Shanghai Cooperation Organization: A Lost Decade? A Partner for the U.S.?* 21st Century Defense Initiative at Brookings, June 20, 2011, 13, http://www.brookings.edu/~/media/research/files/papers/2011/6/shanghai%20cooperation%20organization%20boland/06_shanghai_cooperation_organization_boland.pdf (accessed June 15, 2013).

China used the forum of the SCO to present an international code of conduct for Internet to the UNGA.[91]

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.[92] Georgia left the CIS in 2009, after the Georgia-Russia crisis.[93] 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.[94] It has been alleged that the members of the CIS practice strict Internet censorship. There is also active cooperation

---

[91] China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, *Ministry of Foreign Affairs People's Republic of China*, September 13, 2011, http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm (accessed April 22, 2013).

[92] Commonwealth of Independent States, http://www.cisstat.com/eng/cis.htm (accessed January 12, 2013).

[93] "Georgia Finalizes Withdrawal from CIS," *Radio Free Liberty*, August 18, 2009, http://www.rferl.org/content /Georgia_Finalizes_Withdrawal_From_CIS/1802284.html (accessed August 7, 2012).

[94] Regional Commonwealth in the Field of Communications, http://www.en.rcc.org.ru/index.php/rcc/about-rcc (accessed October 3, 2012).

between Belarusian and Russian special services in cyberspace. In 2000, the CIS concluded agreement among themselves on Cooperation in Combating Offences related to Computer Information.[95]

In the last decade, the region witnessed two cyber wars. The first was a campaign by pro-Russian (and allegedly state-sponsored) hackers, which paralyzed Estonian Internet in May 2007. The second was a similar campaign (also allegedly organized by nationalist pro-government Russian hackers) that occurred at the same time as major combat operations in Georgia (August 2008). The latter campaign targeting Georgian online media and government websites led Georgian authorities to filter access to Russian Internet sites, allegedly as a means of self-defense against Russian cyber propaganda. This resulted in an information vacuum in Tbilisi during the critical days when it was unclear whether Russian troops would stop their advance. The CIS informational controls are similar to those adopted by China and Iran like Internet filtering.[96]

CEC

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, and 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. CE deals particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network

[95] Fyodor Pavlyuchenkoa, Kenneth Geers tr., "Belarus in the Context of European Cyber Security," http://www.ccdcoe.org/publications/virtualbattlefield/11_PAVLYUCHENKO_Belorussia.pdf (accessed October 3, 2012).

[96] Commonwealth of Independent States, *Open Net Initiative*, https://opennet.net/research/regions/cis (accessed October 3, 2012).

security. Its main objective is to pursue a common criminal policy aimed at protecting the society against cyber-crime by adopting appropriate legislation and fostering international cooperation.[97] 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.[98]

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. Twelve countries have signed but not ratified. 39 have signed and ratified.[99] The US ratified the Convention in August 2006. India and Pakistan are not members of the Convention requires not only that the 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 cooperate with each other for the purposes of in-

---

[97] S.A. Ahsan, Current Situation and Issues of Illegal and Harmful Activities in the Field of Information and Communication Technology in Pakistan. Participant's Papers, 140th International Training Course, 2008, http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf (accessed April 22, 2013).

[98] Council of Europe Convention on Cybercrime, Budapest, September 23, 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm (accessed May 1, 2013).

[99] Council of Europe Convention on Cybercrimes (CET No 185), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed May 1, 2013).

vestigating, 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.[100] The CEC, thus far, represents the most substantive, and broadly subscribed multilateral agreement on cybercrime in existence today.[101] In March 2012, the Council adopted an Internet governance strategy.[102]

EU

In June 2010, EU's law enforcement agency, the European Police Office (Europol) created the EU Cybercrime Task Force.[103] 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.[104] 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

---

[100] M. A. Vatis, "The Council of Europe Convention on Cybercrime," *Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (2010): 207-224, http://www.nap.edu/catalog /12997.html (accessed May 1, 2013).

[101] Council of Europe Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS 189), (2003), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. (accessed September 19, 2012).

[102] Council of Europe adopts Internet Governance Strategy, http://www.coe.int/t/DGHL/cooperation/economiccrime /cybercrime/default_en.asp (accessed October 3, 2012).

[103] European Cybercrime Task Force, http://europol.easyred.com/?p=129 (accessed June 8, 2013).

[104] Cybercrime, *Issues Monitor,* July 2011, Vol. 8, KPMG International: 12.

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.[105] The Schengen Information System and the Europol Information System, with inbuilt 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.[106] The EU has also established the European Network and Information Security Agency (ENISA) to advance 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.[107]

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.

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

---

[105] EC3: A Collective EU Response to Cyber-Crime, https://www.europol.europa.eu/ec3 (accessed June 17, 2013).

[106] Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), 7.12.2012, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/20121207_com_2012_735_en.pdf (accessed June 17, 2013).

[107] The Netherlands Country Report, May 2011, http://www.enisa.europa.eu/activities/stakeholder-relations/files /country-reports/Netherlands.pdf (accessed June 8, 2013).

Internet standards developed by its Third Generation Partnership Project (3GPP).[108]

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.[109] 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 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.[110]

Organization of Security and Cooperation in Europe (OSCE)

The OSCE has produced a draft code of conduct on cyber security.[111] In 2011, the 56 participating nations of the OSCE, including the US, voted on a resolution to improve cybersecurity coopera-

---

[108] European Telecommunications Standards Institute, http://www.ihs.com/products/industry-standards /organizations/etsi/index.aspx (accessed September 19, 2013).

[109] Cyber Security, OAS, http://www.oas.org/en/topics/cyber_security.asp (accessed August 20, 2013).

[110] O. A. Hathaway, The Law of Cyber Attack, California Law Review, (2012).

[111] A Comprehensive Approach to Cyber Security, http://www.osce.org/event/cyber_sec2011 (accessed September 24, 2012).

tion. 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.[112] A draft of proposed CBMs floated by the OSCE was circulated among the member states in November 7, 2012. It included six proposals concerning national and transnational ICT security. Most of the suggested CBMs are voluntary and therefore difficult to enforce.[113]

ASEAN

ASEAN member states cooperate and share best practices on ICT and business processes at the forum of Telecom and IT 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.[114] The AIM2015 envisions

---

[112] Resolution on "Overall approach by the OSCE to promote cybersecurity," The text of the proposal is available at http://www.oscepa.org/images/stories/documents/activities/1.Annual%20Session/2011_Belgrade/Supplementary (accessed June 15, 2013).

[113] OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous, posted 13th November 2012 by Jeffrey Carr,http://jeffreycarr.blogspot.com/2012/11/osces-cyber-security-confidence.html
(accessed June 15, 2013).

[114] "Joint Media Statement of the 12th ASEAN Telecommunications and IT Ministers Meeting and its Related Meetings with Dialogue Partners," November 19, 2012, http://www.asean.org/news/asean-statement-communiques/item/joint-media-statement-of-the-12th-asean-telecommunications-and-it-ministers-meeting-and-its-related-meetings-with-dialogue-partners (accessed January 12, 2013).

creating a global ICT hub.[115] The chiefs of ASEAN Police (Aseanapol) meet regularly to discuss issues like cybercrime laws. They intend establishing a partnership with the Interpol's Global Complex (IGC) in Singapore, to enable it respond effectively against challenges presented by cybercrime.[116]

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.[117] Japan supports not only the implementation of AIM2015, it also wants to share its experience on the utilization of ICT in disaster management with ASEAN.[118] In a June 2013, 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.[119] The ARF has also held Cyber Security workshops in

---

[115] Caitríona H. Heinl, "Enhancing ASEAN-Wide Cybersecurity: Time For A Hub Of Excellence? – Analysis," July 19, 2013, http://www.eurasiareview.com/19072013-enhancing-asean-wide-cybersecurity-time-for-a-hub-of-excellence-analysis/ (accessed July 25, 2013).

[116] ASEAN Cybercrimelaw, http://www.cybercrimelaw.net/ASEAN.html (accessed October 3, 2012).

[117] Pliny Han ed., Full Text: The Internet in China, *Xinhuanet*, June 8, 2010, http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm (accessed September 19, 2012).

[118] "ASEAN, Japan boost ICT cooperation," *Vietnam*, May 1, 2013, http://en.vietnamplus.vn/Home/ASEAN-Japan-boost-ICT-cooperation/20135/33994.vnplus (accessed June 15, 2013).

[119] The ASEAN-U.S. Ministerial Meeting: Fact Sheet, Office of the Spokesperson, Washington, DC, July 1, 2013, http://www.state.gov/r/pa/prs/ps/2013/07/211389.htm (accessed July 4, 2013).

collaboration with Australia.[120]

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.[121] The aim of this strategy is to encourage APEC economies to take action for the security of information systems and networks.[122]

League of Arab States

The League of Arab States came into being after the Arab-Israel war of 1967.[123] 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.[124] 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).

---

[120] Henry Fox, "The Contribution of Capacity Building to Developing Confidence between States in Cyber Space – An Australian Perspective, *ARF Seminar on Confidence Building Measures in Cyber Space,* September 11-12, Seoul, aseanregionalforum.asean.org (accessed July 4, 2013).

[121] APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment, http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups /~/media/Files/Groups/TEL/05_TEL_APECStrategy.pdf (accessed September 19, 2012).

[122] APEC Cybersecurity Strategy, http://itlaw.wikia.com/wiki/APEC_Cybersecurity_Strategy (accessed June 15, 2013).

[123] Khartoum Resolution, *CFR*, http://www.cfr.org/world/khartoum-resolution/p14841 (accessed September 24, 2012).

Economic Community of West African States (ECOWAS), African Union (AU) and Common Market for Eastern and Southern Africa (COMESA)

A number of African groups have come up with directives, legal frameworks and model bills concerning cyber security. ECOWAS has produced a number of legislations, including Supplementary Act on Electronic Transactions, Supplementary Act on Personal Data Protection and the Directive on Fighting Cybercrime.[125] In 2011, the 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.[126] In 2011, another African group, the COMESA came up with the Cybersecurity Draft Model Bill.[127]

---

[124] Ashley Blount, "Topic I: Assessing the current state of cybersecurity and its implications for regional defense and economic interest," *Model Arab League 2012-13*, http://ncusar.org/modelarableague/resources/13-mal-bg-jdc.pdf (accessed August 20, 2013).

[125] Teki Akuetteh, Power Point Presentation on Creating the Enabling Environment within the ECOWAS Region, http://meeting.afrinic.net/waigf/presentations/Presentation_%20Ecowas_Teki_Akuetteh/Presentation_Ecowas_Teki_Akuetteh.pdf (accessed January 12, 2013).

[126] *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa*, Version 01/01.2011, Commissioned by the Economic Commission for Africa and the African Union Commission,

[127] *Report of the 30th Meeting of the Council of Ministers: Harnessing Science and Technology for Development (October 2011)*: 37, http://comesabusinesscouncil.org/attachments/article/29/Annex%20IV;%20COMESA %20COUNCIL%20OF%20MINISTERS%20REPORT-%20October,%202011.pdf (accessed June 15, 2013).

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 and holds three meetings in a year.[128]

BILATERAL INTIATIVES

US-Russia 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 cybersecurity incidents. These CBMs:

- 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."

---

[128] Philip Smith, Network Operations Groups, *Power Point Presentation for RIPE 56,* 5-9 May 2008,Berlin, http://meetings.ripe.net/ripe-56/presentations/Smith-Regional_Network_Operations_Groups.pdf (accessed June 1, 2013).

- **Exchange of Cyber Security Notifications.** This measure will permit communications and "formal inquiries about cybersecurity 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.[129] 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 cybersecurity because the two countries are applying similar approaches in arms control contexts e.g. CBMs and hotline communications, to cybersecurity challenges. This strategy dovetails with the needs for better situational awareness and transparency through increased information exchange. It calls 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 not confident of these iCBMs being a panacea for all cyber security ills. American interest is that the Internet remains

[129] Elizabeth Simson, "The U.S.–Russia Cybersecurity Pact: Just Paper," *The Foundry*, June 21, 2013, http://blog.heritage.org/2013/06/21/the-u-s-russia-cyber-pact-just-paper/ (accessed July 4, 2013).

free, open and unfettered of oppressive international laws.[130]

Differing national perceptions have created a lot of ambiguity about what should constitute 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 stop-gap 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

---

[130] David P. Fidler, "Call Me, Maybe: New US-Russia Cybersecurity Initiatives," *Arms Control Law*, http://armscontrollaw.com/2013/06/21/call-me-maybe-new-us-russia-cybersecurity-initiatives/ (accessed July 3, 2013).

* CAMM provides "consistent and complete trust framework to transparently assure information risk management maturity across the supply chain." See http://common-assurance.com/resources/Common-Assurance-Maturity-Model-vision.pdf (accessed July 3, 2013).

£ CSA is a non-profit organization that promotes research into best practices for securing cloud computing and the ability of cloud technologies to secure other forms of computing. See https://cloudsecurityalliance.org/ (accessed July 3, 2013).

€ The Dutch National Cyber Security Strategy (NCSS) Success through Cooperation (2011): 3, http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011 (accessed August 7, 2012) .

mechanisms and processes." [131]

Convention on Cyberspace

Ideally, there should be a Convention on Cyberspace. In 2005, Ahmed Kamal, a Pakistani diplomat based in Geneva produced a monograph suggesting laws for the cyber space.[132] Experts are of the view that a Convention on Cyber Space can be prepared on lines similar to the UN Convention on the Law of the Sea of 1982. Unfortunately, the idea of such a Convention has so far not found international acceptability. Apparently cyber space is more choppy and rough than all the oceans of the world combined together. Similar problems have also been experienced in concluding a treaty on preventing arms race in outer space (PAROS). It is difficult to compare the damages caused by aggressive or illicit behavior in information space to a potentially harmful arms race in outer space. The major difference is that while cyber space is nebulous and ill-defined, activity in outer space can still be tracked and monitored. It has been suggested that in the absence of a cyber-treaty, the law of armed conflict or IHL can be conveniently applied in the cyberspace.[133]

Since damage caused by the cyber-attacks in terms of human deaths or destruction to property is not clearly visible, the applicability of these laws is difficult to comprehend.[134]

---

[131] "Cyber-security. The vexed question of global rules," http://www.stefanomele.it/news/dettaglio.asp?id=285 (accessed July 4, 2013).

[132] Ahmed Kamal, "The Law of Cyber-Space an Invitation to the Table of Negotiations," (Geneva: UNITAR, 2005), www.in.int/kamal/the_law_of_cyber_space (accessed June 8, 2013).

[133] For basic insight into the Law of Armed Conflict consult "The Law of Armed Conflict – Basic Knowledge," ICRC, http://www.icrc.org/eng/assets/files/other/law1_final.pdf (accessed April 25, 2013).

[134] Henning Wegener, "Regulating Cyber Behaviour: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures," http://www.federationofscientists.org/PlanetaryEmergencies/Seminars/45th /Wegener %20 publication.docx ‎(accessed April 25, 2013).

Chapter 3

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. Below is a brief description of the existing rules and regulations in Pakistan and India on the subject of cyber security.

Cybercrime Laws in Pakistan

Following 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[1] and the national media indicate a rise in crime such as identity thefts and illicit use of credit cards;[2] and harassment and blackmailing on the social media.[3] Pakistan currently has no cyber-crime laws. The Prevention of Electronic Crimes Ordinance 2009 lapsed, without being made into a law,[4] and since then no le-

---

[1] Cyber-Crime: Pakistan Criminal Records, http://pakistancriminalrecords.com/tag/cyber-crime/.

[2] "Two cyber 'criminals' arrested," *Dawn*, September 13, 2012, http://dawn.com/2012/09/13/two-cyber-criminals-arrested/ (accessed January 12, 2013); "Four held for cyber crime," Dawn, http://dawn.com/2012/05/16/four-held-for-cyber-crime/ (accessed February 14, 2013).

[3] "FIA swings into action to bust cyber blackmailers," *The News,* February 16, 2012, http://www.thenews.com.pk/Todays-News-7-92964-FIA-swings-into-action-to-bust-cyber-blackmailer (accessed February 14, 2013).

[4] Amir Wasim, "Placing lapsed ordinance in Senate: Law ministry apologises to committee," June 23, 2010, *Dawn*, http://archives.dawn.com/archives/36414 (accessed June 10, 2013).

gal 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,[5] 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.[6] These laws are given in Table II (page 99). 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 as a CERT.[7]

Cyber Security Bill

Pakistan does not have a national cyber security policy. This indicates a serious capacity deficit at the policy planning levels.[8] Official quarters were jolted out of their complacency by revelations that Pakistan was being extensively spied upon through Internet and online communication systems and that 13.5 billion pieces of

[5] S. Raza Hassan, "Alarming Rise in Cyber Crimes," *Dawn*, July 30, 2012, http://dawn.com/2012/07/30/alarming-rise-in-cyber-crimes/ (accessed March 23, 2013).

[6] Kashif Zafar, "Cyber-crime: Two arrested for forgery, credit card fraud," *Express Tribune*, September 12, http://tribune.com.pk/story/435059 /cyber-crime-two-arrested-for-forgery-credit-card-fraud/ (accessed March 23 , 2013).

[7] Profile of National Response Centre for Cyber Crimes, National Response Centre for Cyber Crime (NR3C), FIA, http://www.fia.gov.pk/prj_nr3c.htm (accessed June 8, 2013).

[8] Haseeb Sohail, "Information Technology Ministry: A Chaos so far," *The News*, July 29, 2013, http://blogs.thenews.com.pk/blogs/2013/07/information-ministry-a-chaos-so-far/ (accessed July 30, 2013).

its email, phone and fax communications have been intercepted.[9] 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 since Pakistan was second most spied upon country, sufficient funds should be allocated to execute a Cyber Security Strategy. He suggested the formation of a Cyber Security task force within the Ministry of IT, to propose counter measures. His proposal was unanimously adopted.[10]

In a follow up seminar, 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 are 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 Paki-

---

[9] Global Surveillance Data: US Places Pakistan on Second Position in NSA Spy List, *BBC Record*, http://bbcrecord.com/live/ct-menu-item-17/pakistan/10-pakistan/544-global-surveillance-data-us-places-pakistan-on-second-position-in-nsa-spy-list.html (accessed July 30, 2013).

[10] "Mushahid to table Cyber Security Bill in Parliament," http://www.mushahidhussain.com/news-detail.php?id =MTE0&pageid=media (accessed June 28, 2013).

stan's cyber security. The drafting of 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 of 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 as not to 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.[11]

In January 2014, Government of Pakistan announced that it would be setting up a Cyber Authority, a special court to deal with cyber-crimes and disputes as well as an emergency unit to counter attacks that are against Pakistan's interests. This decision was part of a larger plan to amend a dozen major laws through a consolidated compendium to be called the Electronic Documents and Prevention of Cybercrimes Act, 2014.[12]

---

[11] Senate committee proposes 7-point Action Plan for Cyber Secure Pakistan, *Dawn*, July 12, 2013, http://dawn.com/news/1023706/senate-committee-proposes-7-point-action-plan-for-cyber-secure-pakistan/?commentPage=1&storyPage=2 (accessed July 16, 2013).

[12] Khaleeq Kiani, "Govt to set up cyber authority, court," *Dawn*, January 12, 2014, http://www.dawn.com/news/1079918/govt-to-set-up-cyber-authority-court (accessed January 12, 2014)

Cyber Law of India

India enacted its IT Act in June 2000.[13] This Act was modified in 2008, a copy is attached as an appendix for reference. The Indian justice system allows cyber-crimes 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.[14]

Cyber Defenses of India

CERT-In was established in 2004.[15] The Crisis Management Plan for Cyber Attacks was issued in 2010.[16] 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.[17] 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.[18] By February 2013, NCIIPC had finalized

[13] Government of India Information Technology Act 2000, http://www.cyberlawsindia.net/itbill2000.pdf (accessed June 15, 2013).

[14] Cyber Law of India, http://www.cyberlawsindia.net/ (accessed June 15, 2013).

[15] FIRST Members, http://www.first.org/members/teams/cert-in (accessed September 19, 2012).

[16] "Crisis Management Plan for Cyber Attacks," Press Information Bureau (PIB) GoI, May 6, 2010, http://pib.nic.in/newsite/erelease.aspx?relid=61597 (accessed June 15, 2013).

[17] Muktesh Chander IPS, "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities," Power Point Presentation, http://indiasmartgrid.org/en/Lists/Member/Attachments/19/ISGD%20Plenary%20III%20Muktesh%20Chander%20NCIIPC.pdf (accessed July 4, 2013).

[18] Indrani Bagchi &Vishwa Mohan, "5 lakh cyber warriors to bolster India's e-defence," *The Times of India,* October 16, 2012, http://articles.timesofindia.indiatimes.com/2012-10-16/india/34498075_1_cyber-security-cyber-attacks-cyber-warfare (accessed January 12, 2013).

the national cyber security policy focusing on domestic security solutions reducing dependence on foreign technology.[19] The National Cyber Security Policy 2013 (NCSP-2013) was published on July 2, 2013.[20] After the newsbreak that India was among the top five countries targeted by the US global surveillance programs, it was decided 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.[21] In May 2013, a full-time Cyber Security Coordinator was appointed.[22]

Foreign Collaboration

India is actively collaborating with countries outside the region 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.[23] In October 2012, the Foreign and De-

---

[19] Manu Kaushik and Pierre Mario Fitter, "Beware of the Bugs," *Business Today,* February 17, 2013 http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html (accessed April 22, 2013).

[20] File No: 2(35)/2011-CERT-In, *Ministry of Communication and Information Technology, Department of Electronics and Information Technology (DEITY) Notification on National Cyber Security Policy-2013 (NCSP-2013)*, July 2, 2013, http://indiacybersecurity.blogspot.com/ (accessed July 4, 2013).

[21] Indrani Bagchi, "Government to Roll Out New Cybersecurity Architecture," *The Times of India,* June 13, 2013, http://articles.timesofindia.indiatimes.com/2013-06-13/security/39950586_1_cyber-security-coordinator-cybersecurity-architecture (accessed June 15, 2013).

[22] "Gulshan Rai to be first National Cyber Security Coordinator," *The Indian Express,* May 10 2013, http://www.indianexpress.com/news/gulshan-rai-to-be-first-national-cyber-security-coordinator/1113777/ (accessed June 15, 2013).

[23] United States and India Sign Cybersecurity Agreement, DHS, July 19, 2011, http://www.dhs.gov/news/2011/07/19 /united-states-and-india-sign-cybersecurity-agreement (accessed April 22, 2013)

fense Secretaries of India and Japan met at the 2+2 meeting in Tokyo to decide, among other things an expansion in cyber security collaboration.[24] 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 cyber-crime 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 in 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.[25]

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, UAE, 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.[26]

---

[24] India Japan to Expand Cyber Security Cooperation, http://news.softpedia.com/news/India-and-Japan-to-Expand-Cyber-Security-Cooperation-301524.shtml (accessed August 21, 2013).

[25] Warwick Ashwood, "David Cameron pledges UK collaboration with India to fight Cyber Attacks," *ComputerWeekly.com*, February 19, 2013, http://www.computerweekly.com/news/2240178234/David-Cameron-pledges-UK-collaboration-with-India-to-fight-cyber-attacks (accessed June 15, 2013).

[26] SEA-ME-WE, http://www.seamewe4.com/ (accessed July 10, 2013).

Chapter 4

INFORMATION CBMs BETWEEN PAKISTAN AND INDIA

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 a group of Muslim pilgrims led by the Holy Prophet 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, the agreement to co-exist peacefully for 10 years gave the Muslim time to establish their state and spread their religion in Arabia.[1]

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 (conventional, nuclear, chemical and biological);weapon test notifications; demilitarized or thin-out zones and goodwill visits etc.[2] Non-military CBMs cover political, economic, environmental, social and cultural fields.[3]

According to Norwegian political scientists, Johan Jørgen

---

[1] Martin Lings, *MUHAMMAD (PBUH): His Life based on the Earliest Sources* (Islamic Texts Society, 1991) 252-262.

[2] Confidence Building Measures, Stimson Center, http://www.stimson.org/topics/confidence-building-measures/ (accessed July 4, 2013).

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

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."[4] This concept was further refined as "arrangements designed to enhance such assurance of mind and belief in the trustworthiness of states and the fact they create."[5] 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.[6] The UN Comprehensive Study on CBMs 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

---

[4] Johan Jørgen Holst and Karen A. Melander, "European Security and Confidence Building Measures. *Survival*, Vol. 19, No. 4 (July/August 1977): 147.

[5] Johan Jørgen Holst, "Confidence Building Measures: A Conceptual Framework," *Survival*, Vol. 25, No. 1 (January/February 1983): 2.

[6] *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).

fruitful international cooperation."[7] The primary tools for managing successful CBMs are "communication, constraint, transparency, and verification measures." Together, these make the behavior of states more predictable.[8]

Contemporary CBMs are the legacy of the Cold War and were used extensively to stabilize the East-West relationship.[9] 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."[10] Initially, only teletypewriters were deployed at both terminals. In the 1970s, the hotline was upgraded to a telephonic link.[11] The 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

---

[7] *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/Disarmament Study Series/PDF/SS-7.pdf (accessed April 22, 2013).

[8] "Confidence-Building and Nuclear Risk-Reduction Measures in South Asia," http://www.stimson.org/research-pages/confidence-building-measures-in-south-asia-/ (accessed January 12, 2013).

[9] For details about the Cold War CBMs refer to *Vienna Document of the Negotiations on Confidence- and Security-Building Measures*, adopted at the 269th Plenary Meeting the OSCE Forum for Security Co-operation in Istanbul on 16 November 1999, http://www.osce.org/fsc/41276 (accessed July 15, 2013).

[10] Kelsey Davenport, "Hotline Agreements," *Arms Control Association,* November 2012, http://www.armscontrol.org/factsheets/Hotlines (accessed July 4, 2013).

[11] "Cold War Hotline Recalled," *BBC*, http://news.bbc.co.uk/2/hi/europe/2971558.stm (accessed July 4, 2013).

exchanges.[12]

The hotline was followed by arms control talks between the US and the former USSR. The CBM negotiations were codified in the Helsinki Final Act of 1975.[13] 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.[14] Typically, the CBMs include Transparency, Information Exchange Measures, Observation and Verification Measures, and Constraint Measures.[15] 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 com-

[12] "Welcome to the Nuclear Risk Reduction Center (NRRC): Confidence Building through Information Exchange," http://www.state.gov/t/avc/nrrc/ (accessed July 4, 2013).

[13] "Helsinki Final Act," *OSCE*, http://www.osce.org/mc/39501 (accessed July 4, 2013).

[14] Emily B. Landau, *Assessing the Relevance of Nuclear CBMs to a WMD Arms Control Process in the Middle East Today*, 2nd EU Non-Proliferation Consortium in Support of a Process Aimed at Establishing a Zone Free of WMD and Means of Delivery in the Middle East, Brussels, 5-6 November 2012, http://www.nonproliferation.eu /documents/backgroundpapers/landau.pdf (accessed July 14, 2013).

[15] Confidence Building, UNODA, http://www.un.org/disarmament/convarms/infoCBM/ (accessed July 1, 2013).

> mencement 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.[16]

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.

History of India-Pakistan CBMs

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 towards seeking peaceful solutions to pressing problems constitute 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).[17] A major source of friction continues to be the supply of water from the upper (India) to the lower riparian (Pakistan). 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.[18] In September 1960, the World Bank-brokered Indus Wa-

[16] 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).

[17] Mussarat Qadeem, "CBMs and Conflict Resolution as Approaches to the South Asian Security: How Relevant?" in Moonis Ahmer ed., *Internal and External Dynamics of South Asian Security* (Karachi: Fazleesons Pvt Ltd, 1998), 79.

[18] Charles Herman Heimseth and Surjit Mansingh, *A Diplomatic History of Modern India* (Allied Publishers, 1971), 144.

ters Treaty was concluded.[19]

Pakistan and India formally ended wars through the Karachi Agreement (1949),[20] Tashkent agreement (1966),[21] and the Simla Agreement (1972).[22] 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.[23] Both parties also twice accepted UN intervention twice to monitor 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.[24]

Although India and Pakistan have maintained diplomatic relations even during hostilities, 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.[25] During the 99 Kargil crisis Prime Ministers Nawaz Sharif and Vajpayee did speak on the tele-

---

[19] Indus Waters Treaty, http://siteresources.worldbank.org/INTSOUTHASIA/Resources/223497-1105737253588 /IndusWatersTreaty1960.pdf (accessed April 25, 2013)

[20] Agreement between Military Representatives of India and Pakistan Regarding the Establishment of a Ceasefire Line in the State of Jammu and Kashmir (Karachi Agreement), *UN Peace Maker,* http://peacemaker.un.org/indiapakistan-karachiagreement49 (accessed April 25, 2013).

[21] Tashkent Declaration, http://peacemaker.un.org/india-pakistan-tashkent-declaration66 (accessed September 19, 2012).

[22] Simla Agreement July 2, 1972, MEA GoI, http://www.mea.gov.in/in-focus-article.htm?19005/Simla+Agreement +July+2+1972 (accessed July 4, 2013).

[23] John B. Ray, "The Resolution of the Rann of Kutch Boundary Problem," *The Geographic Bulletin* (1970): 26-32, http://www.gammathetaupsilon.org/the-geographical-bulletin/1970s/volume06/article2.pdf (accessed June 15, 2013).

[24] UN Military Observer Group in India and Pakistan (UNMOGIP) January 1949 to date and UN India-Pakistan Observation Mission (UNIPOM) September 1965-March 1966, *The Blue Helmets: A Review of the UN Peacekeeping* (New York: UN Department of Public Information, 1996), 703-705.

[25] J.N. Dixit*, India-Pakistan: In War & Peace* (London: Routledge, 2002), 271.

phone but this conversation served only to heighten the predicament.[26] Officials have also used the telephonic channels to discuss pressing issues. Indian external affairs secretary J.N. Dixit talked to his Pakistani counterpart Shaharyar M. Khan over the telephone in March 1993.[27] Rather than using the phone Pakistani foreign minister, Sartaj Aziz flew to New Delhi in 1999 in an abortive attempt to defuse the Kargil situation.[28] In 2004, India and Pakistan actually agreed to set up a hotline between the foreign ministers to reduce the threat of accidental nuclear war.[29] A proposed counter terrorism hotline between the interior ministries hasn't been operationalized so far,[30] but media reports indicate that it may still be on the cards.[31] Telephonic conversation has its limitations and diplomats prefer talking directly to one another or communicating through carefully formal diplomatic communiqués and non-papers. After the infamous call by the Indian foreign minister threatening the President of Pakistan with dire consequences,[32] a requirement was felt for additional identification filters and protocols.

---

[26] Michael Krepon and Nate Cohn eds., *Crises in South Asia: Trends and Potential Consequences* (Washington DC: Stimson Center, 2011), 43, http://www.stimson.org/images/uploads/research-pdfs/Crises_Complete.pdf (accessed October 3, 2012).

[27] Dixit, *In War & Peace,* 284.

[28] Krepon and Cohn eds., *Crises in South Asia,* 43.

[29] John Lancaster , "India, Pakistan to Set Up Hotline: Talks End With Deal to Maintain Moratorium on Nuclear Testing," *Washington Post*, June 21, 2004, http://www.washingtonpost.com/wp-dyn/articles/A55542-2004Jun20 .html (accessed September 24, 2012).

[30] Sahil Makkar, "India, Pakistan yet to establish hotline," October 21, 2011, http://www.livemint.com/Politics /jC9kgXUvCENGbaSYO2iHKL/India-Pakistan-yet-to-establish-hotline.html (accessed September 19, 2012).

[31] "Hotline between India-Pak home secys soon," *Hindustan Times,* May 13, 2012, http://www.hindustantimes.com/India-news/NewDelhi/Hotline-between-India-Pak-home-secys-soon/Article1-854994.aspx (accessed August 7, 2012).

[32] "Prank Call Fuels Post-Attack Tensions between Pakistan, India," *Fox News*, December 6, 2008, http://www.foxnews.com/story/2008/12/06/prank-call-fuels-post-attack-tensions-between-pakistan-india/ (accessed September 25, 2012).

One of the most dependable communication links between India and Pakistan is DGMO hotline. This direct link was established after the 1971 war is now routinely used every week.[33] 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.[34] For last ten years, regular biannual meetings are being held 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.[35]

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 two 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 at Kahuta. The situation became very grim during Exercise Brasstacks in 1986-87, when 400,000 Indian troops began military drills perilously close to the Pakistani border in Sindh.[36] The aim was to trigger a conventional

---

[33] "Confidence-Building and Nuclear Risk-Reduction Measures In South Asia," *Stimson Center*, http://www.stimson.org/research-pages/confidence-building-measures-in-south-asia-/ (accessed August 14, 2013).

[34] India-Pakistan Military CBMs Project – Phase 1: Final Report, http://www.acus.org/files/Final%20Project%20report%20-%20Phase%201_Sept%2025.pdf (accessed July 1, 2013).

[35] "India, Pak Coast Guards to set up hotline," *Hindustan Times*, April 28, 2006, http://www.hindustantimes.com /News-Feed/NM9/India-Pak-Coast-Guards-to-set-up-hotline/Article1-91504.aspx (April 22, 2013).

[36] For details read "The Brasstacks Crisis of 1986-87," in P.R. Chari, P.I. Cheema and S.P. Cohen, *Four Crisis and a Peace Process*: *American Engagement in South Asia* (Washington DC: The Brookings Institute, 2007), 39- 79. For the Indian narrative read Raja Menon, *A Nuclear Strategy for India* (New Delhi: Sage Publications, 2000), 98.

war and simultaneously strike Kahuta.[37] 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 retired 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.[38] To make the process more transparent, both parties are required to exchange annually lists of the location of all their nuclear-related facilities. This ritual is being faithfully complied with, despite various phases of tension. Since 1991, there has been an agreement to send advance notices of military exercises and maneuvers and prevent airspace violations.[39]

Both India and Pakistan are signatories to the Chemical Weapon Convention (CWC).[40] On August 19, 1992 the two countries also signed a bilateral agreement on chemical weapons (CW).[41] After the nuclear tests of 1998, both nations placed a voluntary moratorium on further nuclear testing.[42] In September 1998 ses-

---

[37] Feroz Hassan Khan, "Pakistan's Nuclear Future," in Michael R. Chambers ed., *South Asia in 2020*: *Future Strategic Balances and Alliances* (Strategic Studies Institute, 2002), 163.

[38] Khurshid Khoja, "Confidence Building between India and Pakistan: Lessons, Opportunities, and Imperatives,"*A Handbook of CBMs for Regional Security,* 3rd Edition, March 1998.

[39] Tughral Yamin, "Nuclear Risk Reduction in South Asia," *Journal of Contemporary Studies*, National Defence University Islamabad, December 2012.

[40] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention), *Organisation for the Prohibition of Chemical Weapons* (OPCW), http://www.opcw.org/chemical-weapons-convention/ (accessed June 15, 2013).

[41] India- Pakistan Chemical Weapon Text, *Inventory of International Nonproliferation Organizations and Regimes,* Center for Nonproliferation Studies, http://cns.miis.edu/inventory/pdfs/aptindpakch.pdf (accessed June 8, 2013)

[42] International Day against Nuclear Testing: 29 August, http://www.un.org/en/events/againstnucleartestsday/history.shtml (accessed July 4, 2013).

sion of the UNGA, the prime ministers of India and Pakistan pledged abstinence from further testing.[43] 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. The major concerns identified were about nuclear safety and security. The joint statement by the prime ministers 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, improvement of nuclear security and prevention of 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.[44] The Kargil conflict 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,[45] which except for occasional violations held out till, it

---

[43] "India and Pakistan Statements to the United Nations General Assembly, September 1998," http://www.acronym.org.uk/spsep98.htm (accessed September 24, 2012).

[44] Lahore Declaration, USIP Peace Agreements Digital Collection, http://www.usip.org/sites/default/files/file/resources/collections/peace_agreements/ip_lahore19990221.pdf (accessed July 4, 2013).

[45] David J. Karl, "India and Pakistan: The Ties that Bind vs. The Line that Divides," *February* 5, 2013, *Foreign Policy Association,* http://foreignpolicyblogs.com/2013/02/05/india-and-pakistan-the-ties-that-bind-vs-the-line-that-divides/ (accessed April 22, 2013).

was severely disrupted in 2013.[46]

In November 2005, Pakistan and India signed the ballistic missile advance notification agreement.[47] Under this accord, the country's defense ministries are obligated to provide their counterparts at least a 72-hour 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.[48]

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.[49] The slow process of the composite dialogue process notwithstanding,[50] optimists keep

---

[46] There were ceasefire violations in January and August this year. Read Krista Mahr, "India-Pakistan Tensions Spike as Two Sides Trade Fire across the Border," August 12, 2013, *Time World*, http://world.time.com/2013/08/12/cease-fire-violations-continue-along-the-india-pakistan-border/ (accessed August 13, 2013).

[47] Agreement between India and Pakistan on Pre-Notification of Flight Testing of Ballistic Missiles, http://www.stimson.org/research-pages/agreement-between-india-and-pakistan-on-pre-notification-of-flight-testing-of-ballistic-missiles/ (accessed October 3, 2012).

[48] Eric Creegan, "India Pakistan sign missile notification pact," *Arms Control Today*, http://www.armscontrol.org/act/2005_11/NOV-IndiaPak (accessed January 12, 2013).

[49] Brigadiers Asad Hakeem (Pakistan Army) and Gurmeet Kanwal (Indian Army) with Michael Vannoni and Gaurav Rajen, "Demilitarization of the Siachen Conflict Zone: Concepts for Implementation and Monitoring," *Sandia National Laboratories,* SAND2007-5670, (US Department of Energy, 2007).

[50] Maleeha Lodhi, "Pause in the Peace Process," *The News*, March 15, 2013, http://www.thenews.com.pk/Todays-News-9-163510-Pause-in-the-peace-process (accessed March 23, 2013).

floating new ideas on CBMs.[51] 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 promise their 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 identifying 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 stage is to improve, strengthen and possibly upgrade these to the status of treaties and formal accords.

The success and failure of CBMs is contingent 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 place, on 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 skill sets on the negotiating team is always helps in fine tuning a CBM. The domestic media may assist 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.[52] Finally, the chances of CBMs

---

[51] For new ideas on CBMs read "India-Pakistan Military CBMs Project, Phase 1, Final Report." Final%20Project%20report%20-%20Phase%201_Sept%2025.pdf (accessed June 15, 2013).

[52] Collapse of the Agra Summit: The After-Story, *NDTV*, Aired: July 2001, Uploaded May 13, 2013, http://www.ndtv.com/video/player/reality-bites/collapse-of-the-agra-summit-the-after-story-aired-july-2001/274963 (accessed June 8, 2013).

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.

South Asia watchers are of the opinion that India and Pakistan have just been reactive and not proactive in formulating CBMs.[53] This observation may not be germane to South Asia alone. It has happened elsewhere too e.g. the Kremlin-Whitehouse 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.[54] 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 these cases.

Information CBMs

The first mention of information security CBMs was made at the 2005 WSIS summit held in Tunis. It was agreed that it was essential to strengthen the "trust framework, including information security and network security, authentication, privacy and consumer protection, is 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

---

[53] Holly Higgins, Applying Confidence-Building Measures in a Regional context, *Research Paper for the Institute for Science and International Security,* http://isis-online.org/uploads/conferences/documents/higginspaper.pdf (accessed June 8, 2013).

[54] Kenneth W. Allen, "Confidence Building Measures and the People's Liberation Army," in Chien-min Cao and Bruce Dickson eds., *Remaking the Chinese State: Strategies, Society and Security* (London: Routledge, 2001), 252.

"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." Spam was recognized 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." Finally, the WSIS emphasized that "Confidence and security" were "among the main pillars of the Information Society."[55]

Pre-requisites for Information CBMs

A necessary precondition for developing cyberspace CBMs is to have good national cybersecurity policies and practices, particularly for the protection of critical infrastructure.[56] Since all countries and most businesses are digitally linked to one another, their mutual interdependence has increased manifold. Axiomatically, therefore, the national cyber practices and policies have regional and international implications. Poor national cybersecurity practices will most likely weaken collective cyber defenses. It is therefore 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

[55] World Summit on the Information Society Geneva 2003, Tunis 2005, http://www.itu.int/wsis/docs/geneva /official/dop.html (accessed June 19, 2013).

[56] "Developing a Framework to Improve Critical Infrastructure Cybersecurity," *National Institute of Standards and Technology (NIST)*, 02/26/2013, https://www.federalregister.gov/articles/2013/02/26 /2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity (accessed July 26, 2013).

improve the confidence and trust among nations besides strengthening global cybersecurity. Shoring up the cyber defenses cannot be done by governments alone; expertise available in the private sector, as well as in the academic circles, civil society and users can be helpful. This mutual collaboration will require:

Capacity Building: As discussed earlier, a lot of guidance is available on cyber capacity building in the form of 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 inter-governmental agencies, as well as businesses and non-governmental bodies. The prime characteristics of this exercise include stocktaking of the public key infrastructure (PKI);[57] 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 through from basic design questions to the implementation stage.[58]

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 is-

[57] PKI (Public Key Infrastructure), http://searchsecurity.techtarget.com/definition/PKI (accessed July 4, 2013).

[58] Cyber Security, *Global Centre for Cyber Security Capacity Building*, http://www.oxfordmartin.ox.ac.uk /institutes/cybersecurity (accessed August 19, 2013).

sues. 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.[59] This event can help promote secure online practices. Effective partnerships can be established with the industry to address cybersecurity issues by developing and promoting of good practices guidelines. National Cyber Security Awareness Weeks can also be observed to help users and small businesses to understand cybersecurity risks, and develop effective cyber security practices.

Developing Policies and Structures: Countries without robust cyber security structures are the weak links in the international system. Hence, it is important to develop sound national cybersecurity policies. The policies would be based on available cyber ideologies and 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 cybersecurity issues is a key ingredient in managing coordinated responses. Improved government coordination on cybersecurity 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.

Establishing Incident Management and Response Systems: A key element of national cybersecurity 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

[59] Cyber Security Awareness Day Survival Guide and Checklist, *Department of Energy*, http://energy.gov/cio/downloads/cyber-security-awareness-day-survival-guide-and-checklist (accessed July 29, 2013).

Notification; and a Containment and Remediation Plan.[60] 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.

Holding Cyber Security Incident Response Workshops:[61] Workshops aimed at developing 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 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. One challenge could indeed be the information-sharing mechanism before an incident occurs, and to improve 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.

Improving Policies: Developing good cybersecurity 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 cope with emerging challenges. In undertaking this work the governments will have to find out areas of common interest in the realm of cyber security. It would be plausible, to encourage the governments to issue Cyberspace White Paper laying down a framework for maximizing opportuni-

---

[60] Thad Mckinnon & ERM Initiative Faculty, "Cyber Crisis Management – A New Philosophy and Approach to Incident Response," http://www.poole.ncsu.edu/erm/index.php/articles/entry/Cyber-Crisis-Management/ (accessed January 12, 2013).

[61] "IPSC: PECO Workshop Cybersecurity and Incident Response," February 13, 2004, (accessed February 14, 2013).

ties and minimizing the risks of the digital age.[62] 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.

Crafting Cyber Security Work Plan: In the final analysis there is a drive need to develop national cybersecurity work plans. These work plans should provide users not only a guideline to enforce cyber security measures in government and organizations' offices,[63] but also seriously consider ways and means for peaceful collaboration with other nations in cyberspace.

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 regard to 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 hone the skills of first responders.

[62] "Calls for Incoming Government to Develop another Cyber Security White Paper," ABC News, July 29, 2013 (accessed July 29, 2013).

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

3. **Restraint Agreements:** A path breaking form of information space CBM can be an agreement enjoining upon parties involved 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."[64] Commonsense 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.[65] Online hate crime is rife.[66] Cyber intimidation and coercion is now considered part of cyber-terrorism.[67] Such obnoxious behavior can 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.[68]

---

[64] David Gompert and Phillip Saunders, "Mutual Restraint in Cyberspace," (Fort McNair, Washington DC: National Defense University Press), http://www.ndu.edu/press/paradox-of-power-ch6.html (accessed July 30, 2013).

[65] Jose Bolton and Stan Graeve eds., *No Room for Bullies: From the Classroom to Cyber Space* (Nebraska: Boys Town Press, 2005), 179-190.

[66] "What we Investigate, *FBI Albuquerque Division*, http://www.fbi.gov/albuquerque/about-us/what-we-investigate (accessed August7, 2013).

[67] 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.

[68] Warren E. Agin, "Jurisdictions in Cyberspace," American Bar Association Section of Business Law Cyberspace Law Committee Coping with Personal Jurisdiction in Cyberspace, ABA Subcommittee on Internet Law Liability Report #3, March 26, 2008, http://corporate.findlaw.com/law-library/jurisdiction-in-cyberspace.html (accessed August 14, 2013).

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 engender trust in the longer run. 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 international and national legislations.[69]
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 human level.[70] Yet, it is not entirely impossible to investigate cyber-attacks forensically and assign responsibility.[71] 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.

India and Pakistan Information Space CBMs

Given their vast experience in negotiating and practicing CBMs India and Pakistan can find areas of building trust in the information space as well. Following are some of the recommended CBMs:

1. **Bilateral Agreements.** Pakistan and India can choose from a

---

[69] CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, *GAO-13-187*, February 2013, http://www.gao.gov/assets/660/652170.pdf (accessed April 25, 2013).

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

[71] "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).

host of bilateral agreements on cyber security, some of which are fairly benign.

- **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 like online theft. Social issues like child pornography and human trafficking already find mention in law manuals.[72] 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.[73] 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.[74] The two countries can expand on the existing statutes and develop laws to curb this nefarious activity, involving regional and international rings.
- **Agreement on Not to Attack Essential Services:** Drawing inspiration from 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 contain-

[72] 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).

[73] 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).

[74] 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).

ing dangerous forces, namely dams, dykes, and nuclear electrical generating stations, as well as installations located in their vicinity.[75] 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 exclusive zone.[76]

- **Agreement on Not to Target 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 regard to 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.[77]
- **Agreement to Refrain from Hostile Propaganda:** Social media has made spreading of rumors and fanning hatred much easier than the 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 per-

[75] Schmitt, *Tallinn Manual*, 223.

[76] Ibid, 199.

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

ception management by media can aggravate an already tense situation.[78] 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 cessation of hostile propaganda through radio broadcasts. This agreement came into force on October 21, 1974.[79] Although this was never followed in letter and spirit, the concept can be extended to the social media, to avoid toxic fallouts from instances like a potentially damaging video clip going viral.

2. **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 bilateral level or within the framework of regional organizations like SAARC or SCO. Both countries are members of SAARC and have observer status in SCO. Whereas, SAARC has become a moribund organization, a victim of irreconcilable issues between India and Pakistan, SCO is 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 therefore worth exploring.
3. **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 Intepol, Europol and Aseanapol can be put on the menu of information space CMBs.
4. **Training:** There is a lot of scope in building trust by sharing

[78] 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).

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

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.[80] Mutual exchange of IT students for fellowships or regular degrees can be another way of reducing mistrust.

5. **Information Space Hotline:** Hotlines between the national computer emergency response centers will enhance not only 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.

[80] 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).

Chapter 5

THE WAY FORWARD

It has been suggested in this book that before formal laws governing cyber activities are formalized, information space CBMs should be considered. According to UN policy guidelines, the ultimate goal of CBMs is to strengthen international peace and security.[1] 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.[2] Imaginative CBMs can precede complex negotiations on treaty agreements and long-winded ratification procedures. Sometimes, CBMs can be installed even 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 deep feelings of distrust and highly secret cyber military applications. Wide disparities of views among states, insufficient research on important regulatory issues and lack of 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 are 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 part

---

[1] 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).

[2] 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.

of India or Pakistan to broach the subject of cybersecurity. Hence the issue of collaborating or building cyber CBMs is nowhere on the horizon. Once the governments recognize that there is a need to include cyber-security on the negotiation agenda, the process will start and then problems of structure and content will crop up. 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.[3] 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."[4] 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.[5] The political implications and acceptance potential of any of these op-

---

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

[4] *International Strategy for Cyberspace*, 8.

[5] 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).

tions have to be weighed carefully, and international experts could be invited to provide their inputs.

ROADMAP FOR INDIA-PAKISTAN INFORMATION SPACE CBMs

Preliminary Issues

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 disastrous for any meaningful dialogue in South Asia and hence should be avoided. The following roadmap is suggested:

Phase I (Informal Contacts and Capacity Building)

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 its presence both in India and Pakistan. In Pakistan IEEE sections are located in Islamabad, Lahore and Karachi.[6] Peshawar subsection also appears in the IEEE map. The Islamabad section has a Computer Society Chapter.[7] The IEEE regularly organizes international technical

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

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

conferences through its computer society.[8] A SAARC IEEE could have a meaningful cyber presence in the region.

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. Military College of Signals (MCS), NUST School of Electrical Engineering & Computer Sciences (SEECS),[9] and FAST National University of Computers & Emerging Sciences[10] are two world-class schools of computer sciences in Pakistan with adequate potential to contribute towards developing a common cyber security culture in South Asia.

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,[11] bar associations,[12] police training academies,[13] and judicial academies [14] can provide good forums for cyber capacity

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

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

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

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

[12] "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).

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

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

building. Telecommunication authorities of both countries also need to be trained to handle emergencies like politically motivated unrest through rumor mongering on the social media. So far, the telecom agencies in South Asia namely, the Telecommunication Regulatory Authority of India,[15] and Pakistan Telecommunication Authority (PTA),[16] 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,[17] and banning video sharing and social media sites.[18]

Phase II (Non-Military CBMs)

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.[19]

2. Legal Collaboration to Frame Cyber Laws: Neither Pakistan nor India is a signatory to the CEC. They can accede to this agree-

---

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

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

[17] 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).

[18] "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).

[19] "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).

ment 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.
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.

Phase III (Military Cyber CBMs)

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.
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.
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.

PHASE IV (Cyber Cooperation through Treaties)

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.
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.

CONCLUSION

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 indeed is 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 been synchronized with other issues like national security exceptions, human rights and privacy policies, which need careful study.[20] Since cyberspace is becoming ominous day by day, there is a dire need to institute international and regional measures to create healthy respect for national sovereignty in cyberspace.

CBMs between India and Pakistan have a checkered history. Yet, fortunately 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 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 III efforts will be found helpful. While formulating information space CBMs, multiple fac-

---

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

tors should be kept in mind. First, the process should be kept out of 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 cycle of bilateral animosity. SAARC needs to be resuscitated. It can draw inspiration from ASEAN by constructively keeping a low-key approach to contentious issues.[21] 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 naive 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 critical.

[21] 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).

Table I: List of International and Regional Cyber Security Instruments and Short Names

	ASSOCIATION / YEAR	INSTRUMENT	SHORT NAME
1	AU 2012	Draft Convention on the Establishment of a Legal Framework Conductive to Cyber-security 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 criminalisation 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 Internal Market	EU Directive on e-Commerce
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

Table II: Pakistani Criminal Law Addressing Cybercrime

Legal Instrument/ Implementing Authority	Current Status	Provisions on Cybercrimes
Electronic Transaction Ordinance 2002 *This Ordinance was promulgated to recognize and facilitate documents, records, information, communication and transactions in electronic form, and to provide for the accreditation of certification service providers.*	In force	S.36: Violation of privacy of information; S.37: Damage to Information System

Prevention of Electronic Crimes Ordinance 2009 *This Ordinance was promulgated to prevent electronic crimes and to combat any action directed against the confidentiality, integrity and availability of electronic systems, networks and data as well as the misuse of such systems and data.*	Promulgated in 2007, then in 2008 and finally in 2009. This Ordinance was not translated into a Parliament's sanctioned law and has completed its constitutional time period, hence lapsed.	S.3: Criminal Access; S.4: Criminal Data Access; S.5: Data Damage; S.6: System Damage; S.7: Electronic Fraud; S.8: Electronic Forgery; S.9: Misuse of Electronic System or Electronic Device; S.10: Unauthorized Access to Code; S.11: Misuse of Encryption; S.12: Malicious Code; S.13: Cyber Stalking; S.14: Spamming; S.15: Spoofing; S.16: Unauthorized Interception; S.17: Cyber Terrorism; S.18: Enhanced punishment for offences involving sensitive electronic system; S.21: Offences by Corporate Body.
Payment Systems and Electronic Fund Transfers Act 2007 *This Act was enacted by Parliament to provide regulatory framework for payment systems and electronic funds transfer. Moreover, it was meant to provide standards for protection of the consumer.*	In force	S.58: Cheating by use of Electronic Device

Copyrights Ordinance 1962 This Ordinance was promulgated to consolidate the law relating to copyrights in Pakistan.	In force	**Chapter XIV:** Offences & Penalties **S.66:** Offences of Infringement of copyrights or other rights conferred under this Ordinance. **S.66A:** Penalty for publishing collections or compendiums of work which have been adapted, translated or modified in any manner without the authority of the owner of the copyright; **S.66B:** Penalty for unauthorized reproduction or distribution of counterfeit of copies of sound recording and cinematographic work; **S.66C:** Penalty for exploitation and appropriation of recording or audio-visual work intended for private use; **S.66D:** Penalty for making copies or reproduction in excess of those authorized by the copyright owner or his successors in title 39; **S.66E:** Penalty for unauthorized rental of cinematographic works and computer programs;

Pakistan Telecommunication Reorganization Act 1996 This law was enacted for re-organization of telecommunication system and industry in Pakistan.	In force	S.31: Offences and penalties. (1) Whoever (a) establishes, maintains or operates a telecommunication system or telecommunication service or possesses any wireless telegraphy apparatus or carries on any other activity in contravention of this Act or the rules or regulations made there under, the Wireless Telegraphy Act, 1933 (XV of 1933) or the conditions of a license; (b) knowingly or having reason to believe that any telecommunication system or telecommunication service has been established or is maintained or is being operated in contravention of this Act, transmits or receives any intelligence by means thereof, or performs any service incidental thereto; (c) dishonestly obtains any telecommunication service, with the intent to avoid payment of a charge applicable to the provision of that service; (d) unauthorisedly transmits through a telecommunication system or telecommunication service any intelligence which he knows or has reason to believe to be false, fabricated, indecent or obscene;

National Response Centre for Cyber Crimes	Operating under auspices of Federal Investigation Agency (FIA)	The National Response Centre for Cyber Crimes was established for the following purposes: Enhance the capability of Government of Pakistan and Federal Investigation Agency to effectively prevent growing cyber-crimes. Reporting & Investigation Centre for all types of Cyber Crimes in the country Liaison with all relevant national and international organizations to handle cases against the Cyber Criminals. Provide necessary technical support to all sensitive government organizations to make their critical information resources secure. Carry out regular R & D activities to make the Response Centre as a center of technical excellence. Provide timely information to critical infrastructure owners and government departments about threats, actual attacks and recovery techniques. A role of Computer Emergency Response Team (CERT). To provide on demand state-of-the-art electronic forensic services and cyber investigative to support local police. Build local capability in incident handling and security intelligence.

Monitor global security issues and gather IT security intelligence.
Capacity building to investigate and handle cyber-crime cases.
Investigation and prosecution of cyber criminals and cope with high-tech crimes.
To enforce existing laws to combat computer crime and to protect consumers and Internet users.

INDIAN IT ACT, 2008

Ministry of Law, Justice and Company Affairs (Legislative Department) New Delhi, the 9th June 2000/Jyaistha 19, 1922 (Saka)

The following Act of Parliament received the assent of the President on the 9th June 2000 and is hereby published for general information.

As Amended by Information Technology Amendment Bill 2006 passed in Lok Sabha on Dec 22nd and in Rajya Sabha on Dec 23rd of 2008

An Act to provide legal recognition for the transactions carried our 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 filings of documents with the Government agencies and further to amend the Indian Penal Code, 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.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records, BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

I. PRELIMINARY

1. Short Title, Extent, Commencement and Application

1. This Act may be called the Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008]

P.S: IT (Amendment) Bill 2006 was amended by IT Act Amendment Bill 2008 and in the process, the underlying Act was renamed as IT (Amendment) Act 2008 herein after referred to as ITAA 2008.

2. It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person.
3. It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.[Act notified with effect from October 17, 2000. Amendments vide ITAA-2008 notified with effect from....]
4. (Substituted Vide ITAA-2008) Nothing in this Act shall apply to documents or transactions specified in the First Schedule by way of addition or deletion of entries thereto.
5. (Inserted vide ITAA-2008) Every notification issued under subsection (4) shall be laid before each House of Parliament

2. Definitions

1. In this Act, unless the context otherwise requires,
   a. "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
   b. "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
   c. "Adjudicating Officer" means adjudicating officer appointed under subsection (1) of section 46;
   d. "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;
   e. "Appropriate Government" means as respects any matter.
      i. enumerated in List II of the Seventh Schedule to the Constitution;
      ii. relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government

and in any other case, the Central Government;

f. "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

g. "Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24;

h. "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

(ha) "Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)

i. "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

j. (Substituted vide ITAA-2008) "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-

   i. the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

   ii. terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

k. "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software;

l. "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

m. "Controller" means the Controller of Certifying Authorities appointed under sub-section (7) of section 17;

n. "Cyber Appellate Tribunal" means the Cyber Appellate * Tribunal established under sub-section (1) of section 48 (* "Regulations" omitted)

(na) (Inserted vide ITAA-2008) "Cyber cafe" means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

(nb) (Inserted Vide ITAA 2008) "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

o. "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network. ,.and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

p. "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

q. "Digital Signature Certificate" means a Digital Signature Certificate issued under sub- section (4) of section 35;

r. "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

s. "Electronic Gazette" means official Gazette published in the electronic form;

t. "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta) (Inserted vide ITAA-2006) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

(tb) (Inserted vide ITAA-2006) "Electronic Signature

Certificate" means an Electronic
Signature Certificate issued under section 35 and includes Digital Signature Certificate"

u. "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) "Indian Computer Emergency Response Team" means an agency established under sub-section (1) of section 70 B

v. "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)

w. (Substituted vide ITAA-2008) "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

x. "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

y. "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made there under

z. "License" means a license granted to a Certifying Authority under section 24;

(za) "Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "Prescribed" means prescribed by rules made under this Act;

(zc) "Private Key" means the key of a key pair used to create a digital signature;
(zd) "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
(ze) "Secure System" means computer hardware, software, and procedure that -:

a. are reasonably secure from unauthorized access and misuse;
b. provide a reasonable level of reliability and correct operation;
c. are reasonably suited to performing the intended functions; and
d. adhere to generally accepted security procedures;

(zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;
(zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;
(zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether

a. the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
b. the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

2. Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

II. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (AMENDED VIDE ITAA 2008)

3. Authentication of Electronic Records

1. Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature

2. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

a. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
b. that two electronic records can produce the same hash result using the algorithm.

3. Any person by the use of a public key of the subscriber can verify the electronic record.
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

3A. Electronic Signature (Inserted vide ITAA 2006)

1. Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber nay authenticate any electronic record by such electronic signature or electronic authentication technique which-
   a. is considered reliable ; and
   b. may be specified in the Second Schedule
2. For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-
   a. the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;
   b. the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be,the authenticator and of no other person;
   c. any alteration to the electronic signature made after affixing such signature is detectable
   d. any alteration to the information made after its authentication

by electronic signature is detectable; and

e. it fulfills such other conditions which may be prescribed.

3. The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated
4. The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;

   Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable
5. Every notification issued under sub-section (4) shall be laid before each House of Parliament

III. ELECTRONIC GOVERNANCE

4. Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is

a. rendered or made available in an electronic form; and
b. accessible so as to be usable for a subsequent reference

5. Legal recognition of Electronic Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation

For the purposes of this section, "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person,

mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

6. Use of Electronic Records and Electronic Signature in Government and its agencies

1. Where any law provides for
   a. the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
   b. the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
   c. the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.
2. The appropriate Government may, for the purposes of sub-section (1) by rules, prescribe
   a. the manner and format in which such electronic records shall be filed, created or issued;
   b. the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

6A. Delivery of Services by Service Provider (Inserted vide ITAA-2008)

1. The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

   Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.
2. The appropriate Government may also authorize any service provid-

er authorized under sub- section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

3. Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.
4. The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

Provided that the appropriate Government may specify different scale of service charges for different types of services.

7. Retention of Electronic Records

1. Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
   a. the information contained therein remains accessible so as to be usable for a subsequent reference;
   b. the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
   c. the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

4. Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules. regulation, etc.. in Electronic Gazette.

7A. Audit of Documents etc in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form (ITAA 2008, Standing Committee Recommendation)

8. Publication of Rules, Regulation, etc, in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form

9. Sections 6, 7 and 8 not to Confer Right to insist Document should be accepted in Electronic Form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to Make Rules by Central Government in respect of Electronic Signature (Modified Vide ITAA 2008)

The Central Government may, for the purposes of this Act, by rules, prescribe

a. the type of Electronic Signature;
b. the manner and format in which the Electronic Signature shall be

affixed;

c. the manner or procedure which facilitates identification of the person affixing the Electronic Signature;
d. control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
e. any other matter which is necessary to give legal effect to Electronic Signature.

10A. Validity of contracts formed through electronic means (Inserted by ITAA 2008)

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

IV. ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONIC RECORDS

11. Attribution of Electronic Records

An electronic record shall be attributed to the originator

a. if it was sent by the originator himself;
b. by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
c. by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgement of Receipt (Modified by ITAA 2008)

1. Where the originator has not agreed with stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by
   a. any communication by the addressee, automated or otherwise; or
   b. any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

2. Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
3. Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and Place of Despatch and Receipt of Electronic Record

1. Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
2. Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely –
   a. if the addressee has designated a computer resource for the purpose of receiving electronic records
      i. receipt occurs at the time when the electronic record enters the designated computer resource; or
      ii. if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
   b. if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
3. Save as otherwise agreed between the originator and the addressee,

an electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

4. The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
5. For the purposes of this section –
   a. if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;
   b. if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
   c. "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

V. SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

14. Secure Electronic Record

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure Electronic Signature (Substituted vide ITAA 2008)

An electronic signature shall be deemed to be a secure electronic signature if-

(i) the signature creation data, at the time of affixing signature, was under the exclusive
control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber

16. Security procedures and Practices (Amended vide ITAA 2008)

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices.

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

VI. REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers (Amended Vide ITAA 2008)

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees (Inserted vide ITAA 2008) as it deems fit.
2. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
3. The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
4. The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees (Inserted vide ITAA 2008) shall be such as may be prescribed by the Central Government.
5. The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
6. There shall be a seal of the Office of the Controller.

18. The Controller may perform all or any of the following functions, namely

a. exercising supervision over the activities of the Certifying Authorities;
b. certifying public keys of the Certifying Authorities
c. laying down the standards to be maintained by the Certifying Authorities;
d. specifying the qualifications and experience which employees of the Certifying Authorities should possess;
e. specifying the conditions subject to which the Certifying Authorities shall conduct their business;
f. specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;
g. specifying the form and content of a Electronic Signature Certificate and the key;
h. specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
i. specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
j. facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
k. specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
l. resolving any conflict of interests between the Certifying Authorities and the subscribers;
m. laying down the duties of the Certifying Authorities;
n. maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of Foreign Certifying Authorities

1. Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
2. Where any Certifying Authority is recognized under sub-section

(1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

3. The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. (Omitted vide ITA 2008)

21. License to issue Electronic Signature Certificates

1. Subject to the provisions of sub-section (2), any person may make an application, to the
2. Controller, for a license to issue Electronic Signature Certificates.
3. No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature Certificates as may be prescribed by the Central Government.
4. A license granted under this section shall
   a. be valid for such period as may be prescribed by the Central Government;
   b. not be transferable or heritable;
   c. be subject to such terms and conditions as may be specified by the regulations.

22. Application for License

1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
2. Every application for issue of a license shall be accompanied by-
   a. a certification practice statement;
   b. a statement including the procedures with respect to identification of the applicant;
   c. payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
   d. such other documents, as may be prescribed by the Central Government.

23. Renewal of License

An application for renewal of a license shall be
a. in such form;
b. accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license:

24. Procedure for Grant or Rejection of License

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of License

1. The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has –
   a. made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;
   b. failed to comply with the terms and conditions subject to which the license was granted;
   c. failed to maintain the standards specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;" vide amendment dated September 19, 2002]
   d. contravened any provisions of this Act, rule, regulation or order made there under, revoke the license:

Provided that no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

2. The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

Provided that no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

3. No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

26. Notice of Suspension or Revocation of License

1. Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data-base maintained by him.
2. Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

Provided that the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock

Provided further that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

27. Power to Delegate

The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to Investigate Contraventions

1. The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.
2. The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to Computers and Data

1. Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. (Amended vide ITAA 2008)
2. For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

30. Certifying Authority to follow certain procedures

Every Certifying Authority shall-

a. make use of hardware, software, and procedures that are secure from intrusion and misuse:
b. provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;
c. adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (Amended vide ITAA 2008)
   (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted
   vide ITAA 2008)
   (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)
d. observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

32. Display of License

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

33. Surrender of license

1. Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.
2. Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offense and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure

1. Every Certifying Authority shall disclose in the manner specified by regulations
   a. its Electronic Signature Certificate (Amended vide ITAA 2008)
   b. any certification practice statement relevant thereto;
   c. notice of revocation or suspension of its Certifying Authority certificate, if any; and
   d. any other fact that materially and adversely affects either the reliability of a Electronic Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services
2. Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Electronic Signature Certificate was granted, then, the Certifying Authority shall-
   a. use reasonable efforts to notify any person who is likely to

be affected by that occurrence; or

b. act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

VII. ELECTRONIC SIGNATURE CERTIFICATES

35. Certifying Authority to issue Electronic Signature Certificate

1. Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.
2. Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.
3. Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
4. On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application **Provided** that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate

A Certifying Authority while issuing a Digital Signature Certificate shall certify that

a. it has complied with the provisions of this Act and the rules and regulations made there under;
b. it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
c. the subscriber holds the private key corresponding to the public key,

listed in the Digital Signature Certificate;

(ca) the subscriber holds a private key which is capable of creating a digital signature

(Inserted vide ITAA 2008)

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber (Inserted vide ITAA 2008)

d. the subscriber's public key and private key constitute a functioning key pair;

e. the information contained in the Digital Signature Certificate is accurate; and

f. it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate

1. Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate –
   a. on receipt of a request to that effect from -
      i. the subscriber listed in the Digital Signature Certificate; or
      ii. any person duly authorized to act on behalf of that subscriber;
   b. if it is of opinion that the Digital Signature Certificate should be suspended in public interest
2. A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.
3. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate

1. A Certifying Authority may revoke a Digital Signature Certificate issued by it
   a. where the subscriber or any other person authorized by him makes a request to that effect; or
   b. upon the death of the subscriber; or
   c. upon the dissolution of the firm or winding up of the company

where the subscriber is a firm or a company.

2. Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub- section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that -
   a. a material fact represented in the Digital Signature Certificate is false or has been concealed;
   b. a requirement for issuance of the Digital Signature Certificate was not satisfied;
   c. the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
   d. the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.
3. A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
4. On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of Suspension or Revocation

1. Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
2. Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

VIII

40. Generating Key Pair

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, (*) the subscriber shall generate that [substituted for "the" vide amendment

dated
19/09/2002] key pair by applying the security procedure. [*word "then" deleted vide amendment dated 19/9/2002],

40A. Duties of subscriber of Electronic Signature Certificate

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed. (Inserted Vide ITAA 2008)

41. Acceptance of Digital Signature Certificate.

1. A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -
   a. to one or more persons;
   b. in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
2. By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that -
   a. the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
   b. all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
   c. all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of Private Key

1. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the r public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure. ["to a person not authorized to affix the digital signature of the subscriber". Omitted vide amendment dated 19/09/2002]
2. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

IX. PENALTIES , COMPENSATION AND ADJUDICATION (Amended vide ITAA-2006/8)

43. Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -

a. accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008)
b. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
e. disrupts or causes disruption of any computer, computer system or computer network;
f. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
g. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder,
h. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,
i. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)

Steals, conceals, destroys or alters or causes any person to steal,

conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (Inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Explanation - for the purposes of this section -

i. "Computer Contaminant" means any set of computer instructions that are designed -
   a. to modify, destroy, record, transmit data or programme residing within a
   b. computer, computer system or computer network; or by any means to usurp the normal operation of the computer, computer system, or computer network;

ii. "Computer Database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

iii. "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

iv. "Damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

v. "Computer Source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

43 A. Compensation for failure to protect data (Inserted vide ITAA 2006)

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees,

to the person so affected. (Change vide ITAA 2008)

Explanation: For the purposes of this section

i. "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

ii. "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

iii. "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

44. Penalty for failure to furnish information, return, etc

If any person who is required under this Act or any rules or regulations made thereunder to -

a. furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

b. file any return or furnish any information, books or other documents within the time specified therefor in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

c. maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary Penalty

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided,

shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to Adjudicate

1. For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. (amended vide ITAA2008)

(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore

Provided that the jurisdiction in respect of claim for injury or damage exceeding rupees five croore shall vest with the competent court. (Inserted Vide ITAA 2008)

2. The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.
3. No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.
4. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
5. Every adjudicating officer shall have the powers of a civil court which are conferred on the
6. Cyber Appellate Tribunal under sub-section (2) of section 58, and
   a. all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
   b. shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

c. shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908 (Inserted vide ITAA 2008)

47. Factors to be taken into account by the adjudicating officer

While adjudging the quantum of compensation under this Chapter the adjudicating officer shall have due regard to the following factors, namely -

a. the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
b. the amount of loss caused to any person as a result of the default;
c. the repetitive nature of the default

X. THE CYBER APPELLATE TRIBUNAL (Amended vide ITA-2008)

48. Establishment of Cyber Appellate Tribunal

1. The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.
2. The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008)

1. The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint (Inserted vide ITAA-2008)

   Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted Vide ITAA 2008)
2. The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. (Inserted vide ITAA-2008)

3. Subject to the provisions of this Act-
   a. the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof
   b. a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.
      Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)
   c. the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.
   d. the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction. (Inserted vide ITAA-2008)
4. Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench (Inserted vide ITAA-2008)
5. If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. (Inserted vide ITAA-2008)

50. Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal (Substituted vide ITAA 2006)

1. A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (substituted vide ITAA-2008)
2. The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section, shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.
   Provided that a person shall not be appointed as a Member, un-

less he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years. (Inserted vide ITAA-2008)

3. The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that service for a period of not less than five years.

51. Term of office, conditions of service etc of Chairperson and Members (Substituted vide ITAA 2008)

1. The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty -five years, whichever is earlier. (Inserted vide ITAA 2008)
2. Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member. (Inserted vide ITAA 2008)
3. An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. (Inserted vide ITAA 2008)

52. Salary. allowance and other terms and conditions of service of Chairperson and Member. (Substituted vide ITAA 2008)

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed: (Inserted vide ITAA 2008)

52A. Powers of superintendence, direction, etc (Inserted vide ITAA 2008)

The Chairperson of he Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

52B. Distribution of Business among Benches (Inserted vide ITAA 2008)

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order,distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench

52C. Powers of the Chairperson to transfer cases (Inserted vide ITAA 2008)

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench

52D. Decision by majority (Inserted vide ITAA 2008)

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

53. Filling up of vacancies (Amended vide ITAA 2008)

If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding officer Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal (Amended vide ITAA 2008)

1. The Presiding officer Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:
   Provided that the said Presiding officer Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.
2. The Presiding officer Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.
3. The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding officer Chairperson or Member.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Inserted vide ITAA 2008)

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal (Error in amendment...item 28)

1. The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.
2. The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.
3. The salaries and allowances and other conditions of service of the

officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Regulations Appellate Tribunal

1. Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter
2. No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
3. Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:
   Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.
4. On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against
5. The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.
6. The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and Powers of the Cyber Appellate Tribunal

1. The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.
2. The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vest-

ed in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

a. summoning and enforcing the attendance of any person and examining him on oath;
b. requiring the discovery and production of documents or other electronic records;
c. receiving evidence on affidavits;
d. issuing commissions for the examination of witnesses or documents;
e. reviewing its decisions;
f. dismissing an application for default or deciding it ex parte
g. any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed .to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal Limitation

60. Limitation

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction (Amended vide ITAA 2008)

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Provided that the court may exercise jurisdiction in cases where the

claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter. (Inserted vide ITAA 2006)

62. Appeal to High court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of Contravention

1. (1) Any contravention under this Act [substituted for "Chapter" vide amendment dated 19/09/2002] may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify: Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.
2. Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.
   Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.
3. Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of Penalty or compensation (Amended vide ITAA 2006)

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

XI. OFFENCES

65. Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

66. Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

a. the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
b. the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66 A. Punishment for sending offensive messages through communication service, etc. (Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a commu-

nication device,-

a. any information that is grossly offensive or has menacing character; or
b. any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,
c. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66 B. Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C. Punishment for identity theft. (Inserted Vide ITA 2008)

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E. Punishment for violation of privacy. (Inserted Vide ITA 2008)

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation. For the purposes of this section

a. **transmit** means to electronically send a visual image with the intent that it be viewed by a person or persons;
b. **capture**, with respect to an image, means to videotape, photograph, film or record by any means;
c. **private area** means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
d. **publishes** means reproduction in the printed or electronic form and making it available for public;
e. **under circumstances violating privacy** means circumstances in which a person can have a reasonable expectation that
    i. he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
    ii. any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism

1. Whoever,

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

i. denying or cause the denial of access to any person authorized to access computer resource; or

ii. attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
iii. introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

2. Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

67. Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67 A. Punishment for publishing or transmitting of material containing sexually explicit act,etc. in electronic form (Inserted vide ITAA 2008)

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

i. the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science,literature,art,or learning or other objects of general concern; or
ii. which is kept or used bona fide for religious purposes.

67 B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever,

a. publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
b. creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
c. cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
d. facilitates abusing children online or
e. records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

i. The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
ii. which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67 C. Preservation and Retention of information by intermediaries

1. Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
2. Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

68. Power of Controller to give directions (Amended Vide ITAA 2008)

1. The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any

regulations made there under.

2. Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

69. Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)

1. Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
2. The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed
3. The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -
   a. provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or
   b. intercept or monitor or decrypt the information, as the case may

be; or

c. provide information stored in computer resource.

4. The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

69 A. Power to issue directions for blocking for public access of any information through any computer resource

1. Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
2. The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
3. The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69B. Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

1. The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
2. The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized

under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information.

3. The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
4. Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

i. "Computer Contaminant" shall have the meaning assigned to it in section 43
ii. "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

70. Protected system (Amended Vide ITAA-2008)

1. The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

   Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety. (Substituted vide ITAA-2008)
2. The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)
3. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
4. The Central Government shall prescribe the information security practices and procedures for such protected system. (Inserted vide

ITAA 2008)

70 A. National nodal agency. (Inserted vide ITAA 2008)

1. The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection.
2. The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to protection of Critical Information Infrastructure.
3. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.

70 B. Indian Computer Emergency Response Team to serve as national agency for incident response

1. The Central Government shall, by notification in the Official Gazette, appoint an agency of the government to be called the Indian Computer Emergency Response Team.
2. The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.
3. The salary and allowances and terms and conditions of the Director General and other officers and employees shall be such as may be prescribed.
4. The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security,-
    a. collection, analysis and dissemination of information on cyber incidents
    b. forecast and alerts of cyber security incidents
    c. emergency measures for handling cyber security incidents
    d. Coordination of cyber incidents response activities
    e. issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
    f. such other functions relating to cyber security as may be prescribed

5. The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as may be prescribed.
6. For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person
7. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6) , shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
8. No Court shall take cognizance of any offence under this section, except on a complaint made by an officer authorized in this behalf by the agency referred to in sub-section (1)

71. Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72 A. Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008)

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while provid-

ing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

73. Penalty for publishing electronic Signature Certificate false in certain particulars

1. No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that
   a. the Certifying Authority listed in the certificate has not issued it; or
   b. the subscriber listed in the certificate has not accepted it; or
   c. the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation
2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

75. Act to apply for offence or contraventions committed outside India

1. Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2. For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves

a computer, computer system or computer network located in India.

76. Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

77. Compensation, penalties or confiscation not to interfere with other punishment. (Substituted Vide ITAA-2008)

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77 A. Compounding of Offences

1. A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

   Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

   Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

2. The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

77 B. Offences with three years imprisonment to be cognizable

1. Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

78. Power to investigate offences (Amended Vide ITAA 2008)

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act. (Amended Vide ITAA 2008)

XII. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES (SUBSTITUTED VIDE ITA-2006)

79. Exemption from liability of intermediary in certain cases

1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. (corrected vide ITAA 2008)
2. The provisions of sub-section (1) shall apply if
    a. the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
    b. the intermediary does not-
        i. initiate the transmission,
        ii. select the receiver of the transmission, and
        iii. select or modify the information contained in the transmission
    c. the intermediary observes due diligence while discharging his duties under this Act and also observes such other guide-

lines as the Central Government may prescribe in this behalf (Inserted Vide ITAA 2008)

3. The provisions of sub-section (1) shall not apply if-
   a. the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act (ITAA 2008)
   b. upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

XII A . EXAMINER OF ELECTRONIC EVIDENCE (INSERTED VIDE ITA-2006)

79A. Central Government to notify Examiner of Electronic Evidence

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation:- For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

XIII. MISCELLANEOUS

80. Power of Police Officer and Other Officers to Enter, Search, etc

1. Notwithstanding anything contained in the Code of Criminal Pro-

cedure, 1973, any police officer, not below the rank of a Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

Explanation- For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

2. Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
3. The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section

81. Act to have Overriding effect

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970 (Inserted Vide ITAA 2008)

81-A. Application of the Act to Electronic cheque and Truncated cheque-* (Inserted vide Negotiable Instruments Amendment Act 2002, Effective from 6th Day of February 2003.)

1. The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.
2. Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each

House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

Explanation: For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

82. Chairperson, Members, Officers and Employees to be Public Servants (Amended Vide ITA-2008)

The Chairperson, Members and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be Public Servants within the meaning of section 21 of the Indian Penal Code.

83. Power to Give Direction

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

84. Protection of Action taken in Good Faith

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith
done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

84 A. Modes or methods for encryption (Inserted Vide ITA-2008)

The Central Government may, for secure use of the electronic medium and for promotion of e- governance and e-commerce, prescribe the modes or methods for encryption

84 B. Punishment for abetment of offences (Inserted Vide ITA-2008)

Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84 C. Punishment for attempt to commit offences (Inserted Vide ITA-2008)

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

85. Offences by Companies.

1. Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly: Provided that nothing contained in this sub-section shall render any

such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

2. Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation- For the purposes of this section

i. "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
ii. "Director", in relation to a firm, means a partner in the firm

86. Removal of Difficulties

1. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.
(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules

1. The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely

a. the conditions for considering reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A (Substituted vide ITA- 2008)

(aa) the procedure for ascertaining electronic signature or authentication under sub-section

3. f section 3A(Inserted Vide ITA-2006) (Inserted vide ITAA-2008)

(ab) the manner in which any information or matter may be authenticated by means of electronic signature under section 5. (Inserted vide ITAA-2008)

b. (b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

c. (c) the manner and format in which electronic records shall be filed or issued and the method of payment under sub-section (2) of section 6;

(ca) the manner in which the authorized service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A (Inserted vide ITAA-2008)

d. the matters relating to the type of Electronic Signature, manner and format in which it may be affixed under section 10;

e. the manner of storing and affixing electronic signature creation data under section 15 (substituted vide ITAA-2008)

(ea) the security procedures and practices under section 16 (Inserted vide ITAA-2008)

f. the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers, other officers and employees under section 17; (ITAA 2008)

g. (omitted vide ITAA-2008)

h. the requirements which an applicant must fulfill under sub-section (2) of section 21;

i. the period of validity of license granted under clause (a) of sub-section (3) of section 1;

j. the form in which an application for license may be made under subsection (1) of section 22;

k. the amount of fees payable under clause (c) of sub-section (2) of section 22;

l. such other documents which shall accompany an application for license under clause (d) of sub-section (2) of section 22;

m. the form and the fee for renewal of a license and the fee payable thereof under section 23;

(ma) the form of application and fee for issue of Electronic Signature Certificate under section 35.(Inserted vide ITAA-2008)

n. the amount of late fee payable under the proviso to section 23;

o. the form in which application for issue of a Electronic Signature

Certificate may be made under sub-section (1) of section 35;

(oa) the duties of subscribers under section 40A (Inserted vide ITAA-2008)

(ob) the reasonable security practices and procedures and sensitive personal data or information under section 43A (Inserted vide ITAA-2008)

p. the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

q. the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;

r. the qualification and experience which the adjudicating officer shall possess under sub-section (2) of section 46; (Ed: error in the act item number (vii). Bill mentions correction not in the original section-"Presiding Officer" to be replaced with "Chairman and Members")

s. the salary, allowances and the other terms and conditions of service of the Chairman and Members under section 52; (amended vide ITAA-2008)

t. the procedure for investigation of misbehaviour or incapacity of the Presiding Officer Chairman and Members under subsection (3) of section 54; (Ed: Error: bill mentions corrections to (r) and (s) instead of (s) and (t)

u. the salary and allowances and other conditions, of service of other officers and employees under sub-section (3) of section 56;

v. the form in which appeal may be filed and the fee thereof under subsection (3) of section 57;

w. the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52 A (substituted vide ITAA-2008)

(wa) the information, duration, manner and form of such information to be retained and preserved under section 67 C (ITAA 2008)

x. The Procedures and safeguards for interception, monitoring or decryption under sub- section (2) of section 69 (ITAA 2008)

(xa) the procedure and safeguards for blocking for access by the public under sub-section

(2) of section 69 A. (ITAA 2008)

(xb) the procedure and safeguards for monitoring and collecting traffic data or information under sub-section (3) of

section 69 B (ITAA 2008)

y. the information security practices and procedures for protected system under section 70 (Inserted vide ITAA-2008)

(ya) manner of performing functions and duties of the agency under sub-section (3) of section 70 A (ITAA 2008)

(yb) the officers and employees under sub-section (2) of section 70 (B) (ITAA 2008)

(yc) salaries and allowances and terms and conditions of service of the Director General and other officers and employees under sub-section (3) of section 70 B (ITAA 2008)

(yd) the manner in which the functions and duties of agency shall be performed under sub- section (5) of section 70 B (ITAA 2008)

z. the guidelines to be observed by the intermediaries under sub section (4) (2) of section 79 (Inserted vide ITAA-2008)

(za) the modes or methods for encryption under section 84A (Inserted vide ITAA-2008)

3. Every notification made by the Central Government under sub-section (1) of section 70 (A) and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. (ITAA 2008)

88. Constitution of Advisory Committee

1. The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.
2. The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

3. The Cyber Regulations Advisory Committee shall advise -
   a. the Central Government either generally as regards any rules or for any other purpose connected with this Act;
   b. the Controller in framing the regulations under this Act
4. There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

89. Power of Controller to make Regulations

1. The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act .
2. In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely
   a. the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) [Substituted for (m) vide amendment dated 19/09/2002] of section 18;
   b. the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;
   c. the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;
   d. other standards to be observed by a Certifying. Authority under clause (d) of section 30;
   e. the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;
   f. the particulars of statement which shall accompany an application under sub-section (3) of section 35
   g. the manner by which a subscriber communicates the compromise of private key to the Certifying Authority under sub-section (2) of section 42.
3. Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive- sessions, and if, before the expiry of the session immediately following the session or

the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall there after have effect only in such modified form or be of no effect, as the ease may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

90. Power of State Government to make rules

1. The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely -
   a. the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
   b. for matters specified in sub-section (2) of section 6;
3. Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Omitted vide ITA-2006
92. Omitted vide ITA-2006
93. Omitted vide ITA-2006
94. Omitted vide ITA-2006

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyaistha 19, 1922 (Saka)
The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:

THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 of 2000)

[9th June, 2000] An Act to provide 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.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first year of the Republic of India as follows:

CHAPTER I

1. PRELIMINARY

Short title, extent, commencement and application

1. This Act may be called the IT Act, 2000.
2. It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.
3. It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.
4. Nothing in this Act shall apply to
   a. a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
   b. a power-of-attorney as defined in section 1A of the Powers-of-

Attorney Act, 1882;

c. a trust as defined in section 3 of the Indian Trusts Act, 1882;
d. a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
e. any contract for the sale or conveyance of immovable property or any interest in such property;
f. any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2. Definitions

(1) In this Act, unless the context otherwise requires, —

a. "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
b. "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;
c. "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;
d. "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
e. "appropriate Government" means as respects any matter,—
    i. Enumerated in List II of the Seventh Schedule to the Constitution;
    ii. relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
f. "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
g. "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;
h. "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;
i. "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logi-

cal, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

j. "computer network" means the interconnection of one or more computers through (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

k. "computer resource" means computer, computer system, computer network, data,computer data base or software;

l. "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

m. "Controller" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

n. "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

o. "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

p. "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

q. "Digital Signature Certificate" means a Digital Signature Certificate issued under sub- section (4) of section 35;

r. "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

s. "Electronic Gazette" means the Official Gazette published in the electronic form;

t. "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

u. "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

v. "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

w. "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

x. "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

y. "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye- laws and orders issued or made thereunder;

z. "licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that (a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation; (c) are reasonably suited to performing the intended functions; and (d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section

16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

DIGITAL SIGNATURE

3. Authentication of electronic records

1. Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
2. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

   Explanation. For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

   a. to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

b. that two electronic records can produce the same hash result using the algorithm.

3. Any person by the use of a public key of the subscriber can verify the electronic record.
4. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III

ELECTRONIC GOVERNANCE

4. Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is
(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference.

5. Legal Recognition of Digital Signatures

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation. For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies

1. Where any law provides for
   a. the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by

the appropriate Government in a particular manner;

b. the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

c. the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1) by rules, prescribe

   a. the manner and format in which such electronic records shall be filed, created or issued;

   b. the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

7. Retention of electronic records

1. Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if

   a. the information contained therein remains accessible so as to be usable for a subsequent reference;

   b. the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

   c. the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

      Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

2. Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette

Where any law provides that any rule, regulation, order, bye-law, notifi-

cation or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6,7 and 8 not to confer right to insist document should be accepted in electronic form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature

The Central Government may, for the purposes of this Act, by rules, prescribe

a. the type of digital signature;
b. the manner and format in which the digital signature shall be affixed;
c. the manner or procedure which facilitates identification of the person affixing the digital signature;
d. control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
e. any other matter which is necessary to give legal effect to digital signatures.

CHAPTER IV

ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records

An electronic record shall be attributed to the originator

a. if it was sent by the originator himself;
b. by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
c. by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt

1. Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by
   a. any communication by the addressee, automated or otherwise; or
   b. any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
2. Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
3. Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record

1. Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
2. Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :
   a. if the addressee has designated a computer resource for the purpose of receiving electronic records,
      i. receipt occurs at the time when the electronic, record enters the designated computer resource; or
      ii. if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
   b. if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
3. Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
4. The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
5. For the purposes of this section,
   a. if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
   b. if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
   c. "usual place of residence", in relation to a body corporate, means the place where it is registered.

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

14. Secure electronic record

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was

a. unique to the subscriber affixing it;
b. capable of identifying such subscriber;
c. created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including—

a. the nature of the transaction;
b. the level of sophistication of the parties with reference to their technological capacity;
c. the volume of similar transactions engaged in by other parties;
d. the availability of alternatives offered to but rejected by any party;
e. the cost of alternative procedures; and
f. the procedures in general use for similar types of transactions or communications.

CHAPTER VI

REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers

1. The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
2. The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
3. The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
4. The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
5. The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
6. There shall be a seal of the Office of the Controller.

18. Functions of Controller

The Controller may perform all or any of the following functions, namely:

a. exercising supervision over the activities of the Certifying Authorities;
b. certifying public keys of the Certifying Authorities;
c. laying down the standards to be maintained by the Certifying Authorities;
d. (pecifying the qualifications and experience which employees of the Certifying Authorities should possess;
e. specifying the conditions subject to which the Certifying Authorities shall conduct their business;
f. specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital

Signature Certificate and the public key;

g. specifying the form and content of a Digital Signature Certificate and the key,
h. specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
i. specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
j. facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
k. specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
l. resolving any conflict of interests between the Certifying Authorities and the subscribers;
m. laying down the duties of the Certifying Authorities;
n. maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities

1. Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
2. Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
3. The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub- section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository

1. The Controller shall be the repository of all Digital Signature Certificates issued under this Act.
2. The Controller shall

a. make use of hardware, software and procedures that are secure .iJm intrusion and misuse;
b. observe such other standards as may be prescribed by the Central Government,to ensure that the secrecy and security of the digital signatures are assured.

3. The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

21. Licence to issue Digital Signature Certificates

1. Subject to the provisions of sub-section (2), any person may make an application, to the
2. Controller, for a licence to issue Digital Signature Certificates.
   No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government
3. A licence granted under this section shall
   a. be valid for such period as may be prescribed by the Central Government;
   b. not be transferable or heritable;
   c. be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence

1. Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.
2. Every application for issue of a licence shall be accompanied by—
   a. a certification practice statement;
   b. a statement including the procedures with respect to identification of the applicant;
   c. payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
   d. such other documents, as may be prescribed by the Central Government.

23. Renewal of licence

An application for renewal of a licence shall be (a) in such form; (b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of licence

1. The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,
   a. made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
   b. failed to comply with the terms and conditions subject to which the licence was granted;
   c. failed to maintain the standards specified under clause (b) of sub-section (2) of section 20;
   d. contravened any provisions of this Act, rule, regulation or order made thereunder,revoke the licence:
   Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.
2. The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him:
   Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.
3. No Certifying Authority whose licence has been suspended shall is-

sue any Digital Signature Certificate during such suspension.

26. Notice of suspension or revocation of licence

1. Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.
2. Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories: Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

   Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions

1. The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.
2. The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data

1. Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching

or causing a search to be made for obtaining any information or data contained in or available to such computer system.

2. For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures

Every Certifying Authority shall,

a. make use of hardware, software and procedures that are secure from intrusion and misuse;
b. provide a reasonable level of reliability in its services which are reasonably suited to the
c. performance of intended functions;
d. adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
e. observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of Licence

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of Licence

1. Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.
2. Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment

which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure

1. Every Certifying Authority shall disclose in the manner specified by regulations
   a. its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
   b. any certification practice statement relevant thereto;
   c. notice of the revocation or suspension of its Certifying Authority certificate, if any; and
   d. any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.
2. Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall
   a. use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
   b. act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII

DIGITAL SIGNATURE CERTIFICATES

35. Certifying Authority to issue Digital Signature Certificate

1. Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government
2. Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:
   Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.

3. Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
4. On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

   Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that

   a. the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
   b. the applicant holds a private key, which is capable of creating a digital signature;
   c. the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

      Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate

A Certifying Authority while issuing a Digital Signature Certificate shall certify that

a. it has complied with the provisions of this Act and the rules and regulations made thereunder,
b. it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
c. the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
d. the subscriber's public key and private key constitute a functioning key pair,
e. the information contained in the Digital Signature Certificate is accurate; and
f. it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate

1. Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,
   a. on receipt of a request to that effect from
      i. the subscriber listed in toe Digital Signature Certificate; or
      ii. any person duly authorised to act on behalf of that subscriber,
   b. if it is of opinion that the Digital Signature Certificate should be suspended in public interest
2. A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.
3. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate

1. A Certifying Authority may revoke a Digital Signature Certificate issued by it
   a. where the subscriber or any other person authorised by him makes a request to that effect; or
   b. upon the death of the subscriber, or
   c. upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
2. Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a CertifyingAuthority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that
   a. a material fact represented in the Digital Signature Certificate is false or has been concealed;
   b. a requirement for issuance of the Digital Signature Certificate was not satisfied;
   c. the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
   d. the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved,

wound-up or otherwise ceased to exist

3. A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
4. On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation

1. Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
2. Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate

1. A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate
   a. to one or more persons;
   b. in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.
2. By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that

a. the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
b. all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
c. all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key

1. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
2. If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation. For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX

PENALTIES AND ADJUD1CATION

43. Penalty for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

a. accesses or secures access to such computer, computer system or computer network;
b. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c. i ntroduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer

network;

d. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
e. disrupts or causes disruption of any computer, computer system or computer network;
f. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
g. provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
h. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation. For the purposes of this section,

i. "computer contaminant" means any set of computer instructions that are designed
    a. (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
    b. (b) by any means to usurp the normal operation of the computer, computer system, or computer network;
ii. "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
iii. "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;
iv. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to

a. furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
b. file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
c. maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate

1. For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer' for holding an inquiry in the manner prescribed by the Central Government.
2. The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or

award such compensation as he thinks fit in accordance with the provisions of that section.

3. No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.
4. Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
5. Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under subsection (2) of section 58, and
   a. all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;
   b. shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

47. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:

a. the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
b. the amount of loss caused to any person as a result of the default;
c. the repetitive nature of the default

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
(2) The Central Government shall also specify, in the notification re-

ferred to in sub- section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he

a. is, or has been or is qualified to be, a Judge of a High Court; or
b. is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with

the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.

1. The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:
   Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.
2. The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.
3. The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal

1. The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit
2. The officers and employees of the Cyber Appellate Tribunal shall

discharge their functions under general superintendence of the Presiding Officer.

3. The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal

1. Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.
2. No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.
3. Every appeal under sub-section (1) shall be filed within a period of tony-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

   Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of tony-five days if it is satisfied that there was sufficient cause tor not filing it within that period.
4. On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.
5. The Cyber Appellate Tribunal shall send a copy of every order made by it to" the parties to the appeal and to the concerned Controller or adjudicating officer.
6. The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal

1. The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at

which it shall have its sittings.

2. The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:
   a. summoning and enforcing the attendance of any person and examining him on oath;
   b. requiring the discovery and production of documents or other electronic records;
   c. receiving evidence on affidavits;
   d. issuing commissions for the examination of witnesses or documents;
   e. reviewing its decisions;
   f. dismissing an application for default or deciding it ex pane;
   g. any other matter which may be prescribed.
3. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or

to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions

1. Any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

   Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.
2. Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

   Explanation. For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.
3. Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with computer system

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:
2. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with

imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

68. Power of Controller to give directions

1. The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.
2. Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a Fine not exceeding two lakh rupees or to both.

69. Directions of Controller to a subscriber to extend facilities to decrypt information

1. If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.
2. The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.
3. The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

70. Protected system

1. The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
2. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified un-

der sub-section (1).

3. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars

1. No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that
    a. the Certifying Authority listed in the certificate has not issued it; or
    b. the subscriber listed in the certificate has not accepted it; or
    c. the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with

both.

74. Publication for fraudulent purpose

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention committed outside India

1. Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
2. For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act. rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments

No penalty imposed or confiscation made under this Act shall prevent

the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. Network service providers not to be liable in certain cases

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation. For the purposes of this section,

a. "network service provider" means an intermediary;
b. "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

CHAPTER XIII

MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.

1. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act

Explanation. For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

2. Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
3. The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have overriding effect

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

82. Controller, Deputy Controller and Assistant Controllers to be public servants

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

83. Power to give directions

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

85. Offences by companies

1. Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

   Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
2. Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

   Explanation. For the purposes of this section,
   i. "company" means any body corporate and includes a firm or other association of individuals; and
   ii. "director", in relation to a firm, means a partner in the firm.

86. Removal of difficulties

1. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

   Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act
2. Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules

1. The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following mailers, namely:
   a. the manner in which any information or matter may be authenticated by means of digital signature under section 5;
   b. the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;
   c. the manner and format in which electronic records shall be filed, or issued and the method of .payment under sub-section (2) of section 6;
   d. the matters relating to the type of digital signature, manner and format in which it may be affixed undersection 10;
   e. the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;
   f. the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;
   g. other standards to be observed by the Controller under clause (b) of sub- section (2) of section 20;
   h. the requirements which an applicant must fulfil under sub-section (2) of section 21;
   i. the period of validity of licence granted under clause (a) of sub-section (3) of section 21;
   j. the form in which an application for licence may be made under sub-section (1) of section 22;
   k. the amount of fees payable under clause (c) of sub-section (2) of section 22;
   l. such other documents which shall accompany an application for licence under clause (a) of sub-section (2) of section 22;
   m. the form and the fee for renewal of a licence and the fee payable there of under section 23;
   n. the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;
   o. the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;
   p. the manner in which the adjudicating officer shall hold inquiry

under subsection (1) of section 46;

q. the qualification and experience which the adjudicating officer shall possess under sub-section (3) of section 46;
r. the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;
s. the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;
t. the salary and allowances and other conditions of service of other officers and employees under sub-section (3} of section 56;
u. the form in which appeal may be filed and the fee thereof under sub -section (3) of section 57;
v. any other power of a civil court required to be prescribed under clause (g) of sub- section (2) of section 58; and
w. any other matter which is required to be, or may be, prescribed.

3. Every notification made by the Central Government under clause (f) of subsection (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee

1. The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.
2. The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.
3. The Cyber Regulations Advisory Committee shall advise
   a. the Central Government either generally as regards any rules or

for any other purpose connected with this Act;

b. the Controller in framing the regulations under this Act.

4. (4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

89. Power of Controller to make regulations

1. The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:
   a. the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (m) of section 18;
   b. the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19;
   c. the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;
   d. other standards to be observed by a Certifying Authority under clause (d) of section 30;
   e. the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;
   f. the particulars of statement which shall accompany an application under sub-section (3) of section 35;
   g. the manner in which the subscriber shall communicate the compromise of private key to the certifying Authority under sub-section (2) of section 42.
3. Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect

only in such modified form or he of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under (hat regulation.

90. Power of State Government to make rules.

1. The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:
    a. the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
    b. for matters specified in sub-section (2) of section 6;
    c. any other matter which is required to be provided by rules by the State Government.
3. Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860.

The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

92. Amendment of Act 1 of 1872.

The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Scheduleto this Act.

93. Amendment of Act 18 of 1891.

The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1834.

The Reserve Bank of India Act, 1934 shall be amended in the manner

specified in the Fourth Schedule to this Act.

THE FIRST SCHEDULE

(See section 91)
AMENDMENTS TO THE INDIAN PENAL CODE
(45 OF 1860)

1. After section 29, the following section shall be inserted, namely:
   Electronic record.
   "29A. The words "electronic record" shall have the meaning assigned to them in clause (t) of sub- section (1) of section 2 of the Information Technology Act, 2000.".
2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.
3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.
4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.
5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.
6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.
7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.
8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.
9. In section 464,(a) for the portion beginning with the words "A per-

son is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely:

"A person is said to make a false document or false electronic record

First - Who dishonestly or fraudulently

a. makes, signs, seals or executes a document or part of a document;
b. makes or transmits any electronic record or part of any electronic record;
c. affixes any digital signature on any electronic record;
d. makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration. " ; (b) after Explanation 2, the following Explanation shall be inserted at the end, namely:

Explanation 3. For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause (d) of subsection (1) of section 2 of the IT Act, 2000.'

10. In section 466,
    a. for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;
    b. the following Explanation shall be inserted at the end, namely:

Explanation. For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of sub- section (1) of section 2 of the Information Technology Act, 2000.'

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.
12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.
13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.
14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.
15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely: —

    "Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code."
16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.
17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

THE SECOND SCHEDULE

1. In section 3, (See section 92)

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872 (1 OF 1872)

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely: 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'.

2. In section 17, for the words "oral or documentary,", the words "oral or

documentary or contained in electronic form" shall be substituted.
2. After section 22, the following section shall be inserted, namely:
When oral admission as to contents of electronic records are relevant.
"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.".

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.
5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.
6. For section 39, the following section shall be substituted, namely:
What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.
"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.".
7. After section 47, the following section shall be inserted, namely:
Opinion as to digital signature where relevant.
47A. When the Court has 10 form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.".
8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.
9. After section 65, the following sections shall be inserted, namely:
Special provisions as to evidence relating to electronic record.
65 A. The contents of electronic records may be proved in accordance with the provisions of section
65B. Admissibility of electronic records.
65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied

in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,

(a) identifying the electronic record containing the statement and de-

scribing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub- section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
(5) For the purposes of this section,
(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
Explanation. For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.
10. After section 67, the following section shall be inserted, namely:
Proof as to digital signature.
67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.
11. After section 73, the following section shall be inserted, namely:
Proof as to verification of digital signature.
73A. In order to ascertain whether a digital signature is that of the person by whom it purports
to have been affixed, the Court may direct
(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
(b) any other person to apply the public key listed in the Digital Signa-

ture Certificate and verify the digital signature purported to have been affixed by that person.

Explanation. For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000'.

12. Presumption as to Gazettes in electronic forms.

After section 81, the following section shall be inserted, namely:

"81 A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. Presumption as to electronic agreements.

After section 85, the following sections shall be inserted, namely:

"85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

Presumption as to electronic records and digital signatures.

85B. (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Presumption as to Digital Signature Certificates.

85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.".

14. Presumption as to electronic messages.

After section 88, the following section shall be inserted, namely:

'88A. The Court may presume that an electronic message forwarded by the originator

through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his

computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.
Explanation.—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.'.
15. Presumption as to electronic records five years old.
After section 90, the following section shall be inserted, namely:
"90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.
Explanation.—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.
This Explanation applies also to section 81A.".
16. For section 131, the following section shall be substituted, namely: —
Production of documents or electronic records which another person, having possession, could refuse to produce.
"131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.".

THE THIRD SCHEDULE

(See section 93)
AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT 891 (18 OF 1891)

1. In section 2
(a) for clause (3), the following clause shall be substituted, namely:
'(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;
(b) for clause (8), the following clause shall be substituted, namely: '(8) "certified copy" means when the books of a bank,

(a) are maintained in written form, a copy of any entry in such books together with a certificate written;:: the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and
(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'.
2. After section 2, the following section shall be inserted, namely:
Conditions in the printout.
"2A. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be
accompanied by the following, namely:
(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and
(b) a certificate by a person in-charge of computer system containing a brief
description of the computer system and the particulars of
(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;
(B) the safeguards adopted to prevent and detect unauthorised change of data;
(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media; devices;
(F} the mode of identification of such data storage devices;
(G) the arrangements for the storage and custody of such storage
(H) the safeguards to prevent and detect any tampering with the system;

and
(I) any other factor which will vouch for the integrity and accuracy of the system.
(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

THE FOURTH SCHEDULE

(See section 94)
AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934 (2 OF 1934)

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause
(p), the following clause shall be inserted, namely:
"(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;".

BIBLIOGRAPHY

Agin, Warren E. "Jurisdictions in Cyberspace." American Bar Association Section of Business Law Cyberspace Law Committee Coping with Personal Jurisdiction in Cyberspace, ABA Subcommittee on Internet Law Liability Report #3. March 26, 2008. http://corporate.findlaw.com/law-library/jurisdiction-in-cyberspace.html.

Agreement between India and Pakistan on Chemical Weapons. *Inventory of International Nonproliferation Organizations and Regimes*. Center for Nonproliferation Studies. http://cns.miis.edu/inventory/pdfs/aptindpakch.pdf.

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.

Agreement between India and Pakistan on Pre-Notification of Flight Testing of Ballistic Missiles. http://www.stimson.org/research-pages/agreement-between-india-and-pakistan-on-pre-notification-of-flight-testing-of-ballistic-missiles/.

Agreement between USA and the USSR 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.

Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security. Yekaterinburg. June 15, 2009. http://www.fmprc.gov.cn/eng/wjdt/2649/t569701.htm.

Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security. 61st Plenary Meeting. Cited by Jason Healey, "The Five Futures of Cyber Conflict and Cooperation."*Georgetown Journal for International Affairs*. http://journal.georgetown.edu/wp-content/uploads/cyber-Healy.pdf.

Agreement between Military Representatives of India and Pakistan Regarding the Establishment of a Ceasefire Line in the State of Jammu and Kashmir (Karachi Agreement).*UN Peace Maker*. http://peacemaker.un.org/indiapakistan-karachiagreement49.

Ahmer, Moonis ed. *Internal and External Dynamics of South Asian Security*. Karachi: Fazleesons. 1997.

Ahmar, Moonis ed. *The Challenges of Confidence Building in South Asia*. New Delhi: Har-Anand Publications. 2001.

Ahsan, S. A. "Current Situation and Issues of Illegal and Harmful Activities in the Field of Information and Communication Technology in Pakistan." Participant's Paper, 140th International Training Course. 2008. http://www.unafei.or.jp/english/pdf/RS_No79/No79 _00All.pdf.

Akuetteh, Teki. Power Point Presentation on Creating the Enabling Environment within the ECOWAS Region.http://meeting.afrinic.net/waigf/presentations/Presentation_%20Ecowas _Teki_Akuetteh/Presentation_

Ecowas_Teki_Akuetteh.pdf.
Aldrich, Richard W. "The International Legal Implications of Information Warfare." *Airpower Journal*. Fall 1996. http://www.au.af.mil/au/awc/awcgate/au/aldrich.pdf.
Alexander, David. "U.S. reserves right to meet cyber attack with force." *Reuters*. November 15, 2011, http://www.reuters.com/article /2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116.
Allen, Kenneth W. "Confidence Building Measures and the People's Liberation Army," in Chien-min Cao and Bruce Dickson eds. *Remaking the Chinese State: Strategies, Society and Security*. London: Routledge. 2001.
Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Burlington MA: El Sevier Inc., 2011.
Annex I to the Agreement between the Governments of the Member States of the SCO on Cooperation in the Field of International Information Security. June 16, 2009.Unofficial translation reproduced in *International Information Security: The Diplomacy of Peace: Compilation of Publications and Documents*. Moscow 2009.
APEC Cybersecurity Strategy. http://itlaw.wikia.com/wiki/APEC_Cybersecurity_Strategy.
APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment. http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/~/media/Files/Groups/TEL/05_TEL_APECStrategy.pdf.
"APT1: Exposing one of China's Cyber Espionage Units." *Mandiant Report*. www.mandiant.com.
Arimatsu, Louise. "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.
ASEAN Cybercrime law. http://www.cybercrimelaw.net/ASEAN.html.
"ASEAN, Japan boost ICT cooperation." *Vietnam*. May 1, 2013. http://en.vietnamplus.vn/Home/ASEAN-Japan-boost-ICT-cooperation/20135/33994.vnplus.
ASEAN - "Joint Media Statement of the 12th ASEAN Telecommunications and IT Ministers Meeting and its Related Meetings with Dialogue Partners." November 19, 2012. http://www.asean.org/news/asean-statement-communiques/item /joint-media-statement-of-the-12th-asean-telecommunications-and-it-ministers-meeting-and-its-related-meetings-with-dialogue-partners.
ASEAN-U.S. Ministerial Meeting: Fact Sheet, Office of the Spokesperson, Washington, DC. July 1, 2013. http://www.state.gov/r/pa/prs/ps/2013/07/211389.htm.
Ashwood, Warwick. "David Cameron pledges UK collaboration with India to fight Cyber Attacks." *ComputerWeekly.com*. February 19, 2013. http://www.computerweekly.com/news /2240178234/David-Cameron-pledges-UK-collaboration-with-India-to-fight-cyber-attacks.

"At UN, Kazakhstan calls for global cybersecurity treaty to deter hackers." *UN News Center*. September 21, 2011. http://www.un.org/apps/news/story.asp?NewsID=39652&Cr=cyber#.UgK8sZI4vwY.

AU – Draft Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. Version 01/01.2011.http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa /events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.

Bagchi, Indrani & Vishwa Mohan. "5 lakh cyber warriors to bolster India's e-defence." *The Times of India*. October 16, 2012.http://articles.timesofindia.indiatimes.com/2012-10-16 /india/34498075_1_cyber-security-cyber-attacks-cyber-warfare.

Bagchi, Indrani. "Government to Roll out New Cybersecurity Architecture." *The Times of India*.
June 13, 2013. http://articles.timesofindia.indiatimes.com/2013-06-13/security/39950586_1_cyber-security-coordinator-cybersecurity-architecture.

Bajpai, Kanti. "CBMs: Contexts, Achievements, Functions." In Dipanker Banerjee ed. *Confidence Building Measures in South Asia*. Colombo: Regional Centre of Strategic Studies. 1999.

Baker, Stewart. "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.

"Bar Council offers to assist in drafting Cyber Laws." *The Strait Times*. January 24, 1997. http://news.google.com/newspapers?nid=1309&dat=19970124&id=rvxOAAAAIBAJ&sjid=PRUEAAAAIBAJ&pg=3656,3382675.

Blount, Ashley. "Topic I: Assessing the current state of cybersecurity and its implications for regional defense and economic interest." *Model Arab League 2012-13*.http://ncusar.org/modelarableague/resources/13-mal-bg-jdc.pdf.

Bobert, W. Earl. "A Survey of Challenges in Attribution." Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy. http://www.nap.edu/catalog /12997.html.

Boland, Julie. "Ten Years of the Shanghai Cooperation Organization: A Lost Decade? A Partner for the U.S.?" *21st Century Defense Initiative at Brookings*. June 20, 2011, 13. http://www.brookings.edu/~/media/research/files/papers/2011/6/shanghai%20cooperation%20organization%20boland/06_shanghai_cooperation_organization_boland.pdf.

Bolton, Jose & Stan Graeve eds. *No Room for Bullies: From the Classroom to Cyber Space*. Nebraska: Boys Town Press. 2005.

Bumiller, Elisabeth. "Pentagon Expanding Cybersecurity Force to Protect Networks against Attacks."*New York Times*. January 27, 2013. http://www.nytimes.com/2013/01/28/us /pentagon-to-beef-up-cybersecurity-force-to-

counter-attacks.html?_r=0.
Bumiller, Elisabeth & Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*. October 11, 2012.http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.
"Calls for incoming government to develop another Cyber Security White Paper."*ABC News*. July 29, 2013. http://www.abc.net.au/worldtoday/content/2013/s3813166.htm?&section =news.
CAMM. http://common-assurance.com/resources/Common-Assurance-Maturity-Model-vision.pdf.
Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA. O'Reilly Media Inc. 2010.
Carr, Jeffrey. "OSCE's Cyber Security Confidence Building Measures Revealed by Anonymous." November 13, 2012. http://jeffreycarr.blogspot.com/2012/11/osces-cyber-security-confidence.html.
Casey-Maslen, Stuart. "Non-kinetic-energy weapons termed 'non-lethal:' A Preliminary Assessment under International Humanitarian Law and International Human Rights Law." October 2010. http://www.geneva-academy.ch/docs/projets/Non-Kinetic-EnergyOctober2010.pdf.
Chabot, Senator Steve. "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.
"Challenges in Cyber Security: Risks, Strategies and Confidence Building." Conference Report German Ministry of Foreign Affairs. December 13 and 14, 2011. Berlin. http://www .auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/Abruestung/Projekte/Cybersicherheit .html.
Choe Sang-Hun. "South Korea blames North for June Cyber Attacks. *New York Times*. July 16, 2013. http://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html?src=recg&gwh=C1CC11FC0E8EA71B45CA3AD0DC6D7098.
Chander, Muktesh. "National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities." Power Point Presentation, http://indiasmartgrid.org/en /Lists/Member/Attachments/19/ISGD%20Plenary%20III%20Muktesh%20Chander%20NCIIPC.pdf.
Chari, P.R., P.I. Cheema & S.P. Cohen. *Four Crises and a Peace Process: American Engagement in South Asia*. Washington DC: The Brookings Institute. 2007.
"China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations."*Ministry of Foreign Affairs People's Republic of China*. September 13, 2011. http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm.
"China, US Agree to Combat Cyber Crime." *Beijing International*. http://www.ebeijing.gov.cn /BeijingInformation/BeijingNewsUpdate/t1138000.htm.
Churchman, David. *Negotiations: Process, Tactics and Theory*. New York:

University Press of America. 1995.
Clarke, Richard A. & Robert K. Knake. *Cyber War: The Next Threat to National Security and what to do about it*. New York: HarperCollins Publishers.2010.
Clarke, Richard A. and Steven Andreasen. "Cyberwar's Threat does not justify a New Policy of Nuclear Deterrence." *Washington Post*. June 14, 2013. http://www.washingtonpost.com /opinions/cyberwars-threat-does-not-justify-a-new-policy-of-nuclear-deterrence/2013/06/14/91c01bb6-d50e-11e2-a73e-826d299ff459_story.html.
Clemente, Dave. "Building Coherence and Understanding Foundational Work." *Chatham House*. ttp://www.unidir.ch/pdf/conferences/pdf-conf1930.pdf.
Collapse of the Agra Summit: The After-Story. *NDTV*. Aired: July 2001. Uploaded May 13, 2013. http://www.ndtv.com/video/player/reality-bites/collapse-of-the-agra-summit-the-after-story-aired-july-2001/274963.
"Cold War Hotline Recalled." *BBC*. http://news.bbc.co.uk/2/hi/europe/2971558.stm.
COMESA - Report of the 30th Meeting of the Council of Ministers: Harnessing Science and Technology for Development. October 2011. http://comesabusinesscouncil.org/attachments /article/29/Annex%20IV;%20COMESA%20COUNCIL%20OF%20MINISTERS%20REPORT-%20October,%202011.pdf .
Commonwealth of Independent States. http://www.cisstat.com/eng/cis.htm.
Comprehensive Study on Cybercrime Draft. February 2013. *UNODC* .http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013 /CYBERCRIME_STUDY_210213.pdf.
Comprehensive National Cybersecurity Initiative (CNCI). *US NSC*. http://www.whitehouse.gov /cybersecurity/comprehensive-national-cybersecurity-initiative.
Comprehensive Study on CBMs. *Department of Political and Security Council Affairs UN Centre for Disarmament Report of the Secretary-General*. 982. http://www.un.org /disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/SS-7.pdf.
Confidence Building. *UNODA*. http://www.un.org/disarmament/convarms/infoCBM/.
Confidence Building Measures. *Stimson Center*. http://www.stimson.org/topics/confidence-building-measures/.
Confidence-Building and Nuclear Risk-Reduction Measures in South Asia. http://www.stimson.org/research-pages/confidence-building-measures-in-south-asia-/.
Connecting Police for a Safer World. *Interpol*. http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.
Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention). *Organisation for the Prohibition of Chemical Weapons* (OPCW).http://www.opcw.org/chemical-weapons-convention/.

Council of Europe Convention on Cybercrime. Budapest. September 23, 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.
Council of Europe Convention on Cybercrimes (CET No 185). http://conventions.coe.int/Treaty /Commun/ChercheSig. asp?NT=185&CM=8&DF=&CL=ENG.
Council of Europe Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (ETS 189). 2003. http:// conventions.coe.int/Treaty/en/Treaties/Html/189.htm.
Council of Europe adopts Internet Governance Strategy. http://www.coe.int/t/ DGHL/cooperation /economiccrime/cybercrime/default_en.asp.
Creegan, Eric. "India Pakistan Sign Missile Notification Pact."*Arms Control Today*. http://www.armscontrol.org/act/2005_11/NOV-IndiaPak.
Crisis Management Plan for Cyber Attacks. *Press Information Bureau (PIB) GoI*. May 6, 2010. http://pib.nic.in/newsite/erelease.aspx?relid=61597.
CSA is a non-profit organization that promotes research into best practices for securing cloud computing and the ability of cloud technologies to secure other forms of computing. https://cloudsecurityalliance.org/.
Cybercrimes/e-crimes: Model Policy Guidelines and Legislative Texts. HIPCAR. http://www.itu.int/ITU-D/projects /ITU_EC_ACP/hipcar/ reports/wg2/docs /HIPCAR_1-5-B_Model-Policy-Guidelines-and-Legislative-Text_Cybercrime.pdf.
"Cyber Crime - A Growing Challenge for the Governments." *Issues Monitor*. July 2011. Vol. 8, KPMG International. http://www.kpmginstitutes.com/ government-institute/insights/2011/pdf /cyber-crime-growing-challenge. pdf.
Cyber-Crime: Pakistan Criminal Records. http://pakistancriminalrecords.com/ tag/cyber-crime/.
Cyber Law of India. http://www.cyberlawsindia.net/.
"Cyber Laws of USA." http://cyberlawsusa.com/.
"Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. National Research Council of the National Academies. Washington D.C. 2010. www.nap.edu.
Cyber Security. *Global Centre for Cyber Security Capacity Building*. http:// www.oxfordmartin.ox.ac.uk /institutes/cybersecurity.
Cyber Security. OAS. http://www.oas.org/en/topics/cyber_security.asp.
"Cyber-Security – TheVexed Question of Global Rules." http://www. stefanomele.it/news /dettaglio.asp?id=285.
Cyber Security Awareness Day Survival Guide and Checklist. *DOE*.http:// energy.gov/cio/downloads/cyber-security-awareness-day-survival-guide-and-checklist.
Cybersecurity Information Exchange (CYBEX), UN *ITU-T X.1205*.4/2011. http://www.ietf.org /mail-archive/web/mile/current/pdfUoI7Qb1eMb.pdf.

"Cybersecurity High on Agenda of Obama-Putin Meeting." *RiaNovosti*.http://en.ria.ru/russia /20130618/181726010/Cybersecurity-High-on-Agenda-of-Obama-Putin-Meeting.html.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented. *GAO-13-187*. February 2013. http://www.gao.gov/assets /660/652170.pdf.

Cyber Security Planning Guide. *DHS*. http://www.dhs.gov/sites/default/files/publications/FCC %20Cybersecurity%20Planning%20Guide_1.pdf.

"Cyber Security."*NSC*. http://www.whitehouse.gov/cybersecurity.

Cyber Space PolicyReview: Assuring a Trusted and Resilient Information and Communications Infrastructure. *White House*. http://www.whitehouse.gov/assets/documents/Cyberspace _Policy_Review_final.pdf

"Cyber Threat Source Descriptions."*Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*. http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

"Cyber War Games in China Raise Concerns in Western Media." http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130611000105&cid=1101.

"DARPA's Foundational CyberWarfare Plan-X: The Roadmap for Future CyberWar." http://cyberarms.wordpress.com/2012/12/01/darpas-foundational-cyberwarfare-plan-x-the-roadmap-for-future-cyberwar/.

Dalton, Toby. *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/.

Davenport, Kelsey. "Hotline Agreements."*Arms Control Association*. November 2012. http://www.armscontrol .org/factsheets/Hotlines.

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX). 21 December 1965.

Defining Malware: FAQ, http://technet.microsoft.com/en-us/library/dd632948.aspx.

Denning, Dorothy E. "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.

"Developing a Framework to Improve Critical Infrastructure Cybersecurity."*National Institute of Standards and Technology (NIST)*. February26, 2013.https://www.federalregister.gov / articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity.

Developments in the Field of Information and Telecommunications in the Context of International Security.*UNODA*. http://www.un.org/disarmament/topics/informationsecurity/.

Delibasis, Dimitrios."State Use of Force in Cyberspace for SelfDefence: A New Challenge for a New Century."*Peace Conflict Development: An*

Interdisciplinary Journal. February 2006.
"Diplomacy: US, China aligned on North Korea, Climate and Cybercrime." *Deutschewelle*. http://www.dw.de/us-china-aligned-on-n-korea-climate-and-cybercrime/a-16868686.
Disarmament and International Security: First Committee.http://www.un.org/en/ga/first/.
Dixit, J.N. *India-Pakistan: In War & Peace*. London: Routledge. 2002.
Draft Russian Convention on Information Security 2011. http://www.mid.ru/bdomp/ns-osndoc .nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc! Open Document.
EC3: A Collective EU Response to Cyber-Crime. https://www.europol.europa.eu/ec3.
Edward, Michael. "India accuses Pakistan of using social media to stir tensions," August 20, 2012, http://www.abc.net.au/am/content/2012/s3571168.htm.
Even, Shmuel 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.
EU – Strengthening Law Enforcement Cooperation: the European Information Exchange Model (EIXM), 7.12.2012, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/police-cooperation/general/docs/20121207_com_2012_735_en.pdf.
European Cybercrime Task Force. http://europol.easyred.com/?p=129.
"5 SMS per day limit comes into effect." *The Times of India*. August 18, 2012. http://articles.timesofindia.indiatimes.com/2012-08-18/telecom/33260957_1_smses-and-mmses-bulk-messages-ban-period.
Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security. *UNODA*. http://www.un.org/disarmament/HomePage/factsheet/iob /Information_Security_Fact_Sheet.pdf.
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.
Farnsworth, Timothy. "China and Russia Submit Cyber Proposal." *Arms Control Association*. http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal.
FAST-NU for Computer and Emerging Sciences. http://nu.edu.pk/.
Federal Judicial Academy, Government of Pakistan. http://www.fja.gov.pk/.
Fedosov, Sergey."What does a Stable Cyber Environment look like?"http://www.unidir.ch/pdf/conferences/pdf-conf1922.pdf.
FIA – Profile of National Response Centre for Cyber Crimes. National Response Centre for Cyber Crime (NR3C). http://www.fia.gov.pk/prj_nr3c.htm.
"FIA swings into action to bust cyber blackmailers." *The News*. February 16, 2012. http://www.thenews.com.pk/Todays-News-7-92964-FIA-swings-

into-action-to-bust-cyber-blackmailers.
Fidler, David P. “Call Me, Maybe: New US-Russia Cybersecurity Initiatives.” *Arms Control Law*. http://armscontrollaw.com/2013/06/21/call-me-maybe-new-us-russia-cybersecurity-initiatives/.
FIRST is the global Forum for Incident Response and Security Teams. http://www.first.org/.
FIRST Members.http://www.first.org/members/teams/cert-in.
“First Facebook, now Pakistan bans YouTube over ‘un-Islamic’ content.” *Mail Online*. May 21, 2010.http://www.dailymail.co.uk/news/article-1279889/YouTube-Facebook-banned-Pakistan.html.
Fischer, Eric A. “Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions.” *CRS*. November 9, 2012. http://www.fas.org/sgp/crs/natsec/R42114.pdf.
“Four held for Cyber Crime.” *Dawn*. May 16, 2005. http://dawn.com/2012/05/16/four-held-for-cyber-crime/.
Fox, Henry. “The Contribution of Capacity Building to Developing Confidence between States in Cyber Space – An Australian Perspective.” *ARF Seminar on Confidence Building Measures in Cyber Space*. September 11-12, 2012. Seoul.aseanregionalforum.asean.org.
Fulghum, David A. “Cyber Attacks no longer Non-Kinetic.” *Aviation Week*. September 28, 2010. http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%253A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%253Acc9234ab-f505-41d5-895a-8580f4bf4222.
Garret Jr, David. “Cyber Attack is imminent, says DHS Secretary Napolitano.” *Examiner.com*. January 25, 2013, http://www.examiner.com/article/cyber-attack-is-imminent-says-dhs-secretary-napolitano.
Gelbstein, Eduardo & Ahmed Kamal. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security*. New York. UN ICT Task Force/UNITAR. 2002. http://www.un.int/kamal/publications/Information_Insecurity_Second _Edition_PDF.pdf.
“Georgia Finalizes Withdrawal from CIS.” *Radio Free Liberty*.August 18, 2009.http://www.rferl.org/content /Georgia_Finalizes_Withdrawal_From_CIS/1802284.html.
Ghosh, Samarjit.“Indo-Pak Composite Dialogue - 2008: Review,” *IPCS Special Report 65*, February 2009, http://ipcs.org/pdf_file/issue/SR65-Samarjit-Final.pdf.
Gill, Amandeep. “What does a stable cyber environment look like?”*UNIDIR Cyber Security Conference*. November 8-9,2012. Geneva. http://www.unidir.ch/pdf/conferences/pdf-conf1921.pdf.
Gjelten, Tom. Extending the Law of War into Cyberspace. *NPR.COM*. September 22, 2010. http://www.npr.org/templates/story/story.php?storyId=130023318.
Gibilisco, Stan. “Computer Security Incident Response Team (CSIRT).” August

2012, http://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT.
"Global Cyber Law Data Base." http://cyberlawsdb.com/main/.
"Global Surveillance Data: US Places Pakistan on Second Position in NSA Spy List." *BBC Record*. http://bbcrecord.com/live/ct-menu-item-17/pakistan/10-pakistan/544-global-surveillance-data-us-places-pakistan-on-second-position-in-nsa-spy-list.html.
Goldman, Jeff. "Taiwan Says China's Cyber Army Now Numbers 100, 000." May 1, 2013. http://www.esecurityplanet.com/hackers/taiwan-says-chinas-cyber-army-now-numbers-100000.html.
Government of India Information Technology Act 2000.http://www.cyberlawsindia.net/itbill2000.pdf.
"Gulshan Rai to be first National Cyber Security Coordinator." *The Indian Express*. May 10 2013. http://www.indianexpress.com/news/gulshan-rai-to-be-first-national-cyber-security-coordinator/1113777/.
Gupta, Arvind. "CBMs in Cyber Space: What should be India's Approach?" *Institute for Defence Studies and Analysis (IDSA)*. June 27, 2012. http://www.idsa.in/idsacomments /CBMsinCyberspace_ArvindGupta_270612.
Gompert, David and Phillip Saunders. "Mutual Restraint in Cyberspace." Fort McNair, Washington DC: National Defense University Press. http://www.ndu.edu/press/paradox-of-power-ch6.html.
Hakeem, Asad and Gurmeet Kanwal with Michael Vannoni and Gaurav Rajen. "Demilitarization of the Siachen Conflict Zone: Concepts for Implementation and Monitoring." *Sandia National Laboratories*. SAND2007-5670.US DOE. 2007.
Hardy, Chris. "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.
Hassan, S. Raza. "Alarming Rise in Cyber Crimes." *Dawn*, July 30, 2012.http://dawn.com/2012/07/30/alarming-rise-in-cyber-crimes/.
Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue& Julia Spiegel. "The Law of Cyber-Attack." *California Law Review*. 2012. LawOfCyberAttack.pdf.
Healy, Jason. "The Future of US Cyber Command."*The National Interest*. July 3, 2013. http://nationalinterest.org/commentary/the-future-us-cyber-command-8688?page=1.
Heinl, Caitríona H. "Enhancing ASEAN-Wide Cybersecurity: Time for a Hub of Excellence? Analysis." July 19, 2013. http://www.eurasiareview.com/19072013-enhancing-asean-wide-cybersecurity-time-for-a-hub-of-excellence-analysis/.
Heimseth, Charles Herman and Surjit Mansingh. *A Diplomatic History of Modern India*. Allied Publishers, 1971.
"Helsinki Final Act." *OSCE*. http://www.osce.org/mc/3950.
Hildreth,Steven A. Cyberwarfare. *Congressional Research Service*. June 19, 2001. http://www.fas.org/irp/crs/RL30735.pdf.

Hilali, A.Z. "Confidence- and Security-Building Measures for India and Pakistan." *Alternatives: Global, Local Political*. Vol. 30. No 2. April 30 2005.

Higgins, Holly. Applying Confidence-Building Measures in a Regional Context. *Research Paper for the Institute for Science and International Security*. http://isis-online.org/uploads /conferences/documents/higginspaper.pdf.

"Hoax call pushed Pakistan to brink of war with India." *Economic Times*. December 6, 2008. http://articles.economictimes.indiatimes.com/2008-12-06/news/28394766_1_india-and-pakistan-mumbai-attacks-mumbai-killings.

Holst, Johan Jørgen and Karen A. Melander. "European Security and Confidence Building Measures. *Survival*. Vol. 19, No. 4. July/August 1977.

Holst, Johan Jørgen. "Confidence Building Measures: A Conceptual Framework." *Survival*.Vol. 25, No. 1. January/February 1983.

"Homeland Security Top Officer to Work on UN's New Global Internet Rules." http://rt.com /usa/cyber-lute-un-internet-572/.

Horn, Leslie. "Dirty Texting Banned By Pakistan Telecom Authority." *PCMag.com*. http://www.pcmag.com /article2/0,2817,2396659,00.asp.

"Hotline between India-Pak home secys soon." *Hindustan Times*. May 13, 2012. http://www.hindustantimes.com/India-news/NewDelhi/Hotline-between-India-Pak-home-secys-soon/Article1-854994.aspx.

Hurwitz, Roger. "Cross-domain threat assessment in international security: the need for cyberstability." Cyber Security Conference 2012: The Role of Confidence Building Measures in Assuring Cyber Stability. *UNIDIR*. Geneva. November 8-9, 2012.http://www.unidir.ch/pdf/conferences/pdf-conf1927.pdf.

ICJ Reports 1949.Corfu Channel Case (UK & Ireland vs. Albania). http://www.icj-cij.org /docketindex.php?p1=3&p2=3&k=cd&case=1.

ICJ Reports 1986.Military and Paramilitary Activities in and Against Nicaragua (Nicaragua vs. US).http://www.icj-cij.org/docket/files/70/6503.pdf.

ICT4Peace Project.http://ict4peace.org/whoweare/ict4peace-history#sthash.2rxeSuHR.dpuf.

IEEE Computer Society.http://www.ieee-security.org/.

"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.

"India links Pakistan to a Terror Cyber Attack." *TACSTRAT*. August 28, 2012. http://tacstrat.com/content/index.php/2012/08/28/india-links-pakistan-to-a-terror-cyber-attack/.

Indian National Cyber Security Policy-2013 (NCSP-2013). File No: 2(35)/2011-CERT-In, Ministry of Communication and Information Technology, Department of Electronics & Information Technology (DEITY) Notification dated July 2, 2013. http://indiacybersecurity.

blogspot.com/.
India Japan to Expand Cyber Security Cooperation. http://news.softpedia.com/news/India-and-Japan-to-Expand-Cyber-Security-Cooperation-301524.shtml.
"India, Pak Coast Guards to set up hotline." *Hindustan Times*. April 28, 2006. http://www.hindustantimes.com/News-Feed/NM9/India-Pak-Coast-Guards-to-set-up-hotline/Article1-91504.aspx.
Indus Waters Treaty.http://siteresources.worldbank.org/INTSOUTHASIA/Resources/223497-1105737253588/IndusWatersTreaty1960.pdf.
"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.
India-Pakistan Military CBMs Project - Phase 1: Final Report. http://www.acus.org/files/Final %20Project%20report%20-%20Phase%201_Sept%2025.pdf.
Information Operations. US JS Joint Publication. November 27, 2012. http://www.dtic.mil /doctrine/new_pubs/jp3_13.pdf.
Ingersoll, Geoffrey. "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.
Institute of Electrical and Electronics Engineers (IEEE). http://www.ieee.org/index.html.
IEEE Computer Society. http://www.ieee-security.org/.
IEEE Karachi Section. http://ewh.ieee.org/r10/karachi.
IEEE Islamabad Section. http://ewh.ieee.org/r10/islamabad/societies.htm.
"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 .
International Conference on Combating Child Pornography on the Internet. Vienna. 29 September - 1 October 1999. http://textus.diplomacy.edu/thina/txGetXDoc.asp?IDconv =3193.
International Electrotechnical Commission (IEC). http://www.iec.ch/index.htm.
International Day against Nuclear Testing: 29 August. http://www.un.org/en/events /againstnucleartestsday/history.shtml.
International Strategy for Cyberspace: Prosperity Security and Openness in a Networked World. The White House. May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer /international_strategy_for_cyberspace.pdf.
Internet Corporation for Assigned Names and Numbers (ICANN). http://www.icann.org/.
Internet Governance Forum (IGF). http://www.intgovforum.org/cms/.
ITU. http://www.itu.int/en/Pages/default.aspx.
ISO/IEC JTC 1 Information Technology.http://www.iso.org/iso/standards_development /technical_committees/list_of_iso_technical_committees/

iso_technical_committee.htm?commid=45020.
"IPSC: PECO Workshop Cybersecurity and Incident Response." *Times Higher Education*. February 13, 2004. http://www.timeshighereducation.co.uk/186633.article.
ISO/IEC 27032:2012 Information technology – Security Techniques – Guidelines for Cybersecurity, http://www.iso.org/iso/catalogue_detail?csnumber=44375.
ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management, http://www.iso27001security.com/html/27002.html.
Jaspal, Zafar Nawaz. "Nuclear CBMs between India and Pakistan: Utilitarian Approach - How to build Confidence about our Nuclear Intentions." *Defence Journal*. Vol.7. No. 10. May 2004. http://www.defencejournal.com/2004-5/gpa.asp.
Jevans, Dave. "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/.
Jones, S.E. "United Nations set to Define New Worldwide Rules for the Internet." November 6, 2012. http://voices.yahoo.com/united-nations-set-define-worldwide-rules-for-11894888.html.
Jus in bello & Jus ad bellum. http://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/index.jsp.
Karl, David J. "India and Pakistan: The Ties that Bind vs. The Line that Divides." *Foreign Policy Association*. February 5, 2013. http://foreignpolicyblogs.com/2013/02/05/india-and-pakistan-the-ties-that-bind-vs-the-line-that-divides/.
Kamal, Ahmed. "The Law of Cyber-Space an Invitation to the Table of Negotiations." Geneva: UNITAR. 2005. www.in.int/kamal/the_law_of_cyber_space.
Kamal, Ahmed. *The Law of Cyber-Space*. New York:UNITAR.2007. http://www.un.int/kamal /thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf.
Kanuck, Sean."Sovereign Discourse on Cyber Conflict under International Law." https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf.
Kaushik, Manu & Pierre Mario Fitter. "Beware of the Bugs." *Business Today*. February 17, 2013. http://businesstoday.intoday.in/story/india-cyber-security-at-risk/1/191786.html.
Khan, Feroz Hassan. "Pakistan's Nuclear Future," in Michael R. Chambers ed., South Asia in 2020: Future Strategic Balances and Alliances. *Strategic Studies Institute*. 2002.
Khan, Feroz Hassan."Prospects for Indian and Pakistani Arms Control and Confidence-Building Measures," *Naval War College Review*. Vol. 63, No. 3.Summer 2010.
Khan, Rafi uz Zaman. Nuclear Risk Reduction Centers. *Stimson Center*.

October 15, 2003.http://www.stimson.org/images/uploads/research-pdfs/rafikhan.pdf.

Khoja, Khurshid."Confidence Building between India and Pakistan: Lessons, Opportunities, and Imperatives."*A Handbook of CBMs for Regional Security*. 3rd Edition. March 1998.

Kizekova, Alica. "The Shanghai Cooperation Organisation: Challenges in Cyberspace." S.Rajaratnam School of International Studies. NTU. February 22, 2012, http://www.rsis.edu.sg/publications/Perspective/RSIS0332012.pdf.

Khartoum Resolution. *CFR*. http://www.cfr.org/world/khartoum-resolution/p14841.

Koh, Harold Hongju. "International Law in Cyber Space." *Harvard International Law Journal*, September 18, 2012. http://www.harvardilj.org/2012/12/online_54_koh/.

Kostadinov, Dmitar. "The Attribution Problem in Cyber Attacks." *Infosec Institute*. February 1, 2013.http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

Kramer, Andrew E. "NSA Leaks Revive Push in Russia to Control Net." *New York Times*. July 14, 2013. http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html?src=recg&gwh=32551918C3F6092B12097F447F3343BB.

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. 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.

Krepon, Michael & Nate Cohn eds. *Crises in South Asia: Trends and Potential Consequences*. Washington DC: Stimson Center. 2011. http://www.stimson.org/images/uploads/research-pdfs/Crises_Complete.pdf.

Kreppon, Michael & PollyNayak. *The Unfinished Crisis: US Crisis Management after the 2008 Mumbai Attacks*. Washington DC: Stimson Center. 2012. http://www.stimson.org/images/uploads/research-pdfs/Mumbai-Final_1.pdf.

Kuehl, Dan. "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.

Kux, Dennis. *India-Pakistan Negotiations: Is Past Still Prologue?* Washington DC.USIP. 2006.

Kwon Haeryong. "The ARF perspective on TCBMs: Future Work." http://www.unidir.ch/pdf/conferences/pdf-conf1912.pdf.

La Franchi, Howard. "US-China Cybersecurity Talks: Will Snowden leaks thwart US Goals?" *Christian Science Monitor*. http://www.csmonitor.com /USA/Foreign-Policy/2013/0709/US-China-cybersecurity-talks-Will-

Snowden-leaks-thwart-US-goals.
Lahore Declaration. USIP Peace Agreements Digital Collection. http://www.usip.org/sites/default/files/file/resources/collections/peace_agreements/ip_lahore19990221.pdf.
Lancaster, John."India, Pakistan to Set Up Hotline: Talks End With Deal to Maintain Moratorium on Nuclear Testing." *Washington Post*. June 21, 2004.http://www.washingtonpost.com/wp-dyn/articles/A55542-2004Jun20.html.
Landau, Emily B. "Assessing the Relevance of Nuclear CBMs to a WMD Arms Control Process in the Middle East Today."*2nd EU Non-Proliferation Consortium in Support of a Process Aimed at Establishing a Zone Free of WMD and Means of Delivery in the Middle East, Brussels*. November 5-6, 2012. http://www.nonproliferation.eu/documents /backgroundpapers/landau.pdf.
Lewis, James Andrew. "Confidence Building Measures and International Agreements in Cyber Security," *Disarmament Forum*, http://unidir.org/pdf/articles/pdf-art3168.pdf.
Lewis, James A. 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 .
Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." http://www.jonrlindsay.com/research/papers.
Lings, Martin. *MUHAMMAD (PBUH): His Life based on the Earliest Sources*. Islamic Texts Society. 1991.
Lodhi, Maleeha. "CBMs need a Bold Approach." *Khaleej Times*. January 14, 2012. http://www.khaleejtimes.com/displayarticle.asp?xfile=data/opinion/2012/January/opinion_January49.xml&section=opinion&col=.
Lodhi, Maleeha. "Pause in the Peace Process." *The News*. March 15, 2013, http://www.thenews.com.pk/Todays-News-9-163510-Pause-in-the-peace-process.
London Conference. *Chatham House*. http://www.chathamhouse.org/research/security/current-projects/london-conference.
Lupovici, Amir. "Cyber Warfare and Deterrence: Trends and Challenges in Research."*Military and Strategic Affairs*. Vol. 3, No. 3. December 2011.
Lvov, Andrei. "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.
Lyon, Peter. *Conflict between India and Pakistan: An Encyclopedia*. Santa Barbara, Cal. ABC-CLIO Inc. 2008.
Mehdudia, Sujay."Congressional committee calls for strong India-U.S. ties on cyber security," *The Hindu*. July30, 2013. http://www.thehindu.com/news/national/congressional-committee-calls-for-strong-indiaus-ties-on-cyber-security/article4970604.ece.
Mahr, Krista. "India-Pakistan Tensions Spike as Two Sides Trade Fire across the Border." *Time World*. August 12, 2013. http://world.time.

com/2013/08/12/ceasefire-violations-continue-along-the-india-pakistan-border/.

Makkar, Sahil. "India, Pakistan yet to establish hotline." October 21, 2011. http://www.livemint.com/Politics/jC9kgXUvCENGbaSYO2iHKL/India-Pakistan-yet-to-establish-hotline.html.

Markoff, John. "Step Taken to End Impasse Over Cybersecurity Talks." *New York Times*. July 16, 2010. http://www.nytimes.com/2010/07/17/world/17cyber.html?_r=1.

Maurer, Tim. "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security." Discussion Paper 2011-11. Cambridge, Mass. Belfer Center for Science and International Affairs. Harvard Kennedy School. September 2011.http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

Mckinnon, Thad & ERM Initiative Faculty. "Cyber Crisis Management – A New Philosophy and Approach to Incident Response." http://www.poole.ncsu.edu/erm/index.php/articles/entry /Cyber-Crisis-Management/.

Melzer, Nils. "Cyber warfare and International Law." *Ideas for Peace and Security*. 2011. pdf-1-92-905-011-L-en.pdf.

Menon, Raja. *A Nuclear Strategy for India*. New Delhi: Sage Publications. 2000.

Miellmonka, Mathias. Cyber CSBMs: Perspective of the German MoD. http://www.unidir.ch/pdf /conferences/pdf-conf1926.pdf.

"Mushahid to Table Cyber Security Bill in Parliament." http://www.mushahidhussain.com/news-detail.php?id=MTE0&pageid=media.

Napolitano, Janet. US DHS Secretary. Written testimony 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.

Nakashima, Ellen. "Bush Order Expands Network Monitoring Intelligence Agencies to Track Intrusions." *Washington Post*. January 26, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261_pf.html·

Nakashima, Ellen. "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.

Nagaraj, Anitha. Global Telecom Treaty 2012 signed in the ITU World Conference.*Center for Information and Communication Science (CICS)*. June 21, 2013 .http://cicsworld.centerforics .org/blog/2013/01/3/global-telecom-treaty-2012-signed-in-the-itu-world-conference/.

National Institute of Standards and Technology (NIST). http://www.nist.gov/index.html.

National Military Strategy for Cyberspace Operations (NMS-CO). *US Joint Staff Publication 2006*. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_

jointOperations/07-F-2105doc1.pdf
National Police Academy, Government of Pakistan. http://www.npa.gov.pk/.
Nelson, Dean. "WikiLeaks: hoax phone call brought India and Pakistan to brink of war." *The Telegraph*. 23 March 2011. http://www.telegraph.co.uk/news/worldnews/wikileaks/8401391 /WikiLeaks-hoax-phone-call-brought-India-and-Pakistan-to-brink-of-war.html.
Network Warfare: Armed Forces and NCW. *Defence and Security of India (DSI)*. http://defencesecurityindia.com /armed-forces-and-ncw/.
Nuclear Risk Reduction Center (NRRC): Confidence Building through Information Exchange. http://www.state.gov /t/avc/nrrc/.
NUST SEECS. http://seecs.nust.edu.pk/.
Organization for the Advanced Structured Information Standards (OASIS). https://www.oasis-open.org/.
"Obama cancels Moscow summit with Putin in showdown over Snowden." *New York Times*. August 7, 2013. http://www.nydailynews.com/news/politics/obama-cancels-moscow-summit -putin-showdown-snowden-article-1.1419848.
"Obama tells intelligence chiefs to draw up cyber target list – full document text: Eighteen-page presidential memo reveals how Barack Obama has ordered intelligence officials to draw up a list of potential overseas targets for US cyber attacks." *The Guardian*. June 7, 2013. http://www.theguardian.com/world/interactive /2013/jun/07/obama-cyber-directive-full-text.
"Obama, Xi Discuss Military-to-Military Relations, Cybersecurity." *US DOD*. http://www.defense.gov/news/newsarticle.aspx?id=120243.
Ocean Telegraphy: The Twenty Fifth Anniversary. New York. March 10, 1879. http://books.google.com/books?id=dGfJTRgzexYC&pg=PA4&lpg=PA4&dq=telegraphy+across+the+oceans&source=bl&ots=xR-CGvtuNp&sig=JagB _PmdIOxnz09fGxH5V429EY0&hl=en&sa=X&ei=G8bRUc2RfqiMigLUq4DYAg&ved =0CGIQ6AEwBw#v=onepage&q=telegraphy%20across%20the%20oceans&f=false.
OECD Seoul Declaration for the Future of the Internet Economy. *OECD Ministerial Meeting on the Future of Internet Economy*. South Korea. June 17-18, 2008. http://www.oecd.org .futureinternet/.
OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetwork stowardsacultureofsecurity.htm.
OECD – Information Economy. http://www.oecd.org/sti/ieconomy/informationeconomy.htm.
OECD – Report of the Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures. April 12, 2006. http://www.oecd.org/internet/consumer/36494147.pdf.
Office of Cybersecurity and Communications. http://www.dhs.gov/office-cybersecurity-and-communications.

"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.

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.

OSCE – A Comprehensive Approach to Cyber Security. http://www.osce.org/event/cyber_sec2011.

OSCE – Resolution on "Overall approach by the OSCE to promote cybersecurity." http://www.oscepa.org/images/stories/documents/activities/1.Annual%20Session/2011_Belgrade/Supplementary.

OSCE –Vienna Document of the Negotiations on Confidence- and Security-Building Measures, 269th Plenary Meeting the OSCE Forum for Security Co-operation. Istanbul. November 16, 1999. http://www.osce.org/fsc/41276.

OSCE - Guide on Non-Military CBMs. Vienna. OSCE Secretariat.2012. http://www.osce.org /cpc/91082.

Owens, William A., Kenneth W. Dam & Herbert S. Lin eds. *Technology, Policy, Law, and Ethics regarding U.S. Acquisition and Use of Cyber Attack Capabilities*. Washington DC: National Academic Press.2009. www.nap.edu.

Parameswaran, Prashanth. "ASEAN at a Crossroads." *The Diplomat*. November 27, 2012. http://thediplomat.com/asean-beat/2012/11/27/asean-at-a-crossroads/.

Padder, Sajad. "The Composite Dialogue between India and Pakistan: Structure, Process and Agency." *Heidelberg Papers inSouth Asian and Comparative Politics*. Vol. 65.February 2012.http://www.ub.uni-heidelberg.de/archiv/13143.

Paganini, Pierluigi. "China vs. US, Cyber Superpowers Compared."*Infosec Institute Resources*.http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/.

"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.

"Pakistan seeks proof of India exodus messages." *BBC News*. August 20, 2012. http://www.bbc.co.uk/news/world-asia-india-19314937.

Pakistan Telecommunication Authority (PTA). http://www.pta.gov.pk/.

"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.

Pavlyuchenkoa, Fyodor/Kenneth Geers tr., "Belarus in the Context of European Cyber Security." http://www.ccdcoe.org/publications/virtualbattlefield/11_PAVLYUCHENKO_Belorussia
.pdf.

Pérez-Peña, Richard. "Universities Face a Rising Barrage of Cyberattacks." *New York Times*. July 16, 2013. http://www.nytimes.com/2013/07/17/

education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=1&_r=0&nl=todaysheadlines&emc=edit _th_20130717.

Perlroth, Nicole. "Hackers in China Attacked The Times for Last 4 Months." *New York Times*. January 30, 2013.http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0.

Perlroth, Nicole & David E. Sanger."Nations Buying as Hackers Sell Flaws in Computer Code." *New York Times*. July 13, 2013. http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?pagewanted=all&_r=0.

Perrow, Charles. *The Next Catastrophe: Reducing our Vulnerabilities to Natural, Industrial, and Terrorist Disaster*. NJ: Princeton University Press. 2007.

Peterson, Andrea. "The Post just got hacked by the Syrian Electronic Army. Here's who they are." *Washington Post*. August 15, 2013. 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/.

Peterson, Scott. "Exclusive: Iran Hijacked US Drone, says Iranian Engineer (video)." *Christian Science Monitor*. December 15, 2011.http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

PKI (Public Key Infrastructure). http://searchsecurity.techtarget.com/definition/PKI.

Pliny Han ed. "Full Text: The Internet in China."*Xinhuanet*. June 8, 2010. http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm.

"Prank Call Fuels Post-Attack Tensions between Pakistan, India." *Fox News*. December 6, 2008. http://www.foxnews.com/story/2008/12/06/prank-call-fuels-post-attack-tensions-between-pakistan-india/.

Popper, Nathaniel & 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.

"Post-26/11, Mukherjee's words rattled Pakistan: Condoleezza Rice." *The Times of India*. October 28, 2011.http://articles.timesofindia.indiatimes.com/2011-10-28/us/30332002 _1_pranab-mukherjee-mumbai-attacks-external-affairs-minister.

Prasad, K. "Cyber-Terrorism: Addressing the Challenges for Establishing an International Legal Framework." *Proceedings of the 3rd Australian Counter Terrorism Conference*. December 2012.o.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act.

PPD 20: US Cyber Operations. http://epic.org/privacy/cybersecurity/presidential-directives /presidential-policy-directive-20.pdf.

Psaki, Jen. "Statement on Consensus Achieved by the UN Group of

Governmental Experts on Cyber Issues," *US Department of State*, June 7, 2013.

Rasmussen, Anders Fogh. "NATO's Next War – in Cyberspace." *The Wall Street Journal.* June 2, 2013. wsj.com.

"Radio Listeners in Panic, Taking War Drama as Fact: Many Flee Homes to Escape 'Gas Raid From Mars' – Phone Calls Swamp Police at Broadcast of Wells Fantasy." *New York Times*. October 31, 1938. http://www.war-of-the-worlds.org/Radio/Newspapers/Oct31/NYT.html.

Ray, John B. "The Resolution of the Rann of Kutch Boundary Problem." *The Geographic Bulletin*.1970. http://www.gammathetaupsilon.org/the-geographical-bulletin/1970s/volume06 /article2.pdf.

Rebello, Maleeva. "Assam violence: Where it all began." September 1, 2012. http://www.dnaindia.com/india/1735111/report-assam-violence-where-it-all-began.

Regional Commonwealth in the Field of Communications, http://www.en.rcc.org.ru/index.php /rcc/about-rcc.

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.

Rice, Condoleezza. *No Higher Honor: A Memoir of My Years in Washington*. New York. Broadway Paperbacks. 2011.

Richardson, Michael. "When Cyber Attacks Could Lead to War." *The Strait Times*. July 1, 2013.http://www.iseas.edu.sg/ISEAS/upload/files/mr1july13.pdf.

Rodriguez, Gabriel. "Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview with the Man who Leaked PRISM." *Politics*. http://www.policymic.com /articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism.

Rome Statute of the International Criminal Court. http://untreaty.un.org/cod/icc/statute/romefra .htm.

Ronald Reagan Quotes. http://thinkexist.com/quotation/information_is_the_oxygen_of_the_modern_age-it/224364.html.

Rouse, Margret. "Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose." http://searchsecurity.techtarget.com/definition /hacktivism.

Rushkof, Douglas. *Cyberia: Life in the Trenches of Cyberspace*. Manchester. Clinamen Press Ltd. 2002.

Salik, Naeem Ahmad. "CBMs –Past, Present and Future." *Pakistan Defence Review*.1998.

Sanger, David E. & 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.
Sanger, David E. "Differences on Cybertheft Complicate China Talks." *New York Times*. July 10, 2013, http://www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html?cid=nlc-dailybrief-daily_news_brief-link3-20130711.
Sanger, David E. "N.S.A. Leaks Make Plan for Cyberdefense Unlikely." *New York Times*. August 12, 3013. http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html?src=recg.
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.
Security in the use of ICTs.http://files.wcitleaks.org/public/WCIT12%20-%20ITRs%20and %20security.pdf.
Security Tip (ST05-007): Risks of File-Sharing Technology.*US-CERT*. February 13, 2013. http://www.us-cert.gov/ncas/tips/ST05-007.
Segal, Adam. "What to read on Cyber Security." *Foreign Affairs.* November 2012. http://www.foreignaffairs.com/features/readinglists/what-to-read-on-cybersecurity#.
Segal, Adam. "Defending an Open, Global, Secure and Resilient Internet." *CFR Independent Task Force Report No. 70*. June 2013. http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836.
"Senate Committee Proposes 7-Point Action Plan for Cyber Secure Pakistan." *Dawn*. July 12, 2013. http://dawn.com/news/1023706/senate-committee-proposes-7-point-action-plan-for-cyber-secure-pakistan/?commentPage=1&storyPage=2.
Sheldon, John B. "Cyber Incident Information Sharing: A First Step towards Confidence Building?" *UNIDIR*. http://www.unidir.ch/pdf/conferences/pdf-conf1929.pdf.
Sarwar, Beena. "LOC Tensions: Need Facts not Hype." January 14, 2013. https://beenasarwar.wordpress.com/2013/01/14/loc-tensions-need-facts-not-hype/.
Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkley Journal of International Law*. 2009. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil.
Shanker, Thom. "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.
Schell, Bernadette H., Miguel Vargas Martin, Patrick C.K. Hung & 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.

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed."*Harvard International Law Journal*. 2012. http://www.harvardilj.org/2012 /online-articles-online_54_schmitt/.

Schmitt ed., Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press: 2013.

SCO – Cooperation on Security. January 22, 2013. http://www.infosco.eu/index.php/aboutsco /activities.

SCO – Declaration of the Heads of the Member States on International Information Security (Non official translation from the Russian Text). June 15, 2006. http://www.fidh.org /Declaration-of-the-Heads-of-the.

SCO Beijing Summit 2012, Official Website, http://www.scosummit2012.org/english/2012-04/28/c_131558560.htm.

SCO official website, http://www.sectsco.org/.

SEA-ME-WE, http://www.seamewe4.com/.

Segal, Adam. "US-China Cyber Hotline." *The Diplomat*. December 1, 2011. http://thediplomat.com/china-power/us-china-cyber-hotline/.

Siddique, Abubakar. "Pakistan Demands Filters Before Lifting YouTube Ban." *Radio Free Europe/Radio Liberty*. June 13, 2013. http://www.rferl.org/content/gandhara-pakistan-youtube-ban/25016243.html.

Simla Agreement July 2, 1972. *MEA GoI*. http://www.mea.gov.in/in-focus-article.htm?19005 /Simla+Agreement +July+2+1972.

Smith, Philip. Network Operations Groups. *Power Point Presentation for RIPE 56*.May 5-9,2008. Berlin. http://meetings.ripe.net/ripe-56/presentations/Smith-Regional_Network _Operations_Groups.pdf.

Simson, Elizbeth. "The U.S.–Russia Cybersecurity Pact: Just Paper." *The Foundry*. June 21, 2013. http://blog.heritage.org/2013/06/21/the-u-s-russia-cyber-pact-just-paper/.

South Asia Confidence-Building Measures (CBM) Timeline. Stimson Center. http://www.stimson.org/data-sets /south-asia-confidence-building-measures-cbm-timeline/.

"South Korea blames North Korea for cyberattack." *Dawn*. July 16, 2013. http://dawn.com/news/1029460/south-korea-blames-north-korea-for-cyberattack.

Standage, Tom. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century On-line Pioneers*. New York: Walker & Company. 2007.

Starr, Barbara. "Drone that crashed in Iran was on CIA recon mission, officials say." *CNN*. December 7, 2011. http://www.cnn.com/2011/12/06/world/meast/us-iran-drone/index.html.

Strategy for Operating in Cyberspace. US DoD. July 2011. http://www.defense.gov/news /d20110714cyber.pdf.

Stojanovski, Dragan. "Preventing a U.S.-China Cyber War." *EastWest Institute*. http://www.ewi.info/preventing-us-china-cyber-war.

Sofaer, Abraham D., 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 .

Sohail, Haseeb. "Information Technology Ministry: A Chaos so far," *The News*. July 29, 2013, http://blogs.thenews.com.pk/blogs/2013/07/information-ministry-a-chaos-so-far/.

Tashkent Declaration. http://peacemaker.un.org/india-pakistan-tashkent-declaration66.

"Taking the Mystery out of Cyberwar." *Washington Post*. http://www.washingtonpost.com /opinions/cyberwar-the-white-house-is-thinking-ahead/2013/06/16/b4a0ab00-d4fa-11e2-a73e-826d299ff459_story.html.

Telecommunication Regulatory Authority of India (TRAI).http://www.trai.gov.in/.

Tikk, Eneken."Ten Rules for Cyber Security." *Survival*. Vol.53, No.3. June-July 2011. http://www.iiss.org/en/publications/survival/sections/2011-2760/survival-global-politics-and-strategy-june-july-2011-bad3/53-3-12-tikk-4349.

The Dutch National Cyber Security Strategy (NCSS) Success through Cooperation 2011. *European Network & Information Security Agency (ENISA)*. http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

"The Law of Armed Conflict – Basic Knowledge." ICRC. http://www.icrc.org/eng /assets/files/other/law1_final.pdf.

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 .

The Netherlands Country Report. May 2011. *ENISA*.http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Netherlands.pdf.

The Sequester. *The White House*. http://www.whitehouse.gov/issues/sequester.

The Swift Codes. http://www.theswiftcodes.com/.

The US State Department: Office of the Coordinator for Cyber Issues. http://www.state.gov/s/cyberissues/.

Thomas, Timothy L. *Cyber Bytes*. Fort Leavenworth: FMSO. 2004.

Thomas, Timothy L. *Cyber Silhouettes: Shadows over Information Operations*. Fort Leavenworth: FMSO. 2005.

Thomas, Timothy L. *Decoding the Virtual Dragon*. Fort Leavenworth: FMSO. 2007.

Thomas, Timothy L. *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force*. Fort Leavenworth, KS: FMSO. 2009.

Touré, Hamadoun I. "The Quest for Cyber Peace."*ITU and PMP on Information Security World Federation of Scientists*. January 2011. http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

"Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar - Report & Recommendations." *World Federation of Scientists Permanent Monitoring Panel (PMP) on Information Security*.

August 2003.http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf.
"Two cyber 'criminals' arrested." *Dawn*. September 13, 2012. http://dawn.com/2012/09/13/two-cyber-criminals-arrested/.
US Army Cyber Command/2nd Army. http://www.arcyber.army.mil/.
US and India Sign Cybersecurity Agreement.*DHS*. July 19, 2011, http://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement.
US Homeland Security: Cyber Laws & Regulations. *DHS*.http://www.dhs.gov/cybersecurity-laws-regulations.
"U.S. Needs to Deal with E.U. Concerns about NSA Spying." *Washington Post*. July 5, 2013. http://articles.washingtonpost.com/2013-07-05/opinions/40390110_1_nsa-national-security-agency-e-u.
UN Development Group. http://www.undg.org/index.cfm?P=13.
UNGA, http://www.nti.org/treaties-and-regimes/united-nations-general-assembly/.
UNGA: Economic and Financial – The Second Committee. http://www.un.org/en/ga/second /index.shtml.
UNGA – Functions and Powers of the General Assembly. http://www.un.org/en/ga/about /background.shtml.
UNGA – Special Report of the Disarmament Commission to the 3rd Special Session devoted to Disarmament. UN Document A/S/-15/3. May 28, 1988. http://www.un.org/ga/search/view_doc.asp?symbol=A/S-15/3(SUPP)&Lang=E.
UNGA –India and Pakistan Statements. September 1998. http://www.acronym.org.uk/spsep98.htm.
UN Document A/60/202.*GGE Report on Developments in the Field of Information and Telecommunication in the Context of International Security*. August 5, 2005. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf ?OpenElement.
UN Document A/65/201. *GGE Report on Developments in the Field of Information and Telecommunications in the Context of International Security*. July 30, 2010. http://www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.
UN Document A/65/154. *Developments in the Field of Information and Telecommunications in the Context of International Security*. July 20, 2010. http://www.un.org/ga/search/view_doc.asp?symbol=A/65/154.
UN Document A/66/152. *Developments in the Field of Information and Telecommunications in the Context of International Security*. July 15, 2011. http://www.un.org/ga/search/view_doc .asp?symbol=A/66/152.
UN Document A/66/152 Add. 1. *Developments in the Field of Information and Telecommunications in the Context of International Security*. September 16, 2011. http://www.un.org/ga/search/view_doc.asp?symbol=A/66/152 / Add.1.

UN Document A/66/359. *International Code of Conduct for Cyber Security*. Letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the UNSG. September 12, 2011. http://cs.brown.edu/courses/csci1800/sources/2012_UN _Russia_and_ China_Code_o _Conduct.pdf.

UN Document A/67/167. *Developments in the Field of Information and Telecommunications in the Context of International Security*. 2012. Reissued for technical reasons on April 8, 2013. http://www.un.org/ga/ search/view_doc.asp?symbol=A/67/167.

UNGA Resolution 2131 (XX). *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*. December 29, 1965. http://www.un-documents.net/a20r2131.htm.

UNGA Resolution 36/103. *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*. December 9, 1981. http:// www.un.org/documents/ga/res/36 /a36r103.htm.

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.

UNGA Resolution 53/70. *Developments in the Field of Information and Telecommunications in the Context of International Security*. January 4, 1999. http://www.un.org/ga/search /view_doc.asp?symbol=A/RES/53/70.

UNGA Resolution 55/28.*Developments in the Field of Information and Telecommunications in the Context of International Security*. November 20, 2000. http://www.un.org/ga/search /view_doc.asp?symbol=A/ RES/55/28&Lang=E.

UNGA Resolution 57/53. *Developments in the Field of Information and Telecommunications in the Context of International Security*. December 30, 2002. http://www.un.org/depts/dhl /resguide/r57.htm.

UNGA Resolution 58/32. *Developments in the Field of Information and Telecommunications in the Context of International Security*. December 8, 2003. http://www.un.org/depts/dhl /resguide/r58.htm.

UNGA Resolution 58/199. *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. January 30, 2004, 2003. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_ resolution_58_199.pdf.

UNGA Resolution 59/6.*Developments in the Field of Information and Telecommunications in the Context of International Security*. December 3, 2004. http://www.un.org/depts/dhl /resguide/r59.htm.

UNGA Resolution 59/61.*Developments in the Field of Information and Telecommunications in the Context of International Security*. December 16, 2004. http://www.un.org/ga/search/view_doc.asp?symbol=A/ RES/59/61&Lang=E.

UNGA Resolution 60/45.*Developments in the Field of Information and Telecommunications in the Context of International Security*. December

8, 2005. Sponsor: Russian Federation. http://www.un.org/disarmament/HomePage/ODAPublications/ResolutionsDecisions/PDF/ResDes2005.pdf.
UNGA Resolution 60/252.*World Summit on the Information Society*. April 27, 2006. http://www.itu.int/wisd/2006/res-60-252.html.
UNGA Resolution 61/54. *Developments in the Field of Information and Telecommunications in the Context of International Security*. December 19, 2006. http://www.un.org/depts/dhl /resguide/r61.htm.
UNGA Resolution 62/17. *Developments in the Field of Information and Telecommunications in the Context of International Security*. January 8, 2008. http://www.un.org/en/ga/62/ resolutions.shtml.
UNGA Resolution 63/37. *Developments in the Field of Information and Telecommunications in the Context of International Security*. January 9, 2009. http://www.un.org/en/ga/63 /resolutions.shtml.
UNGA Resolution 64/25. *Developments in the Field of Information and Telecommunications in the Context of International Security*. January 14, 2010. http://www.un.org/en/ga/64 /resolutions.shtml.
UNGA Resolution64/211.*Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures*. March 17, 2010.http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/64/211.
UNGA 66/24. *Developments in the Field of Information and Telecommunications in the Context of International Security*. December 13, 2011. http://www.un.org/ga/search/view_doc.asp ?symbol=%20A/RES/66/24.
UNIDIR – The Role of CBMs in Assuring Cyber Stability. *Cyber Security Conference 2012 (CS12)*. http://www.unidir.org/files/publications/pdfs/the-role-of-cbms-in-assuring-cyber-stability-en-384.pdf.
UN Military Observer Group in India and Pakistan (UNMOGIP) January 1949 to date and UN India-Pakistan Observation Mission (UNIPOM) September 1965-March 1966.*The Blue Helmets: A Review of the UN Peacekeeping*. New York: UN Department of Public Information. 1996.
Vallone, Robert P., 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.
Vatis, M. A. "The Council of Europe Convention on Cybercrime." *Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. 2010. http://www.nap.edu/catalog/12997.html.
"Violent Protests against Video Rock Pakistan."*Al Jazeera*. September 22, 2012. http://www.aljazeera.com/news/asia/2012/09/20129219618263113.html.
Vignard, Kirstin. Confronting Cyberconflict. *UNIDIR Disarmament Forum*.2011. http://unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.
Virtual Global Task Force, http://www.virtualglobaltaskforce.com/.

Walker, Ben Basely. "Transparency and Confidence Building Measures in Cyber Space: Towards Norms and Behaviors." *Disarmament Forum - Confronting Cyber Conflict*. 4/2011.

Wasim, Amir. "Placing lapsed ordinance in Senate: Law ministry apologises to committee." June 23, 2010. *Dawn*. http://archives.dawn.com/archives/36414.

Waxman, Mathew C. "Cyberattacks and the Use of Force: Back to the Future of Article 2(4)."*Yale Journal of International Law*. Vol. 36.Issue 2. http://www.cfr.org/cybersecurity/cyberattacks-use-force-back-future-article-24/p25251.

Wegener, Henning. "Harnessing the perils in cyberspace: who is in charge?" *UNIDIR DISARMAMENT FORUM*. 3/2007. http://www.unidir.org/files/publications/pdfs/icts-and-international-security-en-332.pdf.

Wegener, Henning. "Regulating Cyber Behaviour: Some Initial Reflections on Codes of Conduct and Confidence-Building Measures." http://www.federationofscientists.org /PlanetaryEmergencies/Seminars/45th/Wegener%20publication.docx.

Westby, Jody R. ed. *International Guide to Cyber Security*. Chicago: American Bar Association. 2004.

What was the UN ICT Task Force? http://www.itu.int/wsis/basic/faqs_answer.asp?lang=en&faq _id=88.

"What we Investigate?" *FBI Albuquerque Division*. http://www.fbi.gov/albuquerque/about-us/what-we-investigate.

"Who rules the Internet? The U.N. agency that oversees phone, radio and satellite communications last week stopped short of fragmenting the Internet into national fiefdoms." *Los Angeles Times*. December 16, 2012. http://articles.latimes.com/2012/dec/16/opinion/la-ed-itu-united-nations-internet-20121216.

Willson, David. "A Global Problem: Cyberspace Threats Demand an International Approach." *ISSA Journal*. August 2009. http://www.issa.org/Library/Journals/2009/August?Wilson-A%20Global%20Problem.pdf.

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

World Summit on the Information Society Geneva 2003. Tunis 2005. http://www.itu.int/wsis/docs/geneva/official/dop.html.

World Federation of Scientists Permanent Monitoring Panel on Information Security. http://www.unibw.de/infosecur/publications/papers_supporting/infosecur/documents/supporting_documents/westby_cyberspace_security_presentation_2003.

Wolter, Detlev. "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. November 8-9, 2012. http://www.unidir.ch/pdf/conferences/pdf-conf1920.pdf.

Yamin, Tughral. "Nuclear Risk Reduction in South Asia." *Journal of*

Contemporary Studies. National Defence University Islamabad. December 2012.

"Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organisation." *Ministry of Foreign Affairs People's Republic of China*. http://www.fmprc .gov.cn/eng/wjdt/2649/t569701.htm.

Yurcik, William. "Information Warfare: Legal and Ethical Challenges of the Next Global Battleground, " *Proceedings of the Second Annual Ethics and Technology Conference*. June 6-7, 1997. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.15.2345.

Yusha, Muhammad. "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/.

Zafar, Kashif. "Cyber-crime: Two arrested for forgery, credit card fraud." *Express Tribune*. September 12, 2012. http://tribune.com.pk/story/435059/cyber-crime-two-arrested-for-forgery-credit-card-fraud/.

Zulfqar, Saman. "Efficacy of Confidence Building Measures (CBMs) in India-Pakistan Relations."*IPRI Journal*. XIII, No. 1.Winter 2013. http://ipripak.org/journal/winter %202013/std2.pdf.

INDEX

A

B

C

D

E

L

M

N

O

P

R

S

T

U

V

W

Y