Chapter 9
Developing Confidence Building Measures (CBMs) in Cyberspace Between Pakistan and India

Tughral Yamin
National University of Sciences and Technology, Pakistan

ABSTRACT

Cyberspace is at once an area of immense cooperation and a no-holds barred arena for competition. Difficulties in creating a stable environment in cyberspace stem from differing national perceptions regarding the freedom of the Internet, application of international law and problems associated with attribution. Information space has no borders and no recognized rules of engagement or internationally accepted regulatory mechanisms. State parties, freelancers, criminals and terrorists all consider cyber operations beyond the pale of international jurisdiction. Some agreements have emerged concerning cybercrime but cyber warfare remains outside binding legal obligations. In the absence of a consensus on treaty obligations, it is a good idea to begin by constructing credible confidence building measures (CBMs) in information space between rival states. The prospects of an unintentional war as a consequence of a cyber-attack can spell disaster for South Asia. This paper discusses a range of CBMs that can be created between India and Pakistan in cyber space to control malicious cyber behavior and avert an inadvertent war. It advocates cyber cooperation instead of cyber warfare.

THE CONCEPT OF INFORMATION WARFARE (IW)

The success of any management system depends on making quick decisions based on the complete and accurate data shared in real timeing. Means of communication have evolved through the ages from such primitive methods like the word of mouth, drumbeats, smoke signals, bugles, messengers, carrier pigeons, and semaphore to the more sophisticated ones such as the modern computer networks.

Information space is the place, where information resides. In the Internet lexicon terms like cyberspace and information space are used interchangeably. For most people cyberspace signifies the world of computer networks. The *Bing Dictionary* describes **cyberspace** as the "imagined place where electronic

DOI: 10.4018/978-1-5225-7912-0.ch009

data goes," or the "the notional realm in which electronic information exists or is exchanged." Others have defined cyberspace as:

The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify, and exchange data using computer networks (Schmitt 2013).

and

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 (Publication 2006).

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. An elaborate system of encryption ranging from simple codes and cyphers to exotic algorithms has been developed to keep the content of the messages secret. However, information vulnerability has become an issue with governments, corporate sector and business houses.

As nations upgrade their net-centric capabilities, they constantly fret about imminent cyber-attacks of 9/11 proportions (Jr 2013). Resultantly they are investing a lot of time, money and effort into developing cyber defenses to protect critical infrastructure like the national command and control (C^2) systems. At the same time technologically advanced countries are enhancing their offensive capabilities to launch cyber-attacks against hostile computer networks. An all pervasive cyber surveillance campaign is in the works. The prospects have become so frightening that countries like Iran, China, Saudi Arabia and Russia are actually working on creating their own Internets (Segal 2013).

Internet is the glue of modern information management system. It holds together governments, defense organizations and financial services. The airlines, maritime industry, railways, the road traffic system are controlled by computer networks. The waterways, logistics services, emergency services, energy management systems, electrical grids and industrial units are operated by SCADA (Supervisory Control & Data Acquisition) type of industrial control system (ICS) (Brodsky 2013). 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 (Rushkof 2002), instead of becoming an area of cooperation has turned out to be the fifth dimension of war fighting (Hardy 2012). The devastating effects of cyber-attacks have significantly altered the landscape of modern warfare (Kuehl). American scholars claim that the first instance of cyber attacks were detected in 1986 (Healy 2013). Ever since then digitally advanced nations are involved in a bitterly intense competition to dominate cyberspace through the 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