23 October 2012

NM3210 (DW1)

NUS
National University
of Singapore

# Responsibility of National Security and the Indian Government: A Case Study on Cyber Terrorism in India

| | |
|---|---|
| U090760W | Lum Wai Seng, Dave Junia |
| U092049J | Berenice Wong |
| A0083391A | Yeo Kai Zhen, Mabel |
| A0084601M | Tan Chien Ying, Jolin |
| A0074057E | Woo Nicholas |

# Contents

## 1. Introduction

Rapid advancements in info-communication technology have created a convenient channel to large resources of information for people. Nonetheless, with such advantages, there would definitely be cases of misuse for the wrong agenda. Cyber terrorism is, and will doubtlessly continue to be a constant issue for governments that must be handled vigilantly for national security. Terrorism has taken on a new structure and it is no longer limited to an attempt to simply create mass destruction with the use of violence. Some have dubbed it as "info-war".

Branding a "cyber attack" as "cybercrime" or "cyber terrorism" is problematic in its difficulty to determine with certainty identity, intent, or the political motivations of an attacker (Karasavin, 2004). Many definitions ended up being too narrow or broad. We argue that the best representation of cyber terrorism would be a combination of various definitional arguments.

Cyber terrorism is "*an attempt either to intimidate the population of a country, or to intimidate a government by intimidating the population* [and] *to create a state of terror in a society, or some psychological state, resembling terror*" (Waldron, 2003) by causing illegal disruption *to "critical infrastructure supporting medical, utility, transportation, and especially financial systems"* that takes place with the help of a computer or cyberspace. (Essaytown, 2012)

To better comprehend what "terrorism" means, let us look at the meaning of terrorism separately. We intentionally left out "politics" and "ideology" for the definition. We argue that there is no need for ideological intents to enter its definition because the line becomes thin when differentiating "terrorists" with "ethical terrorists". A freedom fighter might resort to terroristic methods to obtain his freedom and in this context; it is a pure characterization of the freedom fighter as a terrorist. (Waldron, 2003) Hence, a political intent is not necessarily required to label an act as terroristic.

To further explain, terrorism works by terrorization where “the terrorists terrorize the population in order to intimidate the government into doing something”, most often to coerce the government into giving something in return. (Waldron, 2003) This is not always the case. Secondly, “population” should not be assumed as the primary target audience. Terrorist acts may also involve sending a message to any “enterprise which [they] think of themselves as belonging or to those who claim to speak for them.” (Waldron, 2003)

Thirdly, terrorism need not be part of a coercive strategy to be characterized as terrorism. Waldron (2003) stated that some violence has the intent to “coerce or intimidate” but it is not necessarily the only reason for employing violence. The act of terrorism may simply be to “attract publicity to the cause of those who perpetrate the atrocity, without any ulterior coercive intent.” (Waldron, 2003) There need not be physical violence to occur in order for an act to be classified as terroristic in nature. We then extend this clearly defined parameters of ‘terrorism’ into ‘cyber terrorism’ where acts in accordance to the definition above are carried out or made possible by the use of computer devices and connected networks.

In differentiating cyber terrorism from cybercrime, cybercrime is the purposeful abuse of the information cyberspace that is enabled by or targets computer. According to Wilson (2008), the primary difference between a cyber attack to commit a crime or to commit terror is found in the intent of the attacker and it is highly possible for actions under the two categories to overlap.

Our paper takes a close look at cyber terrorism in India. With a clear definition of cyber terrorism in mind, we first provide a detailed political, infrastructural and social background of India. Four cases of cyber terrorism are then highlighted before the legal system is introduced and evaluated. No law is effective without proper implementation and enforcement. As such, we then study how successful India has been in law enforcement. This is followed by an evaluation of political, social and economic impacts. The paper then ends with a review comprising comparisons and recommendations.

## 2. An Overview of India

### 2.1 Political Relations and Enemies

Political differences between India and Pakistan head a long way back from the time of the British colonies. Disputes over the sovereignty of Kashmir, the area consisting of the north of India’s border and north-eastern Pakistan continues till today. This has led to wars on three occasions, in 1947-1948, 1965 and 1999. The lack of resolution has led to high tensions and hostility between the two countries. Prolonged violence has, at many points, victimized the people of Kashmir. In June 2012, one of the most esteemed Sufi Muslim shrines in Srinagar, Kashmir’s capital was hit by a fire blast. This sparked clashes between angry Muslim protesters and the police (The New York Times, 2012).

The countries also take on each other by means of indirect contact, such as jailing fishermen who unintentionally cross maritime borders (Sharma, 2012). Innocent civilians bear the consequences of hostility and have been taken away from their families. Such harsh consequences are directly caused by long running unresolved disputes that have caused great strain between the neighboring countries.

India and Pakistan seem to be taking steps to remedy relations. This can be seen in the signing of Visa agreements to ease travel between the two places (Masood, 2012). Nonetheless, it is reckoned that such moves are only superficial and the root causes of conflict, which run deep into the history of the two countries, have yet to be resolved.

India and China have also been long entangled in strained political ties. This is due to several factors. Territorial disputes for Tibet have plagued China and India for more than 50 years. China has accused India for suppressing Tibetan autonomy (Lidarev, 2012). Further disputes led to war in 1962. India also houses the Dalai Lama which is seen to undermine the ruling of Tibet. Given that Tibet is part of China, it is clear why the latter is unhappy.

In another territorial dispute between the two Asian giants, China lays claim to the Indian state of Arunachal Pradesh, and New Delhi to the Chinese-controlled Aksai Chin territory. The two countries have military lines drawn at the frontier, taunting each other over military power in the claim for territory (Denyer, 2012).

China's support of Pakistan in the above mentioned land dispute of Kashmir has also led to further detriment in political ties with India.

On the surface, the two countries have been engaging in policies to manage tensions and repair relations by increasing mutually beneficial trade activities (The Economist, 2012). However, their relationship remains highly unstable and may take a turn for the worse anytime so long as the core disputes are not settled.

### 2.2 IT & Physical Infrastructure

The Indian economy is highly reliant on IT infrastructure. However, the rate of India’s development has far outpaced the advancement in IT infrastructure.

India is putting more emphasis on the IT infrastructure in recent years, with the technology sector growing by 10.3 percent from 2011 to reach USD 2.05 billion in 2012 (Daily The Pak Banker, 2012). However, India is still in slow process of moving towards a more efficient model in centralizing its data centres. At the moment, these centres remain distributed and inefficient.

IT infrastructure is not only required in firms and organizations directly related to economic activity. IT is also playing an increasingly important role in households and also in government key sectors such as healthcare and education. However, there is little support and advancement in infrastructure for these segments and other areas of India’s public service.

The Indians are known to be tech savvy, using a vast number of devices while harnessing various forms of technology. However, infrastructural support for its tech savvy citizens is not comprehensive. Poor cabling standards have plagued the country. This is due to a lack of awareness and understanding on industrial standards for networking and cabling (CIOL, 2011).

Security is another grave area of concern. While India's public IT infrastructure sits on varying encryption standards, everyone else in the country has moved on to AES 256 and / or Blowfish 448 *(Broadhurst & Grabosky, 2005).* It is embarrassing that home users now have access to more secure encryption standards than the government. Steganographic software is widely available in the public sphere and such tools have been found to be fully exploited by cyber terrorists. *(Curran, Smyth & McGrory, 2008)*

The speed of India's development has rendered its IT infrastructure old and incompetent. In order to successfully prevent acts of cyber terrorism, India has to first look at its dated hardware and IT policies to better position itself in defense against increasingly sophisticated attacks.

Organizations such as businesses have expressed unhappiness in the lack of infrastructure in the country, as it prevents them from functioning effectively. Existing transportation, IT infrastructure and safety are issues to their operations costs and development in terms of ability to attract qualified people, competitiveness and expandability (KPMG, 2012). As such, they are unable to better use the money to concentrate on technological advancements. These include network security and secure backup systems, leaving them at risk of cyber-attacks. The lack of physical infrastructures simply does not allow concentration of efforts on cyber security.

### 2.3 Social Infrastructure

India has a young population, healthy dependency ratio, robust investments and savings rates. The outlook of growth of India is hence positive, but India still has long term issues to deal with. Some of the challenges include widespread poverty, inadequate physical infrastructure, a lack of non-agricultural jobs, limited access to education, and internal migration from rural to urban areas (Right Vision News, 2012). All these affect the social infrastructure and balance in the country as citizens are limited from further fulfilling their social needs.

Adding to such imbalance, the lack of schools is also one of the reasons for the lack of proper guided exposure to the cyber world. While the government is trying to build more facilities in various areas, they are only concentrating on selected areas which are termed "special economic zones" (SEZs) (The Economic Times, 2008). Inequalities and lack of education have resulted in an uninformed and ill trained citizenship where only a select few understand cybernetics. Thus, ignorance places India’s social fabric in greater danger to cyber terrorism attacks as the population would be easily intimidated by ruses that they do not understand.

## 3. Case Studies

India has been involved in multiple cyber terrorism attacks the past 20 years. We first look into 2 broader cases that encompass continuous pockets of attacks between India and Pakistan before moving to 2 specific high profile examples.

## 3.1 Cyber Warfare - Pakistan and India

Tensions between Pakistan and India run high yearly in August, when both countries celebrate their independence days. During such periods, amateur hackers from both sides of the border try their hands defacing governmental websites.

According to the Times of India (2010), the Pakistanis were the initiators of this cyber warfare after India conducted its nuclear tests in Pokhran in 1998. A group of Pakistani hackers, known as G-Force, successfully broke into the Bhabha Atomic Research Centre and managed to download sensitive information on weapons design. (Times of India, 2010)

In August 2011, Pakistan Cyber Army (PCA) hacked into largest state-owned telecom company in India and gained access to personal data of 10,000 customers. This act was in response to Indian hackers on various Pakistani universities (Pro Pakistani, 2011). More recently in August 2012, the PCA successfully hacked into Indian Railways official website and 89 other “sub-domains related to Railway department”. (Pro Pakistani, 2012)

With its railways already compromised, it will not be long before India and Pakistan are engaged in high-intensity aggression on networks that control the country’s organizational facilities. (Mid Day, 2010)

## 3.2 The Indian Mujahedeen & Lashkar-e-Taiba

The Indian Mujahedeen (IM) has carried out over a dozen high profile attacks, including the 2008 bombings in Jaipur, Bangalore and Delhi, and more recently, the Mumbai serial blasts in 2011. IM’s modulus operandi revolves around publicity and intimidation. Before every attack, IM activists sent out e-mails to various media organizations without fail. (Bhattacharya, 2012)

Police traced e-mails sent by IM from Uttar Pradesh soon after the 2008 Jaipur blast. In an attempt to cover their tracks, IM activists had utilized an unsecured Wi-Fi connection of an American national residing in Mumbai, minutes before the Ahmedabad attack.

After the 2010 Delhi attack, Delhi Police confirmed that the IM had sent a threatening e-mail from the IP address of a computer in Mumbai. Investigations of the 2010 Varanasi blast highlighted the need for scanning wireless networks to detect threat mails posted by IM, allegedly from Mumbai. (Bhattacharya, 2012)

The Lashkar-e-Taiba (LeT) had also attained a significant degree of 'cyber efficiency', and have been making increasing use of voice over internet protocol (VoIP) for communications. LeT's 26/11 'master-mind', Zaki-ur Rehman Lakhvi, who is presently incarcerated in a Pakistan jail, is known to have been working with LeT cadres even from jail, using a private VoIP on his smart phone. Highlighting the problems this creates, an unnamed intelligence source explained that it was tough to gather intelligence because Lashkar men hold audio or video conferences using encrypted private VoIP that officials have difficulty in breaking into. (Bhattacharya, 2012)

In addition, a number of Pakistani hacker groups have openly circulated instructions for attacking Indian computers lowering the barriers of entry to would-be terrorists. (Bhattacharya, 2012)

### 3.3 Taj Mahal Hotel Bombings

On the 26th September 2008, Pakistani terrorists carried out an attack in Taj Mahal Hotel, Mumbai, leaving 165 people and nine gunmen dead. Reports have noted “Pakistan-backed Lashkar-e-Toiba (LeT)” had made extensive use of technology to prepare for the operations. Besides their above-mentioned dependence on Voice-over Internet Protocol (VoIP) software to orchestrate the attack on a real-time basis (India Blooms, 2010), it was observed that most of the 26/11 planning was also planned meticulously with Google Earth. The terrorists made use of "cellular phone networks for command and control, as well as social media to track and thwart the efforts of Indian commandos." (India Blooms, 2010)

More worryingly, the terrorists demonstrated expertise which bore hallmarks of a professional team. They managed to convert audio signals to data before transmission. This made it almost impossible to Indian security forces detect and intercept given their current level of infrastructure and capabilities. (India Blooms, 2010) Furthermore, the live broadcasts of the attacks on television enabled the perpetrators to quickly inform fellow terrorists of the movements of the security forces and provide them with further instructions (India Bloom, 2010). This reflects the vulnerability and datedness of India's IT infrastructure and media policies.

### 3.4 Terror SMSes Drive North Indian Exodus

Migrant workers fled the north eastern states of India following threats from SMSes and various forms of social media. India accused Pakistan of spreading panic via the use of modified images to spread fear within the tensed states. These were originally images of victims of cyclones in Myanmar that were doctored to give an impression that violence in the north eastern states were escalating. India cited 76 Pakistan based websites bearing such images (BBC, 2012).

Offending websites bore Pakistani internet protocol (IP) addresses but could not be directly linked to the state. While such sites that hosted doctored images were traceable, the source of intimidating SMSes proved to be a much greater challenge. India had difficulty verifying the source of mass SMS threats and had to impose an overarching ban on bulk text messages to prevent further intimidation of those in the north eastern states (Zeenews India, 2012). In a country that feverishly believes in the freedom of speech, the use of such measures was a clear sign of desperation.

Added pressure has been placed on the already tense social fabric leading Prime Minister Manmohan Singh to plead rumor mongers to stop fanning the flames citing that the precarious position of India's "communal harmony" (BBC, 2012).

The costs are high. The 30,000 people that fled the cities of Bangalore and Mumbai also signaled a massive drop in productivity and economic output (FT, 2012). Most of those that fled were migrants. The affected region is an important economic hub having been often termed as the Silicon Valley of India. (BBC, 2012).

Despite the massive search for the perpetrators of this cyber attack, only 8 were apprehended in Bangalore (Zeenews India, 2012).

## 4. Current Cybercrime Laws

The attacks mentioned above have continued even under India's legal efforts to effectively criminalize and stamp out such acts of cyber terrorism. We look at current cybercrime laws in order to better understand why cyber terrorism has continued unabated.

### 4.1 General Statutes and Approaches

The Information Technology Act (ITA) 2000 was first implemented by the Indian government to mainly "provide legal infrastructure for electronic commerce in India, and to facilitate electronic filing of documents with Government agencies" (Indian Institute of Banking and Finance [IIBF], n.d.). However, due to criticisms of the lack of legislations in ITA, Information Technology Amendment Act (ITAA) which contains a more holistic set of cybercrime laws such as inclusion of child pornography and cyber terrorism was then passed by the Parliament in 2008 (IIBF, n.d.).

Data theft - one of the most prevalent offences in India is exclusively protected under the new Section 43A of the ITAA, states that “where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected” (IIBF, n.d.). As such, companies in India are now forced to have more stringent security procedures and regular checks on their data protection due to harsher penalties and greater responsibilities being placed on them (Indian prime minister, 2006)

In addition, Information Technology Rules 2011 was implemented for the purposes of tightening cyber security and regulation of cyber content. The Rules generally require Cyber Café network users’ identification to be kept for at least a year and information in the log register to be submitted to the government on a monthly basis (Sinha, 2011). In this way, the government has strict control of information on who has access to which Internet sites, which increases the ease of tracking cyber criminals or cybercrimes if necessary.

## 4.2 Laws Specific to Cyber Terrorism

As mentioned earlier, ITAA covers cyber terrorism. Under Section 66F, it states that “in order to qualify as a cyber terrorist act, the act must be committed with the intention to threaten the unity, integrity, security or sovereignty of India by way of interfering with authorized access to a computer resource, obtaining unauthorized access to a computer resource or damaging a computer network” (IIBF, n.d.). The acts are punishable if they “cause death or injuries to persons or damage to or destruction of property etc” (IIBF, n.d). Cyber terrorism is exclusively being identified as a significant threat to the stability of India’s government and society, as the inclusion of this cybercrime in ITAA was an immediate result of the 2008 Mumbai terrorist attacks.

Prevention of Terrorism Act 2002 extends to cover cyber terrorism. It is an Act “to make provisions for the prevention of and for dealing with, terrorist activities and for matters connected therewith” (Chaturvedi, 2002). Its main features include, “the measures for dealing with terrorist activities, and the definitions of terrorist organizations” (Chaturvedi, 2002). Under this Act, extremist behavior is under strict scrutiny (Halder, n.d.).

The measures taken by the government to fight cyber terrorism include the “coordination of Indian armed forces with other cyber security agencies for crisis management action plan”. The purpose is to facilitate and strategize better responses in times of crisis. The tight coordination of internal army forces with national organizations is a strategic plan used by the government to counter cyber terrorism (PTI news agency, 2010).

### 4.4 Strengths

Firstly, India has been building good relations with other countries such as the United States to tighten its cyber security. Big companies such as Microsoft helped the police forces in tracking cyber crimes by setting up security teams in the country (Perez, 2003). As such, India is able to tap on the expertise of countries with well-established IT infrastructures, and thus acquire knowledge and skills to upgrade and improve its cyber security systems and legal systems.

Secondly, India has been seeking ways to step up its cyber security levels. For instance, dedicated cyber crime police stations have been consecutively set up in selected provinces in India (PTI News Agency, 2009). In addition, the government is to “build National Cyber Coordination Centre, which will detect malicious cyber attacks and issue early warning alerts”

(Kannan, 2012). Thus, it is evident that the government is active in finding ways to counter cybercrime threats.

Lastly, there is strong financial support from the government to improve cyber crime regulations and measures. According to PTI news agency (2007), “the government Friday announced a grant of 35m rupees [one US dollar equals about 40 rupees] to Central Bureau of Investigation (CBI) for enabling the premier investigating agency acquire latest tools to tackle this menace”. Governmental support is crucial in tackling cybercrimes, as security authorities can have greater financial and legal power in strategically deciding of regulations and IT infrastructure pertaining to reduce cyber threats in the country.

### 4.4 Weaknesses

One of the challenges that the government faces is the problem of extraterritorial jurisdiction, where a “state exercises its Jurisdiction beyond its territorial jurisdiction” (“Extra-territorial jurisdiction,” n.d.). The problem arises when convicting one of another country’s origins if he commits a cyber crime that is considered an offence in India. The prosecution of such crimes is difficult due to the absence of international standardization of laws. It is thus necessary for India to reach a common agreement with other countries to better facilitate prosecution.

In addition, proper cooperation of other countries may not occur and this might create a barrier for India to control the crimes in the country. According to PTI News Agency (2011), it is difficult to seek help from other countries as they tend to delay responses and may provide restricted information due to privacy issues. Thus, the lack of extraterritorial jurisdiction control poses a great problem for India as this allows cyber criminals to take advantage of it, and cyber terrorism can take place in the country easily due to the gap in the system.

Another weakness of Indian’s legal system is that “cyber crimes are often under-reported” (PTI news agency, 2007) due to the need to protect selfish interests and reputation by business companies. The reluctance to report cyber crimes is also caused by the belief that governmental agencies are not capable enough to track such activities (PTI news agency, 2007). The cyber crimes not reported result in additional weaknesses of the legal system as the government is incapable to further examine the issues and improve on its policies.

Lastly, the cybercrime laws are not efficient enough to address the problems, as many cyber criminals are able to get away even with the laws in place (Kannan, 2012). This is being fuelled by the affordances of the Internet, which allow Internet users to carry out their activities online with anonymous identities (Kannan, 2012). According to Kannan (2012), a Fraud Investigation and Dispute Services company failed to identify the profile of an Indian cyber fraudster as he used multiple online identities to carry out the activities. Hence, India’s inability to have stricter law enforcements on its citizens may result in more exploitation of the system’s loophole.

## 5. Law Enforcement

Ironically, the laws that are created to solve the problem of cyber terrorism in India are abetting the cyber terrorists themselves to some extent. The abovementioned laws have enabled the government to track and monitor the web traffic: a fact that terrorists, in the 2011 Mumbai bomb blasts for example, also knew. As such, they have worked around that ‘loophole’. As they know that the government will be monitoring suspicious networks of communications, the terrorists have made use of public information to carry out their schemes. For example, they garnered vital information from Twitter posts made by common people that are less likely to be monitored by the government. ‘Public posts about warning people of sensitive areas’, ‘blood donation camps’, ‘information about missing friends and relatives’ are examples of public information used by the terrorists to carry out their attacks. (Halder, 2011) The government, in this case, was unable to charge the criminals. After all, the Twitter posts were made by common citizens.

This legal loophole had made legal enforcement of such laws a lot more difficult. Prosecutors in the Indian courts are unlikely to use such laws in their prosecution of the accused criminals. It would be a waste of time since accused criminals will be able to work their way around such laws by utilizing legal loopholes. As a result, application of the section 69F has been used very sparingly in the course of prosecuting such cyber terrorists (Madaan, 2011), This renders the laws somewhat useless to a certain extent, much to the benefit of cyber criminals.

However, the legal enforcement of laws fighting cyber terrorism has been strengthened through the provisions in the proposed Information Technology guidelines for cyber cafes, 2011. (Madaan, 2011), as mentioned briefly in the preceding section on India's general statutes. Under such provisions, any cyber café in India is empowered to prohibit the use of the computers to any user should they have 'no valid identity card' and if 'the user is a minor without any accompanying adult'. In addition, the cyber cafés are allowed to make a photocopy of users' identities (Halder, 2011). This is vital for combating cyber terrorism. Cyber terrorists know better than to use their private home computers. This is because such private computers have IP addresses that are easily traceable (Halder, 2011). As such, the usage of computers in cyber cafes would prove to be a wise move for them. Law enforcement officials would have to spend additional time tracking down the IP addresses of the computers being used, before tracking the identities of the users of these computers. Such additional wasted time and resources would then allow culprits involved extra time to escape almost scot-free. These new provisions could prospectively hasten investigations and deter cyber cafés from turning into launch spots for cyber terrorism.

## 6. Impacts

A retrospective view of India’s political, social, infrastructural and legal attributes coupled with a history of the cyber terrorism attacks allows us to better fathom the impacts. We have divided these impacts into three core areas – Political, Social & Economic.

### 6.1 Political

The most glaring political impact of cyber terrorism in India is in its relations with Pakistan. The influx of cyber terrorism has heightened tensions to a new level, especially since Pakistani hackers turned to hacking computers in India, particularly the Indian government websites. Vatis (2002) stated that there were 45 attacks on Indian websites in 1999. This figure has increased steadily ever since. There were 133 attacks in the following year, and 275 by the end of August 2001. Pakistan has continually denied any governmental role in these attacks but India has held the state accountable for the actions of cyber terrorists within Pakistan’s borders. These attacks are aimed to leverage and strain political ties between the two countries, which will worsen in the future if no efforts are being undertaken to improve them.

Internally, the rise in cyber terrorism has caused a marked shift in the government priorities. In his article, Singh, 2012, stated that the Indian government, and the security administration, have become ‘more deeply concerned about security breaches and attacks’ through technology-enabled devices, which includes things like computers, mobiles and other physical devices, as compared to the past, when not as much emphasis have been placed on security breaches but physical border security. Handling cyber terrorism has now turned into an agenda for India’s political parties, which used to be unheard of a decade or so ago. This issue is now deemed to be crucial to India’s sovereignty and cyber terrorism has begun to dominate the local political landscape.

Governments are driven by political incentives. The Indian government has been pushed to work more closely with the public sectors since a cyber-terrorist attack will most probably originate through the telecom networks, using computers and networks which are privately owned. This attack will then affect, amongst others, things like financial corporations, intellectual property, etc, which are government-linked or owned.

The Indian government is fully aware that consequences of such attacks can be very dire to its party end survivability. India is renowned worldwide as the world's back-office, with many multinational companies locating their back-end operations there (Singh, 2012). Companies like major telecommunication companies and financial companies all have their call-operations there. Should a serious cyber-attack happen in India, it will not only lead to a large financial damage, but also hit India's global reputation as the world's back-office, hurt stock prices of the companies affected, and most importantly, degrade the value of these companies. These consequences would reflect a poor performance on the incumbent political party's scorecard, which would erode its hopes of being reelected in the proceeding elections.

## 6.2 Social

India's lack of a strong national policy targeted at its population and proper education has caused issues of cybercrime to not be effectively dealt with on a social level, putting the social sphere of India at risk.

The lack of adequate social infrastructure together with the ease of committing cybercrimes today can largely increase social motives for cyber terrorism take place in the country. These motives are driven by issues such as poverty allowing cyber terrorism to be a way in which people vent their frustrations (Legal Services in India, 2011). This becomes a vicious cycle as internal attacks or the lack of co-operation from citizens directly hampers the development of the country.

Social instability in the country will also bring about loss of investments. It has been reported that there has been more than a 10 fold increase in the number of successful cyber attacks on the infrastructure in India largely encouraged by a weak social fabric (Benoji, 2012). The fear of placing investments in the country is due to India’s failure to address social issues that spur the growth of cyber terrorism.

As such, there is an increased need for relevant help to deal with cyber security not just for firms and the public sector but also for households. This is required to better thwart cyber terrorism and includes training and education together with citizen adoption of anti-malware software for home computers. However, all these do add up to extra cost that could further slowdown the country's economy (Giacomello, 2012).

Moral panic is also one of the considerations of the effects of cyber terrorism. The intention to attack the country via governmental systems and bring it down lingers in the hearts of many as long as the notion of cyber terrorism continues (Duell, 2012). Many claims about wars that cyber crime can bring about which may be detrimental to the reputation of the country. India needs to actively soothe this panic among the people in order to further proceed with its development.

## 6.3 Economic

Akin to general economic approaches, impacts must be considered with time periods in mind. The economic impacts of cyber terrorism in India can be broadly broken into short and long term impacts.

### *6.3.1 Short Term*

Suffering a cyber-terrorist attack yields an immediate short term cost of lowered output. The case studies in the preceding sections saw suspension in production of goods and services due to reasons ranging from safety to a drastic shortfall in workers. The Mumbai attacks also heavily impacted its tourism industry. The exodus of over 30,000 workers in the Northern States crippled multiple firms as economic activity in the region slowed down immensely. Firm profits were not the only components affected; knock on effects such as wages and employment suffered as well. (Economic Times, 2008)

The impact on the private sector is large as India's economic performance requires support of its private firms. Private firms make up over 50.6% of India's GDP. (World Bank, 2012) As such, a single attack that spans even a few days will have detrimental trickle down effects from private firm performance to the country's entire economic outlook.

The above mentioned immediate effect is quickly followed up by a secondary impact still falling firmly within the short term time frame. There are multiple processes that are triggered in the aftermath of an attack. Firms have to recalibrate their production plans to cope with changes in factor inputs such as the availability of workers and materials as it can take months before normal production levels can be expected. (Economic Times, 2008)

Should a cyber terrorist attack cripple technological infrastructure, equipment will have to be replaced or upgraded to prevent future attacks from occurring. Upgrading equipment can be discounted from being a cost since it is a necessary infrastructure upgrade. However, damages such as the loss of sensitive data can cripple the firm and blunt its competitive edge. India's booming outsourcing sector is especially active in the services field where its network infrastructure is the cornerstone of this industry. A successful attack will cripple not only its provision of services but also trust from customers and business partners (Computerworld, 2012). These short term impacts directly cause output and productivity levels to fall hamstringing the effective growth of the Indian economy.

### *6.3.2 Long Term*

Economic activity is based on stability and trust. Attacks weaken confidence in firms and the industry as a whole. In targeting the minorities that were key to the performance of the IT sector, cyber terrorists successfully weakened the incentives for these migrants to continue working and contributing to India's economy, especially in its leading sector. Should India not shore up its defenses and prevent future cases from occurring, it would face difficulty attracting talent both local and foreign to drive its economy in the long run. (BBC, 2012)

It does not simply stop at labor. Capital injections from local entrepreneurs and foreign direct investments are volatile at best and speculative at worst. On either extreme, the same themes of confidence and stability are required to keep investments flowing cautiously. Losing such important channels of inputs can severely deflate the world's tenth largest economy. (Ray, 2012)

India faces competition from other rapidly expanding economies such as China, Brazil and Russia. As such, it is not simply a question of growing on its own but competition against its closest competitors for finite resources that include investments, supply chains and other key production inputs. In order to keep up and even pull ahead in this competition, India must be able to instill confidence and trust in its international partners so that they will choose India over its competitors (Diverse Education, 2012). A major function of cyber terrorism is to strike fear and intimidate. India would never want such terror to strike its key partners. Such an event would be severely detrimental to its economic growth.

## 7. Recommendations

The preceding sections have provided a descriptive and analytical picture of cyber terrorism in India. Here, we evaluate the aforementioned impacts based on India's infrastructural, legal and political constraints while benchmarking policies and providing academic recommendations that will aid its war against cyber terrorism.

### 7.1 Keeping Infrastructure Lean & Dynamic

In cyber warfare, the technological arms race between governments and cyber terrorists is crucial in determining outcomes. India's greatest issue is its failure to keep up in this never ending race. Lean and fast moving cyber terrorists have made it almost impossible for India to respond effectively due to its size and organizational structure. India needs to reorganize its security for services responsible for defending the nation. It needs to keep its cyber security department lean and ready to advance quickly. Bureaucracy and red tape have often been associated with the Indian government and public service. India can ill afford for such to continue in face of a multi-faceted threat such as cyber terrorism. (Bakshi, 2001)

### 7.2 Unifying Laws and Statues

Halder (2011) argues that India's laws are too disparate and its legal approach towards cyber terrorism is unnecessarily limited to unauthorized access to information deemed restricted. In its other sections (69A and 69B), the law is empowered to block public access of information, monitor and collect traffic data and information through computer resources. Unfortunately, Section 69 does not cover cyber terrorism. Treating cyber terrorism as a separate issue thus handicaps India's defense in the legal arena.

The importance of unifying legal resources to deal with cyber terrorism cannot be better emphasized than measures taken by the United States' Patriot Act. The Patriot Act comprises an extensive set of sanctions and titles both created and amended to fight terror. It represents a holistic set of legal ammunition to protect the United States from terrorism as a whole. Much of its laws are deeply entwined to respond to cyber terrorism. (Heritage Foundation, 2004) The

Patriot Act is not without its fair share of criticism but the political will shown by a flag bearer of free speech should encourage India, a fellow democratic champion, to unify its legal resources to respond to cyber terrorism holistically.

## 7.3 Political Relations

Operating as recognized government handicaps India who has to deal diplomatically with Pakistan while coping with the unrelenting attacks and cyber terrorist recruitment coming from a few of those found within Pakistani borders (Colarrik, 2006).

However, this does not mean India should give up on diplomacy. It should take heart from its agreements with ASEAN countries to improve security ties. These include areas such as cyber security where partnerships between domestic agencies and sharing of information have been agreed on (Devare, 2006). Such mutually beneficial moves must be replicated in countries that pose greater danger to India. While it may be difficult for India to push for such moves with Pakistan in light of deteriorating political ties, this remains its most viable option within the realms of diplomacy and good will. Success in other partnerships will encourage Pakistan to join the negotiating table. (Franda, 2002)

## 7.4 Citizen Education

An educated and empowered citizenship is often the most important defense against this type of cybercrime whose main intention is to strike fear and create turmoil. The people are the ears and eyes on ground zero and law enforcement will be greatly aided by a cooperative and empowered citizen base. Additionally, households must be taught how to secure their wireless home networks to prevent attempts such as those by the Indian Mujahedeen. Encouraging and rewarding citizen activism can go a long way in ensuring a safer India (Chia & Lim, 2002).

## 8. Conclusion

There are many reasons and intents behind cyber terrorism. The case studies have shown a broad spread of motives. These include common reasons such as politics and religion right down to mischievous desires to cause mayhem or to attract publicity. As such, our definition of cyber terrorism stands. Cyber terrorism is simply an act enabled by computer devices and connected networks that harms the stability of a nation as a whole.

India has many examples from both others and themselves in combating cyber terrorism. The most important takeaway is that cyber terrorism cannot be fought by a single actor. A complete approach spanning various pillars of society from IT policies, anti-cyber terrorism laws and even common citizens must be put in place. Cyber terrorists attack the weakest link (Colarrik, 2006) and a non cohesive approach will fail as long as a single bond in society is found vulnerable.

The state must be kept lean and highly adaptive to enable a dynamic response to technologically innovative cyber terrorists. Technology is not static. It is an element that is constantly being updated and improved. Likewise, the state has to acclimatize quickly to these changes in technology and update itself constantly. This will prevent reliance on backdated solutions allowing India to effectively combat the latest cyber terrorist threats.

India’s judiciary system must look for ways to both ensure its laws cover the extensive scope of cyber terrorism, and that legal enforcement is swift and efficient. In addition, harsher penalties need to be in place to deter extremist behavior. Cyber terrorists would only become bolder if laws are left in their current ineffective state. With state and judiciary acting hand in hand, citizens must also be encouraged to participate actively to weed out cyber terrorism (Chia & Lim, 2002).

India must also look beyond its borders and foster cooperation with its partners. Cyber terrorism often presents a unique set of problems between two countries. As mentioned above, the country wherewith the terrorist is based on may decide it is better to keep at distance and not cooperate. Extradition of cyber terrorists is also difficult because the act in itself may seem too harmless for an extradition. Some countries also have laws protecting their own citizens, no matter the crime, against extradition (Gilbert, 1998). This is especially true if the expected sentence is deemed too severe. These additional problems are severe barriers to cooperation if one considers the stormy ties with countries such as Pakistan and China. Nevertheless, India has to convince these countries that a partnership is in the best interests of both parties. Having prior agreements such as the one with ASEAN nations would aid its course. Building up ties in face of conflicting interest also has multiple additional benefits. Successful agreements on combating cyber terrorism can lead to future partnerships in other areas such as those from the economics and social domain (Devare, 2006). Therefore, India should be very much motivated to foster such ties.

A country the size and magnitude of India cannot adopt these recommendations immediately. India is the world’s most populous democracy, with a population of over 1.2 billion people, spread out over 3 million square kilometers and 28 different states (CIA, n.d). Enacting and enforcing laws in every single state and territory would undoubtedly take time and a lot of effort. However, India has already taken baby steps, and would do well to quicken its pace. India’s economic potential, social diversity and political standing deserves a stronger unified approach to reduce the threat of cyber terrorism. The incumbent government, the Indian

National Congress, led by Manmohan Singh, calls itself ‘the party of the future’ (Indian National Congress, 2012). Problems that were once deemed of the future are happening now. India’s leadership must harken the urgent call of combating cyber terrorism and make haste in pushing its solutions.

It would be naive to believe that cyber terrorism can be completely stamped out even with a solid, unified plan that is perfectly executed. The nature of terrorism is adaptive and destructively creative (Colarrik, 2006). Coupled with technological leaps that take place constantly, cyber terrorism is an ever evolving problem. Those within the techno sphere usually comment that the only way to stay safe is to unplug everything and live in a sealed, isolated cave. However, no nation can hope to progress by holing itself up and India's economy is very much dependent on decentralized jobs made possible by networks. It is imperative that India's catching up plan must take on a long term view to ensure flexibility and adaptability. This will enable it to be continuously relevant even after India finally catches up with her cyber opponents.

It is widely acknowledged that future wars would be fought in cyberspace (Rattray, 2001). In reality, this has already happened on illegal grounds such as cyber terrorism and even in government backed wars such as the use of long distance remote controlled robotics (e.g. United States air drones) in place of soldiers (Zaloga, 2008). A country's sovereignty and stability has never been in a more precarious position.  It is the state’s responsibility to educate its citizens and ensure national security for foreign investments to flourish. India must put its act together to stay ahead of cyber terrorism and ensure continued stability and growth.

## 9. References

Bakshi, P (2008). Security implications for a wired India: Challenges ahead. *Strategic Analysis*, 25(1), 105-117

Benoji, L. M. (2012). Cyber Terrorism - Quick glance. Retrieved September 24, 2012, from http://legalservicesindia.com/article/article/cyber-terrorism-quick-glance-1263-1.html

British Broadcasting Corporation. (2012). India blames Pakistan for exodus of migrant workers. Retrieved September 14, 2012, from http://www.bbc.co.uk/news/world-asia-india-19309982

British Broadcasting Corporation. (2012). Thousands continue to flee Indian cities. Retrieved September 14, 2012, from http://www.bbc.co.uk/news/world-asia-india-19292570

British Broadcasting Corproation (2012). Thousands continue to flee Indian cities. Retrieved October 16, 2012, from http://www.bbc.co.uk/news/world-asia-india-19292570

Bhattacharya, S. (2012). Cyber Terrorism: The Fifth Domain. Retrieved October 5, 2012, from http://www.ocnus.net/artman2/publish/Dark_Side_4/Cyber-Terrorism-The-Fifth-Domain.shtml

Census. (2011). Literacy Rates in India. Maps of India. Retrieved October, 14, 2012, from http://www.mapsofindia.com/census2011/literacy-rate.html

Chaturvedi, K. N. (2002). The prevention of terrorism act, 2002. Retrieved, September 28, 2012, from http://www.satp.org/satporgtp/countries/india/document/actandordinances/POTA.htm

Chia, S. Y. & Lim, J. J. (2002). *Information Technology in Asia*. Singapore: ISEAS Publications.

Central Intelligence Agency (n. d.). *India*. Retrieved October 20, 2012, from The World Fact Book.

CIOL. (2011). Creating sustainable IT infrastructure CIOL, Cybermedia News, Mumbai, India. Retrieved September 25, 2012, from www.lexisnexis.com

Computerworld (2012). Cost of Cyber Attacks are Skyrocketing. Retrieved October 1, 2012, from http://www.computerworld.in/feature/cost-cyber-attacks-are-skyrocketing-13512012

Commweb. (2006). Indian Prime Minister OKs New Data Security Laws.  Retrieved 14 October, 2012, from http://www.lexisnexis.com/hottopics/lnacademic

Colarrik, A. (2006). Cyber Terrorism Evolution. In Colarrik, A. (Ed), *Cyber Terrorism: Political and Economic Implications.* United States: Idea Group Publishing.

Combating Terrorism Center. (2012). Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace. Retrieved 10 October, 2012, from: http://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

Curran, K., Smyth, N., McGrory, B. (2008). Cryptography. In L. J. Janczewski & A. M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism*. United States: Information Science Reference.

Daily The Pak Banker. (2012). Indian IT infra market to reach $2.05b in 2012: Gartner Daily. Retrieved September 26, 20120, from: www.lexisnexis.com

Denyer, S. (2012). New tensions in India-China border dispute raise concerns. *The Washington Post, World.* Retrieved October 14, 2012, from http://www.washingtonpost.com/world/new-tensions-in-india-china-border-dispute-raise-concerns/2012/02/28/gIQAT26HiR_story.html

Devare, S. (2006). *India & Southeast Asia: Towards Security Convergence.* Singapore: ISEAS Publications.

Diverse Education (2012). Report: China, India Positioned to Compete for Global Economy's 'Best Jobs'. Retrieved September 29, 2012, from http://diverseeducation.com/article/17323/

Duell, Charles (2011) The Cyberterrorism Threat Spectrum. Retrieved October 1, 2012, from http://www.drtomoconnor.com/3400/3400lect06a.htm

Essaytown (2012). What is the Difference Between Cybercrime and Cyberterrorism? Retrieved October 10, 2012, from http://www.essaytown.com/paper/difference-cybercrime-cyberterrorism-17848

Financial Times (2012). Exodus shows alienation of India's north-east. Retrieved September 20, 2012, from http://www.ft.com/cms/s/0/79122052-e86d-11e1-b724-00144feab49a.html

Franda, M. (2002). *China And India Online*. United States: Rowman & Littlefield Publishers.

Gilbert, G. (1998). *Transnational Fugitive Offenders in International Law*. Netherlands: Kluwer Law International.

Giampiero, G. (2012). Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism. Retrieved October 14, 2012, from https://imtlucca.it/whats_new/_seminars_docs/000196-paper_giacomello.pdf

Halder, D. (n.d.). Information technology act and cyber terrorism: A critical review. Retrieved October 20, 2012, from http://www.academia.edu/945156/Information_Technology_Act_and_Cyber_Terrorism_A_Critical_Review

Heritage Foundation (2004). The Patriot Act and Related Provisions. Retrieved October 2, 2012, from http://www.heritage.org/research/reports/2004/11/the-patriot-act-and-related-provisions-the-heritage-foundations-research

Indian Blooms. (2010). Cyber Terrorism: The Fifth Domain. Retrieved October 10, 2012, from http://www.indiablooms.com/MedleyDetailsPage/medleyDetails040612a.php

Indian Institute of Banking and Finance. (n.d.) Cyber Laws in India. Legal Aspects (19). Retrieved October 16, 2012, from http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Indian National Congress (2012). All India Congress Committee - AICC. Retrieved, October 1, 2012, from http://www.aicc.org.in/new/

Kannan, S. (2012). India steps up battle against rising cyber crime wave. *BBC News*. Retrieved September 30, 2012, from http://www.bbc.co.uk/news/business-17950502

KPMG (2012) Transportation, Power and Social Infrastructure need significant push: KPMG global survey. Retrieved October 14, 2012 from http://www.kpmg.com/IN/en/Press%20Release/PR_Global_Survey_2.pdf

Krasavin, K. (2004), What is Cyberterrorism? Retrieved October 10, 2012, from http://www.crime-research.org/analytics/Krasavin/

Law Notes (n. d.) Extra-territorial jurisdiction. Retrieved September 25, 2012, from http://www.lawnotes.in/Extra-Territorial_Jurisdiction

Legal Services in India. (2011). Effect of Terrorism and Organized Crimes on Indian Society. Retrieved October 19, 2012, from http://legalservices.co.in/blogs/entry/Effect-of-Terrorism-and-Organized-Crimes-on-Indian-Society

Lidarev, I. (2012) History's Hostage: China, India and the War of 1962. *The Diplomat*. Retrieved October 13, 2012, http://thediplomat.com/2012/08/21/historys-hostage-china-india-and-the-war-of-1962/?all=true

Madaan, N. (2011). New IT Guidelines to check illegal activities at cyber cafes. The Times of India. Retrieved September 30, 2012, from http://articles.timesofindia.indiatimes.com/2011-05-08/pune/29522380_1_cyber-cafe-pune-and-pimpri-chinchwad-cyber-registration-agency

Masood, S. (2012) India and Pakistan Sign Visa Agreement, Easing Travel. *The New York Times, Asia Pacific*. Retrieved October 13, 2012, from http://www.nytimes.com/2012/09/09/world/asia/india-and-pakistan-sign-visa-agreement-easing-travel.html?ref=relationswithpakistan

Mid Day (2010). When Pakistan sends a Trojan to India. Retrieved October 10, 2012, from http://www.mid-day.com/specials/2010/aug/220810-pakistani-hackers-trojan-virus.htm

Perez, B. (2003). Microsoft steps up fight against cybercrime; the software giant is setting up se-curity teams worldwide to aid police forces. *South China Morning Post*. Retrieved October 1, 2012, from www.lexisnexis.com/hottopics/lnacademic

Pro Pakistani (2012). Welcome to August: Pakistani Hackers Deface Indian Websites. Retrieved October 10, 2012, from http://propakistani.pk/2012/08/08/welcome-to-august-pakistani-hackers-deface-indian-websites/

Pro Pakistani (2012). Pakistan Cyber Army Hacks into Indian BSNL. Retrieved October 10, 2012, from http://propakistani.pk/2011/07/28/pakistan-cyber-army-hacks-into-indian-bsnl/

PTI News Agency. (2007). India takes steps to tackle cybercrime. *BBC Monitoring South Asia - Political*. Retrieved October 3, 2012, from www.lexisnexis.com/hottopics/lnacademic

PTI News Agency. (2009). Dedicated police station in west india to deal with cyber crime. *BBC Monitoring South Asia - Political*. Retrieved October 3, 2012, from www.lexisnexis.com/hottopics/lnacademic

PTI News Agency. (2010). Indian minister urges armed forces to prepare plan against cyber terrorism. *BBC Monitoring South Asia - Political*. Retrieved October 3, 2012, from www.lexisnexis.com/hottopics/lnacademic

PTI News Agency. (2011). Indian official says internet "most potent recruitment tool" for terrorists. *BBC Monitoring South Asia - Political*. Retrieved October 3, 2012, from www.lexisnexis.com/hottopics/lnacademic

Rattray, G. J. (2001). *Strategic Warfare in Cyberspace.* United States: MIT Press.

Ray, S. (2012). Impact of Foreign Direct Investment on Economic Growth in India: A Co integration Analysis. *Advances in Information Technology and Management*, 2(1), 187-201.

Reuters. (2008, July 25). Timeline: Major attacks in India since 2003. Retrieved September 29, 2012, from http://www.reuters.com/article/2008/07/25/us-india-blasts-bangalore-timeline-idUSB68384820080725?sp=true

Right Vision News. (2012). Pakistan: In 65 years, India excels Pakistan in many fields. *Right Vision News, Lahore*. Retrieved October 12, 2012, from: www.lexisnexis.com

Sharma, B. (2012). In a Gujarat Fishing Village, India-Pakistan Tensions Take Huge Toll. *The New York Times, India*. Retrieved, October 13, 2012, from http://india.blogs.nytimes.com/2012/07/03/in-a-gujarat-fishing-village-india-pakistan-tensions-take-huge-toll/?ref=relationswithpakistan

Singh, S. (2012). Government to rope in private players in cyber security. *The Hindu*. Retrieved October 20, 2012, from http://www.thehindu.com/news/national/government-to-rope-in-private-players-in-cyber-security/article3997165.ece

Sinha, M. (2011). Indian it rules 2011. a critical review. Retrieved September 30, 2012, from http://thoughts.manishsinha.net/post/9371815499/indian-it-rules-2011-a-critical-review

The Economic Times. (2008). Govt framing norms for social infrastructure in SEZs: Pillai. Retrieved October, 14, 2012 from http://articles.economictimes.indiatimes.com/2008-06-20/news/28488069_1_sez-board-sez-act-special-economic-zones

The Economic Times (2008). Trident may open in 10 days, Oberoi in a few months. Retrieved October 15, 2012, from http://articles.economictimes.indiatimes.com/2008-12-02/news/28384898_1_oberoi-group-prs-oberoi-trident

The Economist. (2012). Friend, enemy, rival, investor. The Economist, Mumbai. Retrieved October 13, 2012, from http://www.economist.com/node/21557764

The Times of India (2012). No-holds barred cyber war. Retrieved October 10, 2012, from http://articles.timesofindia.indiatimes.com/2003-11-11/chandigarh/27201112_1_hacker-groups-indian-hackers-defaced

The New York Times. (2012). Kashmir. *The New York Times, World*. Retrieved October 13, 2012, from http://topics.nytimes.com/top/news/international/countriesandterritories/kashmir/index.html?inline=nyt-geo

Vatis, M. (2002). Cyber Attacks: Protecting America's security against Digital Threats. Retrieved October 21, 2012, from http://belfercenter.ksg.harvard.edu/files/cyber_attacks_protecting_americas_security_against_digital_threats.pdf

Waldron, J. (2004). *Terrorism and the Uses of Terror.* The Journal of Ethics, 8(1), 5 – 35. Retrieved from http://jstor.org

Wilson, C. (2008), *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* Retrieved October 10, 2012, from http://www.fas.org/sgp/crs/terror/RL32114.pdf

World Bank (2012). *Domestic Credit to Private Sector (% of GDP).* Retrieved October 7, 2012, from World Bank Database.

Zaloga, J. S. (2008). *Unmanned Aerial Vehicles: Robotic Air Warfare 1917-2007*. United States: Osprey Publishing Ltd.

Zeenews India. (2012). North East exodus: India to rake SMSes, MMSes issue with Pak. Retrieved September 25, 2012, from http://zeenews.india.com/news/nation/north-east-exodus-india-to-rake-smses-mmses-issue-with-pak_794576.html