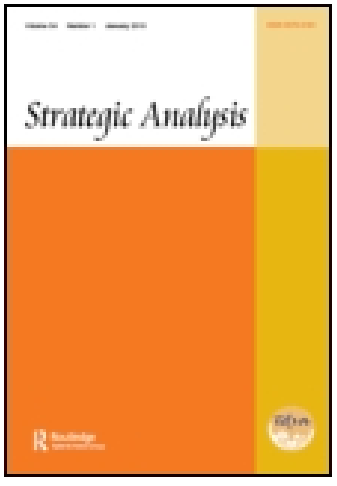

Strategic Analysis
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rsan20

Prospects for India-US Cyber Security Cooperation

Cherian Samuel

Published online: 09 Aug 2011.

To cite this article: Cherian Samuel (2011) Prospects for India-US Cyber Security Cooperation, Strategic Analysis, 35:5, 770-780, DOI: 10.1080/09700161.2011.591249

To link to this article: http://dx.doi.org/10.1080/09700161.2011.591249

Strategic Analysis
Vol. 35, No. 5, September 2011, 770–780

Routledge
Taylor & Francis Group

Prospects for India–US Cyber Security Cooperation

Cherian Samuel

Abstract: Cyber security cooperation should be a natural area of cooperation between India and the United States for a number of reasons; both countries are democracies, with similar values and economic systems, and both have also been severely affected by threats emanating from cyberspace. The structural complementarities between the two economies, especially in the services sector, which is a major user of cyber networks provides further motive for the two countries to cooperate in this sector. Despite this strategic fit, there has been very little in the nature of cooperation, either bilaterally or multilaterally. In fact, both countries seem to have embarked on the futile exercise of securing their respective corners of cyber space in this shapeless and formless domain. Cyberspace would be better served if the two countries utilised their respective leadership positions to work pro-actively towards a cyberspace that is open, global and secure.

Ensuring a safe and secure cyberspace is an increasing priority for governments as it now touches almost every aspect of human existence. The diversity of the stakeholders, from the individual, to corporations, to states makes the reconciling of different priorities and perspectives in an overarching cyber security policy a difficult task. The sheer complexity of this medium, coupled with the rapidity of technological change has meant that much of the cooperation on the framing of the rules of the road has largely been at the purely technical level through organisations such as the International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Corporation for Assigned Names and Numbers (ICANN). While these organisations have played a crucial role in the evolution of cyberspace, the issue of cyber security is increasingly one that requires inter-governmental cooperation since there are interlocking issues in the technical, business, legal, security and international policy arenas that need to be resolved. However, there has been very little movement on these issues within countries because of the sectoral rather than a holistic approach to cyber-security. At the international level, the primary inhibitor has been the distrust amongst governments, who impugn various motives, ideological and otherwise, to the policy initiatives of the other.

Cyber security should be a natural area of cooperation between India and the United States for a number of reasons. The fact that both countries are democracies, with similar values reduces the scope for distrust on ideological grounds; furthermore, the two countries have also been at the receiving end of cyber threats both from state-sponsored and non-state actors. The structural complementarities between the two economies,

Cherian Samuel is an Associate Fellow at IDSA, New Delhi.

ISSN 0970-0161 print/ISSN 1754-0054 online

DOI: 10.1080/09700161.2011.591249
http://www.informaworld.com

especially in the services sector which is a major user of cyber networks provides further incentive for the two countries to cooperate in this sector. Despite this strategic fit, there has been very little in the nature of cooperation, either bilaterally or multilaterally, though that is gradually changing. This paper tries to examine the scope for cyber-security cooperation between India and the United States, and the existing obstacles.

The cyber security conundrum

The focus of national security planners the world over, till recently, can be encapsulated in the definition of cyberspace in the US government's *National Strategy to Secure Cyberspace* which defined it as follows: 'Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow our critical infrastructures to work'.[1] Ensuring the security and integrity of the networks that connect critical infrastructure became of paramount importance since crucial sectors such as the financial, energy, transportation and telecommunications sectors were connected through cyber networks. The scope of this task has expanded in ensuing years as the cyber networks have become interconnected and their user-base has grown to include individuals and private enterprise. The horizontal and vertical expansion of the user base has meant that while the threats and vulnerabilities inherent to the Internet and cyberspace might have remained more or less the same as before, the probability of disruption has grown apace with the rise in the number of users. In general, active focus on cyber security has moved beyond safeguarding critical infrastructures to protecting governmental information and communication networks. However, this still leaves a large section, ranging from enterprises to individuals, with little or no assurance that they are secure in cyber space. In an era where interconnected networks are the crucial arteries of human existence and knowledge has become a valuable commodity, this represents a serious threat to national security. Therefore, in addition to securing critical infrastructure and government information networks, governments also have to ensure that the private sector adheres to protocols that ensure the integrity of their networks and also reassure the public at large that cyber networks on which they have become increasingly dependent, are reliable.

The growth of cyber space has partly been attributed to its relative openness and low barriers (including minimal security features) to entry. However, the same openness has also been responsible for those with malicious intent also to operate with relative ease. Threats[2] have taken advantage of existing vulnerabilities[3], in software, networks or security architecture. The current threats can be disaggregated into four baskets; cyber crime, cyber espionage, cyber terrorism and cyber warfare, depending on the perpetrators and their motives. On the face of it, cyber crime, cyber espionage, and cyber terrorism are online manifestations of law and order problems in the physical world, and should accordingly be mitigated by adapting existing laws. However there are two characteristics of this domain that make such adaptation very difficult. The first is that of blurred boundaries; there are no clear demarcations between civilian and military, state and non-state, and foreign and domestic as in other domains. It is these same characteristics that make it an ideal medium for malafide activities which can have repercussions for national and international security. Even if the boundaries were to be more clearly defined, the second problem, that of attribution or the inability to trace activities or events to their exact point of origin make the task of pinning responsibility a difficult one.[4] These two factors have largely been responsible for cyber

crime. More recently, increased state sponsorship of both cyber espionage and cyber terrorism have added a new dimension to cyber security.

Cyber war has been used loosely to refer to everything from cyber terror to cyber espionage, to cyber sabotage but a distinction needs be made between cyber war which is war in the cyber domain in conjunction with a physical war and cyber warfare which is increasingly the utilisation of those aspects such as blurred boundaries and non-attribution by both state and non-state actors to probe/infiltrate/attack cyber connected infrastructure and networks. Successive reports by research centres, anti-virus firms, and government agencies have documented the rising incidents of cyber warfare.[5] These attacks serve multiple goals from recovering sensitive information and intellectual property, to creating a climate of insecurity so as to prevent the optimum utilisation of cyberspace.[6]

Approaches to cyberspace: US and India

Successive US administrations have grappled with the issue of having a structured response to cyber security but been unable to surmount various obstacles. In the first instance, roughly 85 per cent of the information infrastructure in the United States is in private hands. Secondly, privacy issues and the presence of vigilant interest groups means that the government has to walk a fine line between security and privacy. The government has tried to concentrate on protecting the remaining 15 per cent consisting of its own networks, but even that has been constrained by the variety of agencies that are tasked with different aspects of cyber administration. The Cyber Incident Annex to the National Response Framework of 2004 lists as many as 14 agencies that are directly connected with the management of cyber security, including the departments of defence, homeland security, justice, transportation, energy, and the intelligence community. As President Obama noted in a 2009 speech:

> No single official oversees cyber security policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cyber security, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should — with each other or with the private sector.[7]

To rectify this, the president proposed that the office of Cyber Security Coordinator be based in the White House.[8] In March 2010, responding to criticism that the private sector could not work with the government if the Comprehensive National Cybersecurity Initiative (CNCI), the primary document that spelt out the governments cyber security initiatives remained classified, a summary of the CNCI was declassified.[9]

The declassified summary listed three primary cyber security goals: establishing a front line of defence against immediate threats, defending against the full spectrum of threats and strengthening the cyber-security environment for the future, and spelt out 12 initiatives to attain these goals. By concentrating on cyber defence, the Cyber Security Initiative placed greater store on deterrence by denial as against the existing strategy of deterrence through retribution that has been core US national security strategy since the dawn of the nuclear age.[10] The year 2010 saw a shift in US cyber security

policy with the establishment of US Cyber Command under the leadership of the head of the National Security Agency with specific instructions to co-ordinate and aid the department of homeland security's cyber security efforts.

In India, the primary approach was initially on the economic aspects with a gradual shift towards the safeguarding national security. The Information Technology Act of 2000 was enacted largely to facilitate e-commerce, with cyber crime referred to only in that context.[11] Even the amendments sought to be made in 2006 largely related to bringing in provisions related to outsourcing and indemnifying Internet services against certain liabilities.[12] In the event, these amendments were never passed as they were seen to be too industry friendly. It took the Mumbai attacks of 2008 for the government to complete the process begun in 2006 and enact the Bill after further amendment in 2009. The Act marks a transition in approach to one focused on national security objectives.[13]

It must be noted there is a quantitative and qualitative difference in the cyber scene in the two countries. In India for instance, much of the critical infrastructure, from banks to high technology firms, to the power grid is in the hands of the government, which makes it easier to secure them. Secondly, the slow pace of development has meant that much of the government data infrastructure is still antiquated and has not been updated for the digital age. As a case in point, the Indian army still depends on the three decade old Army Radio Engineering Network (AREN) for connecting its field forces. The AREN does not have data transmission capabilities.[14] That said, there are a large number of sectors that are computerised, ranging from banking to the Indian Railways, and most networks are rapidly being modernised.[15]

Organisational setup – US and India

In the US, the organisational structure as it has evolved consists of the Department of Homeland Security tasked with protecting civilian governmental networks and the US CYBERCOM created in 2010 which has been mandated to 'direct the operations and defence of specified department of defence information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations'. A third component is the National Security Agency which has been directed to provide operational assistance to the DHS. While these organisations sit at the apex, as already mentioned, there are at least 14 different government bureaus, divisions, and departments that are actively involved with cyber security issues.

In India too, as many as 12 agencies are listed as 'stakeholders' in cyber security in a recent draft National Cyber Security Policy document released on 26 March 2011. While some such as the National Disaster Management Authority of India play only a peripheral role and many of the sectoral CERTS are yet to come up, real oversight over cyber security could be said to be distributed amongst the ministries of communication and technology, home affairs, and defence and the office of the National Security Advisor. On the military side also, there is a profusion of agencies, ranging from the Corps of Signals, to the A-CERT (Army Computer Emergency Response Team), to the IT departments of the various HQs and the Integrated Defence Staff (IDS). The Defence Information Assurance and Research Agency (DIARA) has been made the 'nodal agency mandated to deal with all cyber security related issues of Tri Services and Ministry of Defence' according to a statement made by the defence minister in parliament in 2010.

Prospects for India–US cyber security cooperation

Co-operation, in any area, in the first instance, is contingent on there being a positive inclination and push at the highest policy making levels. Mechanisms and protocols then have to be put in place, and habits of co-operation built up through sustained engagement.

Even though Indo-US cyber security cooperation has become a staple discussion of high level summits and subsequent joint statements in the recent past[16], cooperation had been mooted as early as 2002 when the India–US Cyber Security Forum was set up in the very first flush of cooperation between the two countries. The motivation on the US side was to safeguard the interests of US companies who were outsourcing to India; the preamble to the factsheet of the 2006 meeting of the Cyber Security Forum noted :

> The US and Indian governments are intensifying on-going cooperation to address national security issues arising from the increasing interdependency of our critical network information systems involved in outsourced business processing, knowledge management, software development and enhanced inter-government interaction.[17]

On the Indian side, the emphasis was on capacity building and research and development, and the forum provided the opportunity to initiate a number of programmes in this direction, from the establishment of a CERT and the facilitation of discussions on cyber security.[18] Though the forum saw possibilities for cooperation in the law enforcement sphere, in research and development, in the military sphere, in the technological sphere, and in intelligence sharing, most of the emphasis was on building up capacities in areas such as data protection in which the US had a direct interest. The Cyber Security Forum became defunct in 2006 after it was alleged that a US embassy staffer had used the close proximity afforded by the forum to recruit employees of the National Security Council Secretariat (NSCS) which was the coordinating agency on the Indian side to pass on sensitive information.[19]

Consequently, even though the expanding envelope of cyber security threats and vectors have enlarged the scope for cooperation both at the bilateral and multilateral levels, cooperation so far has been piece meal and ad hoc in nature.

Cooperation at the bilateral level

In the field of law enforcement, bilateral cooperation takes place in the routine manner in the absence of an international legal framework and law enforcement regime that takes cognisance of the different requirements of cyber security. While there is recognition that cyber crime can only be effectively combated by a real time response, the only existing avenues for cooperation remain the Interpol and Mutual Legal Assistance Treaties (MLAT).[20] The two governments have tried to widen the scope of co-operation on the back of the more robust engagement in counter-terrorism cooperation.

One of the areas in which there is considerable scope for cooperation is in Research and Development (R&D) which, in the context of cyber security, can run the full gamut from removing loopholes in hardware and software to creating tools for law and enforcement and intelligence agencies and, for military purposes. However, joint research and development is possible only in an open academic environment. In the United States, the government agency entrusted with research and development into cyber security is the National Security Agency (NSA) but the nature of that secretive organisation is such that even the scientific advances made by it, usually built on the

back of scientific advances in academia are not available for peer review or put in the public domain.[21] The most potent weapon in the hands of the NSA is its ability to intercept and decipher encrypted communications in cyberspace. The initial approach of the NSA was to push the US government to ban the export of encryption technology through measures ranging from domestic laws to international arrangements such as the Wassenar Arrangement.[22] Following pressures from industry, the US government had to liberalise the export of encryption technologies, and since then, the NSA has focused on technologies designed to break through those levels of encryption. In India, agencies such as the Defence Research and Development Organisation (DRDO) and the National Technical Research Organisation (NTRO) are developing expertise in intelligence gathering as well as securing cyber space.[23] Past experience shows that intelligence organisations are reluctant to share their competencies with other countries, unless there is an overwhelming compulsion to do so.

Critical information infrastructure protection is the sphere which offers the most scope for cooperation on a number of counts. In the first instance, this has been a major focus in the United States, as stated in an earlier section of this paper. US focus on this issue was also reflected in the bilateral cooperation agenda with experts in this field constituting a majority in the delegations attending the Cyber Security Forum. Two meetings of the Indo-US Critical Infrastructure Protection (CIP) forum were also held, and a workshop on cyber security standards was conducted in Delhi in 2005 on the basis of the CIP forum's recommendations.[24] A number of best practices such as the establishment of the Computer Emergency Response team (CERT-IN) were influenced by the deliberations of the Cyber Security Forum. A National Skills Registry was also set up in 2005 to authenticate individuals working in the IT industry through 'independent verification and biometric identification'.[25] As it happens, the United States is now considering a similar scheme for individuals in the networking space. Other initiatives that were mooted in 2006 but are yet to become operational were an India *Information Sharing and Analysis Centre* modelled on its US counterpart[26] and an India Anti-Bot Alliance.[27]

Secondly, it may be said that both countries share critical information infrastructure not only because of the outsourcing factor, but for many other reasons, ranging from Indian websites being hosted on servers in the United States, to the fact that the Reliance Telecom and Tata Communications, the two largest undersea cable companies in the world, and carrying much of its internet traffic, are Indian companies. This symbiotic relationship provides a multitude of opportunities to overcome the obstacles that have inhibited the operationalising of cyber security. As a case in point, Tata Communications has said that technology has advanced to the extent that ISPs such as Tata have the ability to remove botnets and malware before they strike their intended targets as well as the ability to monitor internet traffic in real time.[28] However, lack of international cooperation brings up jurisdictional obstacles and the lack of an international body has meant that such information stays with the Internet Service Providers (ISPs). Similarly, many of the Internet security companies such as Symantec and McAfee have their research facilities located in India, while India is also becoming the hub of many Internet security start ups.

In terms of best practices, there is much to be learnt from the US National Cyber Security Initiative (NCSI) and particularly from its areas of focus, and its emphasis on timelines and end goals. The intent of the initiative is to plug the existing holes in the cyber infrastructure and to strengthen existing defences. These include reducing the nodal points at which the federal communications infrastructure interfaces with

the Internet from thousands to fifty.[29] Another notable initiative is the deployment of passive sensors designed to detect attempts at illegal access into federal systems. The programme, codenamed EINSTEIN, is currently in its second iteration where it can alert 'US–CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic'.[30] A third iteration 'will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defence' and is being developed in close collaboration with the NSA.

Other gaps are sought to be plugged by developing and implementing a government-wide cyber counterintelligence initiative. This was deemed necessary to 'detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to US and private sector information systems'. Yet another initiative calls for 'developing a multi-pronged approach for global supply chain risk management' since the globalisation of the commercial information and communications technology marketplace has increased the risk of buying technologies and hardware that could have been compromised and be used to 'gain unauthorised access to data, alter data, or interrupt communications'. The long term strategy was described as one:

> . . . aimed at building an approach to cyber defence strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.[31]

That such a top level initiative is necessary in India is evident from a recent study by McAfee in association with the Centre for Strategic and International Studies (CSIS). Titled *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* the report indicated that companies across India were subject to the highest number of DDOS attacks, but at the same time, had the lowest security adoption rates at under 40 per cent. This, despite the fact that India also topped the charts of cyber security regulation with 97 per cent of IT managers saying they were impacted by cyber security regulation or legislation.

Two visible strands of cooperation can be discerned at the bilateral level; a technical strand embodied in the Joint Working Group on ICT which also looks at cyber security, and a security centric strand embodied in recent attempts to include cyber security in the Counter-terrorism Cooperation Initiative, within the overall ambit of sharing best practices.[32] There are indications that the cooperation in the second strand is accelerating, but to succeed, it has to be both a calibrated and equal partnership. Though the Joint Working Group on ICT has tried to take up the slack after the Cyber Security Forum went defunct in 2006, its closed door approach and the fact that cyber security is only a subset of its overall mandate has severely limited its effectiveness.

Cooperation at the multilateral level

Even though cyber crime and cyber fraud have taken on gargantuan proportions, cooperation at the multilateral level has been less than forthcoming. Though there is a crying need for an international framework governing cyberspace, the absence of such a framework is the result of a number of factors including the relative newness of the medium, the fact that it transcends so many spheres and touches on so many issues

from privacy to commerce, and the reluctance of governments to give up national sovereignty over cyberspace. Though the UN system makes it the ideal forum for generating such a framework, the UN has proved to be ineffective, despite many attempts. Forums such as the two World Summits on the Information Society (WSIS) saw countries with different priorities pushing their own agendas, leading to a stalemate. After adopting a hands-off approach towards UN initiatives, more recently, the United States has become more pro-active, especially in the United Nations Group of Governmental Experts (GGE) on Information Security which came out with a consensus document on cyber space to be presented to the UN Security Council. Indian and US experts closely coordinated their positions in this exercise, according to the US government.[33]

As far as law enforcement cooperation is concerned, the only working transnational agreement that addresses criminal activity in cyberspace is the Council of Europe's Convention on Cyber Crime. Adopted in 2004, the Convention is a comprehensive document that lays out the rights and obligations of states in cooperating on cyber crime. Though it has been signed by many European states, Russia has been a notable holdout. Non-European states that have signed the Convention include Canada, Japan, the United States and South Africa; and other countries including India have been repeatedly pressed to join the Convention.[34] Russia's reservations are to do with the fact that it was not included at the drafting stage as well as with the loss of sovereignty implied in Article 32. The Convention has also been criticised on the grounds that it treats attacks on information systems as criminal offences, thereby disregarding the national security dimension of such attacks and that it does not differentiate between attacks on ordinary computer systems and those on critical infrastructure information systems, or between small- and large-scale attacks.

Though terrorism, both in and through the physical and cyber domains is the most immediate danger faced by the world community, counter-terrorism cooperation has proceeded in fits and starts, largely driven by location-specific incidents, and constrained by the in-built suspicion intelligence communities have towards one another. The US shares signals intelligence only with its closest allies and even that is governed by a treaty, the classified UK–USA Security Agreement of 1948 which established an alliance of five countries, Australia, Canada, New Zealand, the United Kingdom and the United States for the purpose of sharing intelligence, especially signals intelligence.[35] Therefore, it is unlikely that intelligence agencies such as the NSA would be willing to share such technologies, considering them to be a strategic asset.[36] At best, the NSA would like to put itself in the position where the intelligence sharing is one way, and given its pre-dominant position and technology expertise, it will connect the dots, provide the analyses, and farm that information back on a need-to-know basis. [37]

Conclusion

Meaningful cooperation in cyber security is possible only if both countries are on the same page both in their understanding and their responses to the problems in cyberspace. A sectoral approach to cyber security has proved to be inadequate and short sighted, and though the United States is now adopting a holistic approach, it falls short on the issue of international cooperation. This flows out of the belief that more cooperation would lead to more regulation, which would be benefit those who seek to restrain the free flow of information on the Internet. However, as James Lewis pointed out in his recent testimony before the US Congress, such an approach is short sighted and

without government intervention, security may be unachievable.[38] However, governments in both countries are working at cross-purposes by striving to secure their own respective corners of cyberspace. This is an exercise in futility given the unique nature of this domain. Cyberspace would be better served if the two countries utilised their leadership position in the information technology domain to collaborate on a range of initiatives from cyberspace treaties to coordinating and funding joint private sector efforts and academic research into preserving the open and global nature of cyberspace. In the case of academic research, the legal, technical and privacy issues that surround cyber security policy making and implementation and the commonality of many of these issues to both countries paves the way for cross collaborative studies, aided further by the presence of many students of Indian origin working on these issues in the United States.

The India–US Cyber Security Forum, in its brief period of existence had been a useful platform to bring all the different stakeholders in government and the private sector together. This dialogue mechanism can be revived and revitalised by opening it up to include non-governmental organisations, students, and other interested parties in the true spirit of cyberspace and, in keeping with the people-to-people contacts that have propelled India–US cooperation, would be sure to throw up new avenues for collaboration. Useful models range from the annual RSA Cyber Security Conference to the UN Internet Governance Forum which is being replicated nationally and regionally.[39]

It goes without saying that the common goals and values espoused in the Indo–US strategic partnership translate into a vision of the cyberspace domain being open, global and secure. Liberal democracies such as India and the United States have had to maintain a delicate balance between ensuring universal democratic rights inherent to their open societies and imposing restraints in the interests of security. The same obtains in cyberspace. Their common challenge is to rebuff actions designed to take advantage of the vulnerabilities of free and open societies as reflected in cyber space. They should also see through the motives behind such actions designed to make cyberspace appear so insecure that countries are moved to embrace an alternate vision of cyberspace that is both closed and closely controlled.

Notes

1. White House, *The National Strategy to Secure Cyberspace*, Washington, DC, February 2003, p. vii.
2. A threat was defined by the US Computer Emergency Response Team (CERT) in 1993 as 'Any circumstance or event that has the potential to cause harm to a system or network that means, that even the existence of a(n unknown) vulnerability implies a threat by definition'.
3. Vulnerabilities are defined as: (a) a feature or bug in a system or programme which enables an attacker to bypass security measures; (b) an aspect of a system or network that leaves it open to attack; and (c) the absence or weakness of a risk-reducing safeguard which had the potential to allow a threat to occur with greater frequency, greater impact or both. Anil Sagar, *An Overview to Information Security and Security Initiatives in India*, Powerpoint Presentation, 18 January 2008, available at www.elitex.in/paper2008/anilsagar.ppt (accessed 15 June 2009).
4. Computer expert Bruce Schneier notes that the closest that a an IP address can be mapped to a physical location is 35 kilometres though more recent research has brought that distance down to less than a kilometre. That could still mean thousands of computers in an urban location. *Schneier on Security* blog, 'Pinpointing a Computer to Within 690 Meters', April 8, 2011, available at http://www.schneier.com/blog/archives/2011/04/pinpointing_a_c.html (accessed 14 May 2011).

5. Reports on India include 'Shadows in the Cloud' brought out by the Munk School of Global Affairs in association with the Information Warfare Monitor in 2010, www.infowar-monitor.net/. . ./shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/. The most recent global cyber incidents report Symantec's *Internet Security Threat Report,* 2011, available at https://www4.symantec.com (accessed 11 May 2011).
6. McAfee, *Unsecured Economies: Protecting Vital Information,* 2008*,* and *Underground Economies,* 2011, available at www.mcafee.com (accessed 11 May 2011).
7. Ibid.
8. The post was filled only in December 2009 after a 'long and tedious search' since many were reluctant to take up the post given the lack of clarity on the job requirements.
9. White House, Comprehensive National Cybersecurity Initiative, available at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 10 December 2010).
10. New York Times, 'In Digital Combat, US Finds No Easy Deterrent'*,* 25 January 2010, http://query.nytimes.com/gst/fullpage.html?res=9404E4DE123BF935A15752C0A9669D8B63 (accessed 15 March 2010).
11. The Preamble of the IT Act clearly stated that it was an act 'to provide legal recognition for transactions carried out by means of electronic date interchange and other means of electronic communication, commonly referred to as "electronic commerce"'.
12. The bill was listed for business in the Rajya Sabha as follows: 'To corporate the recent developments nationally and internationally particularly with reference to provisions related to data protection and privacy in the context of Business Process Outsourcing (BPO) operations, liabilities of network service providers, computer related offences, regulation of cyber cafes, issues relating to child pornography, etc'. Available at http://164.100.24.167/newsite/lb/legislative/bil/billexpected206.htm (accessed 12 June 2008).
13. New rules that have been notified under the provisions of the Act such as Information Technology (Guidelines for Cyber Cafe) Rules, 2011, also emphasise the government's intent to reduce anonymity in cyberspace. In a panel discussion on cyber security at the Munich Security Conference in February 2011, the Indian National Security Advisor noted that the IT Act empowers the government to 'scan Indian cyber space, detect incidents, audit practices, and protect critical and other infrastructure'.
14. Gurmeet Kanwal, 'The Imperative of Modernising Military Communications Systems', *IDSA Comment*, 16 February 2010, available at http://idsa.in/idsacomments/TheImperativeofModernisingMilitaryCommunicationsSystems_gkanwal_160210 (accessed 16 February 2010).
15. These moved at a glacial pace since there was a lot of opposition and resistance within organisations to computerisation. It took five years for the railway reservation systems to be networked across the five zones, beginning 1994.
16. See, for instance, the Joint Statement issued at the end of President Obama's visit to India in 2010 at http://meaindia.nic.in/mystart.php?id=100016632&pid=1849 (accessed 20 December 2010).
17. *US–India Cyber Security Forum: Enhanced Cooperation to Safeguard Shared Information Infrastructures*, 3 March 2006. Available at http://www.america.gov/st/pubs-english/2006/March/20060303142826dpnosmoht0.4864313.html (accessed 17 March 2008).
18. These priorities are brought out in speeches and statements made at the various meetings of the Cyber Security Forum. The joint statement at the end of President Bush's visit to India in 2006 also declared that the two sided 'recognised the importance of capacity building in cyber security and greater cooperation to secure their growing electronic interdependencies, including to protect electronic transactions and critical infrastructure from cyber crime, terrorism and other malicious threats'. Prime Minister's Office, *India–US Joint Statement*, 2 March 2006, available at http://pmindia.nic.in/prelease/content4print.asp?id=409 (accessed 19 August 2008).
19. *Indian Express*, 5 August 2006, Police list 67 documents leaked to US diplomat. Available at http://www.indianexpress.com/news/police-list-67-documents-leaked-to-us-diplom/9977/ (accessed 13 October 2009).
20. The India–US MLAT came into force in October 2005.

21. Network World, *Former NSA Tech Chief: I Don't Trust the Cloud,* 4 March 2010, available at http://www.networkworld.com/news/2010/030410-rsa-cloud-security-warning.html (accessed 1 April 2010).
22. Cryptography, classified as a defensive technology, is in Category 5, part 2 of the Wassenar Arrangement.
23. See last part of interview with V.K. Saraswat, scientific adviser to the defence minister and director-general, DRDO in *Frontline*, 28(1), 2011, available at http://www.frontline.in/stories/20110114280112600.htm (accessed 17 March 2011).
24. *Annual Report of the India–US Science and Technology Forum*, 2005–2006, p. 32 .
25. PIB press release, *Dayanidhi Maran Launches National Skills Registry For IT Professionals,* 18 January 2006, available at http://www.pib.nic.in/release/rel_print_page1.asp?relid=15023 (accessed 17 June 2008).
26. Though an Indian ISAC website has been up and running at http://www.isac.org.in for sometime, there seems to be very little activity otherwise.
27. PIB press release, *India–US cyber security forum – fact sheet*, 2 March 2006, available at http://pib.nic.in/release/rel_print_page.asp?relid=16132 (accessed 17 October 2009).
28. Searchsecurity.com, *Major ISPs can Remove Botnets, Malware, CISO Says,* 17 March 2010, available at http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1456728,00.html (accessed 20 November 2010).
29. According to officials, this initiative is an ongoing one with the number currently around hundred.
30. The White House, *The Comprehensive National Cybersecurity Initiative*, available at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 15 December 2010).
31. Ibid.
32. There seems to be greater interest in cyber security cooperation on the US side. In the course of his remarks at the signing ceremony of the Memorandum of Understanding between the Indian Ministry of Home Affairs and the US Department of Homeland Security in July 2010, US Ambassador Roemer mentioned cyber security as one of the areas envisaged for cooperation in the future while this issue was not mentioned in the Indian home secretary's remarks. See http://newdelhi.usembassy.gov/pr072310.html for US ambassador's remarks and http://pib.nic.in/release/rel_print_page.asp?relid=63434 for home secretary's remarks (accessed 12 March 2011).
33. Ibid.
34. *Outlook* magazine, 'India Asked to Join Convention on Cyber Crime', 30 March 2009, available at http://news.outlookindia.com/item.aspx?657030 (accessed 12 February 2010).
35. The existence of such a Treaty has not been publicly acknowledged by the United States.
36. The NSA's equivalent here, the National Technical Research Organisation(NTRO), would be equally reluctant to share intelligence or technologies.
37. Kathryn Stephens and Larry McKee, *Cyber Espionage: Is the US Getting More Than It's Giving*?, NSCI White Paper, National Security Cyberspace Institute, 11 February 2010.
38. James Lewis, Testimony to the US Congress, *Cybersecurity: Next Steps to Protect Critical Infrastructure,* 23 February 2010, available at http://csis.org/testimony/cybersecurity-next-steps-protect-critical-infrastructure (accessed 15 November 2010).
39. A full link of such initiatives can be found on the IGF website at http://www.intgovforum.org/cms/regional-igfs (accessed 12 January 2011).