CHAPTER THREE
CYBER SECURITY POLICY IN INDIA

The Government of India has identified Militarisation of Space and Cyber Security as one among the five medium term threats/challenges faced by our country. The spectre of nuclear proliferation and cyber terrorism and their connection with international terrorism also represent problems for Indian national security for which solutions must necessarily rely on international cooperation. "The apparent stability of the nuclear balance and the quest for seeking new areas for military advantage may prompt some states to move towards weaponisation of space. India, with its yet limited space capability, will face a major challenge in protecting its space assets in case of a conflict. Similarly, cyber space will be a greater challenge going forward—both for security and economy"

India on its growth path is vulnerable. Located in an unstable region where the larger neighbours possess this capacity, it is logical to assume that the country is under serious threat and constant attack. The impact on national security is thus serious and such that all institutions and organs of the state must jointly work to counter this challenge

The Government of India has recently taken several steps to ensure greater focus on these issues within the country. It has recently notified the National Cyber Security Policy 2013 with the goal of addressing the cyber security domain comprehensively from a national perspective. The main goal of the policy is to make the cyberspace secure and resilient for citizens, businesses, and the government. The policy envisages the establishment of national and sectoral mechanisms to ensure cyber security through the creation of a National Critical Information Infrastructure Protection Centre (NCIIPC). Computer Emergency Response Team (CERT-In) shall act as the nodal agency for coordination of all cyber security and crisis management efforts. It will also act as the nodal organisation for coordination and operationalization of sectoral CERTs in specific domains in the country.

Though efforts are being made to create an effective policy framework to deal with cyber security in the country, there are areas where significant challenges lie. E-

governance is a specific case in point. The country has put in place a separate core ICT infrastructure for e-governance consisting of statewide area networks (SWANs) and state data centres (SDCs) in each state and union territory. Common Service Centres (CSCs), run by private village level entrepreneurs (VLEs), act as the front end for delivery of these services in rural areas. Currently, over 100,000 CSCs are operational across the country. Recently, mobile governance has been implemented to bring all government services on the mobile platform. The National e-Governance Plan is the flagship programme in e-governance consisting of 31 Mission Mode Projects (MMPs) spanning across a large number of government ministries and departments both at the national and state levels. During the last seven years of its implementation, NeGP has achieved considerable success with 23 out of the 31 projects delivering services electronically to the citizens and businesses.

Though National e-Governance Plan (NeGP) has been a success, ensuring cyber security remains a big challenge as it involves protecting critical ICT infrastructure such as SWANs, SDCs and the applications of various departments running on them. Though scheme specific guidelines have been issued and several states have made significant efforts to protect their cyber assets, there is a need for a comprehensive policy on cyber security in e-governance and ensuring uniformity in its implementation across the country. Application level security is another important domain where greater effort is required.

Building a national strategy for cyber security is the first step in establishing a national cyber security program. A national policy framework should explain the importance of cyber security; help stakeholders understand their role, and set goals and priorities. The national strategy should integrate security fundamentals (such as raising awareness) and emphasize cooperative relationships among national stakeholders. The national strategy can also serve as a backdrop for the creation of laws that relate to areas such as computer crime, the protection of intellectual property, and privacy. The goals that a nation identifies and promotes through its strategy align the program to a consistent vision and establish a clear direction for the efforts of the program. The strategy should include sufficient detail to allow stakeholders—including the National CSIRT—to understand the stated goals and evaluate their progress toward achieving them. Finally, the national strategy should

reconcile the need for security with the rights of citizens, as well as national values and norms.

The National CSIRT should be deliberately aligned with national cyber security strategic goals to ensure that its work contributes to achieving them. While establishing a national strategy is the first step, doing so may not always be feasible. Getting a large number of stakeholders to agree on a strategy can be difficult. Alternatively, national leaders may judge that the need to establish an incident management capability is more pressing than creating a fully integrated strategy. In these cases, creating an effective strategy may occur concomitantly with building incident management capability. Regardless, the National CSIRT sponsor or proponent should work with the government to consider national needs and priorities throughout the process of building a National CSIRT.

India's approach to cyber security has so far been ad hoc and piecemeal. A number of organisations have been created but their precise roles have not been defined nor synergy has been created among them. As it transcends a vast domain, this falls within the charter of the NSCS. However, there appears to be no institutional structure for implementation of policies. Neither the private sector nor government has been able to build information systems that can be described as reasonably robust. There has not been enough thinking on the implications of cyber warfare.

Meanwhile, many countries are seriously engaged in attending to their cyber security doctrines and strategies. The US, Russia, UK, France, Australia, Germany, New Zealand, South Korea, China, Brazil, South Africa, Denmark, Sweden, EU, Singapore, Malaysia – the list is long and growing – are actively engaged in ensuring a safe and secure cyber environment for their citizens. The international community is also engaged in a variety of discussions.

NATO has taken the task of creating cyber security institutions in member countries. A group of governmental experts (GGE), set up by the UN Secretary General, gave a report in 2010 on "developments in the field of ICT in the context of international security". The report noted that there was increasing evidence that states were developing ICTs as "instruments of warfare and intelligence, and for political

purposes". To confront challenges in cyberspace, the GGE recommended cooperation among likeminded partners, among states, between states, and between states and civil society and the private sectors.

The strongest countries in terms of cyber military capabilities are the US, China, Russia, the UK and Israel. In the imminent future there is no doubt that countries that do not invest in IT protection will become [or already are] easy targets of criminal elements. On comparison with our enterprising neighbor China, the Indian statistics pales. As per an estimation of the National Security Council, China, with its 1.25 lakh cyber security experts, is a potential challenge to India's cyber security. In humiliating contrast, India has a mere 556 cyber security experts. At stake is India's US$ 2.1 trillion GDP, power grids, telecommunication lines, air traffic control, the banking system and all computer-dependent enterprises.

India and China's cyber security preparedness is a striking study in contrast. India is a reputed information technology-enabled nation while China struggles with its language handicap. India, with a massive 243 million internet users, has digitized its governance, economy and daily life on an industrial scale without paying adequate attention to securitize the digitization plan. In the digital era, national security is inextricably linked with cyber security, but despite being the single biggest supplier of cyber workforce across the world India failed to secure its bandwidth and falters to detect the simplest of cyber crimes, which often leads to devastating consequences.

Key Stakeholders of National Cyber Security

Governments have a multitude of roles and responsibilities to strengthen national cyber security. Their primary role is to define national strategy and provide the policy framework. The policy framework of any government describes the architecture by which national efforts are built and operated. Following that, the government has a responsibility to participate with all stakeholders in efforts to identify, analyze, and mitigate risk. The government also has a key role to play in the arena of international relations and cyber security, particularly in the creation of treaties relating to cyber security and the harmonization of national laws relating to cybercrime.

Executive Branch of the Government

In most nations, the executive branch enforces laws and ensures security. It also may include the military. The executive branch is often the sponsor of the national cyber security program. They ensure that the cyber security program remains viable and has appropriate resources (for example, is authorized, staffed, funded, and so on).

Legislative Branch of the Government

The legislative branch provides effective laws that promote cyber security. Whether through appropriations of resources or funding, legislation that mandates execution of national strategy, privacy or tort laws, or laws that establish criminal behaviors, the legislature must ensure that national cyber security program has necessary support.

The Judiciary

The nation's judiciary and legal institutions provide clarity and consistency in areas of law that can affect cyber security. Privacy law is an example of one of these areas. By working with their global counterparts, the legal community can limit the ability of criminals and other malicious actors to take advantage of differences in legal jurisdictions.

Law Enforcement

Law enforcement ensures that legislation related to cyber security is enforced. Additionally, law enforcement can serve as an important source of intelligence about malicious activity, exploited vulnerabilities, and methods of attack. Sharing this information allows critical infrastructure owners and operators to learn from others' experiences and improve security practices and management. Law enforcement can also enhance cyber security by cooperating with counterparts in other nations on the pursuit and apprehension of international criminal actors.

Intelligence Community

The intelligence community plays an important watch and warning role for technical infrastructure. Intelligence organisations usually monitor various sources for threats and vulnerabilities to a nation's infrastructure. This information should be distilled and provided to the National Computer Security Incident Response Team (National CSIRT) and, where appropriate, to infrastructure owners. This distribution of information helps both groups efficiently anticipate, recognize, and resolve attacks.

Critical Infrastructure Owners and Operators

Critical infrastructure components depend on the nation's economic system and technological sophistication, among other factors. A general definition for critical infrastructure is systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructure owners and operators are important stakeholders in the nation's overall cyber security strategy. Infrastructure operators typically understand how security threats and vulnerabilities affect their sector. This knowledge frequently includes proprietary systems and software, such as Supervisory Control and Data Acquisition Systems (SCADA).

Infrastructure operators also implement security recommendations or mandates created by the national government and other authorities. They must reconcile the need for security with the occasionally contradictory goals of efficiency and profitability. Because of their unique position, infrastructure owners and operators frequently possess valuable information, ranging from the actual software problems and cyber attacks they might experience, to the efficacy of countermeasures or risk mitigation strategies. They are also a primary consumer of information about security vulnerabilities. Because of their practical experience implementing security standards and complying with the law, owners and operators may have valuable input into the development of effective, realistic rulemaking and legislation.

Vendors

Vendors of information technologies and services contribute to national cyber security through development practices and ongoing vulnerability reduction efforts. Vendors are often the source of vulnerability information; they ensure that users have up-to-date information and technical solutions to mitigate known vulnerabilities. Ideally, vendors will cooperate with National CSIRTs and extend the analytical and problem-solving capabilities the National CSIRT needs to conduct incident response. Information sharing among vendors, their major customers, and the National CSIRT can create partner relationships that continuously improve security.

Academia

Educational institutions play a key role in developing the human capital and technical skills needed to solve complex problems, such as aspects of cyber security. Academics conduct research that enhances the technical, legal, and policy aspects of cyber security. In many countries, educational institutions have championed and hosted National CSIRTs.

Foreign Governments

Nations have a shared interest in mitigating cyber risk and working together to respond to incidents. Partnerships should be established to discuss global risk and interdependence as well as economic, political, and infrastructure concerns. Countries aligned with one another can exchange valuable intelligence and promote regional cyber prevention and preparedness.

Citizens

The citizens of a nation have a stake in the reliable performance of a nation's strategy for cyber security and are an inherent part of that strategy.

Cyber Security Actors in India

The draft cyber security policy document put out by the Department of Information Technology (DIT) for public discussion is an important step but it is essentially a departmental effort, not taking a whole- of-government approach. DIT does not have jurisdiction over departments.

The document lists a number of major stakeholders, including:

(1) National Information Board (NIB);

(2) National Crisis Management Committee (NCMC);

(3) National Security Council Secretariat (NSCS);

(4) Ministry of Home Affairs (MHA);

(5) Ministry of Defence (MoD);

(6) Department of Information Technology (DIT);

(7) Department of Telecommunications (DoT);

(8) National Cyber Response Centre (NCRC);

(9) CERT-In; (Computer Emergency Response Team – India)

(10) National Information Infrastructure Protection Centre (NIIPC);

(11) National Disaster Management Authority (NDMA);

(12) Standardisation, Testing and Quality Certification (STQC) Directorate;

(13) Sectoral CERTs.

However, only CERT-In is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security. The Act also provided for a national nodal agency for protection of CII but it is not clear whether such an organisation exists other than on paper; NDMA and some others play only a peripheral role; and

many of the sectoral CERTs are yet to come up. In the meantime, real oversight over cyber security is to be distributed amongst the Ministries of Communication and Technology, Home Affairs and Defence, and the office of the NSA.

Recently, Government of India has combined both the DIT and DoT and created a new department namely Department of electronics and information technology (DeitY). This department now oversees all the affairs regarding cyber security policy in India.

Cyber Security Strategy in India

The following is the strategy followed by Government of India with regard to policy:

Security Policy, Compliance and Assurance – Legal Framework

- National Cyber Security Policy (NCSP) 2013
- IT Act, 2000
- IT (Amendment) Bill, 2006 – Data Protection & Computer crimes
- Best Practice ISO 27001
- Security Assurance Framework- IT/ITES/BPO Companies

Security Incident – Early Warning & Response

- CERT-In National Cyber Alert System
- Information Exchange with international CERTs

Capacity building

- Skill & Competence development
- Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
- Training in the area of implementing information security in collaboration with Specialised Organisations in US

Setting up Digital Forensics Centres

- Domain Specific training – Cyber Forensics
- Research and Development
- Network Monitoring
- Biometric Authentication
- Network Security
- International Collaboration

It is interesting to analyse NCSP from market driven versus regulatory approach. The policy conveys that the government is taking a combination of both the approaches – market and regulatory driven. For instance, the policy on one hand mentions encouraging organisations to designate Chief Information Security Officer, (CISO) to develop information security policies, adopt guidelines for procurement of trustworthy ICT products and services, earmarking of specific budget for security and goes to the extent of providing fiscal schemes and incentives to encourage organisations for strengthening information infrastructure with respect to cyber security. It encourages 'all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures.' But on the other hand, the policy mentions 'mandatory periodic audit and evaluation of the adequacy and effectives of security of information infrastructure, as may be appropriate.' The policy does not however specify which 'information infrastructure' and is subject to further clarification. However, if one analyses other sections of the policy, and relates them with the above mentioned, one may reach the conclusion that the intention of the policy is to mandate security measures for e-governance services and critical information infrastructure. (DSCI Report)

The policy also 'mandates implementation of global security best practices, business continuity management and cyber crisis management plan for all e-governance initiatives'. The same has been mandated for critical sector entities in addition to 'encouraging and mandating as appropriate, the use of validated and certified IT products', 'mandating security audit of critical information infrastructure on periodic basis' and 'secure application / software development process' and goes to the extent of 'mandating certification for all security roles.' The policy, however, does not specify the critical information infrastructure, though the DeitY has enlisted critical

sectors as Defence, Finance, Energy, Transportation and Telecommunications. It is important to explicitly identify the critical information infrastructure. The provisions, which are mandatory in the policy, need deeper analysis based on the experience of other countries and the Indian context. For E.g. US had to withdraw the cyber security bill, which mandated security standards in the wake of industry finding it difficult and costly to implement. In the process, they lost time in making their critical information infrastructure more secure.

Too much of government intervention through regulations can also undermine business innovation; it can make it uncompetitive. The better approach would be to incentivize the private sector to invest in security beyond what is required by business requirements through appropriate instruments such as the government funding, tax reliefs, awards & recognition, liability protection, cyber insurance, etc. Only when such market driven approach fails, should the government think of bringing lightweight legislation for critical information infrastructure protection that is developed in partnership with the industry.

Another focus area of the NCSP is indigenous development of cyber security products through cutting edge R&D. The policy direction to work with the industry through joint R&D projects and setting up Centers of Excellence is a step towards greater Public Private Participation (PPP). However, the key objective of developing indigenous security technologies is to enhance security levels especially to address national security concerns. This objective is in line with the Triad Policies of the government on Electronics, IT and Telecommunications. In the Securing Our Cyber Frontiers report it has been emphasized that India should be able to mitigate security risks arising from procurement of ICT products, especially from foreign vendors, and yet take full benefits from the global supply chain that includes access to world class products, services and expertise at competitive prices. Giving preference to indigenous products for national security reasons may not be the right policy direction, primarily for two reasons – Firstly, deploying domestically developed products may not necessarily reduce the supply chain risks, since these need to be tested globally in real life environment. Secondly, if other countries take such an approach to this problem, it will adversely impact India's outsourcing industry, which will be set to lose out to domestic companies in such countries. Therefore, to

effectively address such risks without affecting business competitiveness and country's image as a promoter of global trade & market, India should build its capacity to mitigate ICT supply chain risks.

The focus should be on building testing infrastructure and facilities for IT security product evaluation. The infrastructure should be rolled out on priority in PPP mode. Work is already underway to conceptualize this project under the JWG at National Security Council Secretariat (NSCS). The focus on developing indigenous products must be there but for the reasons of economic growth, targeting the global security market, and not solely driven by national security concerns.

International Cooperation and Advocacy is one of the key dimensions of any country's cyber security strategy or policy as no nation can secure itself in isolation - cyberspace is without boundaries, cutting across multiple jurisdictions. The NCSP does have provisions to facilitate information sharing and cooperation with other countries by developing bilateral and multilateral relationships, however, these statements do not seem to fully establish the leadership role that India, as a large economy, huge domestic IT market, preferred IT supplier and third largest internet base, should play in the international arena. India needs to take leadership in a variety of areas in cyber security including development of international security standards, protection profiles for testing of ICT products, cyber security norms and conventions, solutions to the issues of Internet governance, among many others. A separate strategy, similar to other strategies enlisted in the policy, supported by requisite activities could have been articulated to give more prominence to international cooperation and advocacy.

The revelation of PRISM program in the US has reignited global debate on national security versus right to privacy. Many governments' programs for national security and cyber security raise privacy concerns. It is the responsibility of the governments to assuage such concerns by establishing adequate safeguards for protecting privacy. In this context it is appreciable that one of the objectives of NCSP is to enable safeguarding of privacy of citizen's data, even though no specific strategy or activity to achieve this objective has been mentioned in the policy.

India started a process of economic liberalization in the 1990s. One of the main features of this process has been to simplify rules and regulations to attract foreign investment. As a result of this, India is becoming easier to enter from a regulatory and commercial point of view but there are still issues to overcome, one of them being Indian privacy standards for the outsourcing company. India lacks specific laws on privacy and data protection, how ever; there are proxy laws and other indirect safeguards, which provide adequate protection to companies off shoring work (Yadav & Priyadarshini 2008).

Indian IT act in conjunction with other related acts provide basic legal framework. One of the biggest drawbacks to securing cyberspace in the Indian context is the lack of adequate data. Whatever data is available does not adequately convey the full picture, or worse, can be misleading. Skewed data also results in skewed priorities; the continued highlighting of website hackings leads to a great deal of time being spent on securing government websites, irrespective of their importance, at a time when greater attention should be paid to other facets of cyber security such as securing critical infrastructure or auditing the cyber security preparedness of companies in critical sectors. To illustrate, according to the annual report of the National Crime Records Bureau, cyber-related crimes were a mere 1,322 in 2010, making up 0.19 per cent of all crimes in the country.

At the same time, according to figures from the Reserve Bank of India as recently reported to Parliament, the total amount involved in cases of financial fraud over the Internet in 2011 was Rs.787.39 lakh or US $1.6 million. Finally, according to the Computer Emergency Response Team-India (CERT-In), 13,301 security incidents were reported to it in 2011. While these indices have been monitored over the past few years and provide a general idea of the upward trend in cyber-related incidents, they do not lend themselves easily to further analysis in the absence of more detailed data.

For instance, in the case of financial fraud, it would be useful to know whether these were perpetrated by exploiting technical vulnerabilities or through other means such as social engineering, or by a combination of the two. The absence of more precise figures creates an information gap between the various stakeholders, be it the

government, the various service providers primarily in the private sector, and the end users of these services. Much of the data lies with different organisations and is not available in the public domain. With cyber infrastructure and data largely in the hands of the private sector, there needs to be much more by way of standardisation and sharing of data between the government and the private critical information infrastructure companies such as the Internet Service Providers.

Cyber Regulatory Laws

- Indian Telegraph Act 1885
- Information Technology Act 2000
- Information Technology (Amendment) Act 2008
- Indian Penal Code + Criminal Procedure Code

Cyber Security Market Size

The cyber security market in India was estimated to be around USD 252 million in 2012, with a year-on-year growth rate of 20-30 percent and a Compound Annual Growth Rate (CAGR) of 16.4 percent from 2012- 2017. It is expected to reach USD 529 million in 2017. Some of the major drivers of the industry include a rise in the use of IT enabled services, improved internet penetration and the awareness of SMBs on the importance of investing in IT security in order to protect data.

According to a survey report by security vendor Symantec, SMBs have become alert about the installation of IT security programs that are more than basic antivirus solutions. The survey further revealed that 67 percent of the SMBs in India consider data loss to be a major concern; 60 percent referred to cyber crime as a potential business risk. Thus, the report clearly indicates that IT security has become the top IT priority for large enterprises and as well as for SMBs.

Security solutions such as antivirus and firewalls are not fool proof against data theft or cyber crime. Hence, there has been a considerable change in the way IT services are being used by enterprises. This has led to changes in the demand for security

solutions. The use of virtualization and cloud computing has replaced network gateways.

Regulatory norms are driving the adoption of security solutions in India, as it is mandatory for the Indian outsourcing industry to abide by regulations such as the Sarbanes Oxley Act and the Health Insurance Portability and Accountability Act (HIPPA). The Reserve Bank of India has also put in place strict norms for scheduled commercial banks on the issue of data security. This has led to higher adoption of security solutions in the banking domain, which has largely contributed to the growth of the country's IT security market.

According to a report by industry experts, the banking and the financial services, market (BFSM) is the largest user of cyber security solutions in India. This segment accounts for 36 percent of the country's total cyber security. The report further states that the SMB segment is the fastest growing segment in the adoption of security solutions. The rise in spending by SMBs is based on basic cyber security solutions such as firewalls, antivirus, protection for a Virtual Private Network (VPN); major domain to communicate through a dedicated server to corporate network.

The Indian cyber security market has huge opportunities for further investment as more and more enterprises become aware of the potential threat of data theft. These organisations are increasingly spending a major chunk of their budgetary allocation on IT security solutions.

Market Trend/Analysis

What are the opportunities and challenges that such a situation presents to nations like India? To analyse these aspects, it is important to understand the key trends in emerging technologies and how they impact the security scenario in cyber space.

Internet Mobility

The most important phenomenon that is driving the expansion in the usage of Internet worldwide is mobility. The advent of mobile devices has brought an unprecedented number of users online, and has consequently increased the risks associated with

cyberspace as many of the mobile and tablet users may be first time users of Internet and may not be skilled enough to understand the risks. An expansion in the usage of smartphones and tablets has also brought into focus the security of the operating systems and applications that run on them. As the usage expands, so will the attempts by hackers to break into these devices and steal sensitive personal and corporate information. While this poses challenges for the device manufacturers and OS developers, it presents great opportunities for Indian firms working in the mobility domain. As India is known for its prowess in software development, developing security solutions and secure applications for the mobile world is an unprecedented opportunity globally that is just waiting to be grabbed.

Cloud Platform

The second important technology trend that is driving the ICT industry is the emergence of the cloud platform. While this phenomenon emerged a few years ago, it is only now maturing and cloud based solutions are being deployed across a number of domains in business, industry and government. Ensuring proper security of applications and data on the cloud is a major challenge and its entire implications are still not clear. Even a few cloud failures can result in massive breaches in security and devastating loss of data for the users. As the cloud encompasses the entire gamut of infrastructure, platform, and software as services, developing security solutions for this platform presents the Indian industry with an outstanding opportunity globally. A related segment which also presents great opportunities is data centre operations and management. Another related phenomenon is the emergence of security as a service on the cloud. This space offers good opportunities for Indian firms.

Multiple Authentications

The third important trend that has recently emerged is the use of multi-factor authentication to improve security. Just a simple password is not enough to ensure access to a host of applications and services in areas such as banking, insurance, financial transactions and government services. In India, an Aadhaar based biometric authentication has emerged as a new mechanism to authenticate the identity of users.

This presents an excellent opportunity for Indian industry to develop applications in this domain and address security concerns.

Morphing

The fourth trend impacting on cyber security globally is the continuous morphing of hacker groups and individuals to maintain their anonymity. This poses serious challenges for organisations and government agencies trying to secure cyberspace, as the attacks cannot be attributed to any specific entity. However, this situation also presents opportunities to continuously evolve technologies that can help in unmasking the identity of these anonymous attackers. Active cooperation amongst government agencies and organisations internationally is required to achieve the desired objectives in this area. Agencies such as the United Nations are active and the issue of global cyber security is likely to come up at the 68th session of the UN General Assembly in September 2013.

Intrusion by State Actors

The fifth trend that is impacting the cyber security scenario is the increasing involvement of state actors in cyber war aimed at crippling the information and communication infrastructure of their targeted countries and crippling their social, economic, government and military activities. There is enough evidence of involvement of state actors in several recent incidents of cyber attacks. Stuxnet is a case in point. It presents a serious challenge for countries like India, surrounded by several inimical neighbours. However, this also presents the country with a big opportunity to develop solutions to secure its ICT infrastructure and cyber assets.

Privacy & Confidentiality

The sixth emerging trend is the related issue of ensuring privacy and confidentiality of information pertaining to individuals and businesses. One of the motivations for cyber attacks is to gain access to or steal information that has commercial value or that helps

the attackers to commit fraud with that information. To protect privacy, effective laws and regulations need to be put in place to ensure what data can be used and shared and for what purpose. It also has a bearing on where the data can be stored in servers. This is already a major concern in some domains such as healthcare, where privacy and security concerns about hosting and sharing health data are significant. As India is the world leader in IT services outsourcing business, it offers a big opportunity for the Indian government to put in place effective policies to assure the international community that the country respects the concerns on privacy and confidentiality of data. Indian industry should exploit this opportunity to get a bigger share of the worldwide market in IT and IT enabled services.

International Co-operation

Lastly, there is a greater effort being made internationally at the multilateral level to address global concerns on cyber security. Recently, the international Group of Governmental Experts, representing 15 countries including India, has submitted a report to the United Nations secretary general on enhancing cyber security globally. International cooperation in cyber security presents great opportunities for India to spearhead and lead the efforts to build a global consensus around the approaches to address the issues. It would also open up tremendous opportunities for Indian industry to develop and showcase its capabilities to offer technical solutions to deal with the threats.

The National Informatics Centre (NIC) was set up as early as 1975 with the goal of providing IT solutions to the government. Between 1986 and 1988, three NWs were set up: INDONET, connecting the IBM mainframe installations that made up India's computer infrastructure; NICNET (the NIC Network), being a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), to serve the academic and research communities.

Growth Trends

Policies such as the New Internet Policy of 1998 paved the way for multiple Internet service providers (ISPs) and saw the Internet user base grow from 1.4 million in 1999 to over 15 million by 2003. Though the rate of growth has slowed subsequently, with Internet users now approximately numbering 100 million, exponential growth is again expected as Internet access increasingly shifts to mobile phones and tablets, with the government making a determined push to increase broadband penetration from its present level of about 6%. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

Despite the low numbers in relation to the population, Indians have been active users of the Internet across various segments. The two top email providers, Gmail and Yahoo, had over 34 million users registered from India.[3] Similar figures have also been seen in the social networking arena, which is the most recent entrant to the cyber platform. India currently has the fastest growing user base for Facebook and Twitter, the two top social networking sites. An indication of the rapid pace of adaptation to the Internet in India is that Indian Railways, India's top e-commerce retailer, saw its online sales go up from 19 million tickets in 2008 to 44 million in 2009, with a value of Rs. 3800 crore ($875 million)

As in most countries around the world, the cyber security scenario in India is one of relative chaos and a sense of insecurity arising out of the periodic reports of cyber espionage, cyber terrorism, cyber warfare and cyber crime. The complexity of the issue has resulted in a virtual paralysis. Legal and law enforcement mechanisms have not shifted gears fast enough to grapple with growing cyber crime. Periodic newspaper reports indicate that a wide variety of offensive measures are being contemplated by various agencies, but that is all. The lack of a coherent cyber security policy will seriously interfere with India's national security and economic development.

It is essential that more attention at the highest levels be paid to ensure that cyber-related vulnerabilities that can impact on critical sectors are identified and removed. A coherent and comprehensive cyber security policy will have several major elements, including accurate conceptualisation of cyberspace threats; building of robust

cyberspace through a variety of measures, including technical, legal, diplomatic, international cooperation; creation of adequate organisational structures; strengthening of PPPs; HR development; and implementation of best practices and guidelines. The list is only illustrative.

The government has done a commendable job by bringing a comprehensive cyber security policy. The road ahead in terms of defining the implementation plan will be an arduous task. The due diligence for defining the plan must take into consideration the possible implications – positive and negative both - of each policy statement. So, for instance, the impact of mandating stringent security measures on critical sectors that are not mature in security implementations, or implications of mandating procurement of verified IT products without having adequate testing facilities (resulting in procurement delays or adversely affecting 'go to market' strategy of products) must be considered when drafting the action plan for effective implementation.

The policy is expected to boost the cyber security products and services market in India, providing significant opportunities to security product and services companies and auditing firms. It is also likely to give impetus to the domestic security industry esp. the start-ups offering niche and innovative security products. The policy items once implemented would create direct and indirect jobs as many new infrastructures such as training institutes, testing labs, centers of excellence, R&D projects, sectoral CERTs, among others would be established.

Overall, the policy implementation can be expected to contribute positively to the economic growth of the country, but this contribution should not come at the cost of policy becoming a hurdle for businesses and that too without necessarily improving or strengthening security posture. To avoid such risks, a well thought out implementation plan that is practical and relevant, which balances the desired goals and on ground realities and takes into account the interests of concerned stakeholders including the industry will be crucial. Further, the policy implementation plan must take cognizance of existing initiatives undertaken or being planned by different entities including government agencies and industry and take a cohesive and collaborative approach to achieve desired outcomes and avoid duplication of efforts.

Core Issues

Cyber-security issues are challenging for academics more generally. Experts of all sorts widely disagree how likely future cyber-doom scenarios are – and all of their claims are based on (educated) guesses. While there is at least proof and experience of cyber-crime, cyber-espionage or other lesser forms of cyber-incidents on a daily basis, cyber-incidents of bigger proportions (cyber-terror or cyber-war) exist solely in the form of stories or narratives. The way one imagines them influences our judgment of their likelihood; and there are an infinite number of ways in how one could imagine them. Therefore, there is no way to study the "actual" level of cyber-risk in any sound way, because it only exists in and through the representations of various actors in the political domain. As a consequence, the focus of research necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat.

In India, the government is in the process of making a cyber security policy and establishing an elaborate cyber security infrastructure. Public-private partnership (PPP) is being preferred. Yet, Indian cyber space, which is growing at a rapid pace, is insecure and highly vulnerable, as the spate of recent cyber attacks has shown. A Computer Emergency Response Team (CERT) India, functioning since 2004, is the lone institution generating some awareness about cyber security. Unfortunately, the institution is under funded and under resourced.

Cyber security effort is fragmented with little coordination among myriads of institutions. The National Technical Research Organisation (NTRO), mainly for the sensitive agencies, does some work on cyber security. Given the scale of the problem, this seems insufficient. There is no clarity on how to deal with cyber warfare issues. What should be India's approach on cyber security? It should take cyber attacks extremely seriously and urgently build its defensive technical and legal capabilities. At the same time it should have deterrent capabilities to deter hackers from attacking its cyber space. It should also consider setting up a cyber command type of structure in the armed forces and incorporate cyber conflict in its military doctrines.

India needs to ensure its national interests are protected during cyber security negotiations. It has yet to take firm position on issues such as the rules of the road, state behaviour in cyber space, confidence building measures, application of the law of the armed conflict to cyber conflicts and cyber weapons. It must strike a balance between open, insecure internet and an overregulated an over protected cyber space. These issues must be debated so that a societal consensus can emerge.

Prerequisite Strategic Approach

Consistent with need, the primary objectives for securing country's cyber space are:

- Preventing cyber attacks against the country's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimise damage and recovery time from cyber attacks

Actions to secure cyberspace include:

- Forensics and attack attribution
- Protection of networks and systems critical to national security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- Research and technology development that will enable the critical infrastructure organisations to secure their IT assets

To pursue the strategic objectives the following major initiatives identified need to be comprehensively prepared:

- Security Policy, Compliance and Assurance
- Security Incident - Early Warning & Response
- Security Training - Skills/competence development & user end awareness.
- Security R&D - For Securing the Infrastructure, meeting the domain specific needs and enabling technologies
- Security - Publicity & Promotion

Security Policy, Compliance and Assurance

Focus: Creation, Establishment and operation of Cyber Security Assurance Framework aimed at enabling Government, Critical Infrastructure Organisations and other key IT users of nation's economy

(a) Critical Information Infrastructure Protection

Many of the critical services that are essential to the well being of the economy are increasingly becoming dependent on IT. As such, the Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organisations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include Defence, Finance, Energy, Transportation and Telecommunications. Consequently, many in the industry and critical infrastructure organisations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices.

(b) Cyber Security Assurance Framework

Cyber Security Assurance Framework is a National framework for "Cyber Security Assurance" to assist National level efforts in protecting critical information infrastructure. It aims to cater to the security assurance needs of Government and critical infrastructure organisations through "Enabling and Endorsing" actions.

Enabling actions are essentially Promotional/Advisory/Regulatory in nature and are best done by Govt. or its authorized entity that can be seen and perceived as independent of bias and/or commercial interests. They involve publication of "National Security Policy Compliance requirements" and IT security guidelines and supporting documents to facilitate IT security implementation and compliance.

Endorsing actions are essentially commercial in nature and may involve more than one service provider offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include:

- Assessment and certification of compliance to IT security best practices, standards and guidelines (Example. ISO 27001/BS 7799 ISMS certification, IS system audits etc.)
- IT Security product evaluation and certification as per 'Common Criteria' standard ISO 15408 and Crypto module verification standards
- IT security manpower training and other services to assist user in IT security implementation and compliance

(c) Trusted company certification

With India emerging as a leading outsourcing partner, there is a need to address perceptible gap among Indian IT/ITES/BPOs in respect of compliance to international standards and best practices on security and privacy. Today, although increasing number of organisations in India have aligned their internal processes and practices to international standards such as ISO 9000, CMM, Six Sigma, Total Quality Management, ISO 27001 etc., it is to be noted that existing models such as SEI CMM levels cover exclusively software development processes and do not address security issues. As such, there is a need for a comprehensive assurance framework that can enable compliance within the country and provide assurance on compliance to out sourcing organisations and rest of the world. Accordingly, efforts are on to create a model that is based on self-certification concept and on the lines of Software capability maturity model (SW-CMM) of CMU, USA.

Security Incident - Early Warning & Response

Focus: Creation of National Cyber Alert System for Rapid identification & response to security incidents and information exchange to reduce the risk of cyber threat and resultant effects.

a) *Rapid Identification, Information Exchange, and Remediation*

These can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Because no cyber security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and have the resilience to restore full operations in their wake. The National Cyber Alert System will involve critical infrastructure organisations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

(b) Essential Actions under National Cyber Alert System

- Identification of focal points in the critical infrastructure
- Establish a public-private architecture for responding to national level cyber incidents
- Tactical and strategic analysis of cyber attacks and vulnerability assessments;
- Expand the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspace security;
- Improve national incident response capabilities (CERT-In and Sectoral CERTs)
- Exercise cyber security continuity plans and drills

(c) Creation and Augmentation of Response Capabilities

I. Augmentation of CERT-In:

CERT-In is operational since January 2004 and is catering to the security needs of Indian Cyber community, especially the Critical Information Infrastructure. In line with the expectation of the user community and various stake holders, there is a need

to augment the facilities at CERT-In in terms of Manpower, Communication systems, tools, etc. for vulnerability prediction, analysis & mitigation, Cyber forensics/artifact analysis, Cyber space monitoring & interception Capabilities and Critical information infrastructure Security health check. The National Information Board and National Security Council have endorsed the need for augmentation of facilities at CERT-In.

II. Creation/augmentation of Sectoral CERTs:

For an effective National Cyber Security Alert System, there is a need to create sectoral CERTs to cater to the very specific domain needs of different sectors. In this direction, Army, Air force and Navy have established sectoral CERTs in Defense sector, IDRBT in Finance sector. However, the facilities of these sectoral CERTs are at primitive levels and need to be augmented to meet the needs of respective sectors. Similarity sectoral CERTs with state-of-the-art facilities need to be created in other critical sectors such as Aviation, Energy, Telecommunication, and Railways etc.

(d) International Cooperation and Information Sharing

The cyber threat sources and attacks span across countries. As such as there is a need to enhanced global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly it is vital to have well developed Cyber Security and Information Assurance research and development programme which is executed through different government agencies in broad collaboration with private sectors, partners and stakeholders in academia, national and international agencies.

In this context the priorities for collaboration are:

- Cyber Security and Information Assurance Technology to prevent, protect against, detecting, responding, and recovering from cyber attacks in critical information infrastructure that may have large-scale consequences.
- Collaboration for training personnel in implementing and monitoring secure government intranets and cyber space
- Joint R&D projects in the area of Steganography, water marking of

documents, security of next generation networks and Cyber Forensics

- Coordination in early warning, threat & vulnerability analysis and incident tracking
- Cyber security drills/exercises to test the vulnerability & preparedness of critical sectors

Security Training - Security, Digital Evidence & Forensics

Focus - To meet the specific needs of Law Enforcement, Judiciary and other users such as E-Governance project owners catering for

- *A baseline for IT Security awareness*
- *Skill & Competence development*
- *Advanced Manpower Certification programmes*

Many cyber vulnerabilities exist because of lack of cyber security awareness on the part of computer users, system/network administrators, technology developers, auditors, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Corporates. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities. The following strategy has been identified for major actions and initiatives for user awareness, education, and training:

- Promote a comprehensive national awareness program
- Foster adequate training and education programs to support the Nation's cyber security needs
- Increase the efficiency of existing cyber security training programs and devise domain specific training programs (ex: Law Enforcement, Judiciary, E-Governance etc.)
- Promote private-sector support for well-coordinated, widely recognized professional cyber security certifications.

Security R&D

Focus: Facilitating Basic research, Technology demonstration and Proof-of concept and R&D test bed projects

Indigenous R&D is an essential component of national information security measures due to various reasons- a major one being export restrictions on sophisticated products by advanced countries. Second major reason for undertaking R&D is to build confidence that an imported IT security product itself does not turn out to be a veiled security threat. Other benefits include creation of knowledge and expertise to face new and emerging security challenges, to produce cost-effective, tailor-made indigenous security solutions and even compete for export market in information security products and services. Success in technological innovation is significantly facilitated by a sound S&T environment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Private sector is expected to play a key role in meeting needs of short term R&D leading to commercially viable products. Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading research organisations.

Privacy

A report titled "Report of the Group of Experts on Privacy " chaired by Justice A P Shah proposed the following five salient features of a framework in the contect of privacy:

Technological Neutrality & Interoperability with International Standards

> The Group agreed that any proposed framework for privacy legislation must be technologically neutral and interoperable with international standards. Specifically, the Privacy Act should not make any reference to specific technologies and must be generic enough such that the principles and enforcement mechanisms remain adaptable to changes in society, the

marketplace, technology, and the government. To do this it is important to closely harmonise the right to privacy with multiple international regimes, create trust and facilitate co-operation between national and international stakeholders and provide equal and adequate levels of protection to data processed inside India as well as outside it. In doing so, the framework should recognise that data has economic value, and that global data flows generate value for the individual as data creator, and for businesses that collect and process such data. Thus, one of the focuses of the framework should be on inspiring the trust of global clients and their end users, without compromising the interests of domestic customers in enhancing their privacy protection.

Multi-Dimensional Privacy

This report recognises the right to privacy in its multiple dimensions. A framework on the right to privacy in India must include privacy-related concerns around data protection on the internet and challenges emerging therefrom, appropriate protection from unauthorised interception, audio and video surveillance, use of personal identifiers, bodily privacy including DNA as well as physical privacy, which are crucial in establishing a national ethos for privacy protection, though the specific forms such protection will take must remain flexible to address new and emerging concerns.

Horizontal Applicability

The Group agreed that any proposed privacy legislation must apply both to the government as well as to the private sector. Given that the international trend is towards a set of unified norms governing both the private and public sector, and both sectors process large amounts of data in India, it is imperative to bring both within the purview of the proposed legislation.

Conformity with Privacy Principles

This report recommends nine fundamental Privacy Principles to form the bedrock of the proposed Privacy Act in India. These principles, drawn from best practices internationally, and adapted suitably to an Indian context, are

intended to provide the baseline level of privacy protection to all individual data subjects. The fundamental philosophy underlining the principles is the need to hold the data controller accountable for the collection, processing and use to which the data is put thereby ensuring that the privacy of the data subject is guaranteed.

Co-Regulatory Enforcement Regime

This report recommends the establishment of the office of the Privacy Commissioner, both at the central and regional levels. The Privacy Commissioners shall be the primary authority for enforcement of the provisions of the Act. However, rather than prescribe a pure top-down approach to enforcement, this report recommends a system of co-regulation, with equal emphasis on Self-Regulating Organisations (SROs) being vested with the responsibility of autonomously ensuring compliance with the Act, subject to regular oversight by the Privacy Commissioners. The SROs, apart from possessing industry-specific knowledge, will also be better placed to create awareness about the right to privacy and explaining the sensitivities of privacy protection both within industry as well as to the public in respective sectors. This recommendation of a co-regulatory regime will not derogate from the powers of courts which will be available as a forum of last resort in case of persistent and unresolved violations of the Privacy Act.

Key Objectives of NCSP

The Ministry of Communications and Information Technology (MoCIT) has notified the National Cyber Security Policy 2013 (NCSP). The NCSP underscores the need for the creation of a secure computing environment and generating adequate trust in online systems and networks.

As per the latest notification key objectives of the policy are:

- To create a secure cyber ecosystem and build adequate confidence in IT systems and transactions.
- To strengthen the regulatory framework for ensuring secure cyber ecosystem.
- To create and enhance mechanisms for monitoring and resolving cyber

security threats.

- To enhance the protection and resilience of the nation's critical information infrastructure.
- To create a workforce of five lakh specialists in cyber security over the next five years. To achieve these objectives, the NCSP proposes to implement following strategies:
- Establish a round-the-clock National Level Computer Emergency Response Team as the designated national nodal agency for coordination on cyber security, supported by round-the-clock Sectoral Level Computer Emergency Response Teams.
- Implement a Cyber Crisis Management Plan to deal with incidents impacting critical processes, public safety or national security.
- Encourage all public and private organisations to appoint Chief Information Security Officers and implement information security policies.
- Develop a dynamic legal framework with provisions for periodic review and harmonisation with international frameworks.
- Mandate periodic audit and evaluation of information infrastructure security.
- Establish cyber security training infrastructure through public private partnerships.
- Establish institutional mechanisms for capacity building of law enforcement agencies.

India's Cyber Preparedness

To guarantee and retain information superiority, appropriate defensive measures and countermeasures are a must. While the debate on the exact definition of critical information infrastructure (CII) rallies on, the IT (Amendment) Bill 2008 attributes the designation of a national nodal agency for the protection of CII and the Indian Computer Emergency Response Team (CERT-In) to undertake incidence response under the Sections 70A and 70B, respectively.11 MoD also mandates Defence agency Information Assurance and Research Agency (DIARA) as the nodal cyber security for the Tri-Services.12 However, substantive resolution is needed on the role imparted to the National Informatics Centre (NIC), the IT infrastructure services organisation managing a majority of the government websites. A government-wide information

security and regulatory compliance policy, dealing with issues like electronic document classification, compartmentalisation and centralised security clearance, is also the need the hour.

Any attempt to arrive at a possible solution to the aforementioned issues from a geopolitical, strategic affairs and policy making perspective will need a holistic approach taking into account the technical, legal and international complexities. India's National Security Advisor proposed the ratification of a global cyber-security regime or a cyber-arms control treaty.13 Similar endeavours of international regulation in domains like chemical, nuclear and space warfare have been impactful. The primary stakeholders are even receptive to the idea of re-engineering the underlying communication protocols of the Internet to reach a level of moderation. While most nations, including those engaged in questionable activities over this medium sounded amenable, the talks have broken down repeatedly.

In this scenario, the responsibility of honing the discourse lands on the shoulders of able policy makers, strategic affairs analysts and geopolitical experts who can go to the depths of the problem and evangelise to the international security community with a fervent zeal. However, there exists a great chasm between the technical security professionals and high- level interlocutors. The special interest groups on information warfare and cyber-security lack the contribution of technologists with hands-on exposure, thus succumbing to misdirection and confusion. It is imperative that we inculcate in the thought process of contemporary policy makers the multifaceted views of such professionals.

The question that looms large is whether we can reach a coherent and agreeable consensus on attribution, deterrence and pre-emption of cyber- attacks. While India has made tall strides in order to assert its place in the fifth dimension of war, more awareness and seamless initiative is needed. Mere wishful thinking of being the next cyber-power would not take India too far. One must always keep in mind that hacking has its origins as a counter cultural movement preaching fierce individualism, full disclosure and an emphasis on breaking things. The very act of institutionalisation is an antithesis to a domain, which breeds on chaos and anarchy.

India's inertia to induct cyber security as an essential element of national security and growth is tremblingly palpable. Cyber security is less debated, sporadically written about, and rumoured at best in India. Because of this apathy and despite India's grand stature in the cyber world, India is vulnerable to the cyber snarls of China and other countries.

With its archaic governmental architecture, India is still in expansion mode with little time spared on digital security. One of the significant reasons of India's inertia is its lack of understanding and appreciation of the gravity of cyber security. The Ground Zero Summit, which is considered as the Mecca of India's cyber security debate and an earnest endeavor of cyber security professionals, failed to get a single political figure to deliberate on the issue. India is nowhere in the cyber war that has engulfed the globe. India's response to such a critical situation is a timid National Cyber Security Policy that the government circulated in 2013. There is no national overhaul of cyber security and the Indian Computer Emergency Response Team, the statutory body to look after cyber attacks, has little critical strength or capability. Its endeavour to recruit young talent and meaningfully engage them is still to take off.

After the 2013 National Security Council note that exposed India's cyber security unpreparedness, the government decided to augment infrastructure and hire more professionals. However, what is required is a strategic vision to ensure stealth in India's cyber security and a political conviction to plug strategic vulnerabilities. The National Technical Research Organisation has regularly been alerting successive governments about the danger from Chinese cyber attacks. India cannot afford to be passive and unresponsive because if it does not act now, by the time a sophisticated cyber-attack happens, it will probably be too late to defend against it effectively.

India's immediate requirement is to understand the impending cyber security threat from China and build better network filters and early warning devices and add new firewalls around computers that run the Indian economy and regulate vital civil and military installations. However, in any battle the attackers are always embedded with all advantages from choosing the battlefield to deciding the time of war to the choice of instrumentalities. Poor defenders end up defending an attack that they even cannot imagine.

The Institute for Defence Studies and Analyses (IDSA), New Delhi made an exhaustive study of existing state of cyber security affairs in the country. They came out with a task force report, which gives an all-inclusive picture of how matters relating to cyber security are being tackled in the country. The following is the set of recommendations they came up with:

General Recommendations

- In view of the rapidly growing threats to national security in cyberspace, there is urgent need for the government to adopt a cyber security policy. The government should immediately adopt such a policy so that urgent actions in a coordinated fashion can be taken to defend India's economy and society against cyber attacks.
- Cyber security policy will necessarily be an evolving document in view of the changing nature of cyber vulnerabilities, risks and threats. The government will need to review the document periodically.
- Cyber security should be regarded as an integral component of national security. Urgent attention should be given to the issues of cyber crime, cyber terrorism, cyber warfare and CII protection.

Government

- The NSA, through NIB, should be put in charge of formulating and overseeing the implementation of the country's cyber security policy within the ambit of a larger national security policy. This body should be serviced by the NSCS for policy measures and DIT and other departments (e.g. Telecom, space, etc.) for operational measures.
- A Cyber Coordination Centre should be established at the operational level, staffed by personnel from the relevant operational agencies. This centre would serve as a clearing-house, assessing information arriving in real time and assigning responsibilities to the agencies concerned, as and when required.
- MHA should be the nodal agency for handling cyber terrorism. To handle cyber terrorism and cyber crime, a slew of measures will be needed, ranging

from monitoring and surveillance, investigation, prosecution etc. Cyber terrorism should be regarded as a part of the nation's overall counterterrorism capabilities. The National Counter Terrorism Centre being set up should have a strong cyber component. NIB, with MHA as the nodal agency, should be tasked with the responsibility of formulating and implementing a policy to deal with cyber terrorism. The issues of ethical hacking and immunity for defence and intelligence officers should be considered.

- MHA should also be the nodal agency for dealing with cyber crime. In dealing with cyber crime, some of the measures needed will overlap with those required to deal with cyber terrorism but extra effort will be required to ensure greater awareness, strengthening of the legal framework, law enforcement, prosecution, etc. Particular focus should be placed on awareness and enforcement. MHA, in collaboration with DIT and the Law Ministry should make a necessary roadmap in this regard.
- Headquarters IDS should be the nodal agency for preparing the country for cyber warfare in all its dimensions. The necessary structures should be created in a time-bound manner. Since cyberspace is integral there should be an appropriate interface between defence and civilian departments. NIB should smooth out the difficulties.
- NSCS should be given the nodal agency for coordinating the efforts to protect critical infrastructure of the country. This will require identification of the critical infrastructure and formulation and implementation of strategies to ensure protection of each component from cyber attacks.
- DIT should be tasked with creating the necessary cyberspace situational awareness, strengthening PPP, promoting international cooperation, and other residual measures. DIT will necessarily have other nodal agencies. The interface between DIT and other agencies should be smoothed out by the NIB.
- Cyber security education, R&D and training will be an integral part of the national cyber security strategy. The government should set up a well-equipped National Cyber Security R&D Centre to do cutting edge cyber security R&D. This Centre should be a PPP endeavour. Cyber security research should also be encouraged in public and private universities and institutions. DIT could come up with a roadmap for cyber security research in the country. The country's strengths in ICT should be leveraged. DRDO

should conduct specialised research for the armed forces and NTRO should do so for the country's intelligence agencies.

- DIT's CERT should be the nodal agency, much like the Met Department for weather forecasting, to create and share cyberspace situational awareness in the country. DIT should make public awareness of risks, threats and vulnerabilities in cyberspace and how these should be managed.
- Disaster management and recovery must be an integral part of any national cyber security strategy. The DIT should be the nodal agency for such efforts. It should coordinate its efforts with NDMA and also other government departments as well as private bodies.

Specific Recommendations

- There is need to place special emphasis on building adequate technical capabilities in cryptology, digital signatures, testing for malware in embedded systems, operating systems, fabrication of specialised chips for defence and intelligence functions, search engines, artificial intelligence, routers, new materials, SCADA systems, etc. Cyber security should be mandatory in computer science curriculum and even separate programmes on cyber security should be contemplated.
- Emphasis should be placed on developing and implementing standards and best practices in government functioning as well as in the private sector. Cyber security audits should be made compulsory for networked organisations. The standards should be enforced through a combination of regulation and incentives to industry.
- The government should launch a National Mission in Cyber Forensics to facilitate prosecution of cyber criminals and cyber terrorists.
- International cooperation is crucial to handle cyber crime, cyber terrorism and in managing risks in cyberspace. It is necessary to participate in multilateral discussions on rules of behaviour in cyberspace. The government should also consider joining the European Convention on Cyber crime. A 24x7 nodal point for international cooperation with cyber authorities of other countries should be set up. The Indian agencies should also participate in regional fora on cyber security. Engagement of Indian cyber authorities with internationally

renowned cyber professional bodies should be encouraged.

- The impact of the emergence of new social networking media, and convergence of technologies on society including business, economy, national security should be studied with the help of relevant experts, including political scientists, sociologists, anthropologists, psychologists, and law enforcement experts. It should be ensured that the issues of privacy and human rights are not lost sight of and a proper balance between national security imperatives and human rights and privacy is maintained.

Cyber Warfare

- Need to lay down red lines, define objectives and enunciate a doctrine. Flesh out a policy of proactive cyber defence with emphasis on actions taken in anticipation to prevent an attack against computers and NWs.
- Raise a Cyber Command and build up offensive capabilities.
- Create a pool of trained people such as Cyber TA Battalions who can provide "surge capacity" to bolster the country's resources during critical periods or in the event of hostilities
- Study the impact of social NWs with respect to national security and perception management, especially during crisis.

Critical Infrastructure

- Government should initiate a special drive of implementing practices in the critical infrastructure sectors and provide necessary budgetary support for such implementation.
- Develop security expertise for protection of CII by providing hands on training to professionals, especially from the government sector.
- Government should establish a mechanism for measuring preparedness of critical sectors such as security index, which captures preparedness of the sector and assigns value to it. Operationalise the mechanism for routinely monitoring preparedness.
- Government should incorporate IT Supply Chain Security as an important

element of e-security plan to address security issues.

- Government should promote R&D in private industry through active government support for industry-led research projects in the areas of security. Establish enabling mechanisms to facilitate this.
- Government should focus on creating a workforce of security professionals in the country keeping in view the requirements of the future.
- PPP model should be explored for taking security to the regions and industry sectors.
- Strengthening telecom security – one of the key pillars of cyber security, especially through development of standards and establishment of testing labs for telecom infrastructure (equipment, hardware).
- Capacity building in the area of cyber crime and cyber forensics in terms of infrastructure, expertise and availability of HR and cooperation between industry, LEAs and judiciary.

Legal

- Need for trained and qualified experts to deal with the highly specialised field of cyber security. Awareness with regard to the threat to ICT infrastructure needs to be created and the necessary legal provisions to ensure cyber safety must be developed.
- Substantive laws dealing with illegal access, illegal interception, data interference, misuse of devices, computer-related forgery, child pornography, etc. must be implemented.
- Procedural laws need to be in place to achieve cooperation and coordination of international organisations and governments to investigate and prosecute cyber criminals.
- The police must work closely with both governmental and non-governmental agencies, Interpol and the public at large to develop a comprehensive strategy to address the problems.
- Lobbying at an international level for the harmonisation of existing national legislation to ensure that such laws provide a fair measure of deterrence to cyber criminals and cyber terrorists, thereby making cyberspace a safer place

for national and international transactions.

- Government must put in place necessary amendments in existing laws or enact a new legislation like a Data Protection/Privacy Act to safeguard against the misuse of personal information by various government agencies and protect individual privacy.

Miscellaneous

- Examine the impact of cloud computing and wireless technologies and formulate appropriate policies.
- Make it a mandatory requirement for all government organisations and private enterprises to have a designated Chief Information Security Officer (CISO) who would be responsible for cyber security.
- Establishment of a cyber range to test cyber readiness.
- More powers to Sectoral CERTs.
- Establish an online mechanism for cyber crime-related complaints to be recorded.

The IDSA have come out with a comprehensive set of recommendations or the government. The government needs to take their inputs seriously and implement them while preparing the policy bill on national cyber security policy.

Conclusion

Cyber security management in India is a complicated process. It requires both technological expertise and legal compliances. Some developed nations have enacted cyber security regulations but they have outlived their natural lives. The present day cyber security regulations require a techno legal orientation that is a big challenged for legislators around the world.

India has enacted the information technology act, 2000 that governs legal issues of e-commerce, e-governance, cyber crimes, etc. However, techno legal experts believe that Indian laws like IT Act 2000 and telegraph act require urgent repeal and new and

better techno legal laws must be enacted to replaces these laws.

There are no dedicated cyber security laws in India. Indian government has drafted the cyber security policy of India 2013 but the same has not been implemented so far. Further, the policy is also suffering from many shortcomings including lack of privacy and civil liberties protection and absence of cyber security breaches disclosure norms. The cyber security trends of India have also shown poor cyber security preparedness of India to protect its cyberspace and critical infrastructures.

India has still to take care of issues like critical infrastructure protection, cyber warfare policy, cyber terrorism, cyber espionage, e-governance cyber security, e-commerce cyber security, cyber security of banks, etc. Companies and individuals are also required to cyber insure their businesses from cyber threats. Indian government is in the process of formulating a cyber crime prevention strategy. This has come in the wake of a public interest litigation (PIL) filed at the Supreme Court of India that has asked the centre to frame regulations and guidelines for effective investigation of cyber crimes in India. Simultaneously, the cyber crime investigation trainings in India are also needed.

The offensive and defensive cyber security capabilities of India are also required to be developed. A cyber attacks crisis management plan of India must also be formulated to tackle cyber attacks and cyber terrorism against India. The proposed National Cyber Coordination Centre (NCCC) of India is a good initiative regarding strengthening of Indian cyber security capabilities. The National Critical Information Infrastructure Protection Centre (NCIPC) of India would also come handy in protecting Indian cyberspace.

To guarantee and retain information superiority, appropriate defensive measures and countermeasures are a must. While the debate on the exact definition of critical information infrastructure (CII) rallies on, the IT (Amendment) Bill 2008 attributes the designation of a national nodal agency for the protection of CII and the Indian Computer Emergency Response Team (CERT-In) to undertake incidence response.

The ambitious project named Digital India would also require very robust and effective cyber security infrastructure and capabilities on the part of Indian government and its agencies. There is no international cyber security treaty or cyber law treaty that can help in resolving conflict of laws in cyberspace. Even a simple task of obtaining digital information from foreign companies like Google takes months to achieve.

In today's information age, Internet is the engine for global economic growth and the cyber security initiatives of any country should not impede it. Cyber security must be considered as a key enabler for India's economic growth and the government and industry efforts/initiatives should reflect this realization. To establish itself as the knowledge hub of the world, the key imperative for India is to address the cyber security challenges by leveraging the strengths of public and private sectors through public-private partnerships, considering the issue of cyber security at the board level within organisations and taking leadership and partnering with other nations for addressing global concerns in cyber security.