Chapter 1

Setting the Scene

1.1 Preamble

The evolution of technology impacts the nature of conflict and war. Amongst the recent aspects of involving in conflict is "***no contact war***" (NCW) wherein there is no "physical" or "kinetic" action across borders. Operations are conducted in a covert manner using resources such as agents in the information domain to weaken or strike at an adversary to achieve political objectives. These are clouded in ambiguity and deniability. The enemy is unseen and the victim unsure of how and where to react.

Several states are on the way to achieving this capability. Historically speaking, China studied Gulf War I in detail and analysed that it could not defeat the USA with numbers or in technology. It therefore adopted the concept of asymmetric war based on vulnerabilities of the USA in the cyber domain. This was structured around the concept of *"Wangluohua"* – networkisation as a part of unrestricted and asymmetric warfare. Amongst others, a Task Force was created for Information War (IW), four universities set up, hacker groups supported, regular exercises held and IW units raised in 2003. Through a process of cyber espionage, reverse engineering, source-code sharing, manufacture of hardware, supported by a huge human resource (HR) base, China has greatly developed its capacity in this regard to formidable proportions. Unlike any other forms of warfare, there is no convention or ban on sharing of information with respect to the cyber domain. Thus countries which are inimical could put together resources. Additionally, this capability could be shared with terrorist and fundamentalist groups to wreak mayhem on an intended adversary.

As India progresses, its reliance on the Internet will increase[1] at a rapid pace. Globalisation and governance require a wired society. Along with this India's vulnerability to the threat of IW will become greater. This danger must be foreseen and planned for. Failure to do so can result in a catastrophe and severely

---

[1] The number of Internet users increased from 1.4 million in 1998 to 100 million in 2010. Internet penetration during this period rose from 0.1% to 8.5%. Asia Internet Stats.

affect the country's status and international partnerships, especially in the financial sector. To understand the impact of IW a hypothetical situation at the end of this decade is presented here.

1.2 Regional Security Scenario, 2020

The regional situation is uncertain. Relations with China and Pakistan have not seen any major change. The J&K dispute and the boundary issue with China have not been resolved and tension prevails. Pakistan continues to flounder, with an unsettled situation in Afghanistan. India's continued growth in the region of 7 to 9% has generated an increased demand for water, energy resources and raw materials. Competition for resources and global business has grown. Global warming has had adverse environmental and demographic effects.

1.3 Back to the Future: 1997 to 2012

How bad will it be? An indicative answer emerges if we look back 15 years ago, i.e. 1996-97. Vast changes have taken place in this period. The rate and pace has been exponential in every field, whether it is the economy, the telephone revolution, industrial growth, standard of living, left-wing extremism, threat of terrorism, regional instability or the very way in which the government functions. In retrospect, despite the political instability of that period, India in a manner was much safer and insulated. Applying the same escalatory model, the security situation in 2020 is bound to be far more complex and dangerous. The standard of living will go up, however, it will be a more wired society with the e-governance, communication, power and transportation NWs, financial transactions, health and medicine, all dependent on the cyber domain. Alongside will be the aspect of increased transparency and instant dissemination or democratisation of information. All this will also create vulnerabilities and impact on security with disastrous consequences.

1.4 Events of 30 June 2020

It has been a long hot day in a summer of internal and regional tension. At 1900 hours, when everyone is likely to call it a day, Internet traffic has broken down all over. CERT-In sends a message to the National Security Council Secretariat (NSCS) and the National Command Post that *"Large-scale movement of several different zero day malware programs on Internet affecting critical infrastructure."* Copies are sent globally. Soon thereafter come in reports from different ministries, state governments, establishments and institutions all over the country. A scenario of what could happen in isolation, or in combination, in the next few hours, follows.

- ***Telephone NWs Collapse***

BSNL exchanges hang and switching centres of mobile NWs (hardware mostly of Chinese origin) shut down or behave erratically. Defence NW routers are failing and rebooting. Close to 1000 million telephones are functioning erratically,

affecting every aspect of life. Worrisome messages abound. There is panic and uncertainty.

- ***Satellites out of Control***

Communication, remote sensing and surveillance satellites are thrown out of gear. TV and other transmissions are disrupted, spreading alarm. The Indian GPS system, operationalised in 2016, malfunctions, affecting traffic and security systems.

- ***SCADA Systems Controlling Power Grids Collapse***

The whole of North and Western India and some other regions suffer a power blackout. This affects all services, including rail and road traffic. There is chaos on the roads as traffic lights and systems are not working and the police are unable to cope with the rush-hour flow. Reports of accidents and traffic jams come in from all over the country. It also results in looting and police are unable to control the mobs.

- ***ATC Management Collapses***

The international air traffic control (ATC) system, based on communication NWs and the Internet, is malfunctioning. Manual backup systems cannot meet the requirements. There is chaos at airports like Delhi and Mumbai which handle 2000 to 3000 flights a day. There are reports of at least three mid-air collisions from different parts of India. Rumours abound and there is widespread alarm and hysteria.

- ***Railway Traffic Control Collapses***

The complex Indian Railway management and traffic system is clogged. Rail traffic on a number of routes is suspended due to power failure. There are reports of derailments and accidents. The metro and local train systems in major cities are also suffering from chaos.

- ***Oil Refineries***

There are messages of explosions and devastating fires in major refineries with extensive damage and loss of life. Pipelines are ruptured and oil flow is disrupted.

- ***Collapse of Financial Services***

Dedicated denial of service (DDOS) attacks paralyse the financial systems. There is data theft, destruction and clogging. Millions of transactions are distorted. Banks cut off the systems from the Internet. ATM machines across the country hang. There is talk that money has run out with resultant panic.

- ***Collapse of Health and Civic Services***

Health and civic services, dependent heavily on the Internet, collapse. Data in respect of emergency facilities are not available. Coupled with power and communication failures, the situation in hospitals is close to breaking point.

- ***Chemical Plants***

The safety systems of chemical plants, governed by computer systems, fail. Lethal clouds of noxious gases billow, creating panic and deaths.

- ***Defence Forces***

A large tri-service exercise, that has been underway, is in a crucial phase. There is complete dislocation due to failure of communication and GPS systems as also large-scale DDOS attacks. Amongst others:

- Avionics on the latest MMCR aircraft blank out.
- Computer-controlled systems in the C-17 not responding.
- The ANTPQ-37 WLRs go into seizure.
- The newly developed tri-service logistic management system is affected by virus and fails.

1.4.1 Damage and Loss

Millions of Indians have been affected. The loss of lives has been in thousands. Given the reach of the media as also the visibility that any such event would invite, it could, in a few hours constitute a disaster for the country far greater than all the wars and natural catastrophes put together. It would expose India as weak and unprepared, unsafe to live in, an unreliable business partner and vulnerable in every sense of the word. India's credibility as a country would be affected without a shot having been fired in anger. It is difficult to imagine a greater national humiliation.

The other aspect is that there would be no attributability. When investigated, these attacks will appear to have come from all over the globe as also servers within the country. Much as India would like to retaliate, there would be nobody who could be definitely identified. Even if identified, it could be denied.

The foregoing scenario, which is only partial of what could happen, must serve as a wake-up call for urgent measures in this regard.

CHAPTER 2

CYBER SECURITY – AN OVERVIEW

2.1 A COMPLEX ISSUE

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for governments because different domains are typically administered through siloed ministries and departments. The task is made all the more difficult by the inchoate and diffuse nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

The rapidity in the development of information technology (IT) and the relative ease with which applications can be commercialised has seen the use of cyberspace expand dramatically in its brief existence. From its initial avatar as an NW created by academics for the use of the military, it has now become a global social and economic and communications platform.

The increasing centrality of cyberspace to human existence is exemplified by facts and figures brought out recently by the International Telecommunications Union (ITU), according to which the number of Internet users has doubled between 2005 and 2010 and surpasses two billion. Users are connecting through a range of devices from the personal computer (PC) to the mobile phone, and using the Internet for a variety of purposes from communication to e-commerce, to data storage.

The rise in the Internet population 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. While such disruptions are yet to cause permanent or grievous damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Governments are constrained in their responses by pressures exerted by politico-military-national security actors at one end and economic-civil society actors at the other.

2.2 INTERNET GOVERNANCE – CHALLENGES AND CONSTRAINTS

The success of the Internet has partly been attributed to its relative openness and low barriers (including minimal security features) to entry. However, the same

openness, while allowing companies to flourish, has also facilitated those with malicious intent to operate with relative ease.

The origins of the Internet can be traced back to the attempts by the Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense to create a communications NW that would survive a nuclear exchange between the two superpowers of the time. It was subsequently used by academia as a means of communicating and collaborating on research projects. The uniqueness of the Internet in being an open structure with few barriers to entry is the outcome of the circumstances in which it was conceptualised and a result of the worldview of its initial champions. Though a military project, its very nature of being a communications project plus the fact that it was quickly adopted by academics as a means of collaboration led to a quick crossover to the civilian domain. The fact that the technology did not belong to any one company saw the implementation of standards for its various protocols, which was responsible for continuing innovation and improvements of its capabilities.

In the early stages of development of the Internet, much of the task of developing cyberspace was in the hands of line organisations such as the Department of Information Technology (DIT) at the national level or the ITU at the international level, and other expert bodies. While these organisations were competent in their own right, they were unable to bring a holistic perspective to the issue, given their domain-specific focus on issues. This also resulted in fragmented approaches to cyber security, dictated by different requirements and priorities at different points in time.

Among the many institutions that came up and have endured are the Internet Engineering Task Force (IETF), set up in 1986. It comprised a number of experts on various aspects of the Internet who worked through a cooperative consensus-based decision-making process. The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998 on similar principles to manage the Domain Name System (DNS), another key infrastructure of the Internet. Most of the ICANN's powers and functions were devolved to it by the US government, which hitherto controlled DNS. The multi-stakeholder approach to discussing the development of the Internet that was institutionalised though these organisations was further carried forward in the UN-sponsored series of conferences beginning with the World Summits on the Information Society held in 2003 and 2005, and ultimately resulting in the Internet Governance Forum (IGF), convened by and reporting to the UN Secretary General.

The US has had a major influence on the development of cyberspace by virtue of the fact that much of the initial infrastructure and use was centred in that country and it continues to be a major force in its development and use. The US has thus been in a position to fend off periodic attempts to challenge its supremacy, and those times when it has been forced to shed some of its control, as in the case of

ICANN, it has done so very reluctantly. Though it has been a participant in multilateral fora, the United States' agenda invariably has been to ensure that its dominant position is not disturbed. More recently, approaches to cyberspace have taken on ideological hues, with countries ultimately seeking to gain effective control over deciding the form and shape of cyberspace within their national boundaries.

The jockeying for influence to impact Internet governance issues has seen increased activity in recent times. Most of these have taken place at the multilateral level, with countries forming coalitions and introducing resolutions at multilateral fora. While Russia has been introducing resolutions on cyber security at the United Nations since 1998, it recently joined hands with China, Tajikistan and Uzbekistan to introduce an "International Code of Conduct for Information Security" (ICCIS). Some of the clauses within this resolution have been criticised as an attempt to increase control over content and information in the guise of securing cyberspace. Proposals by the IBSA forum (India, Brazil, South Africa) have also been seen with similar scepticism. One of the unstated goals of the recent Cyber Security Summit held by the British government would be seen as an effort on the part of the advanced economies to regain the initiative in drawing up norms for cyberspace that highlight core Western values.

2.3 The Indian Cyberspace

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.

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%.[2] 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

[2] According to the Report for 2010 of the Telecom Regulatory Authority of India (TRAI), over 381 million mobile subscribers possessed the ability to access the Internet through their mobiles, with 35 million having accessed at least once.

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).[4]

Even though the Indian government was a late convert to computerisation, there has been an increasing thrust on e-governance, seen as a cost-effective way of taking public services to the masses across the country. Critical sectors such as Defence, Energy, Finance, Space, Telecommunications, Transport, Land Records, Public Essential Services and Utilities, Law Enforcement and Security all increasingly depend on NWs to relay data, for communication purposes and for commercial transactions. The National e-governance Program (NeGP) is one of the most ambitious in the world and seeks to provide more than 1200 governmental services online.

Looking to the future, the Cisco Visual Networking Index estimates that India's Internet traffic will grow nine-fold between now and 2015, topping out at 13.2 Exabytes in 2015, from 1.6 Exabytes in 2010. That will be the equivalent of the data contained in 374,372 DVDs being carried every hour through these NWs.

In terms of contribution to the economy, the ICT sector has grown at an annual compounded rate of 33% over the last decade. The contribution of the IT-ITeS industry to GDP increased from 5.2% in 2006-7 to 6.4% in 2010-11. Much of the activities of the IT/BPO sector, which was responsible for putting India on the services export map, would not have been possible but for the cost-efficiencies provided through the expansion of global data NWs.

The government has ambitious plans to raise cyber connectivity. There has been a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility. As in other countries, much of the infrastructure related to cyberspace is with the private sector, which also provides many of the

[3] According to Internet research firm Comscore, 62% of Internet users in India use Gmail.

[4] A report compiled by the Indian Market Research Bureau (IMRB) projects domestic e-commerce to be in the region of $10 billion by the end of 2011.

critical services, ranging from banking, to electricity to running airports and other key transportation infrastructure.

Taking telecommunications as a case in point, CII in India comprises around 150 Internet and telecom service providers, offering Internet, mobile and wireless connectivity to a user base of nearly 800 million. A major portion of data communication is facilitated by submarine cables. India has landing points for major submarine cable systems which are minimally protected. A preview of what could happen by way of these cables being disabled took place in 2008 when a series of outages and cable cuts in undersea cables running through the Suez Canal, in the Persian Gulf and Malaysia caused massive communications disruptions to India and West Asia.

Other sectors that could be subject to serious threats include the financial sector, which has largely transferred operations online. Stock exchanges in the United States and Hong Kong have reportedly been subject to cyber attacks. The electricity grid is also vulnerable with the inevitable move towards a smart grid, given the economic and efficiency factors. The protection of critical infrastructure is a complex task requiring forethought, planning, strong laws, technologies, PPP and resources. For all these reasons it needs to be given top priority by the government. The country cannot afford to wait indefinitely for a robust policy to protect this critical infrastructure. Above all, the political will needs to be mustered to take the challenge head on.

The government would necessarily have to work closely with the private sector, particularly in promoting cyber security practices and hygiene.

2.4 Cyber Threats

Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets: cyber espionage, cyber warfare, cyberterrorism, and cyber crime. Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DOSS attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.

2.4.1 Cyber Warfare

There is no agreed definition of cyber warfare but it has been noticed that states may be attacking the information systems of other countries for espionage and for disrupting their critical infrastructure. The attacks on the websites of Estonia in 2007 and of Georgia in 2008 have been widely reported. Although there is no clinching evidence of the involvement of a state in these attacks, it is widely held that in these attacks, non-state actors (e.g. hackers) may have been used by state actors. Since these cyber attacks, the issue of cyber warfare has assumed urgency in the global media. The US has moved swiftly and set up a

cyber command within the Strategic Forces Command and revised its military doctrine. In the latest official military doctrine, the US has declared cyberspace to be the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. It is almost certain that other countries will also respond by adopting similar military doctrines. The issue whether cyber attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare is being hotly debated. Multilateral discussions are veering around to debating whether there should be rules of behaviour for state actors in cyberspace. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution.

There is, however, ongoing debate between those who believe that cyber warfare is over-hyped and those who believe that the world is heading towards a cyber Armageddon. Both sides have valid arguments, but even as that debate continues, cyber warfare as a construct has become inevitable because the number of countries that are setting up cyber commands is steadily growing. These commands have been accompanied by efforts at developing applicable military doctrines. There is, therefore, a pressing need to think about norms for cyber warfare, whether the laws of armed conflict (LOAC) can be adapted to cyber warfare, and how principles like proportionality and neutrality play out in the cyber domain. Current rules of collective security such as Art. 41 of the UN Charter and Chapter 7 are found wanting in the context of cyber warfare, particularly when it comes to the rapidity of cyber attacks, and the inordinate time it takes for decision-making and action under these rules.

2.4.2 Cyber Crime

The increasing online population has proved a happy hunting ground for cyber criminals, with losses due to cyber crime being in billions of dollars worldwide. While other countries are reporting enormous losses to cyber crime, as well as threats to enterprises and critical information infrastructure (CII), there are hardly any such reports coming out of India other than those relating to cyber espionage. Though the report of the National Crime Records Bureau (NCRB) for 2010 reported an increase of 50% in cyber crime over the previous year, the numbers were quite small in absolute terms.[5] The total number of cases registered across various categories was 698; but these low numbers could be because cyber laws have proved ineffective in the face of the complex issues thrown up by Internet. As a case in point, though

[5] http://ncrb.nic.in/CII%202009/cii-2009/Chapter%2018.pdf

the cyber crimes unit of the Bengaluru Police receives over 200 complaints every year, statistics show that only 10% have been solved; a majority of these are yet to be even tried in the courts; and the cases that did reach the courts are yet to reach a verdict since the perpetrators usually reside in third countries. Even though the Information Technology Act (IT Act) 2000 confers extraterritorial jurisdiction on Indian courts and empowers them to take cognisance of offences committed outside India even by foreign nationals provided "that such offence involves a computer, computer system or computer network located in India", this has so far existed only on paper.

Similarly, there are relatively few reports of Indian companies suffering cyber security breaches of the sort reported elsewhere. Companies attribute this to the primacy placed on information assurance in the outsourcing business. Industry bodies such as the National Association of Software and Services Companies (NASSCOM) also attribute this to the fact that they have been at the forefront of spreading information security awareness amongst their constituents, with initiatives such as the establishment of the Data Security Council of India (DSCI) and the National Skills Registry. The Indian government has also aided these initiatives in a variety of ways, including deputing a senior police officer to NASSCOM to work on cyber security issues, keeping the needs of the outsourcing industry in mind.

That said, cyberspace is increasingly being used for various criminal activities and different types of cyber crimes, causing huge financial losses to both businesses and individuals. Organised crime mafia have been drawn to cyberspace, and this is being reflected in cyber crimes gradually shifting from random attacks to direct (targeted) attacks. A cyber underground economy is flourishing, based on an ecosystem facilitated by exploitation of zero-day vulnerabilities, attack tool kits and botnets. The vast amounts of money lubricating this ecosystem is leading to increased sophistication of malicious codes such as worms and trojans. The creation of sophisticated information-stealing malware is facilitated by toolkits such as ZueS, which are sold on Internet for a few thousands of dollars. At the other extreme, components of critical infrastructure such as Programmable Logic Control (PLC) and Supervisory Control and Data Acquisition (SCADA) systems were targeted by the Stuxnet malware that attacked supposedly secure Iranian nuclear facilities. Stuxnet exploited five distinct zero-day vulnerabilities in desktop systems, apart from vulnerabilities in PLC systems, and exposed the grave threat to critical infrastructure such as nuclear plants and other critical infrastructure. Cyber criminals are using innovative social engineering techniques through spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. While large enterprises are ploughing more resources into digital security, it is the small enterprises and individuals that are falling prey to cyber crime, as evinced by the increasing number of complaints on consumer complaint forums.

The low levels of computer security are also apparent in recurring statistics that show that India is the third-largest generator of spam worldwide, accounting for 35% of spam zombies and 11% of phishing hosts in the Asia-Pacific-Japan region. Over 6,000,000 computers were part of bot NWs. India ranked first in the Asia-Pacific region and contributed 21% to the regional total. A continuing trend for Internet users in India was that of the threat landscape being heavily infested with worms and viruses. The percentage of worms and viruses in India was significantly higher than the Asia-Pacific regional average. According to CERT-In, India sees an average of 788 bot-infected computers per day. With regard to web-based attacks, India has seen a significant increase and has ranked seventh, with 3% of the world attacks, and second in the Asia-Pacific region.

2.4.3 Cyberterrorism

Cyberspace has been used as a conduit for planning terrorist attacks, for recruitment of sympathisers, or as a new arena for attacks in pursuit of the terrorists' political and social objectives. Terrorists have been known to have used cyberspace for communication, command and control, propaganda, recruitment, training, and funding purposes. From that perspective, the challenge of non-state actors to national security is extremely grave. The shadowy world of the terrorist takes on even murkier dimensions in cyberspace where anonymity and lack of attribution are a given. The government has taken a number of measures to counter the use of cyberspace for terrorist-related activities, especially in the aftermath of the terrorist attack in Mumbai in November 2008. Parliament passed amendments to the IT Act, with added emphasis on cyberterrorism and cyber crime, with a number of amendments to existing sections and the addition of new sections, taking into account these threats. Further actions include the passing of rules such as the Information Technology (Guidelines for Cyber Cafe) Rules, 2011 under the umbrella of the IT Act. In doing so, the government has had to walk a fine balance between the fundamental rights to privacy under the Indian Constitution and national security requirements.

While cyber hactivism cannot quite be placed in the same class, many of its characteristics place it squarely in the realm of cyberterrorism both in terms of methods and end goals.

2.4.4 Cyber Espionage

Instances of cyber espionage are becoming quite common, with regular reports of thousands of megabytes of data and intellectual property worth millions being exfiltrated from the websites and NWs of both government and private enterprises. While government websites and NWs in India have been breached, the private sector claims that it has not been similarly affected. It may also be that theft of intellectual property from private enterprises is not an issue here because R&D expenditure in India is only 0.7% of GDP, with government expenditure accounting for 70% of that figure. Companies are also reluctant to disclose any attacks and exfiltration of data, both

because they could be held liable by their clients and also because they may suffer a resultant loss of confidence of the public. As far as infiltration of government NWs and computers is concerned, cyber espionage has all but made the Official Secrets Act, 1923 redundant, with even the computers in the Prime Minister's Office being accessed, according to reports. The multiplicity of malevolent actors, ranging from state-sponsored to hactivists, makes attribution difficult; governments currently can only establish measures and protocols to ensure confidentiality, integrity and availability (CIA) of data. Law enforcement and intelligence agencies have asked their governments for legal and operational backing in their efforts to secure sensitive NWs, and to go on the offensive against cyber spies and cyber criminals who are often acting in tandem with each other, and probably with state backing. Offence is not necessarily the best form of defence in the case of cyber security, as seen in the continued instances of servers of the various government departments being hacked and documents exfiltrated.

2.5 Need for a Comprehensive Cyber Security Policy

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, cyberterrorism, 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 is paid to ensuring 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.

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 draft cyber security policy document put out by the 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) NSCS; (4) Ministry of Home Affairs (MHA); (5) Ministry of Defence; (6) DIT; (7) DoT; (8) National Cyber Response Centre (NCRC); (9) CERT-In; (10) National Information Infrastructure Protection Centre (NIIPC); (11) National Disaster Management Authority (NDMA); (12) Standardisation, Testing and Quality Certification (STQC) Directorate; and (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 may be said to be distributed amongst the Ministries of Communication and Technology, Home Affairs and Defence, and the office of the NSA.

2.6 Need for a Nodal Authority

The NIB is tasked with national-level policy formulation and creation of suitable institutions and structures on Cyber and Information War (CIW). It is considered that the Secretariat of the NSC needs to be suitably structured and strengthened with the appointment of a Director General (DG) as head of CIW. To ensure the desired level of coordination, the DG must be suitably empowered and should be a person who combines a technical, operational and innovative mind with a proactive and decision-oriented approach.

The NIB as structured finds it difficult to meet frequently. It is therefore recommended that a smaller effective and

flexible apex body be created to oversee and deliberate on policy and other issues in respect of CIW, with coordination and monitoring left to the DG. This apex body could constantly review the situation and institute remedial measures, where required. With experience, and confidence in delegation it could possibly take on the role of the NIB. A suggested structure with charter of the apex and executive bodies is at Appendix 1. As these include public and private agencies, the Planning Commission's experience, which incorporates expertise from all fields, could serve as a guide. The success of the Indian BPO industry is based on ensuring demanding security requirements of clients. This experience can usefully be adapted and harnessed. Tasked as it is, the NIB could under its powers establish this apex body and DG CS&IW office as proposed. Permanence in functioning could be ensured by the allocation of business rules.

2.7 Need for an International Convention on Cyberspace

Cyber security is becoming an indispensable dimension of information security. The rapid growth of ICTs has contributed immensely to human welfare but has also created risks in cyberspace, which can destabilise international and national security. Global and national critical infrastructure is extremely vulnerable to threats emanating in cyberspace. Additionally, the growth of social media (Twitter, Facebook, etc.) has created a new medium for strategic communication that bypasses national boundaries and national authorities. The global data transmission infrastructure also depends critically on the NW of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

The UNGA resolution of 8 December 2010 (A/RES/65/41) deals with the impact of ICT on international security. The underlying concern is that ICT should not be used to destabilise international peace and stability.

Given the positive as well as negative potential of cyberspace, there has been talk of devising an international convention on cyber security which would ensure that states behave responsibly in cyberspace. There already exist several international conventions (chemical weapons convention, biological toxins and weapons convention, NPT, etc.) and a body of international humanitarian law (Geneva and Hague conventions) from which inspiration to draw up a cyber warfare convention can be drawn.

A pressing question to be considered in the current unpredictable cyber scenario is the following. Should India actively engage itself in international efforts in framing a treaty or drawing up a framework of coherent cyber laws? Or, alternatively, should it wait till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes that may evolve as subsidiaries of a proposed cyberspace treaty?

Such a question has faced decision-makers right from the missile to nuclear technology control regime eras.

Opponents of a cyberspace-related treaty argue that even though the international efforts for harmonisation of international legal frameworks for cyberspace do not refer to technology control regimes in their current manifestations, it would be just a matter of time before ancillaries/corollaries of such a treaty may emerge which would be based on technology control regimes; and signing such a treaty would result in undermining national sovereign interests. Similar arguments are brought up in respect of the European Convention on Cyber crime, specifically Article 32, which, countries like Russia maintain, undermines their sovereignty.

The argument is that such treaties are biased in favour of the requirements of the major international players/powers and that India should stay aloof from such exercises till its own cyber capabilities mature to a level that they are beyond the ambit of control regimes. But this type of isolationist approach is extensively dependent on capability maturity model; and derives little or no benefit of the opportunities that can be capitalised by following an engagement model towards these treaties and conventions.

On the other hand, most of these cyber treaties are currently in their infancy and are undergoing development at various tier 2 and tier 1 forums. If at this stage India proactively engages with the international community in drafting these cyber treaties and conventions, and capitalises on this opportunity by moulding these cyber treaties and conventions to suit its sovereign interests, then the benefits achieved by the engagement approach would, without doubt, outweigh the potential outcomes of an isolationist approach.

Can there be a convention to govern cyber warfare, cyber weapons, use of force in cyber warfare, prevent cyber crime, etc.? As debate on these issues goes on, there is as yet no convention governing cyberspace. One idea that has been mooted is that critical systems like those of schools and hospitals should be protected from attacks in cyberspace, as attacking them would be tantamount to violating international humanitarian law. It is a separate matter whether such information systems can be marked for protection and whatever source of attack can be identified and sanctioned.

A cyber convention would be unlike existing conventions in many ways. This is because in cyberspace attribution and identification is extremely difficult and identities can be easily masked. Cyber attacks also typically involve systems located in many countries. Often, cyber attacks are silent and go unnoticed for long periods.

UNGA has regularly passed resolutions on information security. Information security summits have been held in which cyber security has also been discussed. Several regional initiatives like the European Convention on Cyber crime have been in existence for decades. These efforts can be consolidated in the form of a cyberspace convention. The key issues for consideration for a possible cyberspace convention would be:

- National critical infrastructures should not be harmed.
- Secure, stable and reliable functioning of the Internet should be ensured.
- A common understanding of Internet security issues should be evolved.
- National governments should have the sovereign right to make national policies on ICT consistent with international norms.
- A global culture of cyber security based on trust and security should be encouraged.
- The digital divide should be overcome.
- International cooperation should be strengthened.
- PPP should be encouraged.
- CIA of information systems should be ensured.
- Balance between the need to maintain law and order and fundamental human rights should be maintained.

Such a convention would also define more precisely what constitutes threat in cyberspace and what would be the basic principles of information security. It would have many don'ts, as for instance the obligations on states not to take any overt or clandestine measures which would result in cyber warfare. It would also need to define what the use of force in cyberspace would mean and in what circumstances such force can be used, if at all. How would a state react if it is subjected to cyber attacks by a state, or a non-state actor, or by a combination of the two? Given the nature of cyberspace, where attribution is difficult, these prohibitions will be hard to define and even harder to agree upon.

Arriving at a cyberspace convention would prove highly contentious. Yet, in India we need to debate openly the merits and demerits of the international law on cyberspace. Is such a convention possible at all? An Indian view needs to be evolved.

CHAPTER 3

PREPARING FOR CYBER WAR

3.1 THE NEED TO BE PREPARED

The growing threat of cyber warfare has not been well appreciated or sufficiently understood. Cyber warfare is a term that has been loosely used to describe almost all events in cyberspace, irrespective of perpetrator, motive or scale. Cyber warfare forms a part of Information War (IW), which extends to every form of media, and inter alia includes aspects of propaganda and perception management. Cyberspace, though technically restricted to the Internet, is now increasingly linked by convergence to every communication device. With greater connectivity, this divide is narrowing and every citizen or aspect of life is vulnerable. It is also an important constituent of NCW. The cyber realm, like the universe, is expanding and it is estimated that by 2015 there will be almost double the number of devices connected to the Internet as there are people. The scope for exploitation by inimical elements, ranging from mischievous hackers, to criminals, terrorists, non-state actors as also nation states, is thus unlimited. The damage could be immense and many countries are pressing ahead and taking steps to build capabilities and capacities for defending themselves, as also taking offensive action in cyberspace.

The United States was the first country to formally declare this as the fifth domain warfare after land, sea, air and space. It has also formally classified the use of cyberspace as a "force", a euphemism for offensive capability. The Chinese adopted the concept of "*informationalisation*" in the mid-1990s and have relentlessly built up structures and operations in this domain. Consequent to the raising of the US Cyber Command (USCYBERCOM), South Korea followed with the creation of a Cyber Warfare Command in December 2009. This was also in response to North Korea's creation of cyber warfare units. The British Government Communications Headquarters (GCHQ) has begun preparing a cyber force, as also France. The Russians have actively been pursuing cyber warfare. In 2010 China overtly introduced its first department dedicated to defensive cyber warfare and information security in response to the creation of USCYBERCOM. The race is thus on.

India is a target. There have been numerous incidents of sensitive government and military computers being

attacked by unknown entities and information being stolen. The frequency and intensity of such episodes is increasing. There is enough evidence to suggest that this is the action of nation states either directly or through proxies. There have also been cases of offensive action such as reports of shutting down of power systems. Such attacks on critical infrastructure either singly or in multiples are of serious concern, especially with respect to national security. The draft National Cyber Security Policy (NCSP) mainly covers defensive and response measures and makes no mention of the need to develop offensive capacity. This is a must if we are to ensure capability for self-defence granted under Article 51 of the UN Charter. This leads to the question: what is cyber warfare?

In the absence of a formal definition of cyber warfare, we may define it as *"actions by a nation-state or its proxies to penetrate another nation's computers or networks for the purposes of espionage, causing damage or disruption"*. These hostile actions against a computer system or NW can take two forms: cyber exploitation and cyber attacks.

Cyber exploitation is in a manner non-destructive and includes espionage. It is usually clandestine and is conducted with the smallest possible intervention that allows extraction of the information sought. It does not seek to disturb the normal functioning of a computer system or NW. The best cyber exploitation is one that a user never notices. These are silent and ongoing, and as mentioned earlier, have shown an upward trend.

Cyber attacks on the other hand are destructive in nature. These are deliberate acts of vandalism or sabotage – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy an adversary's computer systems or NWs or the information and programs resident in or transiting these systems or NWs.

Actors in both types of activities cover a wide range, as mentioned earlier. Of these, nation states and their proxies are of the greatest concern. For easier understanding, the domains of cyber warfare may broadly be classified as:

3.1.1 Espionage

Intelligence gathering and data theft. Examples of this were *Titan Rain* and *Moonlight Maze*. These activities could be by criminals, terrorists or nations as part of normal information gathering or security monitoring.

3.1.2 Vandalism

Defacing web pages or use DDOS to take them down. Such actions were evident in Estonia or Georgia.

3.1.3 Sabotage

This has the most serious implications and includes DDOS, destruction of data, insertion of malware and logic bombs. It also encompasses actions in war such as those taken for preparation of the battlefield.

3.2 Fifth Domain of Warfare

The cyber warfare that this section addresses is that which is practised mainly by nation states or their proxies. The potency of this threat has compelled almost every country to develop capabilities in the cyber domain, as is the case for land, air, sea and space. According to Spy Ops, by the end of 2008 nearly 140 countries possessed varying degrees of cyber attack capabilities. In addition, an unknown number of extremist groups and non-state actors have developed or acquired cyber weapons. Some commercially available products are flexible enough to be classified as dual-purpose – security testing tools and weapons of attack. Thus some organisations have or are developing cyber weapons and cloaking them as security testing tools. All this is classified information and each nation works on its own. An assessment of cyber warfare threat matrix by the USA, which covered over 175 countries and organisations, made a watchlist in which the top ten in order of priority were: China; Russian business NW; Iran; Russia tied with France; extremist/terrorist groups; Israel; North Korea; Japan; Turkey; and Pakistan.

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. In order to understand the challenge, the following issues need to be addressed.

3.2.1 Coordination

It is appreciated that in keeping with current needs, the Defence forces, DRDO, NTRO, CERT-In, RAW, IB, C-DAC, Ministries, NIC, NASSCOM, private industry et al. have to work in concert. The impact of this on every aspect of electronic media requires a coordinated and integrated approach. Given its all encompassing nature, it also follows that control of all cyber and IW activities at the national level must fall under the purview of the NSC and controlled by its Secretariat ie the NSCS as mentioned in Chapter 2. Within this lead agencies for executing offensive cyber operations *inter alia* could be the NTRO, CIDS and the DRDO.

3.2.2 Defining Objectives and Doctrine

Application of such measures must be in accordance with clearly defined objectives that would be in keeping with customary international law and practice. The primary objective would be to garner knowledge to find how systems are breached and thus provide the ability for defensive measures to be developed and put in place. There is a further argument that it must be visible as an armour of self-defence so as to deter an attack. While this capability will be ambiguous, subtle signals and clear definition of objectives will lend credibility. Moral arguments stand thin in the face of realities. There is

therefore a need to lay down the objectives and include them in the draft NCSP or issue a doctrine in this regard.

3.2.3 Proactive Cyber Defence

This comprises actions taken in anticipation to prevent an attack against computers and NWs. As opposed to the current practice of passive defence, it provides a via media between purely offensive and defensive action: interdicting and disrupting an attack, or an adversary's preparation to attack, either pre-emptively or in self-defence. Proactive cyber defence will most often require operationalising upstream security mechanisms of the telecommunications or Internet providers. The most compelling reasons for a proactive defence can be couched in terms of cost and choice. Decision-makers will have few choices after an impact, and all of them are costly to start with. Proactive defence is thus the key to mitigating operational risk. The USA had set up a Proactive Pre-emptive Operations Group (P2OG) in 2002. Such actions thus find international acceptability.

3.2.4 Critical Infrastructure

There is a need to prioritise and protect critical infrastructure. In the USA 18 sectors have been identified. In India's case, the sectors of power, water supply, communications, transportation, defence and finance are vital constituents of national security. These need to be defined and suitable protection measures ensured as laid down in the IT Act. Steps to guard against threats, i.e. destructive actions or cyber exploitation will constitute a basis for research on offensive action. The electric power system merits top priority. While the risk of an attack can be reduced, it would be unrealistic to assume that an attack can be prevented. This leads to the conclusion that containment, isolation, minimising the impact, backup systems and reactivation are areas of capacity building. The debate on which agency will undertake this in India rages and begs immediate resolution. As critical infrastructure spans both the public and private domains, the organisation to ensure its protection has to be in the public realm and, in a manner, accountable.

3.2.5 Legal Provisions

The IT Act of 2008 covers all actions in this domain. Sections 69, 69A and 69B contain provisions for intercepting, monitoring or blocking traffic where, amongst other reasons, there is a threat to national security. Section 70A covers protection of critical infrastructure. There is a need to work within these provisions. LOAC provide the primary legal framework within which one can analyse constraints for offensive cyber operations. Immunity for actions taken against another nation, institutions, hostile group or individual is possible if taken under LOAC or for self-defence under Article 51 of the UN Charter. The cyber realm, with scope of non-attributable actions as also ease of deniability, provides immense scope for exploitation. The fact that there are no international cyber laws or treaties at present is also used to advantage. Offensive cyber operations by their very nature have to remain in the grey realm and restricted. Each nation would thus determine the structure best suited to its

needs. However, the necessity to clearly enunciate such measures or self-defence actions in a doctrine as also the NCSP is essential for steps in this regard; it also acts as an element for deterrence. The emphasis must remain on protecting NWs, systems and users.

3.3 Meeting the Cyber Warfare Challenge

Cyber warfare encompasses government and public and private domains. As clarified earlier, this must be coordinated by the NSCS. In the USA it comes directly under the White House. Thus the need to create a Directorate or Special Wing in the NSCS for this as proposed in Chapter 2. It would oversee and coordinate both defensive and offensive cyber operations. There is also a requirement for intimate involvement of the private sector, as they are equal, if not larger, stakeholders. Regular meetings must be held and, if needed, working groups created. Current organisations which could be tasked to take on the cyber warfare challenge include the NTRO, HQ IDS, DRDO, RAW and IB. Representatives of CERT, NASSCOM, etc. will invariably be involved. Each would have to function under guidelines and through proxies.

3.3.1 Raising of Cyber Command

While cyber warfare is ongoing activity during peacetime, there is a dire need to develop this capacity for a warlike situation. Cyber warfare in a manner is NCW and will form an essential part of preparation of the battlefield in any future conflict. Such attacks may also precede the kinetic war. Building this capability will take time and must remain covert and ambiguous. It could also form part of the strategic deception process. This should be the responsibility of the Armed Forces (HQ IDS) along with the DRDO and other experts. Detailed discussions and consultations in this regard require to be initiated.

India must raise a Cyber Command. This will comprise not only the three services but personnel from the DRDO and scientific and technological community. It could work with the space command because many aspects overlap and would economise on resources. It will oversee all activities undertaken during peacetime, as also plan for offensive cyber operations as required, to include preparation of the battlefield. It must work in close concert with the NTRO. To determine the structure it would be prudent to study the mission and objectives of USCYBERCOM as a guide.

USCYBERCOM plans, coordinates, integrates, synchronises and conducts activities to: *"direct the operations and defense of specified Department of Defense information NWs and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."* The Command is charged with pulling together existing cyberspace resources, creating synergy and synchronising war-fighting effects to defend the information security

environment. It comes under the Strategic Command, which also has the Space Command as a constituent. A similar structure for India could be considered, especially as the US has evolved its structure based on experience and also because it functions as an open democracy. India already has the Strategic Forces Command, which could be augmented with both Space and Cyberspace Wings. These may be of smaller size to start with, and will develop in accordance with threats and needs. Each service has its own requirements. The structure therefore has to be need-based and flexible. The various elements of this could be:

- ***Army, Navy and Air Force CERTs***

These would monitor traffic, disseminate information, ensure remedial measures to ensure ongoing security to NWs and systems. They would also in a manner be charged with protection of critical infrastructure of each service, i.e. communication backbone, power systems, high-priority NWs, et al. The structure thus envisages a Defence CERT which works in concert with each service CERT.

- ***Intelligence and information operations***

A Defence Intelligence Agency exists under HQ IDS. Its cyber and information operations elements could work with this command. Intelligence gathering is an accepted reality and cyberspace possibly provides the best scope for this as also information operations.

- ***Defence communication NWs***

Each service has its special requirements and own communication directorates. Joint operations, strategic communications as also high-security NWs need to be coordinated under HQ IDS and the proposed Cyber Command.

- ***Cyber operations which are required for preparation of the battlefield.***

This again would be a tri-service organisation, with additional experts from the DRDO or any other such institution. This would include R&D.

3.3.2 Territorial Army (TA) Battalions for Cyber Warfare

While cyber warfare is ongoing, there are periods of heightened threat. A recent example was the Commonwealth Games, when NWs were subjected to attacks. There is therefore need to create and maintain a "**surge capacity"** for crisis or warlike situations. Young IT professionals constitute a vast resource base and a large number would be willing to loyally serve the nation when required. This resource must be capitalised by raising of cyber warfare TA battalions similar to those for Railways and ONGC, which could be embodied when required. In addition to purely "defence" requirements these could also provide for protection of critical infrastructure.

3.3.3 Perception Management and Social NWs

In the current age of "democratisation" or "instant availability of information" and growth of social NWs, there is tremendous scope for perception management and manipulation of information. The year

2011 saw extensive use during the "Arab Spring" and London Riots. This media is seen as a potential tool for psychological and no-contact warfare and must form part of any offensive or defensive action. All this requires central coordination and study with respect to national security.

3.4 Capacity Building

Capacity building is vital. It must also be sustainable and of larger benefit. There is a need to create an R&D base and institutions. Growth forecasts of Internet usage, especially with e-governance, will create an employment potential for "cyber doctors" and sleuths. Just as the terrorist attack on Mumbai in November 2008 created a whole new dimension of requirement of physical security, protection of Internet usage and transactions will create millions of jobs in the near future. It will be a seller's market for which India with its HR base must be ready. Consequently, the government must accelerate this process. Some thoughts in this regard are:

3.4.1 Partnerships

India cannot go it alone. Various past attempts have not been of much success. It has to be seen as a global issue and capacities developed.

3.4.2 HR and R&D

DIT has set up the Information Security Education and Awareness (ISEA) programme with funding of Rs 100 crore. Other options which need to considered are government and public and private institutions. The Chinese models could be studied in this regard. They set up four universities for this purpose in 1999. Security of data for the BPO industry has brought up the necessity for such institutions. Talent spotting with competitions is an easy option. Programmes and competitions such as "Cyber Patriot" need to be followed up in schools and educational institutions. These could be self-financed. Army Training Command (ARTRAC), as also the other two services, must take the lead in partnership with the private sector.

3.4.3 Testing and Certification

The outsourcing model has affected testing and certification. Hardware and HR in this regard has to be Indian. This can then be adapted for proactive defence. Steps taken by DIT need to be implemented.

3.4.4 Language Training

HR trained in language of our potential adversaries is a must. This must be provided suitable incentives and permanence of employment.

3.4.5 Legal Capital

Legal aspects of developing capacities, understanding use of cyberspace as a "force", implications of the UN Charter, negotiating international laws and treaties – all of this needs trained personnel. While the legal aspects are covered in a separate section, expertise with respect to cyber warfare needs special attention.

3.4.6 Understanding Vulnerabilities

Study of vulnerabilities both of own systems as also those of potential adversaries must be undertaken to prevent intrusion and exploit weaknesses.

3.4.7 Identification of Technologies

There is a need to identify technologies in this regard. Section 4.2.3 of the Draft NCSP mentions these. These should also include isolation of NWs within the country, close monitoring of gateways and backbone, identification of "zero day" vulnerabilities, protection of power grids, secure communications for defence and critical services, penetration, et al.

3.5 Summary

Understanding the threat of cyber warfare and developing capacity for offensive actions in this domain is a *sine qua non.* Nations, non-state actors, terrorist groups and individuals pose a challenge to growth, which is increasingly going to be dependent on the cyber domain. Cyber warfare will also be central to any hostile or conflict situation. Clearly defined objectives and national doctrine in this regard along with supporting structures and matching capabilities are thus inescapable.

CHAPTER 4

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION THROUGH PUBLIC-PRIVATE PARTNERSHIP

4.1 THE NEW CONTEXT FOR PPP IN NATIONAL SECURITY

National security has traditionally been the sole responsibility of governments. But as the world has moved into the information age, with increased dependence on information infrastructure for production and delivery of products and services, the new responsibility of securing the critical information infrastructure (CII) against the rising number of cyber attacks has come within the ambit of national security. This new responsibility is not, however, solely that of government; and the private sector has a major role to play since more and more CII is owned and operated by it. DIT has identified such critical IT-dependent infrastructure, namely Defence, Finance, Energy, Transportation and Tele communications.

The IT Act, 2000, as amended in 2008, provides for protection of CII under section 70A. The government will designate an organisation as the national nodal agency for CII protection, which will be responsible for all measures to protect CII. In fact, the concept of protected system, under section 69, has been there in the Act since 2000. However, no system of the government has probably been declared as protected so far.

As of now the government has not declared the nodal agency for CII protection. As and when such an agency comes into being, it will create the framework and rules for CII organisations.

The following analysis of some of these sectors shows that a significant part of the CII is owned and operated by the private sector in India:

- The *telecom sector* is mostly governed by private players, except MTNL and BSNL. The global undersea cable communication infrastructure (GUCCI) is largely owned by private players.
- The *banking sector*, where more than 30% of the transactions are done online, and the value of these transactions is over 80% of total transaction value, has a large number of foreign and private banks
- *Stock Exchanges* – The major stock exchanges BSE and NSE are private players, wherein most of the transactions are done through the electronic medium.

- *The airline industry* is dominated by private players, with Air India being the only government enterprise.
- *Energy and Utilities* – Though this sector is largely dominated by government players, the distribution in major cities is largely controlled by private partners.

Thus, the private sector is equally important when it comes to securing a nation's cyberspace. However, the government cannot leave it to the private sector alone for securing its own CII. This is because if any cyber attack takes place on CII owned by a private company, the consequences of such an attack may have an adverse impact on the entire nation and not restricted to the company owning the CII. For example, if there is a cyber attack on one of our national stock exchanges, it could possibly bring down the entire trade operations, impacting the economy and creating panic among investors. Therefore, there is an urgent need of appropriate collaboration and partnership between the government and the private sector for securing CII. The private sector needs to be greatly involved in government's cyber security initiatives through various mechanisms, including PPP.

Given the foregoing background, following are some of the issues in protecting CII and recommendations for protecting CII.

4.2 Information Sharing and Coordination

While CERT-In is doing an excellent job in the government sector, the same needs to be replicated for the private sector through establishment of **Security Information Sharing and Analysis Centres** within each of the identified private sectors, that coordinate with CERT-In and/or National Nodal Centre that may be created. Information sharing between government-to-private and private-to-private should be promoted.

In this context it is pertinent to study the effectiveness of information sharing programmes elsewhere in the world, especially in the United States, which has put in place voluntary approach based on information sharing and PPP at the centre of cyber security policy. The difficulties they have encountered include private entities' inability to share information because of liability, anti-trust, and business competition risks. From the government side, difficulties of sharing classified information with the private sector have been reported. It seems that many of the information-sharing activities will require even legal changes to make this programme work.

It is recognised throughout the world that the private sector follows high standards of security compared to its counterparts in the public sector, and that the latter can learn from the practices in the private sector. There should be appropriate mechanisms for the public sector to use such security practices as are followed in the private sector, for enhancing the cyber security posture and preparedness of the public sector infrastructure. Appropriate processes and structures need to be established to make this happen in our own environment.

There should be a **National Command and Control Centre,** which should be responsible for coordinating cyber security-related activities at the national level for both the public and private sectors and also assign roles and responsibilities.

Both the private and public sectors should coordinate within their verticals with respect to the following:

- Security Alerts and Vulnerabilities impacting their ICT infrastructure
- Tracking botnet, phishing sites, spam, malware, etc. and the steps to overcome these issues
- Sharing of best practices
- Early-watch-and-warning system
- Incident response mechanism
- Work with their respective counterparts nationally and internationally. For example, the Indian banking sector CERT should work closely with its counterpart internationally, much the same way as CERT-In does with the CERTs of other countries.

4.3 Innovation in Regulatory Approach

The government can intervene in protection of CII by the private sector by enacting stringent regulations (as is being done traditionally). Though regulations are necessary they should not add cost without necessarily improving security of CII. Too much of government intervention through regulations can also undermine business innovation.

In addition to enacting promotional legal framework for securing CII, ***the government must also create incentives for industry to invest in security of CII beyond what is necessitated by companies' business plans***. Examples of such incentives could be tax deductions and rebates on security investments, lower-cost loans for SMEs that implement best security practices, reduced liability for improved security, recognition, etc.

4.4 Innovation in Security Programmes

Information security is considered as one of the biggest inhibitors to business innovation. As per IDC global survey conducted in 2008, IT security risk is the single biggest inhibitor to business innovation, with more than 80% of the executives surveyed admitting their organisations have "occasionally" or "often" backed away from innovative business opportunities because of information security concerns. This could be partly because of the following issues in security programmes:

- ***Compliance driven*** Focus of security investments, efforts and time is on compliance documentation rather than managing real risks, making the programme bulky. As per IDC, "C-level executives indicate business alignment of information security as a high priority, yet the compliance or fear driven nature of many organizations reveals the disconnect between the desired and actual state."
- ***Security certification, which brings comfort factor***, results in a static

nature of security while security requires complete dynamism.

- ***The controls approach falls short*** of comprehending the changing threat landscape and quick aligning of organisational response. Also, such an approach hinders business innovation and, as per the IDC survey, "The majority of organizations consider themselves 'compliance/control driven' when it comes to security; with only 21% reporting that their security efforts are strategic, proactive and using security to enable innovation."
- Bulky security program ***neglects challenges to the specific data***, where security of each data element is now critical.

The government should encourage adoption of security standards/ frameworks/practices that:

- enable an organisation to focus on real threats in its environment;
- assess the organisation's maturity in implementing security in different areas with a view to continually improve it;
- help the organisation draw a strategic plan based on evolution of different disciplines of security, and their interdependencies, with continuous focus on protecting data; and
- promote dynamic and vibrant security that enables quick response to threats, vulnerabilities and actual cyber attack with compliance as an outcome.

DSCI has created such a security standard – DSCI Security Framework (DSF), which is based on a set of security principles.[6]

Government should recognise security standards such as DSF and encourage implementation in both the public and private sector companies.

4.5 Proactive Threat and Vulnerability Management

The success of a security programme lies in the ability of an organisation to swiftly respond to security threats and attacks. This requires more proactive delivery of security intelligence. CERT-In may like to

[6] DSF principles are as follows:

a. **Visibility**: consolidated view of all the data elements, understanding of environment
b. **Vigilance over recent trends and threats**: Strengthen defence against perennial and evolving threats, Aligns protection to address new threats
c. **Coverage and Accuracy**: To ensure the scope of security initiatives is extended to all the desired elements, Assures that critical vulnerabilities or weaknesses are not left unaddressed
d. **Strategic, Tactical and Operational views of disciplines**: structured understanding of security and defence, allocation of sufficient resources and efforts at all layers, Brings clarity in roles and responsibilities
e. **Discipline in Defence**: continuous discipline in defence and govern security initiatives effectively
f. **Compliance Demonstration** from security initiatives

partner with the private sector for a focused effort to create enablers for increasing interactivity with security organisations of critical sectors for sharing the research findings and information.

Government should enhance interactivity of security organisations with national cyber security machinery, with active participation of the private sector.

4.6 Promoting Best Practices in Critical Infrastructure Sectors through Government Funding

There is an urgent need to revitalise security in the critical infrastructure sectors as they become obvious and lucrative targets of security threats. This requires significant resources and efforts. For example, SCADA systems may require a sustained nationwide security analysis centre. A programme is required to create an inventory of information assets. The sectors may not be in a position to fund the investment. For proactive defence, the government needs to intervene to fund implementation of security practices in these sectors.

Government should initiate a special drive of implementing practices in the critical infrastructure sectors and provide necessary budgetary support for such implementation.

4.7 Assessing and Monitoring Security Preparedness of Sectors (Security Index)

National cyber security can be measured by assessing the performance of key industry segments against the rising challenges of security. Critical infrastructure sectors, because of their increasing dependence on IT, are posing a new set of challenges to national security. Hence, it becomes necessary to develop a mechanism that assesses the preparedness of these sectors and monitors progress in their preparedness in a measurable form.

Government should establish a mechanism for measuring preparedness of critical sectors such as security index, which captures the preparedness of the sector and assigns value to it: operationalise the mechanism for routinely monitoring the preparedness.

4.8 Security in Information Technology Supply Chain

IT supply chain, in its reach and characteristics, reflects a high level of globalisation. In fact, that has been one reason for the success and continuous growth of the Internet. Innovations of technology, products and services, with components such as chips, tool sets, operating systems, databases, applications, and so on have ensured that no single country can claim to innovate, design, test, manufacture, operate and maintain hardware and software products and services. A veritable global chain has emerged – the ICT Supply Chain. This poses a critical challenge for obtaining assurance over the security of the product and services being outsourced to, and procured from global technology providers. With increased dependency on cyberspace, increased concern about cyber

threats, and increased appreciation of the globalisation of the development, manufacture, and maintenance of ICT systems, fears have grown that adversaries will taint the supply chain to engage in espionage. They might introduce hidden malware, and change functionality of products and services with a view to give their own countries advantages that are difficult to gain otherwise. For example, a service could be disrupted at critical junctures, or kill switches may be planted to disable a CII organisation. Addressing such threats is a major concern of governments around the world. From the Indian perspective, there is need to pay attention to two types of concerns:

- ***Concerns with respect to global products***

Concerns with respect to vulnerabilities in products offered by global technology providers, which are deployed in critical sectors.

- ***Services delivered from offshore***

Concerns with respect to services being offered from the country to the rest of the world, like application code development offered by Indian companies.

A pragmatic policy environment, adequate partnership with industry, technical competence and focused initiatives are required. DIT may undertake a focused program for security assurance in the ICT supply chain. The first requires setting up of testing labs; the second requires a joint effort of DIT, in partnership with NASSCOM and DSCI, to assure secure delivery of services from India.

The Government should incorporate IT Supply Chain Security as an important element of e-security plan to address security issues.

4.9 Taking Leadership and Participating in International Efforts

The Government of India should take leadership in international efforts and cooperation for cyber security as many cyber attacks on CII originate from foreign countries. For example, India could lead an international co-operation that makes a ***nation responsible for the actions in cyberspace of individuals who are resident in its territory***. A good example of similar effort is the Financial Action Task Force (FATF). FATF began as a group of nations opposed to money laundering. They established practices and rules for banks and for banking authorities to make money laundering more difficult. Nations that did not comply faced greater difficulty in participating in the global financial NWs – higher costs, longer delays, more impediments. A similar approach to nations that tolerate cyber crime could be to make it more difficult for them to connect to the global NW, or to have their national NWs face additional scrutiny and impediments. These constraints would not be foolproof but they would increase the cost to nations that act as sanctuaries and provide incentives for changed behaviour.[7]

[7] James Andrew Lewis, *The Cyber War Has Not Begun*, Center for Strategic & International Studies, March 2010.

4.10 R&D in Security

Cyber security demands creation of key capabilities in the nation that can help raise strength of deterrent, proactive and reactive measures. The extent of investment in R&D can prove an important differentiating factor in the cyber world. However, this requires close participation of private industry to ensure that the outcomes of the investment are converted into usable products and solutions that can stand the test of international scrutiny and capture the global markets. The government, apart from working with academic institutions, should fund security research projects in the private sector. This requires adequate budgetary arrangement, effective techniques for management of research projects, and enabling mechanisms for engaging the private sector. Some of the grant conditions are difficult to fulfil.

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.

4.11 Capacity Building in Security Skills and Training and Awareness

The Government should focus on creating a workforce of security professionals in the country, keeping in view the requirements of the future. This would require introducing security-related courses in formal education in engineering courses, and postgraduate courses such as MCA, M.Tech and MBA. Simultaneously, specialised security courses should be designed for the working professionals.

On the other hand, there is continuous need for ***providing training and education to the professionals working in the critical sectors*** – both specialised training and general awareness, depending on the work profile of the professionals.

The scope and extent of security training initiatives and outreach programme, undertaken under the leadership of CERT-In, should be expanded to cover other cities and private industries. This will improve access of regional establishment and private sectors to the skill improvement programme and ensure their participation in cyber security initiatives. Organisations like DSCI can partner with the government for expanding the scope of the programme, arranging experts from industry and sustain delivery of the programme. ***PPP model should be explored for taking security to the regions and industry sectors***. This will require creating enablers to engage private organisations like DSCI. These institutions will augment the capability of CERT-In by setting up training programmes, develop content, arrange experts, and develop training platforms. Apart from capability enhancement, they will also ensure sustained delivery of the programme.

4.12 PPP in Cyber Security

Some of the possible areas for PPP are:

4.12.1 Capacity Building in the Area of Cyber Crime and Cyber Forensics

Such capacity building can take place in terms of infrastructure, expertise and availability of HR and cooperation between industry, law enforcement authorities (LEAs) and judiciary. A successful example is the Cyber Labs Programme run by DSCI, which got a boost with the support of the DIT for opening a cyber lab in Kolkata, and augmenting the existing infrastructure of Mumbai, Bengaluru and Pune cyber labs. This programme is further poised to become a full-fledged Cyber Forensics Programme for which a proposal is under consideration of the Union Government.[8]

4.12.2 Developing Security Expertise for Protection of CII

Security expertise for protection of CII could be developed by providing hands-on training to professionals, especially from the government sector, who are responsible for safeguarding such infrastructure by utilising the expertise available within the private sector. DSCI has been working with CERT-In to provide security training to government and public sector units, and organisations that fall under the definition of CII. More than 700 officials from different government departments and organisations across the country have attended these training sessions.

4.12.3 Imparting Education and Awareness

Imparting education and awareness is necessary, because no amount of education and awareness is enough and there is a continuous need for PPP in all sectors of the Indian economy. DIT and NASSCOM jointly funded a project "Cyber Security Awareness Program", which was executed by DSCI, wherein a number of events, conferences, seminars and workshops were organised to create awareness amongst different stakeholders in cyber security, including security professionals, government employees and children.[9]

4.12.4 Developing Approaches, Best Practices and Standards

Approaches, best practices and standards need to be developed based on international standards to protect CII (e.g.

---

[8] Till date, around 9000 police officers have been trained through this programme. Also, DSCI has developed a Cyber Crime Investigation Manual to help police officers in cybercrime investigations using cyber forensic tools and standard operating procedures. NASSCOM and DSCI have also signed a Memorandum of Understanding with the CBI to establish collaboration between law enforcement agencies and the Indian IT industry.

[9] Under this project, computer-based training in different areas of data protection such as Internet security awareness, privacy, etc. was also created. To create a platform for sharing knowledge on data security and privacy, this programme created 10 E-security forums across 10 major cities in India. Currently, more than 1000 security and privacy professionals are members of these forums.

GUCCI, SCADA systems, etc.). This can be achieved by creating an expert group having representation from both the public and private sectors. For example, international efforts are being made for protecting GUCCI (by global think-tanks like EastWest Institute), as over 99% of intercontinental communications traffic is carried through GUCCI and 95% of these cables are privately owned and maintained. Such groups can also act as an agency for information dissemination and information sharing. For example, such a group can spread the learning of Stuxnet attack in industries that use SCADA systems.

4.12.5 Bringing Innovation through R&D

This can be done with the government funding the private sector for conducting research in the area of cyber security.

4.12.6 Taking Leadership and Participating in International Efforts on Cyber Security

Participation in international efforts on cyber security could be through global think-tanks and institutes such as EastWest Institute, where government officials, NASSCOM and DSCI are part of the global conferences and NASSCOM/DSCI will be hosting the 3rd EWI Global Cyber Security Summit in Delhi in 2012, which will be attended by top government, industry and technical experts from different countries.

4.12.7 Strengthening Telecom Security

Strengthening telecom security is a pillar of cyber security, especially through development of standards and establishment of testing labs for telecom infrastructure (equipment, hardware).

4.12.8 Collaborating in Specific Areas

Such areas for collaboration could include reduction of spam, malware, etc. A relevant example is the report released by the EastWest Institute and the Internet Society of China on "*fighting spam to build trust*". This is the first joint China-United States report on cyber security. Spam, which comprises as much as 90% of all email messages carried in NWs, irritates end-users, clogs NWs, and carries the malicious codes used by hackers for fraud and other crimes. To fight spam, the experts made two key recommendations: first, the creation of an international forum to deal with spam; second, that NW operators, ISPs and email providers follow mutually agreed best practices.[10]

[10] http://www.ewi.info/fighting-spam-build-trust