TASK FORCE MEMBERS

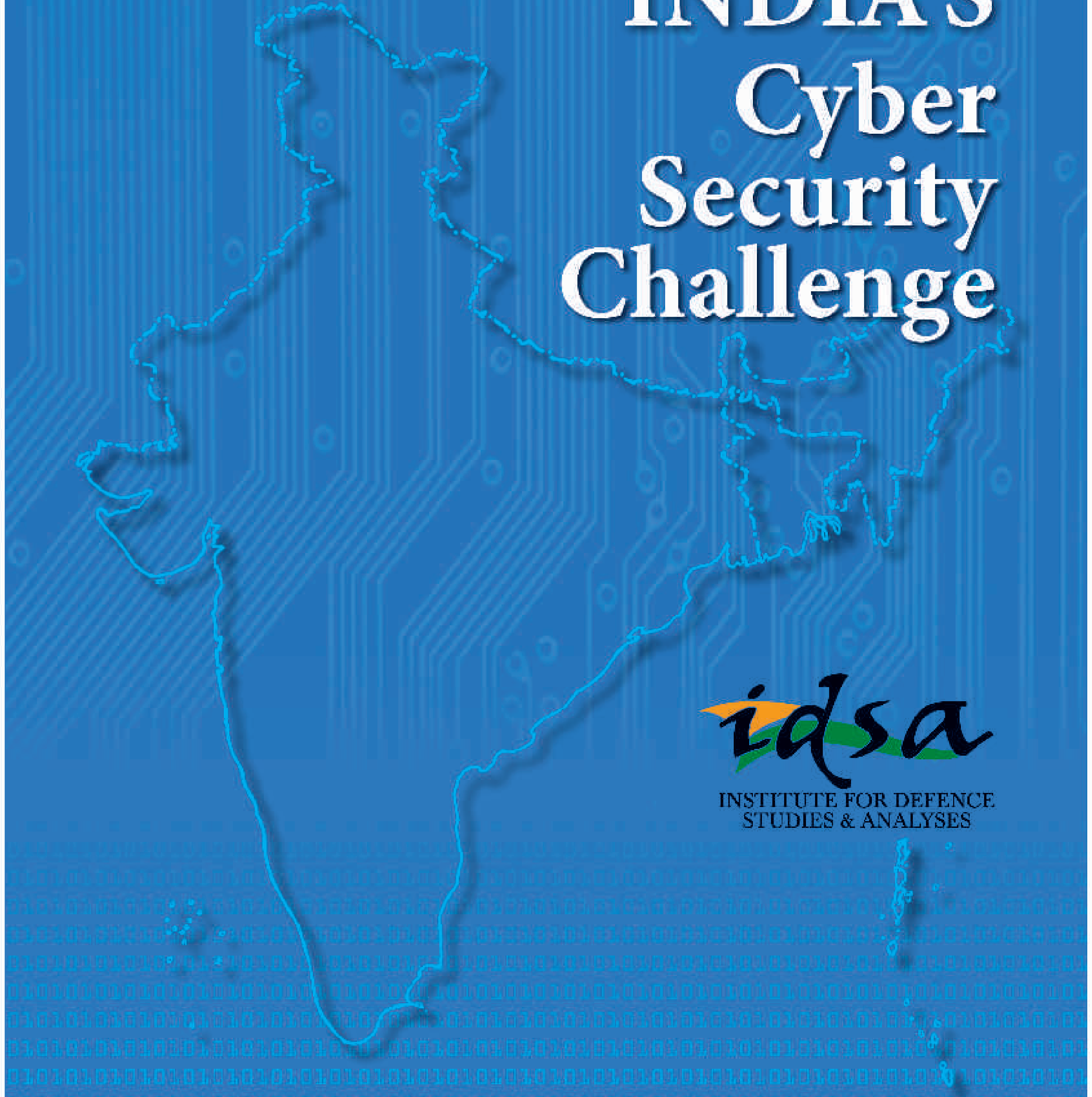
Nitin Desai
Arvind Gupta
Aditya Singh
Kamlesh Bajaj
B. J. Srinath
Salman Waris
Amit Sharma
Ajey Lele
Cherian Samuel
Kapil Patil

Institute for Defence Studies and Analyses
No. 1, Development Enclave, Rao Tula Ram Marg
Delhi Cantt., New Delhi - 110 010
Tel.: 91-11-2671-7983 Fax: 91-11-2615-4191
E-mail: contactus@idsa.in Website: http://www.idsa.in

ISBN 81-86019-98-7
9 798186 019985

IDSA Task Force Report

INDIA'S Cyber Security Challenge



idsa
INSTITUTE FOR DEFENCE
STUDIES & ANALYSES

IDSA Task Force Report

March 2012

INDIA'S CYBER SECURITY CHALLENGE

idsa
INSTITUTE FOR DEFENCE
STUDIES & ANALYSES

Map on the cover is only indicative and not to scale.

ISBN: 81-86019-98-7

Disclaimer: The views expressed in this Report are of the Task Force Members and do not necessarily reflect those of the Institute for Defence Studies and Analyses or the Government of India.

First Published: March 2012

Price: Rs. 125/-

Published by: Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
E-mail: contactus@idsa.in
Website: http://www.idsa.in

Layout &
Cover by: Vaijayanti Patankar and Geeta Kumari

Printed at: M/s Printline
H-10, IInd Floor, NDSE-I
New Delhi - 110049
Tel: (91-11) 24651060, 24643119
Mob: 9716335119
Email: printline2003@yahoo.co.in

Contents

Appendices

Acronyms and Abbreviations

APEC	-	Asia-Pacific Economic Cooperation
ARTRAC	-	Army Training Command
ASEAN	-	Association of South East Asian Nations
ATC	-	Air Traffic Control
ATM	-	Any Time Money
BPO	-	Business Process Outsourcing
BPR&D	-	Bureau of Police Research & Development
BSE	-	Bombay Stock Exchange
BSNL	-	Bharat Sanchar Nigam Limited
CBI	-	Central Bureau of Investigation
C-DAC	-	Centre for Development of Advanced Computing
CDTS	-	Central Detective Training School
CEITU	-	Council of Europe, International Telecommunication Union
CERT-In	-	Computer Emergency Response Team India
CFSL	-	Central Forensic Science Laboratory
CIA	-	Confidentiality, Integrity and Availability
CIDS	-	Chief of Integrated Defence Staff
CII	-	Critical Information Infrastructure
CISO	-	Chief Information Security Officer
CIW	-	Cyber and Information War
CIWEC	-	CIW Executive Committee
CS&IW	-	Cyber Security and Information Warfare
CSIS	-	Centre for Strategic and International Studies
DARPA	-	Defence Advanced Research Projects Agency
DDOS	-	Dedicated Denial of Service
DG	-	Director General

DIARA	-	Defence Information Assurance and Research Agency
DIT	-	Department of Information Technology
DNS	-	Domain Name System
DoT	-	Department of Telecommunications
DRDO	-	Defence Research and Development Organisation
DSCI	-	Data Security Council of India
DSF	-	DSCI Security Framework
DVD	-	Digital Versatile/Video Disc
ERNET	-	Education and Research Network
EU	-	European Union
FATF	-	Financial Action Task Force
GCHQ	-	Government Communications Headquarters
GDP	-	Gross Domestic Product
GGE	-	Group of Governmental Experts
GPS	-	Global Positioning System
GSLV	-	Geo-synchronous Satellite Launch Vehicle
GUCCI	-	Global Undersea Cable Communication Infrastructure
HQ IDS	-	Headquarter Integrated Defence Services
HR	-	Human Resource
IB	-	Intelligence Bureau
IBSA	-	India, Brazil, South Africa
ICANN	-	Internet Corporation for Assigned Names and Numbers
ICCIS	-	International Code of Conduct for Information Security
ICT	-	Information and Communications Technology
IDC	-	International Data Corporation
IETF	-	Internet Engineering Task Force
IGF	-	Internet Governance Forum
IPC	-	Indian Penal Code
ISEA	-	Information Security Education and Awareness

ISP	-	Internet Service Provider
ISRO	-	Indian Space Research Organisation
IT Act	-	Information Technology Act
ITU	-	International Telecommunications Union
IW	-	Information Warfare
J&K	-	Jammu and Kashmir
LEA	-	Law Enforcement Authority
LOAC	-	Laws of Armed Conflict
M.Tech	-	Master of Technology
MAG	-	Multi-stakeholder Advisory Group
MBA	-	Master of Business Administration
MCA	-	Master of Computer Applications
MHA	-	Ministry of Home Affairs
MMCR	-	Multi Medium Combat Role
MoD	-	Ministry of Defence
MTNL	-	Mahanagar Telephone Nigam Limited
NASSCOM	-	National Association of Software and Services Companies
NATO	-	North Atlantic Treaty Organisation
NCMC	-	National Crisis Management Committee
NCRB	-	National Crime Records Bureau
NCRC	-	National Cyber Response Centre
NCSP	-	National Cyber Security Policy
NCW	-	No Contact War
NDMA	-	National Disaster Management Authority
NeGP	-	National e-Governance Plan
NIB	-	National Information Board
NIC	-	National Informatics Centre
NICNET	-	NIC Network
NIIPC	-	National Information Infrastructure Protection Centre

NKN	-	National Knowledge Network
NOFN	-	National Optical Fibre Network
NPT	-	Non-Proliferation Treaty
NSA	-	National Security Adviser
NSCS	-	National Security Council Secretariat
NSE	-	National Stock Exchange
NTRO	-	National Technical Research Organisation
NW	-	Network
OECD	-	Organisation for Economic Cooperation and Development
ONGC	-	Oil and Natural Gas Corporation
P2OG	-	Proactive Pre-emptive Operations Group
PCs	-	Personal Computer
PLC	-	Programmable Logic Control
PPP	-	Public-Private Partnership
RAW	-	Research and Analysis Wing
RBI	-	Reserve Bank of India
SCADA	-	Supervisory Control and Data Acquisition
SDC	-	State Data Centre
STQC	-	Standardisation, Testing and Quality Certification
TA	-	Territorial Army
TRAI	-	Telecom Regulatory Authority of India
TV	-	Television
UK	-	United Kingdom
UN	-	United Nations
UNGA	-	United Nations General Assembly
US	-	United States
USCYBERCOM	-	US Cyber Command
VSAT	-	Very Small Aperture Terminal
WLR	-	Weapon Locating Radar

Preface

Airplanes were used militarily for the first time in the Italo-Turkish war of 1911. This was some eight years after the Wright brothers' maiden airplane flight. However, the recognition of airspace as a potential theatre of war may be said to have occurred when the first independent air command was formed with the establishment of the RAF towards the end of World War I in 1918. The use of airplanes for civilian purposes came before their military use. The military use itself evolved from supporting land and sea operations to the independent use of air power with strategic bombing, an evolution that took about a decade or so.

The present situation with regard to cyberspace is similar. The development of the Internet and low-cost wireless communication is the contemporary equivalent of what airplanes were a hundred years ago. Their use in economic, social and political transactions has increased at a rate that far exceeds the growth in airplane use over the last century. These technologies already play an important part in military operations in the traditional spheres of land, sea, air and the newer one of space. There are signs that they have been used for aggressive purposes by some states. There is also ample evidence of their use by criminals and terrorist groups. It is only a matter of time, like air power a hundred years ago, before cyberspace becomes an independent theatre of war.

There is one important nuance in the treatment of cyberspace as a fifth potential theatre of war along with land, sea, air and space. The use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks (NWs), telecom exchanges, routers, data servers, and so on. Protecting or attacking these is in the domain of the traditional arms of the military. Cyberspace as an independent theatre of war is about attacks that compromise the capability to use these facilities: they cannot be prevented by the security services in isolation. The defence of cyberspace necessarily involves the forging of effective partnerships between the public organisations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens.

The defence of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest. It is not possible for a country to ignore what is happening in any part of this space if it is to protect the functionality of the cyberspace relevant for its own nationals. Moreover, a key part of this space, the global Internet system, is still under the control of one country. Hence national defence and international cooperation are inevitably intermeshed. This means that a country's government must ensure coherence between its security policy and the diplomatic stance taken by it in multilateral and bilateral discussions on matters like Internet and telecom governance, human rights related to information freedoms, trade negotiations on infotech services, and so on.

There is another feature of cyberspace that complicates the design of security structures and policies compared to the other theatres of conflict. In cyberspace it is very easy for an attacker to cover his tracks and even mislead the target into believing that the attack has come from somewhere else. This difficulty in identifying the perpetrator makes it difficult to rely on the capacity to retaliate as a deterrent. Whom will you penalise when the perpetrator cannot be clearly identified? Moreover, the costs of mounting an attack are very modest. These two factors make cyberspace an ideal vehicle for states and non-state actors who choose to pursue their war aims through clandestine means. In this situation effective security policy for cyberspace requires a high priority for early warning, intelligence and pre-emptive defence.

The technologies that are used in cyberspace are still very new and are evolving rapidly. Hence investing in technological capacities to keep track of global developments, developing countermeasures and staying ahead of the competition is as central to the defence of cyberspace as the more conventional security measures.

This report argues that Government and the private sector should recognise these aspects, give cyber security some priority in their security and risk management plans, and do this jointly. Being a report that is addressed to the security community in the widest sense and intended to stimulate public discussion, it relies on publicly available information. Its central messages are:

- The need to strengthen the inter-ministerial coordination arrangements for cyberspace security under the National Security Adviser (NSA).
- The case for a new Cyber Command in the structure of the defence forces to manage cyber defence and cyber warfare.
- Public-private partnerships (PPP) for information security in identified sectors dependent on the use of IT.
- Legislative measures to handle the special features of crime and security in cyberspace.
- A proactive diplomatic policy to create an international legislative environment that can facilitate national defence.
- Capacity building all around to cope with a potentially crippling shortage of qualified personnel.

The process of preparing this report reflects the public-private and multi-sectoral nature of the problem. The initiative for doing this came from the Institute for Defence Studies and Analyses, New Delhi, the premier security policy think-tank in the country. The participants in the exercise included individuals with some exposure to Internet and telecom-related policy issues at the national and global level, former defence personnel, those involved in Internet and data security today, defence technology researchers, and a lawyer who specialises in cyber law. As the Chair of this eclectic group I wish to thank all of them for the time and effort they devoted to this exercise, mainly because of our shared perception that this area needs urgent attention. But above all I am grateful to Shri Arvind Gupta for his leadership on this issue not just in this group but also earlier. On behalf of the group I would also thank Shri Cherian Samuel from IDSA and Kapil Patil from Pugwash India who contributed greatly to the efficiency with which the group functioned.

Nitin Desai

New Delhi
March 2012

(NITIN DESAI)
Chairman, Cyber Security Expert Group, IDSA

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 70Acovers 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 prog ramme.

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

Chapter 5

Harmonising the National Legal Regime with the International Legal Regime

5.1 Areas for Intervention

Cyberspace has become, in present times, the fifth common space, along with land, air, space and sea. Technology has grown rapidly, and law has not been able to keep pace. Since the Internet and crimes committed thereon are not limited by geographic or territorial boundaries, it is becoming increasingly imperative that an effective mechanism be set up to curb the rampant growth of crime and terrorism online, by means either of an international legislation in this regard (which may be in the form of modifying existing legislation to suit cyberspace, or by way of setting up international agencies under the aegis of the United Nations to deal specifically with cyber crime and cyberterrorism) or to ensure international cooperation to achieve the end of harmonising existing national and regional cyber crime legislation to create a seamless, borderless cyberspace.

India was the 12th nation in the world to legislate on cyber law, adopting an IT Act, and has also brought about amendments to the Indian Penal Code (IPC) and the Indian Evidence Act to aid in cyber crime investigation. The government has made efforts towards putting in place an NCSP that addresses several areas related to cyber security, particularly incident response, vulnerability management and infrastructure security.

This chapter seeks to highlight some of the areas in which more regulatory and legislative intervention is needed in order to give a detailed perspective on harmonising the national laws with the international legal regime.

5.2 Legal Responses

In the absence of international legislation to curb the ever-increasing threat posed to the world at large by cyberterrorists, it has been proposed that existing legislation be modified to some extent and adopted at an international level. Two probable methods of doing so were: either to apply the Council of Europe Convention on Cyber crime at an international level; or to apply LOAC to Cyberterrorism.

5.3 European Convention on Cyber crime

The European Convention on Cyber crime is aimed at harmonising national cyber crime laws within the EU. Signatories to it numbered 34 in November 2001; as of December 2009 it had been signed by 46 states and ratified by 26.

Argentina, Botswana, Egypt, Nigeria, Pakistan and the Philippines, among others, have modelled parts of their legislation on the Convention without formally acceding to it. But compared to global standards, the number and speed of signature and ratification has remained an issue.[11] The convention was drafted mostly by and for European states, and is also now somewhat outdated.[12]

The treaty has been criticised as being fundamentally unbalanced. It includes sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but has no correspondingly detailed standards to protect privacy and limit government use of such powers.[13] Another concern has been that law enforcement interests have dominated the drafting process from the outset, and 19 drafts were completed before it was released for public comment. The Council of Europe has made little effort to address the concerns of other stakeholders in the process.[14] The problems relating to the definitions of terms in the treaty, privacy issues, and the investigative powers raise many concerns, including from India. In this light, the Convention is considered as largely symbolic; its long-term effectiveness has been brought into question on numerous occasions. Overall, it leaves too many loopholes in terms of the lack of definitions and inconsistencies that will allow criminals to continue to commit criminal offences. India chose not to emulate the convention because it would have introduced a completely alien legal framework into the Indian legislative process.

Current international law can be applied to cyber warfare if cyber warfare is viewed as involving the use of a new technology to gain military advantage. The concept of warfare is no longer restricted to armed attack in the traditional sense of the term. The crippling of critical information systems of a country, or cyber attacks that block government websites for a few hours, are also now being considered as methods of gaining military advantage. This only emphasises the pressing need for an international regime to check cyber crime and cyberterrorism. There would, however, be a corresponding need to also expand the definitions of key terms in international law such as sovereignty, use of force, armed attack, and combatants, so as to apply them in the cyber context.

[11] http://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf

[12] http://www.stlr.org/2010/03/a-global-convention-on-cyber crime/

[13] http://www.crime-research.org/library/CoE_Cyber crime.html

[14] Ibid.

While LOAC seems the most suitable existing international regime that might be extended to cyberterrorism and cyber crime, it also has a large number of limitations, as mentioned earlier, and would most likely not serve as an effective means of addressing the pressing issue of cyber crime. Aside from these specific issues in extending LOAC to the cyber context, LOAC would also suffer from the general concerns that arise in the application of international law.

International law is merely soft law, and most countries still give supreme sovereignty to their own municipal laws, even if they are not in consonance with international law, and as such, the application of LOAC would be highly subjective and would only apply when a country so desires.

5.4 Harmonisation of Legislation

The main obstacles in meeting cyber threats have been identified as: technical hurdles, lack of social responsibility, and inadequate international cooperation.[15] While the first and second issues can be overcome by increasing investments in technology, education and R&D, the greatest obstacle remains the reluctance of states to cooperate in cyberspace. Being transnational crimes, cyber crimes can only be tackled with the combined efforts of the international community. Regulations and cooperation agreements or the inclusion of an additional protocol on cyber crime to the Geneva Convention that may enable countries to assist each other in bringing to book offenders who use to their advantage the lack of an effective punitive mechanism are essential. The long-established national and international criminal codes were developed in an era prior to the Internet; criminal codes therefore need to be amended to create criminal offences to ensure the protection of information and communication in cyberspace. An impartial international body on the lines of Interpol can be set up to coordinate international efforts with regard to prevention of cyber crimes. Such an organisation could also act as a facilitating body in bringing about harmonisation of cyber crime legislation among the member nations.

In the last couple of years alone, a large number of countries, including Russia, Japan, Australia, USA, Canada, Ireland, Cameroon, Namibia, Kenya, Bangladesh, Jordan, UAE, Jamaica, Portugal and Norway have enacted laws relating to cyberspace or amended substantially the existing national law in this regard. Over a period of two decades, regional organisations have sought to establish uniform Internet regulations at a regional or local level, including the Council of Europe, ITU, ASEAN, OECD, NATO, Commonwealth of Nations, APEC,

[15] *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway,* East West Institute, April 2010.

League of Arab States, Organisation of African States, Shanghai Cooperation Organisation and the G-8 countries.

Despite the efforts made by countries and regional organisations in last 20 years, apart from a few common trends, there are considerable variations in national cyber crime legislation. The main reason for this is the variance of the effect of cyber crimes on different countries. Spam, for instance, is a bigger threat to developing countries than developed countries. Similarly, certain online content may be unlawful in some countries while others may protect it under the freedom of speech. It is therefore clear that such issues cannot be addressed at a local or regional level and it is necessary to develop a common understanding in the international community and harmonise legislation.

Consequent to the need for an effective machinery to address cyber crime in India, the IT Act, 2000 was enacted in keeping with the Model Law on Electronic Commerce adopted by the UN General Assembly in 1997. The IT Act criminalised tampering with computer source documents, hacking, and publishing of obscene information in electronic form under Sections 65, 66 and 67. These provisions were, however, found inadequate and the 2008 amendments, which came into force in 2009, widened the scope of cyber crime, criminalising a greater number of offences than its predecessor. Section 66F was the most significant as it for the first time defined and criminalised cyberterrorism, making it punishable with life imprisonment. Amendments have also been made to the IPC to criminalise cyber offences and set out procedures and punishments for the same. However, there still is a huge gap between existing laws and the required laws to fully combat cyber threats. To bridge this gap DIT issued a Discussion draft on NCSP on 26 March 2011. It called for greater international cooperation which can be achieved through the harmonisation of national laws and enforcement procedures. Dynamic legal framework in synchronisation with technological changes and international developments in the area of information security has been pointed out as an area of priority.

5.5 Criminalisation of Cyber Offences

The Preamble of the European Convention on Cyber crime laid down as its objective the prevention of action directed against CIA of computer systems, NWs and computer data as well as the misuse of such systems, NWs and data. To counter such activities the convention suggested that certain conducts be classified as criminal offences and procedural measures be introduced to investigate these crimes.

Cyber crimes usually originate from states with comparatively lenient laws and enforcement mechanisms. Domestic laws do sometimes cover electronically perpetrated crimes but are not always effective in their application and enforcement. They may provide for insufficient punishment, antiquated definitions of key elements, or words may render a provision of law inapplicable and there is always the problem of jurisdiction. Singapore is the only exception where the law provides that in the case of certain specified offences, even if an offence is committed outside its borders, courts in Singapore shall have jurisdiction to hear the same.

The key elements of effective cyber deterrence have been identified as: first, attribution (understanding who perpetrated cyber attack); second, location (knowing where the strike came from); third, response (being able to respond, even if attacked first); and lastly, transparency (being the cyber criminal's knowledge of a state's capability and intent to counter cyber attacks with massive force).[16] These principles should be incorporated in all cyber legislation for it to be an effective deterrent. Criminalisation of illegal access, illegal interception, illegal data interference, illegal system interference, computer-related fraud and forgery are the standard provisions in most cyber laws enacted in countries around the world. However, some countries have taken stricter action and have also criminalised the production and distribution of tools (both software and/or hardware) that can be used to commit cyber crime, acts related to child pornography, "grooming" or hate speech.

Cyber law in India has been primarily developed to further e-commerce. However, elements of cyber deterrence have been introduced through criminalisation of various offences. The IT Act and the IPC have included tampering with source-code documents, hacking, publishing and transmitting of obscene electronic information, and misrepresentation of any material facts to the Certifying Authority for procuring a digital signature certificate as criminal offences. Efforts have been made by the government in this direction, but several loopholes in law still exist. Additional resources, time and efforts are needed to effectively tackle the problem. Allocation of more funds in addition to a comprehensive cyber security plan is the primary means to improve and strengthen cyber security in India. It is imperative that substantive laws dealing with illegal access, illegal interception, data interference, misuse of devices, computer-related forgery, child pornography, etc. must be implemented. Besides, procedural laws also need to be in place to achieve cooperation and coordination of international organisations and governments to investigate and prosecute cyber criminals.

5.6 National Security and Issues Relating to Privacy and Freedom of Expression

The paradox is that security measures intended to protect a democracy can end up actually eroding civil liberties like individual privacy and freedom of expression that are at the heart of the democratic setup: the right balance needs to be struck between national security and civil liberties.

[16] Ibid.

With various government initiatives on national security, like the National Grid, designed as an NW of 21 available databases across government and private agencies and meant to help flag potential terrorist threats and also the Aadhar programme, for issuing unique identity numbers, there have arisen serious concerns about privacy as personal data are compiled in central databases and accessed by the various government agencies. It is essential that proper amendments or necessary laws like a separate data protection/privacy legislation be put in place to safeguard against the misuse of such personal information and protect individual privacy.

Similarly, there need to be put in place proper legislative as well as procedural measures to ensure that the freedom of expression guaranteed under Article 19 of the Constitution is not compromised at the altar of national security.

5.7 Investigation Procedures

Due to the peculiar nature of cyber crime, existing methods adopted by investigative agencies have been largely unsuccessful. Owing to the ease with which identities can be changed and data altered and destroyed, it becomes difficult to obtain evidence and perform investigative procedures. Specific search-and-seizure procedures, expedited preservation of computer data, disclosure of stored data, interception of content data and collection of traffic data are some of the comprehensive regional frameworks specially put in place to further cyber crime investigation.

The identification of path of packets with the help of ISPs, seizure of computers and storage media, collection of traffic data in real time, establishing jurisdiction over substantive offences and the power to collect data in real time are some of the investigative techniques that may be used by agencies.

With regard to investigative procedures, the cases that brought to light the need for the development of specific cyber crime investigative measures, the different procedures and techniques developed at regional and national levels, the provisions required by law agencies to work more effectively and differences in approach in common law and civil law countries are the key points that need to be deliberated upon to plug the existing loopholes in investigative techniques, that play a significant role in poor cyber deterrence.

The foremost challenge that cyberspace in India faces is the multiplicity of cyber offences that have led to an urgent need to place adequate tools for investigation and prosecution. The Central Forensic Science Laboratories and General Examiners of Questioned Documents at Chandigarh, Hyderabad, Kolkata and Shimla, and CFSL and CBI at New Delhi are the major computer forensic centres set up in India. In spite of the efforts of the government to set up such centres, the cyber crime fighting infrastructure remains inadequate. The fact that cyber criminals are highly educated is a huge challenge for the investigative agencies, since most investigating officers are not as technically well versed as the offenders.

The CPC only makes scientific examination conducted by a certain specified laboratory admissible. This has increased the workload, thus leading to an urgent need to substantially expand the number of the computer forensic laboratories in India. Greater investment is required in the development of training centres for law enforcement officers and upgrading police stations so they can house the essential infrastructure to investigate cyber crime. Computer forensics must be the focal point for modernisation of the police force and other investigative agencies in India. Besides, 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.

5.8 International Cooperation

As mentioned earlier, international cooperation is increasingly becoming the cornerstone for the development of an effective legal framework against cyber crime. Limited number of treaties and agreements, disparity between the legislation of nations, varying policies and procedures of states act as major deterrents to the development of an effective global understanding and agreement on the subject. Extradition laws, mutual legal assistance in criminal matters, and cooperation for the purpose of confiscation are some of the legal procedures necessary to garner international cooperation.

Four main sources for international cooperation have been identified. International agreements like the United Nations Convention against Transnational Organized Crime and the Council of Europe Convention on Cyber crime are recognised as the foremost instruments to build formal cooperation among nations. Regional treaties on international cooperation, like the Council of Europe, Inter-American and Southern African Development Community conventions on extradition or mutual legal assistance in criminal matters are the second recognised source.

Bilateral agreements on extradition and mutual legal assistance containing provisions regarding the kind of requests that can be made, the modes of contact used, rights and obligations of the requesting and requested states and procedures to be followed form the third source of international cooperation. Lastly, domestic laws dealing with international cooperation, like assistance on reciprocal or a case-by-case basis, can also be used effectively.

International cooperation is seen as a very important aspect in the fight against cyber crime in India. Article 51 of the Directive Principles of State Policy provides that the state shall endeavour to promote respect for international law and treaty obligations. Article 253 empowers Parliament to make laws for implementing any international treaty, agreement or convention. The IT Act under Section 75 gives extraterritorial jurisdiction to the Act if the offence committed involves a computer, computer system or NW located in India. It shall apply to all persons irrespective of their nationality. Hence, it is essential that the government should lobby at an international level for the harmonisation of existing national legislation to ensure that laws provide a fair measure of deterrence to cyber criminals and cyberterrorists, thereby making cyberspace a safer place for national and international transactions.

5.9 Electronic Evidence

The collection and admission of electronic evidence pose separate sets of challenges for LEAs. When it comes to digital crime, the evidence is often at the byte level, deep in the magnetics of digital media, initially invisible to the human eye. That is just one of the challenges of digital forensics, where it is easy to destroy crucial evidence, and often difficult to preserve correctly.[17] Another challenge faced by digital forensics is that the fundamental aspects of the field are still in development. Whether it is the terminology, tools, definitions, standards, ethics and more, there is a lot of debate amongst professionals about these areas.[18] Provisions concerning the handling and admissibility of electronic evidence, the analysis of different approaches used to identify electronic evidence in common-law and civil-law countries and the development of common principles are focal study points.

The Indian Evidence Act 1872 has been amended to include provisions dealing with the admissibility and recognition of electronic evidence by the courts. The various legislative amendments to accommodate and recognise the changes that the advent of the Internet has brought about are an indicator of progress with respect to the admissibility of digital evidence. Courts' affirmative outlook towards recognising digital evidence is a step forward towards the appreciation of digital evidence. However, there is still a long way for India to go to be at par with global developments. There is an urgent need for trained and qualified experts to deal with the highly specialised field of cyber security. Also, 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.

5.10 Liability of ISPs

ISPs with LEAs play a significant role in building trust in online transactions and making the best use of multifaceted technology. The character of cyber crime is such that even though the offender acts alone, several entities get automatically involved. For instance, sending a simple email requires the service of the e-mail provider, access providers and the routers who forward the e-mail message to the recipient. In achieving this objective these organisations are faced with the dilemma of how best to collaborate with each other to make the Internet safer without infringing the fundamental rights of users.

[17] https://www.infosecisland.com/blogview/16705-Digital-Evidence-and-Computer-Crime.html

[18] Ibid.

The role of ISPs is essential as it is not possible to commit cyber crime without their involvement in one way or another. But it is not always possible for the ISPs to prevent the commission of cyber crime. The point to be looked into is whether their role should be limited. The implications of the answer directly affect the economic development of the ICT infrastructure.

The discussion draft on NCSP suggests that ISPs must be closely associated in providing for secure information flow through their NWs and gateways. Legally binding agreements to support law enforcement, information security incident handling and crisis management processes are the need of the hour. Differentiating between different service providers to regulate their responsibility, limitation of responsibility and the possible areas of cooperation with LEAs to prevent cyber crime need to be analysed.

The role and legal responsibility of the NW service providers in India has been defined by the IT Act. Section 79 restricts the liability of service providers in certain cases. It provides that the service providers shall not be responsible for any third-party information or data provided by them if they had no knowledge of it or had exercised all due diligence to prevent the offence from being committed. However, these provisions shall not apply if the service provider has conspired, abetted or aided in the commission of the offence or where the ISP fails to cooperate with the government in preventing the commission of an unlawful act.

Their liability in India is also determined by Licence for Internet Services, Clause 33 and Clause 34 of which set out the various responsibilities of the service providers, some of which are:

- ISPs must prevent unlawful content, messages or communications including objectionable, obscene, unauthorised content from being carried on their NW.
- They must ensure that content carried by them does not infringe cyber laws.
- They must comply with the IT Act provisions and must assist the government in countering espionage, subversive acts, sabotage or any other unlawful activity.
- Privacy of communication online is ensured by preventing unauthorised interception of messages.
- Government can take over their equipment and NWs in times of emergency, war, etc.

The role of NW service providers is an important one and needs to be strengthened to tackle cyber crime. The draft NCSP also states that the NW services providers must play a greater role in the betterment of cyber security in the county. DoT shall provide guidelines to service providers to guarantee the uninterrupted availability and development of alternate routing in case of physical attacks on the NWs. It sets out that the ISPs must ensure compliance with international security best practices, service quality and service level agreements, keep up with changing technology, make sure that all legal obligations are complied with, and develop crisis management strategies and emergency response plans.

5.11 Conclusion

Cyberspace being the fifth common space, it is imperative that there be coordination, cooperation and uniformity of legal measures among all nations with respect to cyberspace. The exponential growth of cyberspace is possibly the greatest development of the current century. Unfortunately, this development has also led to the near-simultaneous growth of the misuse of cyberspace by cyber criminals and in recent times. Cyberspace has been vulnerable to a large number of attacks on crucial information infrastructure by cyberterrorists. The peculiar nature of cyberspace implies that existing laws are largely ineffective in curbing cyber crime and cyberterrorism, thus creating an urgent need to either modify existing legislation or to enact laws that are effective in checking the growing menace online. Internet security is a global problem and cyber crime and cyberterrorism are increasingly becoming a worldwide nuisance. Only international cooperation will enable the nations of the world to crack down more efficiently on cyber crime and ensure healthy development of the Internet.

Since the Internet is not limited by national geographic boundaries, it requires that any regime that is set up with regard to the Internet be one that is applicable not only to a given state, but should have global application anywhere on the Internet. To meet this end, it is the need of the hour that nations of the world cooperate and make constructive efforts to reduce vulnerabilities, threats and risks to manageable levels. Attempts that have been made so far, including the European Convention on Cyber crime or the OECD Guidelines and even the probable extension of LOAC to cyberspace are not without their respective glaring loopholes and deficiencies.

This is increasingly taking the shape of a global crisis that can only be contained by harmonising various national legislations and creating an international regime that is not a result of tweaking outdated pieces of legislation, but by proactive steps being taken by countries towards making the Internet a seamless space, not one that is a haven for terrorists due to lack of legislation, investigative agencies, enforcement mechanisms and, above all, due to lack of international cooperation.

It is time that the countries of the world, including India, realise that a well-protected cyberspace would only be an asset to developing and developed nations alike. With regard to the present legal situation in India, certain commendable advances have taken place that have placed India in a relatively strong position. However, there are still gaping loopholes not only in legislation but also investigation and enforcement that have allowed India to become prey to cyber crime.

CHAPTER 6

RECOMMENDATIONS

6.1 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, cyberterrorism, cyber warfare and CII protection.

6.2 TO 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 cyberterrorism.** To handle cyberterrorism and cyber crime, a slew of measures will be needed, ranging from monitoring and surveillance, investigation, prosecution, etc. Cyberterrorism 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 cyberterrorism. 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 cyberterrorism 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.

6.3 Specific Recommendations

(These recommendations deal with specific technical and legal measures to strengthen cyber security. They are being flagged in view of their criticality. They can be part of the action plans and roadmaps to be developed by NIB, NSCS, DIT, MOD, MHA, etc.)

- 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 cyberterrorists.
- **International cooperation** is crucial to handle cyber crime, cyberterrorism 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.

6.3.1 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.

6.3.2 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.

6.3.3 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 cyberterrorists, 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 so as to safeguard against the misuse of personal information by various government agencies and protect individual privacy.

6.3.4 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.

APPENDIX 1

PROPOSED COORDINATION STRUCTURE FOR CYBER AND INFORMATION WAR

PROPOSED COORDINATION STRUCTURE FOR CYBER AND INFORMATION WAR(CIW)

1. NSA with the NSCS should be the national controlling and coordinating agency for CIW. An omnibus board could be created in the NSCS along with a CIW Executive Committee(CIWEC). These could be established by the NIB. Recommended composition and roles of these two bodies in brief is given in the succeeding paragraphs.

CIW BOARD

2. Composition

Amongst others:

(a) **Chairman**. NSA.

(b) **Members Government**. Cabinet Secretary, DG RAW, Secy DIT, Representatives (Reps) from MHA, MEA, I&B, Ministry of Power.

(c) **Members Ministry of Defence**. CIDS(Or CDS when created) and DG DRDO.

(d) **Private Sector**. Chairman NASSCOM.

(e) **DG CIW.**

(f) **Member Secretary(Secy)**. Dy NSA.

Notes:

i. Reps of ministries should be of a status in keeping with other members of this Committee.

ii. The Board may invite or co-opt technical or other experts as required.

iii. The Board should meet at least once a quarter or as required.

3. Charter

(a) Overall review and policy for CIW.

(b) Formulation of strategy for meeting emerging threats.

(c) Ensure necessary coordination between all public and private agencies at the national level as also monitor implementation of all aspects of CIW.

(d) Ensuring all international treaties and agreements are vetted in keeping with needs of national security.

CIWEC

4. Executive Committee

The Dy NSA who is the Secy of the Apex Body could chair the CIWEC, DG CIW will be the Secy with support from the NSCS. He will be responsible to ensure day to day coordination and follow up on all CIW issues and report to the apex body through Dy NSA. The composition of this CIWEC could include:-

(a) **Members Public Agencies**. Chairman NTRO, DG CERT, Reps from MHA, RAW, CSIR, DIT, Public IT related services, ie, Finance, Railways, Telecom, Civil Aviation, Power, HR and I&B. Also reps from Rep from MEA who is an expert on international agreements.

(b) **Members MoD**. Rep IDS. Reps of Cyber Command(When formed) & DRDO.

(c) **Private Sector**. Reps from NASSCOM representing different spheres of the IT industry.

(d) **Academic Institutions**. At least three.

5. Charter

CIWEC will be a coordinating agency which will issue policy guidelines and monitor all activities on a regular basis. Its organization will be flexible to ensure representation of all agencies. Sub groups could be formed for specific aspects such as proactive defence or protection of critical infrastructure. The CSIWEC will meet at least once a month to oversee and report progress on all issues which include:-

(a) NCSP as also international cooperation in this regard. All agreements on IT with respect to needs of national security. This will also include recommendations for simplifying and laying down flexible procedures to meet requirements of the IT domain.

(b) Technology development for protection of NWs and systems, as also proactive defence.

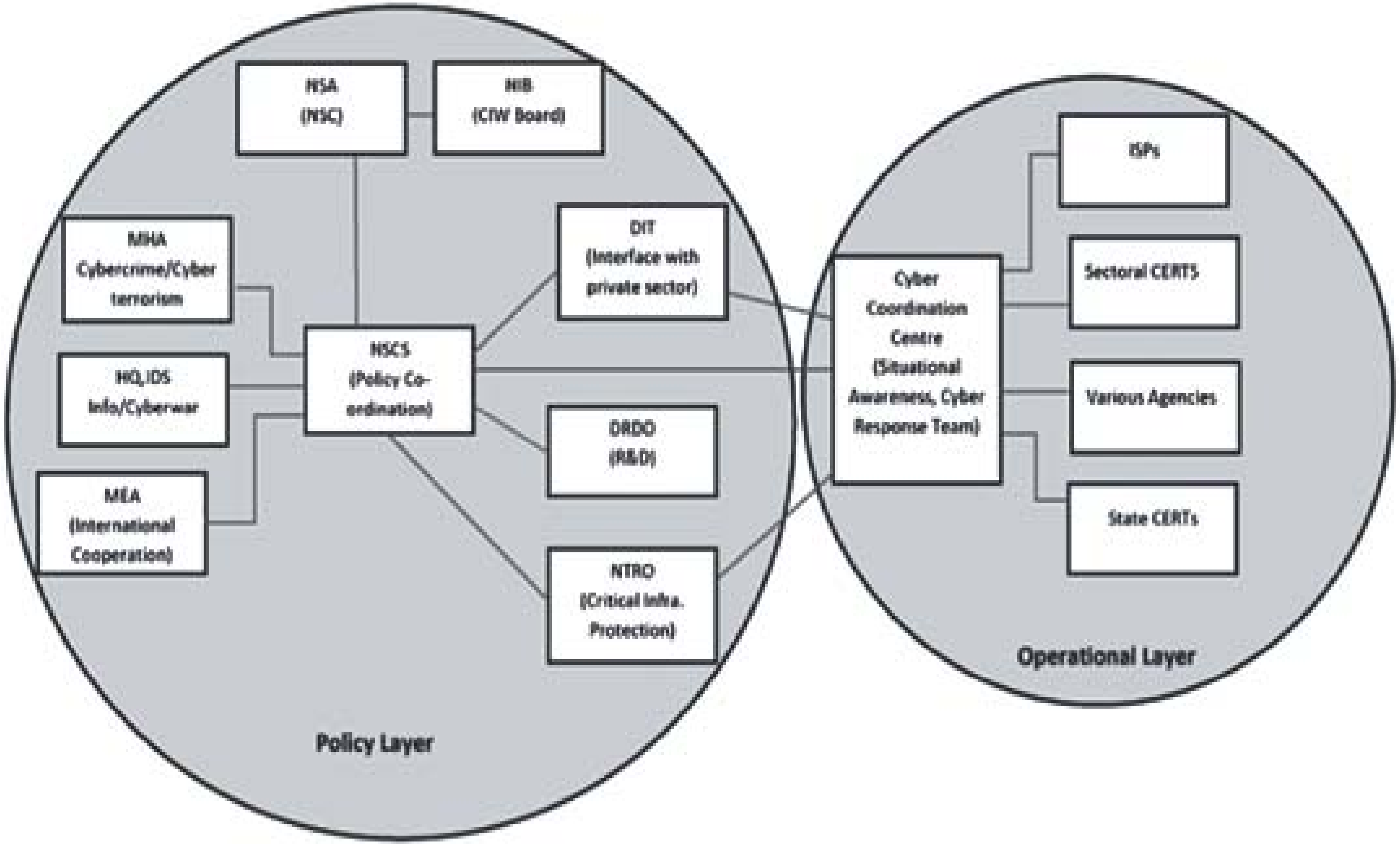
(c) Installation of systems, monitoring and response management, specially for emergencies.

(d) Development of HR and public awareness.
Recommendations for funding in this regard both in the public and private spheres.

(e) Standardization and certification. This will include creation of test beds.

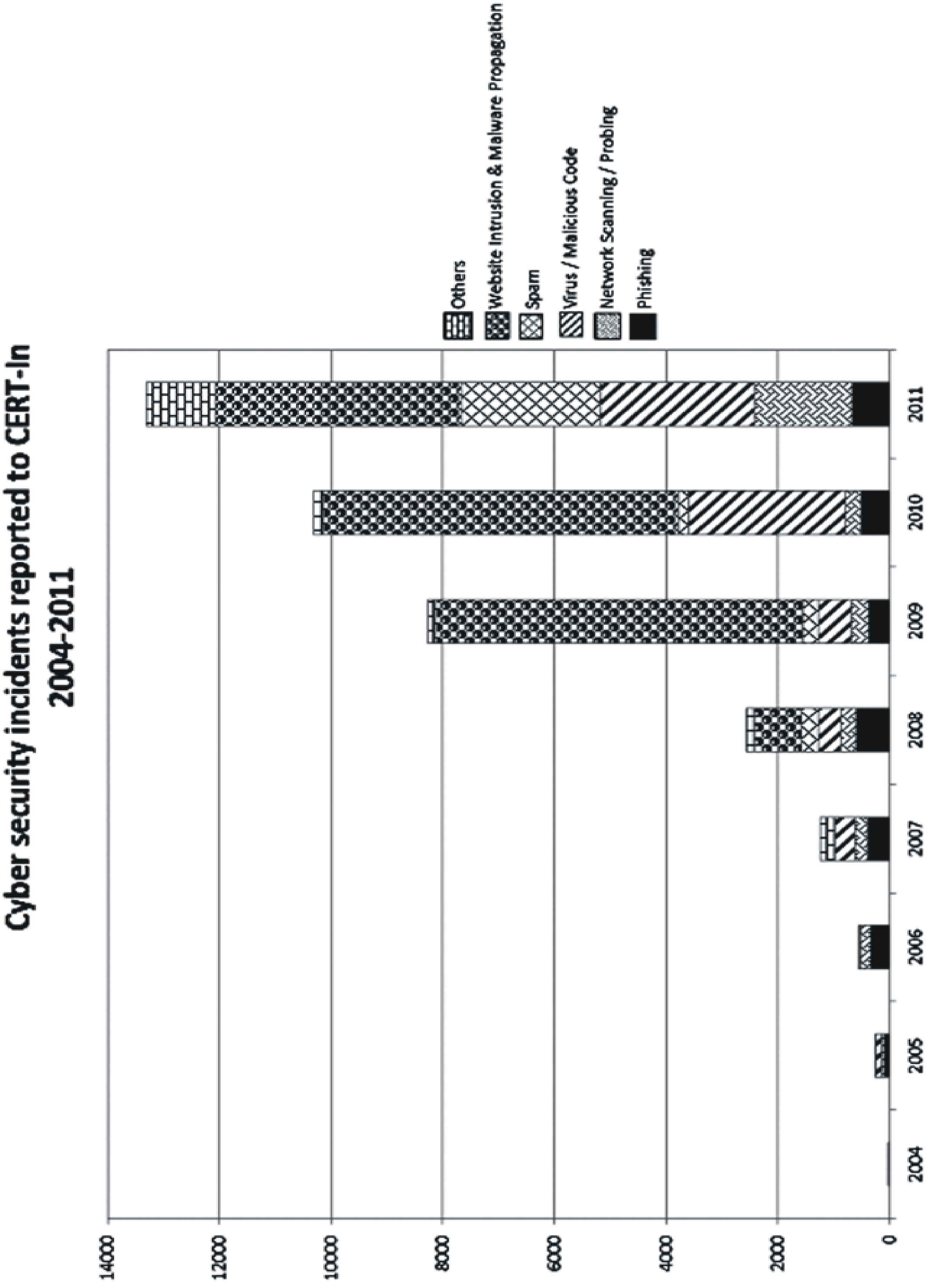
6. Organisation & Functioning

CIWEC should be an empowered body. DG CIW should be of appropriate level to ensure executive action and compliance by agencies. All public agencies like the DRDO, HQ IDS, NTRO, DIT, National CERT, CSIR, NIC are represented and could constitute its executive arms. For necessary coordination and follow up, the office of DG CIW in NSCS must comprise of security, legal and technical experts. It could be a small body to start with. Allocation of business rules must formalize functioning. Policy and conduct of offensive cyber operations could also be coordinated by a sub group drawn from the above.


NSA
(NSC)
NIB
(CIW Board)
MHA
Cybercrime/Cyber
terrorism
HQ, IDS
Info/Cyberwar
MEA
(International
Cooperation)
NSCS
(Policy Co-
ordination)
DIT
(Interface with
private sector)
DRDO
(R&D)
NTRO
(Critical Infra.
Protection)
Policy Layer
Cyber
Coordination
Centre
(Situational
Awareness, Cyber
Response Team)
ISPs
Sectoral CERTS
Various Agencies
State CERTs
Operational Layer

Appendix 2

Cyber Security Incidents 2004-2011



Appendix 3

Speech of Mr Sachin Pilot, Minister of State for Communications and Information Technology, at the London Conference on Cyberspace

London, 1 November, 2011

The internet is arguably the most important invention of the previous century. An increasing proportion of the world's population is migrating to cyberspace to communicate, enjoy, learn, and conduct commerce. With this, new possibilities and opportunities are opening up. With the free flow of information to everyone at marginal incremental cost, businesses can reach clients and governments can reach citizens quickly, almost free, and directly. Internet has truly been an agent of change – a change for the better.

Cyberspace is not restricted by conventional physical boundaries. If we attempt to trace digital pathways, we will find that the entire world is connected as never before. These connections are more numerous than air routes, rail networks, highways, shipping lanes, and even dust tracks put together. Cyberspace will define the future of humanity, and the only restrictive aspect is the limits of our imagination to leverage it for improving the lives of our citizens.

Mobile phones, tablets, and computers are not just means of communication, but are tools of empowerment. The cyber world is also fostering collaborative creativity and sharing of expertise. To derive maximum benefit from cyber space on a social scale, all states must strive to provide universal digital access.

India has been growing at an impressive rate of 7-9 percent in recent years, and will continue to do so in the near future. Along with economic prosperity has come an expected shift in how we conduct governance, economic activity, and even our personal lives. There has also been an exponential growth in the dominance of IT networks, and the increased importance of these networks to the way we live. Internet users in India have gone up from 5 million in 2000 to 100 million in 2011. Globally there was just 1 website in 1990, 130 websites in 1993, 100,000 websites in 1996 and 200 million websites today.

India has one of the most ambitious National e-Governance Plan (NeGP) to create a citizen-centric and business-centric environment for governance. The NeGP was approved by the Government in 2006 with the objective of creating the right governance and institutional mechanisms, capacity building initiatives, core infrastructure, policies & standards, and necessary legal framework for adoption of e-Governance in the country.

The NeGP is a comprehensive plan and is being implemented all the way down to our local governments. Under the plan, more than 1100 government services will be online; State Data Centres (SDCs) will serve as the repository of data at state level; and, the National Knowledge Network (NKN) will connect about 1500 institutes and organizations of higher learning, research, and governance.

The Electronic Delivery of Services Bill provides for delivery of public services by the Government to all persons by electronic mode to enhance transparency, efficiency, accountability, accessibility and reliability. The 'Unique Identity' project providing a unique number to each citizen is yet another link that will help us take government services to citizens more easily and efficiently.

Economy activity everywhere has become heavily reliant on IT networks because of cost-effectiveness, the ability of IT solutions to make business processes more streamlined and integrated, improving transparency and reaching out to consumers. While big businesses in India have been heavy investors in IT for a while, it is small and medium scale businesses that are joining the cyber world in large numbers now.

Using IT solutions and the internet is no longer a luxury, but a necessity for Indian companies to be able to compete domestically, and also globally. With an increasing number of people with access to the internet, and advancements in mobile banking and mobile trading, online financial transactions are fast becoming a reality for everyone.

India is also sharing its expertise in the IT sector with other countries. We have set up a Pan-African Network, in which 47 African countries now participate. This is one of the biggest projects of distance education and tele-medicine ever undertaken in Africa. It is also equipped to support e-governance, e-commerce, infotainment, resource mapping and meteorological and other services in the African countries.

The total number of broadband subscribers in India at nearly 13 million is set to rise rapidly with an expanding broadband infrastructure. The Government has approved a scheme for the creation of a 'National Optical Fibre Network' (NOFN) for providing broadband connectivity at village level, which will help in offering governance, banking and health services online. In addition to connecting all villages with broadband in the next 2 years, the government is working together with the industry to provide an improved business environment for the broadband industry, bring prices down through increased competition, and ensure high quality connectivity.

Under the National Broadband Plan, India will connect 160 million Indian households with high-speed Internet connections by 2014. We want every Indian to be connected to the information highway. In urban areas, mobile penetration rates have risen exponentially. Broadband connectivity too is on the rise. However, our focus now is on ICT penetration in rural areas where a large number of potential beneficiaries of e-governance actually reside. As a nation, we are committed to ensuring that the benefits of cyber space reach every corner of the country.

Our draft Information Technology policy, which is up for public comments, proposes to make Internet access a right of our citizens. No other county of India's size and diversity is moving so steadfastly in this direction. We are preparing for the future, and the policy framework will establish a digital infrastructure that will not only take care of India's immediate needs, but also sustain India's growth over the long-term.

Along with equity, we should also be concerned about issues of privacy. From social networking sites to financial transactions, an increasing number of us have an online personality. Who owns the rights to digital data of individuals? Another issue of global concern is 'freedom of speech' online. Dictating individual/ corporate behaviour online is not advisable but we do need to have a debate on norms of behaviour.

Unfortunately a more active cyber space is also inviting more malicious activity whether it is related to online fraud, theft of information or disruptive activities that may manifest in many forms including attacks on critical national infrastructure. These developments are likely to concern all such nation states that are increasingly relying on use of internet to improve governance and make the growth process more inclusive.

At stake are concerns about confidential data being used for illegal activities; the very survival of new business models like e-commerce is also dependent on the security of cyber systems. We know that in recent years, there has been a sharp rise in the number of cyber attacks, which we are closely monitoring. India is not alone in being the target of such acts. The UK and many other countries have been at the receiving end too.

Ensuring cyber and IT security is hard because networks can be attacked from anywhere in the world, and the motives to attack them may include simply demonstrating technical prowess, casual hacking, political orientation, fraud, crime or an extension of state conflict. Further still, digital footprints are easy to hide. Global coordination can ensure that the internet continues to thrive without the constant fear of misuse of information.

We have to think of safety in the cyber world as a global public good and address this problem together. Many countries, including India, have called for a discussion on whether laws covering international armed conflict, such as those under the Geneva Convention can also cover cyber attacks. India was one of the strongest voices at the 47th Munich Security Conference this year arguing for such a review.

India remains committed to being a responsible member of the international community and a willing participant in efforts to stimulate action around this issue. Together we can ensure that the information highways are secure. At the global level, we can coordinate our efforts on multiple fronts including setting standards, safeguarding digital intellectual property rights, sharing best practices, capacity building of developing countries, providing critical intelligence information, and establishing relevant security parameters. As the cyber world continues to unravel itself at a breakneck speed, our efforts to create and maintain a safe cyber space for individuals, corporations and countries remains a challenge that will require all of our collective efforts to come to the fore sooner rather than later.

Thank you.

(Courtesy: UK High Commission)

APPENDIX 4

SELECT PARLIAMENTARY QUESTIONS RELATED TO CYBER

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

Lok Sabha Starred Question No 160

Answered on **08.03.2010**

NATIONAL CYBER SECURITY POLICY

160. Shri PRALHAD VENKATESH
JOSHI
GANESH SINGH

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:-

(a) whether the Government has formulated a National Cyber Security Policy to deal with the unabated cyber crimes challenging the security and sovereignty of the nation;

(b) if so, the details thereof and if not, the reasons therefor;

(c) whether the Government has developed and established any Cyber Security system which can instantly detect any cyber crime/hacking attempts to take pre-emptive action to diffuse such criminal act;

(d) if so, the details thereof and if not, the reasons therefor;

(e) whether an audacious attempt was recently made by some foreign based hackers to hack the computers of some important offices of the Government of India; and

(f) if so, the details thereof along with the action taken by the Government in this regard?

ANSWER

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (ANDIMUTHU RAJA)

(a) to (f) A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. 160 FOR 8.3.2010 REGARDING NATIONAL CYBER SECURITY POLICY

(a) and (b) As a prelude to having a

National Cyber Security Policy, the Government as formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Further, an information security action plan for protection of critical information infrastructure is in place. The plan is aimed at enabling Government and critical sectors in improving the security of their Information Technology systems and networks and verification through periodic risk assessments and annual audits by third party auditing organizations. The plan has been circulated to Government and critical sector organizations. In accordance with information security action plan, Government and critical sector organizations are required to do the following on priority: ' Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a 'Point of contact', responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology (DIT). ' Prepare information security plan and implement the security control measures as per IS/ISO/IEC 27001: 2005 and other guidelines/standards, as appropriate. ' Carry out periodic Information Technology security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/ objectives. ' Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for Information Technology systems and networks. Especially, Test and evaluation may become necessary after each significant change to the Information Technology applications/ systems/ networks and can include, as appropriate the following:

Penetration Testing (both announced as well as unannounced)

- Vulnerability Assessment
- Application Security Testing
- Web Security Testing ' Carry out Audit of Information infrastructure on an annual basis and when there is major up gradation/change in the Information Technology Infrastructure, by an independent Information Technology Security Auditing organization. ' Report cyber security incidents, as and when they occur and the status of cyber security, periodically to CERT-In. In support of the above action plan, Indian computer Emergency Response Team (CERT-In) has created a panel of 40 Information Technology security auditors to help the organizations to get their Information Technology infrastructure and information systems audited from the point of view of Risk assessment, penetration of network and vulnerability assessment.

(c) and (d) National Informatics Centre (NIC) provides network and systems services to Central Government and State Government departments. As a service provider, NIC has installed state-of- art Cyber Security System, which monitors the events on the network for detection and prevention of malicious traffic on the network. The Cyber Security System includes:

Intrusion Prevention Systems, Firewalls, Anti-virus solution and application firewalls.

Similarly, other large Government organizations running services on their own also have installed Cyber Security System to protect their Systems and Network. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Section 69B empowers Government tomonitor and collect traffic data or information through a computer resource for Cyber Security. The Indian Computer Emergency Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development. Sectoral CERTs have been functioning in the areas of defence and Finance for catering critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

(e) and (f) There have been attempts of foreign origin from time to time to penetrate high security cyber network operating in some important offices of the Government of India. Investigations have revealed that these are merely attempts and no system has been found to be hacked or infected. National Informatics Centre has been conducting the security audit of the computer systems at regular intervals and has not found any hacked systems or infected. The following attempts have been detected on the network of NIC, in the recent past:

- Maliciously crafted email with attachments containing malware to a number of mail recipients attempting to infect the client machines.
- Scanning and probing of IT infrastructure. These attacks have been observed to be coming from the computers installed in a number of foreign countries.

However, these computers could be compromised and may be under the control of hackers from other parts of the world. Most of the attacks are stopped with the help of Cyber Security System deployed for detection and prevention of such attempts.

Rajya Sabha Unstarred Question No-4470

Answered on-**06.05.2010**

CYBER ESPIONAGE IN INDIAN COMPUTER SYSTEM

4470 . SHRI P. RAJEEVE

(a) whether Government has taken any

steps to prevent cyber espionage network hacking into computer systems of Indian Government;

(b) if so, the details of the preventive measures taken; and

(c) whether preventive steps had been extended to several Indian Embassies abroad ?

ANSWER

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

(SHRI SACHIN PILOT)

(a) and (b) The Government has taken several measures to detect and prevent cyber attacks/espionage. The details are:

1. As per existing computer security guidelines issued by Government, no sensitive information is to be stored on the systems that are connected to Internet.
2. The Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
3. The organizations operating critical information infrastructure have been advised to implement information security management practices based on International Standard ISO 27001.
4. Ministries and Departments have been advised to carry out their IT systems audit regularly to ensure robustness of their systems. The Indian Computer Emergency Response Team (CERT-In) has already empanelled a number of penetration testing professionals through a stringent mechanism of selection to carryout audits.
5. National Informatics Centre (NIC), providing services to Ministries/ Departments is continuously strengthening the security of the network operated by them and its services by enforcing security policies, conducting regular security audits and deploying various technologies at different levels of the network to defend against the newer techniques being adopted by the hackers from time to time.
6. The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with hacking and security breaches of information technology infrastructure.

   Section 70 of the Act provides to declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

   Further, Section 70B has empowered Indian Computer Emergency Response Team to serve as national nodal agency in the area of cyber security.
7. The Indian Computer Emergency

Response Team (CERT-In) scans the Indian Cyber Space to detect traces of any untoward incident that poses a threat to the cyber space. CERT-In performs both proactive and reactive roles in computer security incidents prevention, identification of solution to security problems, analyzing product vulnerabilities, malicious codes, web defacements, open proxy servers and in carrying out relevant research and development.

Sectoral CERTs have been functioning in the areas of defence and Finance for catering critical domains. They are equipped to handle and respond to domain specific threats emerging from the cyber systems.

CERT-In has published several Security Guidelines for safeguarding computer systems from hacking and these have been widely circulated. All Government Departments/ Ministries, their subordinate offices and public sector undertakings have been advised to implement these guidelines to secure their computer systems and information technology infrastructure.

CERT-In issues security alerts, advisories to prevent occurrence of cyber incidents and also conducts security workshops and training programs on regular basis to enhance user awareness.

(c) Yes, Sir. Ministry of External Affairs has issued a comprehensive set of IT security instructions for all users of MEA and periodically updates them on vulnerabilities. The Indian Missions abroad have been regularly sending information on safe computing practices. All personnel posted to Indian Missions and Posts abroad are being imparted IT security training.

Rajya Sabha Unstarred Question No-1203

Answered on-**05.08.2010**

CYBER ATTACKS

1203 . SHRIMATI SHOBHANA BHARTIA

(a) whether Government is aware that many Indian companies are losing several crores every year due to cyber attacks;

(b) if so, whether Government, in consultation with the State Governments, proposes to enact a law to check such cyber attacks;

(c) if so, the details thereof; and

(d) whether any separate wing is likely to be created to check such cyber attacks and also to prosecute the culprits involved?

ANSWER

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY

(SHRI SACHIN PILOT)

(a) Cyber attacks such as phishing and information stealing software programmes, denial of service attacks are intended for conducting financial frauds wherein users‘ personally identifiable information such as credit card details etc. are stolen. Due to these incidents financial institutions (Banks) and users suffer financial losses.

Department of Financial Services, Ministry of Finance has reported online banking frauds worth Rs. 590.49 lakhs in the year 2009.

(b) and (c) The primary responsibility of prevention, detection, registration, investigation and prosecution of all cases of crime, including cyber crimes, lies with the concerned State Governments(s). The Union government however attaches highest importance to the matter of prevention of crime. The Information Technology Act 2000 is a Central Act to address cyber crimes and is applicable in all the States/ Union Territories. The cyber crimes are technology driven crimes and with changing technologies new crimes need to be addressed. Aware of this fact, the Government has amended the Act and further strengthened the legal framework. The IT (Amendment) Act, 2008 which came into force from 27.10.2009 has special provisions for checking new forms of cyber crimes like phishing, identity theft, data privacy etc. The Act provides legal framework to address the cyber crimes seen largely at present.

(d) The State Police Departments have set up separate cyber police stations/cells in many states/ Union Territories which handle all the cyber crime cases including cyber attacks.

Rajya Sabha Unstarred Question No-1779

Answered on-**11.03.2011**

CYBER ATTACKS FROM OTHER COUNTRIES

1779 . SHRI KUMAR DEEPAK DAS

(a) whether it is a fact that India is facing increasing cyber espionage cases from countries including China;

(b) if so, the details of number of such cases registered by the relevant agencies in the country;

(c) whether initiatives have been taken to combat the menace of cyber attacks and to build cyber defence shield around the Ministries and security establishments;

(d) if so, the details thereof; and

(e) if not, the reasons therefore?

ANSWER

MINISTER OF STATE FOR
COMMUNICATIONS AND
INFORMATION TECHNOLOGY

(SHRI GURUDAS KAMAT)

(a) and (b) There have been attempts from time to time to penetrate cyber networks operating in Government. A large number of these attacks have been observed to be coming from the computers installed in a number of foreign countries. However, some of the attacks have been traced to be originating from systems located in China.

Specific information on such cases is not maintained by National Crime Records Bureau (NCRB), which is the nodal agency maintaining the records of crime cases. However, the cases reported under Section 72 of Information Technology Act (Breach of confidentiality / privacy) and Sections 405, 406, 408 & 409 of Indian Penal Code (IPC) related to Cyber Criminal Breach of trust / Fraud during 2007-2009 are enclosed at Annexure.

(c) and (d) Government is following an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks in the country. Salient details are given below:

(i) Computers Security Policies, Standard Operating Procedures and guidelines were formulated and circulated to all Ministries/Departments for implementation.

(ii) All Central Government Ministries / Departments and State/Union Territory Governments have been advised to conduct security auditing of entire Information Technology infrastructure including websites periodically to discover gaps with respect to security practices and take appropriate corrective actions.

(iii) National Informatics Centre (NIC) has been directed not to host web sites, which are not audited with respect to cyber security.

(iv) The "Crisis Management Plan for countering cyber attacks and cyber terrorism" was prepared and circulated for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(v) The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with security breaches of information technology infrastructure.

(vi) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

(e) Does not arise

Press Information Bureau Release November 2011

Cyber Attacks

Government is aware of misuse of Internet/ emails by anti-social elements and criminals. National Investigation Agency during investigation of certain terror cases has found that terrorists had been using Internet and communicating through Email to execute the terror action.

Cases involving misuse of Internet / Emails is not maintained separately by Government. However, as per the general cyber crime data maintained by National Crime Records Bureau, a total of 217, 288, 420 and 966 Cyber Crime cases were registered under Information Technology

Act during 2007, 2008, 2009, 2010 respectively, thereby showing an increasing trend. A total of 339, 176, 276 and 356 cyber crime cases were reported under Cyber Crime related Sections of Indian Penal Code (IPC) during 2007, 2008, 2009, 2010 respectively.

Internet has emerged as an online medium / platform to enable users to share ideas, activities & events and express views/ opinions on specific topics / events. Several groups and individuals have hosted content on Internet for a variety of purposes, which may be liked by one section of society and used gainfully. Such sites can be accessed by all sections of users. Millions of users worldwide from all sections of society use Internet. The technology and the associated applications allow the users to post the content of their choice automatically after registration with such sites, without the role of service providers hosting such sites. Most of the large number of users logging on the sites and millions of pages on such sites make it practically very difficult to keep a vigil on all contents posted/hosted on these sites. Most of the sites are hosted outside the country. Further, Government does not regulate content of such sites hosted on Internet.

A total no. of 90, 119, 252 and 219 Government websites as reported and tracked by the Indian Computer Emergency Response Team (CERT-In) were defaced by various hacker groups in the year 2008, 2009, 2010 and January – October 2011 respectively.

Government has notified Intermediary Guidelines Rules, 2011 under Section 79 of the Information Technology Act, 2000. These rules provide for the intermediaries to follow self-regulation. Any affected person may report the misuse of networking sites to the intermediary hosting these networking sites and request for removal / disabling of wrongful facts or objectionable content. The intermediaries are also required to designate a grievance officer to redress such requests by the affected person.

The Information Technology Act, 2000 has already been amended by Information Technology (Amendment) Act, 2008 w.e.f. 27.10.2009. The amended Act is a comprehensive Act and provides legal framework to fight all prevalent cyber crimes. Stringent punishment ranging from imprisonment of three years to life imprisonment and fine has been provided for various acts of cyber crime.

This reply was given by Shri Sachin Pilot, the minister of State in the Ministry of Communication and Information Technology in response to a question in Lok Sabha on 30 November 2011.

MINISTRY OF DEFENCE

Lok Sabha Unstarred Question No 79

Answered on **26.07.2010**

HACKING OF SECURITY INFORMATION

79 . Shri RAJAGOPAL LAGADAPATI

Will the Minister of DEFENCE be pleased to state:-

(a) whether the Government proposes to

deal with the hackers which have allegedly stolen vital security data recently from the Indian defence networks;

(b) if so, the details thereof;

(c) whether the Government is planning to coordinate with national cyber agencies to deal with such hackers;

(d) if so, the details thereof;

(e) whether the Government has any cyber security policy in this regard; and

(f) if so, the details thereof?

ANSWER

MINISTER OF DEFENCE (SHRI A.K. ANTONY)

(a) The report of hacking Indian Defence Networks put up by a group of researchers at the Munk School of Global Affairs, University of Toronto, Canada was analysed thoroughly. It was ascertained that certain internet facing computers were compromised by the hackers which had no sensitive defence data.

(b) To mitigate such incidents from recurring in the future, organizations under Ministry of Defence have worked out a Crisis Management Plan for measured response in case of any untoward incident.

(c) & (d) Defence Information Assurance and Research Agency (DIARA), a nodal agency mandated to deal with all cyber security related issues of Tri Services and Ministry of Defence is having a close coordination with national agencies like Computer Emergency Response Team – India (CERT-In) and National Training Research Organisation (NTRO).

(e) & (f) Specific Cyber Security Policies have been devised at all levels. Services Headquarters have an Information Security Policy and their networks are audited as per the guidelines.

Lok Sabha Unstarred Question No 5452

Answered on **13.12.2010**

CYBER WARFARE STRATEGY

5452 . Shri MANISH TEWARI

Will the Minister of DEFENCE be pleased to state:-

(a) whether the Government has a Cyber Warfare strategy to deal with attempts to infiltrate and cripple the command, control and communication systems of the Defence Establishments of the three Services and other establishments under the Ministry and if so, the details thereof;

(b) if so, whether the Government has a Cyber Warfare doctrine like the neighbouring countries to engage in asymmetric warfare given India‘s prowess in the software aspect of Information Technology (IT);

(c) if so, whether there are rules of engagement that have been formulated internationally or multilaterally for engagement in cyber space/warfare;

(d) the number of occasions when Information Technology networks of the Indian Defence Establishments were infected by the Stuxnet worm that caused havoc in Indonesia and Iran;

(e) whether the failed launches of GSLV and Prithvi could be attributed to the presence of Stuxnet in ISRO and DRDO systems as Symantec reported that eight per cent of all Stuxnet infestations were reported from India; and

(f) if so, the details of efficiency of firewall processes adopted by the Defence Establishments to protect their IT systems and the frequency with which the same is upgraded?

ANSWER

MINISTER OF DEFENCE (SHRI A.K. ANTONY)

(a) to (f) The Government has elaborate cyber security policies. Various organizations have prepared Cyber Crisis Management Plans for appropriate responses. No formal rules of engagement in cyber space/warfare exist at present at international or multilateral level. No Defence establishment has reported being effected by Stuxnet worm. Defence networks have adequate defensive measures which are upgraded as per Standard Operating Procedures.

MINISTRY OF HOME AFFAIRS

Lok Sabha Unstarred Question No 285

Answered on **27.07.2010**

CYBER MONITORING

285 . Shri GORAKHNATH

Will the Minister of HOME AFFAIRS be pleased to state:-

(a) whether there are reports indicating the usage of internet/e-mails by terrorists;

(b) if so, the details thereof alongwith the total number of such incidents detected in the current year;

(c) whether the Union Government, in coordination with the States has taken any steps to enhance the technical infrastructure for skill upgradation as well as for cyber monitoring; and

(d) if so, the details thereof alongwith the measures taken in this regard?

ANSWER

MINISTER OF THE STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI AJAY MAKEN)

(a) to (d) Available inputs indicate that terrorists are using several means for communication inter-alia, including use of internet and e-mail. The Department of Information Technology (DIT) has initiated a major programme on cyber forensics specifically focused towards development of cyber forensic tools, setting up of infrastructure for investigation and training of law enforcement and judicial offices in use of cyber forensic tools, to collect and analyse the digital evidence. Further, DIT has set up cyber forensic training labs at CBI and Kerala Police for skill upgradation in the area of cyber crime investigations and have also sponsored projects in the North Eastern States to establish cyber forensic training facilities at the state police organizations. Besides, Indian Computer Emergency Response

Team (CERT –In) under DIT has been set up for creating awareness about cyber security. It performs both pro-active and reactive roles.

Lok Sabha Unstarred Question No 1199

Answered on **29.11.2011**

TRAINING IN CYBER CRIMES

1199 . Shri NISHIKANT DUBEY

Will the Minister of HOME AFFAIRS be pleased to state:-

(a) whether the Government has taken any initiative for providing training to security agencies/police officials to deal with increasing cyber crime cases in the country; and

(b) if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

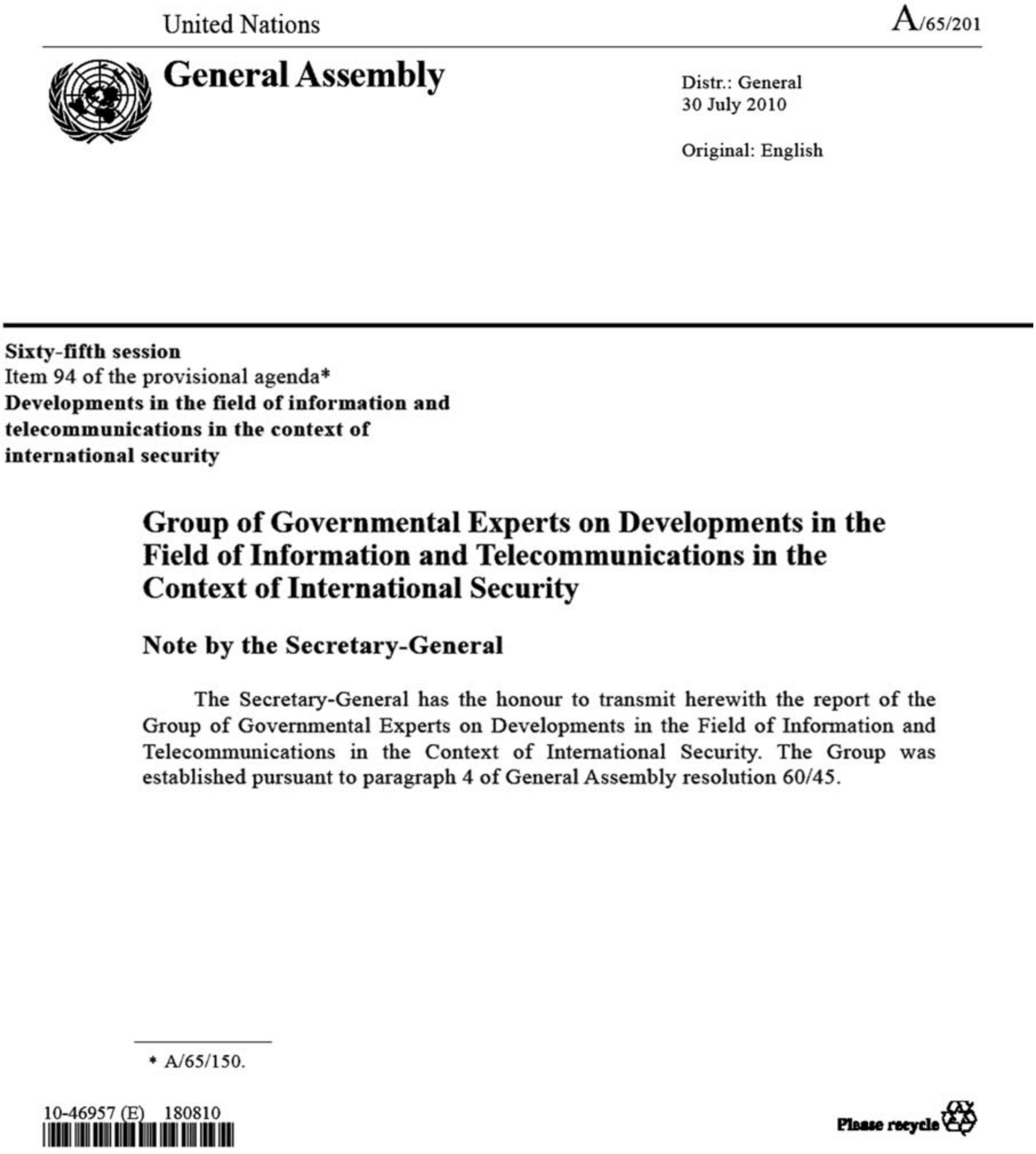
(SHRI JITENDRA SINGH)

(a) to (b) Bureau of Police Research & Development (BPR&D) and other organizations under Ministry of Home Affairs organize courses regularly for Police Officers at various levels on Information Technology in Police and Cybre Crime.

Police being a state subject, training of police personnel is primarily the responsibility of State Governments. As a part of the process of capacity building of the police, the efforts of the State Governments and Union Territories are supplemented by the Central Government. Courses on "Cyber Crime" are conducted at Central Detective Training Schools (CDTSs) every year for state police officers and CAPF personnel. National Police Academy, North- Eastern Police Academy, Central Bureau of Investigation are also conducting training on cyber crime.

APPENDIX 5

REPORT OF UN GROUP OF GOVERNMENTAL EXPERTS



United Nations

A/65/201

General Assembly

Distr.: General
30 July 2010

Original: English

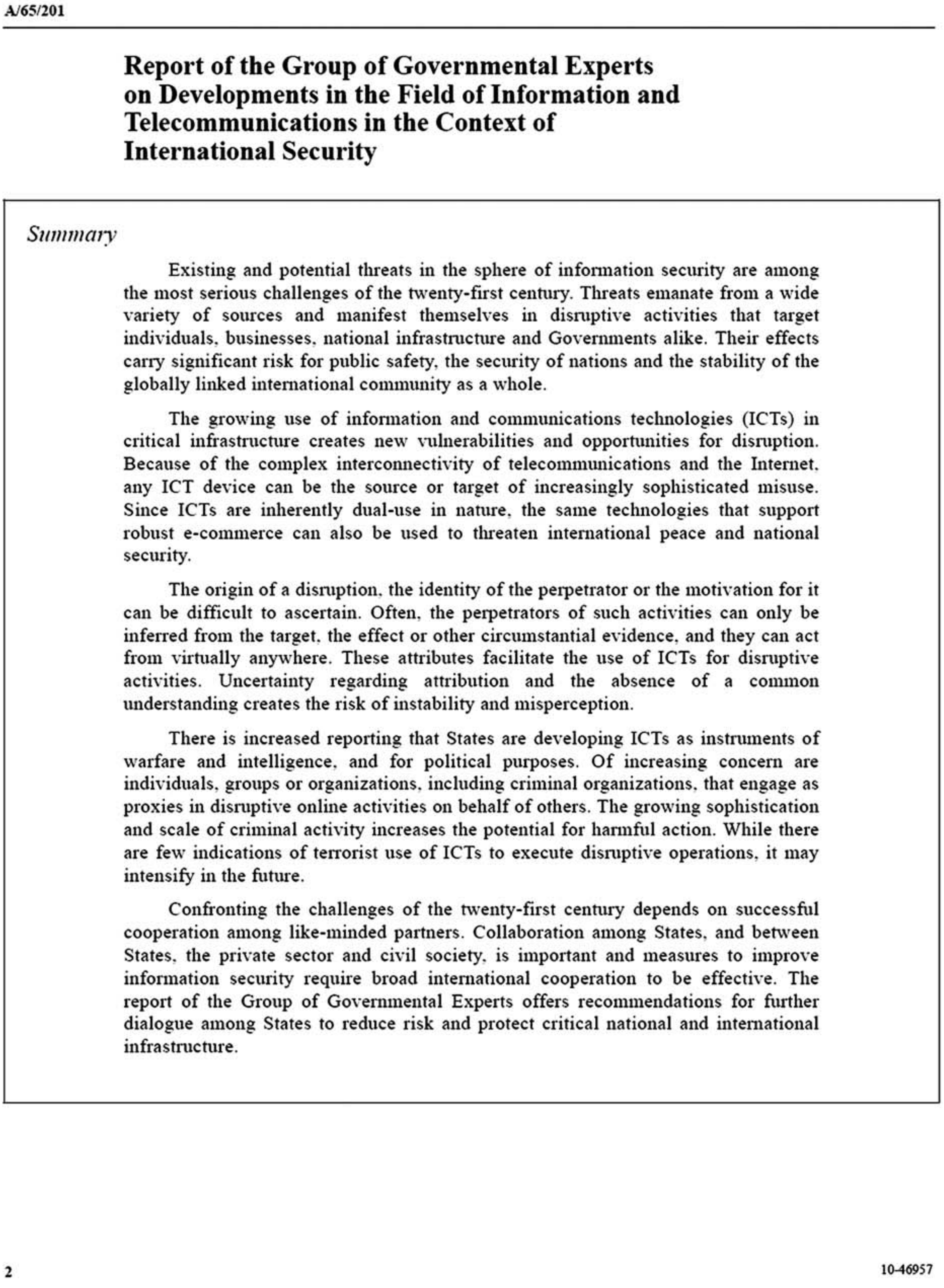
Sixty-fifth session
Item 94 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 60/45.

* A/65/150.



Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Summary

Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. Threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

The growing use of information and communications technologies (ICTs) in critical infrastructure creates new vulnerabilities and opportunities for disruption. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Since ICTs are inherently dual-use in nature, the same technologies that support robust e-commerce can also be used to threaten international peace and national security.

The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence, and they can act from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities. Uncertainty regarding attribution and the absence of a common understanding creates the risk of instability and misperception.

There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. The growing sophistication and scale of criminal activity increases the potential for harmful action. While there are few indications of terrorist use of ICTs to execute disruptive operations, it may intensify in the future.

Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. The report of the Group of Governmental Experts offers recommendations for further dialogue among States to reduce risk and protect critical national and international infrastructure.

CONTENTS PAGE

Foreword by the Secretary-General

A decade ago we could not have foreseen how deeply information technologies and telecommunications would be integrated into our daily lives, or how much we would come to rely on them. These technologies have created a globally linked international community and, while this linkage brings immense benefits, it also brings vulnerability and risk.

Considerable progress has been made in addressing the implications of the new technologies. But the task is arduous and we have only begun to develop the norms, laws and modes of cooperation needed for this new information environment.

With that in mind, I appointed a group of governmental experts from 15 States to study existing and potential threats in this sphere, and to recommend ways to address them. I thank the Chair of the Group and the experts for their diligent and careful work, which has produced this report, a concise statement of the problem and of possible next steps.

The General Assembly has an important role to play in the process of making information technology and telecommunications more secure, both nationally and internationally. Dialogue among Member States will be essential for developing common perspectives. Practical cooperation is also vital, to share best practices, exchange information and build capacity in developing countries, and to reduce the risk of misperception, which could hinder the international community's ability to manage major incidents in cyberspace.

This is a rich agenda for future work. The present report is meant to serve as an initial step towards building the international framework for security and stability that these new technologies require. I commend its analysis and recommendations to Member States and to a wide global audience.

Letter of transmittal

16 July 2010

I have the honour to submit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established in 2009 pursuant to paragraph 4 of General Assembly resolution 60/45. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In that resolution, entitled "Developments in the field of information and telecommunications in the context of international security", the General Assembly requested that a group of governmental experts be established in 2009, on the basis of equitable geographical distribution, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as concepts aimed at strengthening the security of global information and telecommunications systems. The Secretary-General was requested to submit a report on the results of that study to the General Assembly at its sixty-fifth session.

In accordance with the terms of the resolution, experts were appointed from 15 States: Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, Qatar, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America. The list of experts is contained in the annex.

The Group of Governmental Experts met in four sessions: the first from 24 to 26 November 2009 in Geneva; the second from 11 to 15 January 2010 at United Nations Headquarters; the third from 21 to 25 June 2010 in Geneva; and the fourth from 12 to 16 July at United Nations Headquarters.

The Group had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. Furthermore, the Group took into account the views expressed in the replies received from Member States in response to General Assembly resolutions 60/45, 61/54, 62/17 and 63/37, respectively entitled "Developments in the field of information and telecommunications in the context of international security", as well as contributions and background papers made available by individual members of the Group.

The Group wishes to express its appreciation for the contribution of the United Nations Institute for Disarmament Research, which served as consultant to the

Group and which was represented by James Lewis and Kerstin Vignard. The Group also wishes to express its appreciation to Ewen Buchanan, Information Officer of the Information and Outreach Branch of the Office for Disarmament Affairs of the Secretariat, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(*Signed*) Andrey V. **Krutskikh**
Chairman of the Group

I. Introduction

1. Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century. These threats may cause substantial damage to economies and national and international security. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole.

2. Information and communication technologies (ICTs) have unique attributes that make it difficult to address threats that States and other users may face. ICTs are ubiquitous and widely available. They are neither inherently civil nor military in nature, and the purpose to which they are put depends mainly on the motives of the user. Networks in many cases are owned and operated by the private sector or individuals. Because of the complex interconnectivity of telecommunications and the Internet, any ICT device can be the source or target of increasingly sophisticated misuse. Malicious use of ICTs can easily be concealed. The origin of a disruption, the identity of the perpetrator or the motivation can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. These attributes facilitate the use of ICTs for disruptive activities.

3. Considering the implications of these developments for international security, the United Nations General Assembly asked the Secretary-General, with the assistance of governmental experts, to study both threats in the sphere of information security and relevant international concepts and to suggest possible cooperative measures that could strengthen the security of global information and communication systems.

II.Threats, Risks and Vulnerabilities

4. The global network of ICTs has become an arena for disruptive activity. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of State conflict. The source of these threats includes non-State actors such as criminals and, potentially, terrorists, as well as States themselves. ICTs can be used to damage information resources and infrastructures. Because they are inherently dual-use in nature, the same ICTs that support robust e-commerce can also be used to threaten international peace and national security.

5. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

6. Thus far, there are few indications of terrorist attempts to compromise or disable ICT infrastructure or to execute operations using ICTs, although they may intensify in the future. At the present time terrorists mostly rely on these technologies to communicate, collect information, recruit, organize, promote their ideas and actions, and solicit funding, but could eventually adopt the use of ICTs for attack.

7. There is increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes. Uncertainty regarding attribution and the absence of common understanding regarding acceptable State behaviour may create the risk of instability and misperception.

8. Of increasing concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others. Such proxies, whether motivated by financial gain or other reasons, can offer an array of malicious services to State and non-State actors.

9. The growing use of ICTs in critical infrastructures creates new vulnerabilities and opportunities for disruption, as does the growing use of mobile communications devices and web-run services.

10. States are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect the normal, secure and reliable use of ICTs. The inclusion of malicious hidden functions in ICTs can undermine confidence in products and services, erode trust in commerce and affect national security.

11. The varying degrees of ICT capacity and security among different States increases the vulnerability of the global network. Differences in national laws and practices may create challenges to achieving a secure and resilient digital environment.

III. Cooperative Measures

12. The risks associated with globally interconnected networks require concerted responses. Member States over the past decade have repeatedly affirmed the need for international cooperation against threats in the sphere of ICT security in order to combat the criminal misuse of information technology, to create a global culture of cybersecurity and to promote other essential measures that can reduce risk.

13. Over the past decade, efforts to combat the threat of cybercrime have been conducted internationally, in particular, within the Shanghai Cooperation Organization, the Organization of American States, the Asia-Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Cooperation in Europe and the Council of Europe, as well as through bilateral efforts between States.

14. Non-criminal areas of transnational concern should receive appropriate attention. These include the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major incidents. This argues for the elaboration of measures designed to enhance cooperation where possible. Such measures could also be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability.

15. As disruptive activities using information and communications technologies grow more complex and dangerous, it is obvious that no State is able to address these threats alone. Confronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective. Therefore, the international community should examine the need for cooperative actions and mechanisms.

16. Existing agreements include norms relevant to the use of ICTs by States. Given the unique attributes of ICTs, additional norms could be developed over time.

17. Capacity-building is of vital importance to achieve success in ensuring global ICT security, to assist developing countries in their efforts to enhance the security of their critical national information infrastructure, and to bridge the current divide in ICT security. Close international cooperation will be needed to build capacity in States that may require assistance in addressing the security of their ICTs.

IV. Recommendations

18. Taking into account the existing and potential threats, risks and vulnerabilities in the field of information security, the Group of Governmental Experts considers it useful to recommend further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions:

    (i) Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;

    (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;

    (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;

    (iv) Identification of measures to support capacity-building in less developed countries;

    (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.

Annexeure

List of members of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Mr. Vladimir N. Gerasimovich
Head of the Department of International Security and Arms Control
Ministry of Foreign Affairs
Belarus

Mr. Aleksandr Ponomarev (third session)
Counsellor of the Permanent Mission of the Republic of Belarus to the
United Nations Office at Geneva

Mr. Alexandre Mariano Feitosa
Commander
Brazilian Marine Corps, Brazilian Navy
Policy, Strategy and International Affairs Secretariat
Ministry of Defence
Brazil

Mr. Li Song (first and second sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs
China

Mr. Kang Yong (third and fourth sessions)
Deputy Director General
Department of Arms Control and Disarmament
Ministry of Foreign Affairs, China

Mr. Linnar Viik
Associate Professor
Estonian IT College
Estonia

Mr. Aymeric Simon
Relations internationales
Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
France

Mr. Gregor Koebel
Head of the Division for Conventional Arms Control
Federal Foreign Office
Germany

Mr. B. J. Srinath
Senior Director
Indian Computer Emergency Response Team
Department of Information Technology
India

Ms. Rodica Radian-Gordon
Director
Arms Control Department
Ministry of Foreign Affairs
Israel

Mr. Vincenzo Della Corte (first and third sessions)

Director of Communication Security Sector

Presidency of the Council of Ministers

Italy

Mr. Walter Mecchia (second and fourth sessions)

Communication Security Sector

Presidency of the Council of Ministers

Italy

Mr. Rashid A. Al-Mohannadi (first session)

Commander of the Land Forces Signal Company

Amiri Signal Corps

Qatar

Mr. Saad M. R. Al-Kaabi

Lieutenant Colonel (Engineer)

Ministry of Defence

Qatar

Mr. Lew Kwang-chul

Ambassador

Ministry of Foreign Affairs and Trade

Republic of Korea

Mr. Andrey V. Krutskikh

Deputy Director

Department of New Challenges and Threats

Ministry of Foreign Affairs

Russian Federation

Ms. Palesa Banda (first session)

Deputy Director, Internet Governance

Department of Communication

South Africa

Maj. Gen. Mario Silvino Brazzoli

Government Information Technology Officer

Department of Defence

South Africa

Mr. Gavin Willis

International Relations Team

National Technical Authority for Information Assurance (CESG)

United Kingdom of Great Britain and Northern Ireland

Ms. Michele G. Markoff

Senior Policy Adviser

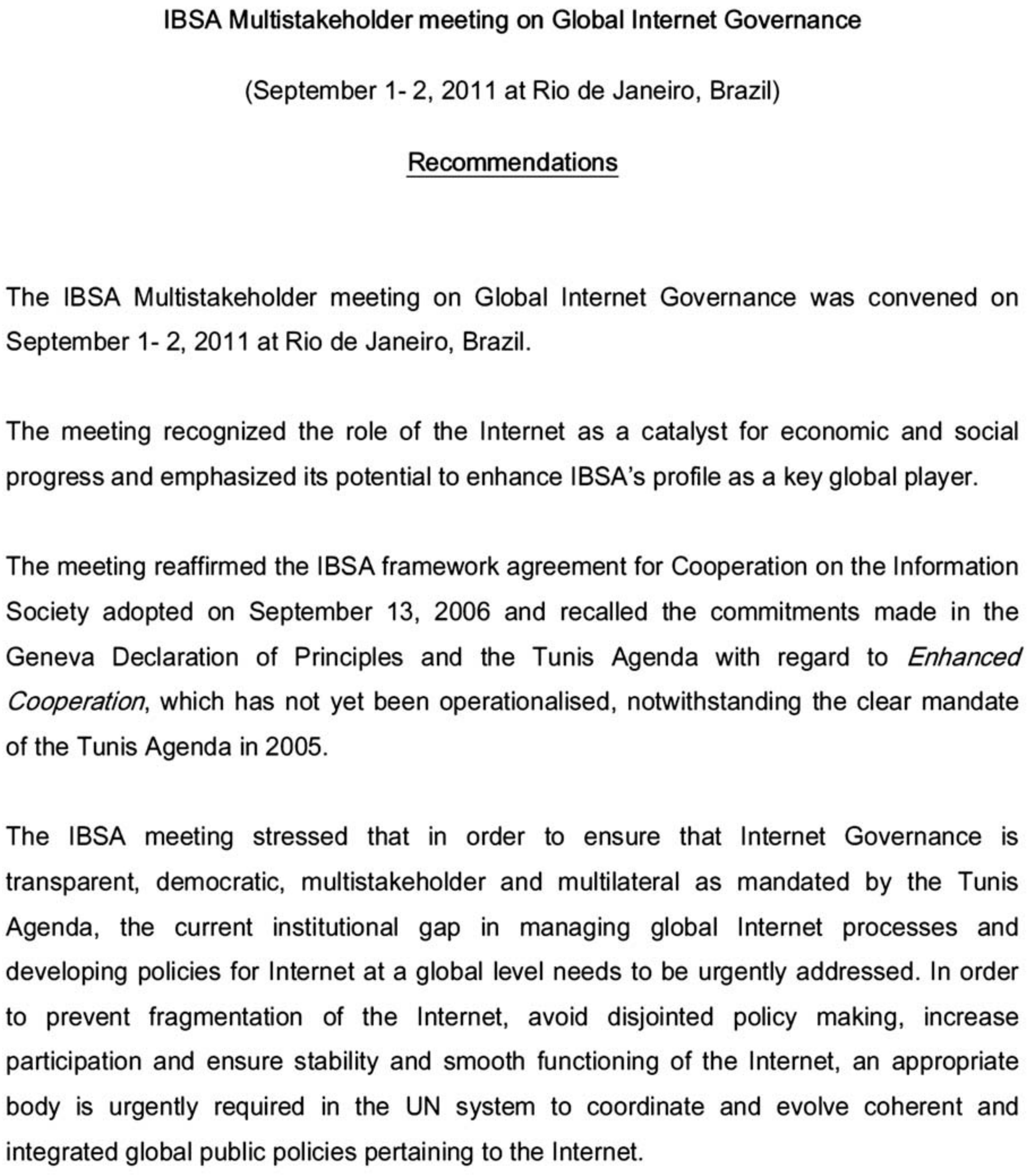
Office of Cyber Affairs

US Department of State

United States of America

APPENDIX 6

IBSA MULTISTAKEHOLDER MEETING ON GLOBAL INTERNET GOVERNANCE



IBSA Multistakeholder meeting on Global Internet Governance

(September 1- 2, 2011 at Rio de Janeiro, Brazil)

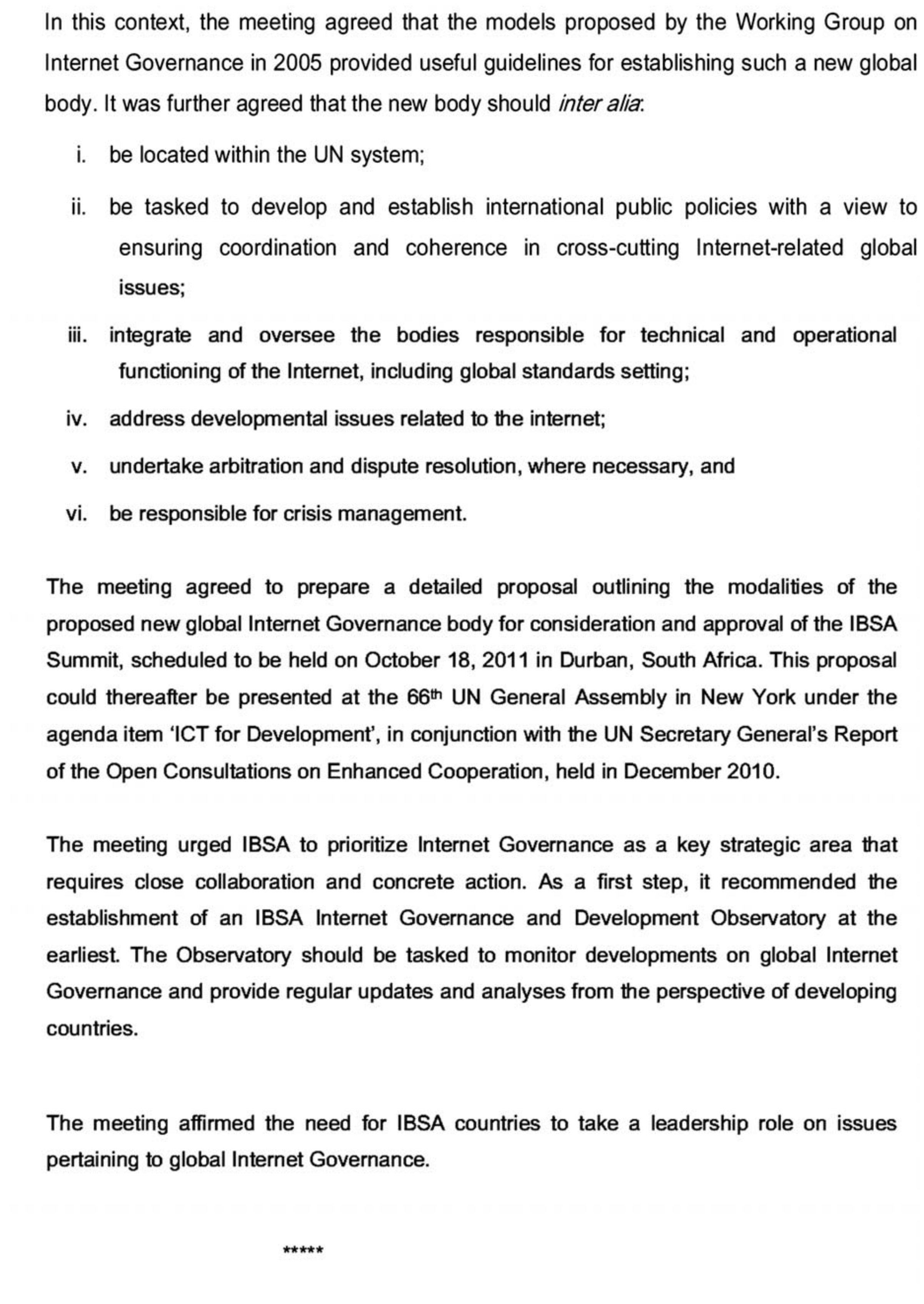
Recommendations

The IBSA Multistakeholder meeting on Global Internet Governance was convened on September 1- 2, 2011 at Rio de Janeiro, Brazil.

The meeting recognized the role of the Internet as a catalyst for economic and social progress and emphasized its potential to enhance IBSA's profile as a key global player.

The meeting reaffirmed the IBSA framework agreement for Cooperation on the Information Society adopted on September 13, 2006 and recalled the commitments made in the Geneva Declaration of Principles and the Tunis Agenda with regard to *Enhanced Cooperation*, which has not yet been operationalised, notwithstanding the clear mandate of the Tunis Agenda in 2005.

The IBSA meeting stressed that in order to ensure that Internet Governance is transparent, democratic, multistakeholder and multilateral as mandated by the Tunis Agenda, the current institutional gap in managing global Internet processes and developing policies for Internet at a global level needs to be urgently addressed. In order to prevent fragmentation of the Internet, avoid disjointed policy making, increase participation and ensure stability and smooth functioning of the Internet, an appropriate body is urgently required in the UN system to coordinate and evolve coherent and integrated global public policies pertaining to the Internet.



In this context, the meeting agreed that the models proposed by the Working Group on Internet Governance in 2005 provided useful guidelines for establishing such a new global body. It was further agreed that the new body should *inter alia*:

i. be located within the UN system;

ii. be tasked to develop and establish international public policies with a view to ensuring coordination and coherence in cross-cutting Internet-related global issues;

iii. integrate and oversee the bodies responsible for technical and operational functioning of the Internet, including global standards setting;

iv. address developmental issues related to the internet;

v. undertake arbitration and dispute resolution, where necessary, and

vi. be responsible for crisis management.

The meeting agreed to prepare a detailed proposal outlining the modalities of the proposed new global Internet Governance body for consideration and approval of the IBSA Summit, scheduled to be held on October 18, 2011 in Durban, South Africa. This proposal could thereafter be presented at the 66th UN General Assembly in New York under the agenda item 'ICT for Development', in conjunction with the UN Secretary General's Report of the Open Consultations on Enhanced Cooperation, held in December 2010.

The meeting urged IBSA to prioritize Internet Governance as a key strategic area that requires close collaboration and concrete action. As a first step, it recommended the establishment of an IBSA Internet Governance and Development Observatory at the earliest. The Observatory should be tasked to monitor developments on global Internet Governance and provide regular updates and analyses from the perspective of developing countries.

The meeting affirmed the need for IBSA countries to take a leadership role on issues pertaining to global Internet Governance.

*****

IDSA Task Force on Cyber Security

Chairman

Dr Nitin Desai was formerly Chief Economic Adviser in the Ministry of Finance, GOI and later Under Secretary General of the UN and Chair of the Multi-stake holder Advisory Group that organises the annual UN Internet Governance Forum.

Members

Dr Arvind Gupta is Director General, IDSA.

Lt Gen Aditya Singh retired as General Officer Commanding-in-Chief, Southern Command, of the Indian Army. He served as a member of the National Security Advisory Board from 2008 to 2010.

Dr Kamlesh Bajaj is the CEO of the Data Security Council of India(DSCI) and was the founding Director of the Indian Computer Emergency Response Team (CERT-In) at the Ministry of Communications and IT.

Mr B J Srinath is a Senior Director (Scientist 'G') in the 'Indian Computer Emergency Response Team (CERT-In), Department of IT, Ministry of Communications and IT, Government of India.

Mr Salman Waris is currently a Partner with a prominent Delhi based law firm and expert on Cyber law issues.

Mr Amit Sharma is a Joint Director in the Office of Secretary, Dept of Defence (R&D), Ministry of Defence.

Wg Cdr Ajey Lele is Research Fellow at the IDSA.

Dr Cherian Samuel is Associate Fellow at the IDSA.

Mr Kapil Patil is Research Assistant, Pugwash India.