MANEKSHAW PAPER No. 23, 2010

National Strategy for Cyberspace Security

S R R Aiyengar

Centre for Land Warfare Studies
New Delhi

KNOWLEDGE WORLD
KW Publishers Pvt Ltd
New Delhi

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone: +91.11.25691308 Fax: +91.11.25692347
email: landwarfare@gmail.com website: www.claws.in

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

The views expressed in this paper are those of the author and do not represent the views of the Centre for Land Warfare Studies.

ISBN 13: 978-93-80502-42-7

KNOWLEDGE WORLD
www.kwpub.in

Published in India by

Kalpana Shukla
KW Publishers Pvt Ltd
NEW DELHI: 4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110002
Phone: +91.11.23263498 / 43528107
email: mail@kwpub.in / knowledgeworld@vsnl.net
MUMBAI: 15 Jay Kay Industrial Estate, Linking Road Extn., Santacruz (W), Mumbai 400054
Phone: +91.22.26614110 / 26613505
email: mumbai@kwpub.in

Printed and Bound in India

Contents

National Strategy for Cyberspace Security

In security matters, there is nothing like absolute security. We are only trying to build comfort levels because security costs money and lack of it costs much more. Comfort level is a manifestation of efforts as well as realisation of their effectiveness and limitation[*]

Introduction

It was science fiction writer William Gibson who coined the term 'cyberspace' in his short story "Burning Chrome". He later popularised the concept in his debut novel *Neuromancer* (1984)**.** Unlike most computer terms, cyberspace does not have a standard, objective definition. Instead, it is used to describe the entire virtual world of computers. For example, an 'object' in cyberspace refers to a block of data floating around a computer system or network.[1] With the advent of the internet, cyberspace now extends to the global network of computers. It is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow our critical infrastructure to work. Thus, the healthy functioning of cyberspace is essential for our economic and national security.

In the past few years, threats in the domain of cyberspace have risen dramatically. Securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused efforts from the entire society – the central, state and local governments, the private sector, and the ordinary citizens who use the internet (Netizens). In the current digital era, where governance as well as business is increasingly being led by Information Communications Technology (ICT), any discussion on national

[*] Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, Ministry of Communications and Information Technology, Government of India.

security cannot be complete without a discussion on the cyberspace in which e-governance and e-commerce takes place.

Our attention is usually drawn to 'cyber security' when we hear about 'cyber crimes'. Any cyber attack, whether targeted at individuals, small businesses or corporations, can have serious results – intellectual property can be compromised, personal and business information can be stolen, normal business operations can be disrupted and major financial losses can occur. Attacks on government machinery carry the increased threat of theft of state and military secrets. There is also the real possibility that a cyber attack could disable defence command systems, bring down power grids, open the floodgates, paralyse telecommunications and transportation, and create mass confusion and hysteria – any or all of which could be precursors to conventional military attacks by land, sea or air, or even through nuclear weapons.

Among the host of questions that pop up in relation to cyberspace are: Who is responsible for protecting cyberspace? Do we have a strategy to combat the threats to cyberspace? What must we do to reduce our vulnerability to these threats before they can be exploited to damage the cyber systems supporting our nation's critical infrastructure? How can we ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible? There's a single answer to the above questions: devising a coherent national strategy for the protection of cyberspace so that the information systems for running critical infrastructure are never disrupted and thereby, national and economic security never compromised. Sadly, India lacks such a coherent national strategy presently.

Threat Scenario and Assessment of Vulnerabilities

Every day, we get reports of hackers breaking into computer networks, vandalising web pages, and accessing sensitive information. We hear how they tamper with medical records, disrupt emergency systems and siphon money from bank accounts. Could 'information terrorists', using nothing more than a personal computer, cause planes to crash, inflict widespread power blackouts, or unleash financial chaos? Such real and imaginary scenarios and our defence against them are the components of information warfare – a variant of warfare that targets or exploits information media to achieve certain objectives.

The Symantec India 2009 Security and Storage survey revealed that in 2008, India registered a sizeable increase in nefarious web activities, with 12 percent of spam detected in the Asia-Pacific/Japan region originating from here, as against 4 percent in 2007. These figures catapulted India to the third position in the region, with a staggering 250 percent increase in 'bot'-infected computers. (Bot is an application software that runs automated tasks over the internet). As many as 103,812 distinct bot-infected computers were observed in 2007, with a daily average of 836 bots. Globally, Symantec declared, a 31 percent increase in bot-infected computers.[2]

Similarly, the internet security company McAfee stated in its 2007 annual report that approximately 120 countries had been developing ways to use the internet as a weapon and target financial markets, government computer systems and utilities. In activities reminiscent of the Cold War, which led countries to engage in clandestine activities, intelligence agencies are routinely testing networks to locate weaknesses. These techniques for probing weaknesses in the internet and global networks are growing more sophisticated every year and 'cyber crime' is now a global issue. It has evolved significantly and is no longer a threat just to industry and individuals, but increasingly to the security of nations. It is predicted that future attacks will be even more sophisticated. Attacks have progressed from initial curiosity probes to well-funded and well-organised operations for political, military, economic and scientific espionage.

Cyber attackers can be of two types. They may be by non-state actors whose intent is criminal and who may be subject to the jurisdiction of one or more sovereign states. Their attacks generally constitute crimes against individuals and property. Terrorists constitute a more serious set of non-state actors and are of concern to law enforcement and national security agencies. The second type of cyber attacker is a sovereign state waging information warfare. The attackers' targets are other sovereign states, although specific targets may be identical to those of non-state actors.

Defence against these attackers is the responsibility of both external and internal security and intelligence agencies, who need to act in concert. Depending on the nature of the target and the attackers' objectives, damage can occur rapidly, as in denial of service, or it can be in the form of 'Trojan' attacks. The impact of other attacks, such as viruses distributed by e-mail, is felt more slowly.

Threat Characteristics

Threats are often classified on the basis of the nature and mission of the attacker. In terms of cyberspace, there are six major categories: hackers, insiders, corporate spies, criminals, terrorists and nation-states.

- A *hacker* is a person who gains access to, or breaks into, computers and networks, in a way that was not intended and who is not authorised to access the same.
- *Insiders* consist of current and former employees, temporary workers, contractors and others with inside access to an organisation's information systems. They are often the culprits behind the most serious attacks, including theft of trade secrets, financial frauds, and sabotage of data.
- *Corporate spies* include both foreign and domestic companies. They steal primarily trade secrets for competitive advantage.
- *Criminals* refer to the category of hackers who attack systems for money. They steal credit card numbers, identities and intellectual property.
- *Terrorists* have, so far, used the internet primarily to support their physical operations, rather than to launch cyber attacks. However, there is a growing concern that they might launch cyber attacks against critical infrastructure.
- *States* are often considered the most serious threat, if not the most likely. They have the most resources and may decide to employ cyber weapons to augment or replace conventional ones.

Over the years, cyber criminals across the globe have organised themselves into groups. Their level of sophistication has increased from the early days of the 'I Love You' virus. 'Hacking for profit' has subsumed 'hacking for fun'. Recent attacks show how dangerous and expensive cyber attacks can be if carried out in coordination. Common threats include spam, spoofing, phishing, viruses, worms, Trojans, spyware, repudiation, information disclosure, denial of service, elevation of privilege, botnets and pirated software. Details of these threats and their intended effects are listed in the Appendix.[3]

The above-mentioned threats are only some of the observed threats known today. Uncertainties exist regarding the intent and full technical capabilities of several observed attacks. The increasing number of mobile devices and the growing number of users are targets of unauthorised and potentially harmful software, including worms, viruses, and spyware. As a result, it becomes essential for any organisation to secure and manage these devices and the data stored in them.

In-depth analysis is needed to address long-term trends related to threats and vulnerabilities. What is known today is that attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users is improving.

Increasingly superior computer attack tools make it possible for any number of actors to launch assaults against a country's infrastructure and cyberspace. During peace-time, adversaries may conduct espionage on governments, university research centres, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping the enemy's information systems, identifying key targets, lacing its infrastructure with back doors and other means of unauthorised access to be exploited later. During war-time or crises, adversaries may seek to intimidate a nation's political leaders by attacking critical infrastructure and key economic functions or eroding public confidence in information systems.

As mentioned earlier, cyber attacks on information networks can have serious consequences such as disrupting critical operations, causing loss of revenue, intellectual property, and even lives. Since cyberspace provides a means for attacking infrastructure from a distance, countering such an attack requires the development of robust capabilities, which would allow countries to reduce their vulnerabilities and deter those with the capabilities and intent to harm critical infrastructure.

Cyber attacks require only commodity technology and enable attackers to obfuscate their identity, location and path of entry. Not only does cyberspace provide for the ability to exploit weaknesses in critical infrastructure, it also provides a fulcrum for leveraging physical attacks by allowing the possibility of disrupting communications, hindering defensive or offensive response, or delaying emergency responses that would be essential, following a physical attack.

Managing threats and reducing vulnerabilities in cyberspace are particularly complex challenges because of the number and range of users involved. Cyberspace security requires action at multiple levels and by a diverse group of actors, because millions of devices are interconnected by a network of networks. The challenges in implementing cyber security can fall under the following categories:

Attackers vs. Defenders: The attacker needs to exploit only one vulnerability whereas the defender needs to secure all vulnerable points. Attackers have unlimited time while defenders work with time and cost constraints. An attacker will use a variety of open-source data to select targets, and will use widely available means of attack and information about a system's vulnerability to identify possible approaches to them. The attacker would also remain undetected throughout his preparatory period. Early discovery of an attack or attack plan and the detection of the attacker's probes and his/her identification are important elements of defence.

Security vs. Usability: Secure systems are more difficult to use, as complex and strong passwords are difficult to remember. Users prefer simple passwords. Human beings are often the weakest link in this regard. They make mistakes, pick easy passwords, and are vulnerable to social engineering (being conned by attackers into providing passwords or access to systems).

Security as an Afterthought: Developers and the management think that security does not add any business value. Addressing vulnerabilities just before a product is released is often expensive. There could possibly be other pressing issues of survival that relegate security to the backburner. Very often security purchases and practices are based on other factors such as industry best practices, fear of attack, product ratings, salesmanship, advice from consultants, budget restrictions, and so on.

Addressing Vulnerabilities at Various Levels: The various levels at which cyber vulnerabilities need to be addressed would include home users/ small businesses, large enterprises, critical infrastructure, and national- and global-level organisations. Hence, cyber security requires action at all these multiple levels and by a diverse group of actors. The trend towards ubiquitous computing affects cyber security in two ways. First, there are more targets to attack by more attackers. Second, attacks can have real-world consequences.

Constructive and Destructive Uses of IT: IT has become increasingly pervasive. It is ubiquitous throughout our offices, homes and automobiles. It resides in both fixed and mobile devices. But technology's inevitable complexity is often exploited by attackers. While this dichotomy between constructive and destructive uses is common to all technologies, the rapid spread of IT makes the resolution of this issue particularly urgent. While advanced technology usually remains in the hands of a few specialists who can be trained and licensed in its use, the convenience of IT lends itself to wide misuse through malevolence, carelessness and irresponsibility.

Cost-Exchange Ratio: Absolute defence against attack has rarely been achieved. Each defensive measure generates a counter-measure by an attacker, driving the defender to adopt ever-stronger procedures. The concept of cost-exchange ratio ensures that defensive measures are designed to require an attacker to spend inordinately greater resources to defeat them. Ideally, security should be free, fast, and foolproof. In practice, it is never all three, and one needs to make hard decisions/choices about how much to spend and what to spend on.

Software Vulnerabilities: Software developers themselves contribute to cyberspace insecurity by supplying software that has security weaknesses, leaving it to future security patches to correct the bugs which should have been corrected at the beta level itself. Some software developers take refuge under Intellectual Property Rights to shield their source codes and prevent users from making a proper security assessment. Many security professionals believe that major software vendors deliberately keep room for backdoor entry for apparently legitimate purposes, but with dangerous consequences. If vendors are held liable for security flaws, or at least flaws resulting from poor software-development practices, there would be a stronger incentive for delivering better products.

Threats to National Security

India's cyberspace is linked to that of the rest of the world. Mounting defences against attacks occuring at lightning speed and distinguishing between malicious activity originating from criminals, nation-states, and terrorists in real-time is difficult. Systems supporting a country's critical defence and intelligence community must be secure, reliable and resilient enough to withstand attacks, regardless of their place of origin.

The internet has become a weapon for political, military and economic espionage. Organised cyber attacks that have been witnessed in the recent past include:

- A single attack in the summer of 2007 disabled a reported 1,500 computers in the Pentagon.
- According to the Pentagon, the Department of Defence detects three million unauthorised 'scans' – attempts by intruders to access official networks – on its computers every day.
- Experts claim that China and North Korea, among other countries, are escalating the use of cyber warfare techniques and are actively training new hackers.
- A coordinated attack on Estonia's cyber infrastructure was thought by some to be the result of a disagreement with Russia and was termed 'Web War I' by Estonia's Deputy Minister of Defence.
- The Georgian Embassy in the UK had accused forces within Russia of launching a coordinated cyber attack against Georgian websites, to coincide with military operations in the breakaway region of South Ossetia.
- Cleaning up cyber attacks on the National Defence University, Naval War College and Fort Hood cost the US Administration $20-30 million each.
- In 2007, reports confirmed that cyber attacks emanating from the Chinese military had penetrated the Pentagon, the German Chancellery and England's Whitehall.
- There have been reported breaches of the US electricity grid and the F-35 fighter jet programme. President Barack Obama mentioned a cyber attack – blamed by some on foreign spy services – on the computer hub of his 2008 presidential campaign.
- On 12 January 2010, Google posted on its official blog that it had detected a "highly sophisticated and targeted attack" originating from China that stole intellectual property. Further investigations revealed that the attack had targeted at least 20 other large companies as well as Google e-mail accounts of Chinese human rights activists.

Some of the software used to carry out these attacks indicates that the strikes were clearly designed and tested with much greater resources than usually possessed by individual hackers. Traditional protective measures are not enough to defend against attacks such as those on Estonia, since the complexity and coordination involved in these 'botnets' are totally new. National networks with less sophisticated monitoring and defence capabilities could face serious threats to their security. There are signs that intelligence agencies around the world are constantly probing others' networks and developing new ways to gather information. An adverse consequence of inadequate state response to perceived national security threats is the emergence of techno-savvy private hacker groups that try to counter-hack foreign websites known to be inimical to their own national interests.

By the turn of the 21st century, virtually all known terrorist groups had secured a presence on the internet. There is overwhelming evidence of terrorist groups utilising the internet to engage in psychological warfare, propaganda, data mining, fund raising, recruiting, networking, information sharing, and planning and coordination. Terrorists today are highly sophisticated in their use of weapons, communications and planning techniques. They operate in a highly decentralised manner, which makes them more difficult to locate and track than a small cell of a terrorist group at any given time. These groups are using the internet to collect open-source information to be used for the preparation and execution of their operations. Radical Islamic terrorist organisations, in particular, are seen as being on the 'cutting edge of organisational networking', having demonstrated an ability to harness information technology for offensive operations as well as for the more typical propaganda, fund-raising and recruiting purposes.[4] Many of these terrorist organisations have recruited members with academic qualifications in areas such as computer science, biology and chemistry.

In order to effectively collect intelligence, conduct investigations and run operations against these threats, we have to identify their methods and be able to operate in the same medium. To catch a thief, or in this case, a cyber terrorist, one has to think like one. IT professionals have been conditioned to think defensively, draping their networks with sensor-studded barbed wires and using firewalls and intrusion-prevention systems to lock down the perimeter. But there is an emerging school of thought that says only a more proactive approach towards security can help nations prepare for the unexpected.

Chinese and Pakistani Threat to Indian Cyberspace

China: Technological developments, especially after the Gulf War (1991) and the war in Kosovo (1999), have forced China to take a fresh look at its defence policies, capabilities and priorities. China has understood that confrontation with systems is the principal mode of modern battle. A 2007 US Department of Defense (DoD) report to Congress stated that the Chinese army sees computer network operations as critical to achieving 'electromagnetic dominance'. The report, which for the most part focuses on China's land, air, sea and space capabilities, also noted that numerous intrusions into computer systems at the DoD and its contractors emanated from China. Although it is unclear if these intrusions were conducted by or with the endorsement of the People's Liberation Army (PLA) or other elements of the Chinese government, the report stated that developing capabilities for cyber warfare was consistent with authoritative PLA writings on the subject.

Attacks which appear to come from China have a variety of motives, including theft of intellectual property, gathering of intelligence, research on the operations of the US military, and the creation of beachheads inside US military networks for future use. "It's hard to believe it's not government-driven," a Netwarcomm official told *Federal Computer Weekly*. In its section on information warfare, the public report covered China's development of electronic counter-measures, its inclusion of offensive cyber attacks in military exercises and its development of viruses to attack enemy computer systems. German, British and American government officials have previously reported that attacks coming from China had targeted government networks. The German media has accused the Chinese military of sponsoring attacks targeting the computers of Germany's top officials, while MI 5, the United Kingdom's intelligence service, warned top corporations to watch out for Chinese attacks targeting their systems.

While attacks from Chinese servers have garnered the most attention, security experts still question the ultimate source of the attacks. Most developed nations have military teams capable of launching offensive cyber attacks and profit-driven cyber crime continues to be the largest source of attacks.[5] A report released in October by the US-China Economic and Security Review Commission described an unseen cyber war, in which hackers – most of whom appear to reside in China – constantly bombard American agencies and defence contractors with malicious software designed to steal data only a nation-state would want. According to the report prepared by Northrop Grumman,[6] the hackers seek defence-engineering specifications, military operational information and US-China policy documents. The attacks yielded a "substantial amount of reconnaissance" that would help the attackers to "map out" US military telecommunications networks and "understand who is talking to whom, and what means [we] are using to communicate."[7]

Pakistan: We are all aware of the wars India and Pakistan have fought and the resultant destruction, especially of precious human lives. In the current information age, battles are fought not only with guns and tanks but also through the media. Since the spread of information technology among the masses of South Asia from the mid-1990s, the pace of cyber wars between Pakistan and India has accelerated. These wars between the two countries started in May 1998, when India conducted its nuclear tests. Soon after India officially announced the tests, a group of Pakistan-based hackers called 'Milkworm' broke into the Bhabha Atomic Research Centre website and posted anti-India and anti-nuclear messages. Such defacements continued during the Kargil war in 1999 and during December 2001-02, when the tension between India and Pakistan was at its peak. Therefore, the period from 1999 to 2002 was very crucial, when the troops were exchanging gunshots across the Line of Control (LoC), the hackers were defacing each other's sites. Thankfully, the cyber war between India and Pakistan has not escalated into anything more than website defacements.

According to *attrition.org,* a website that tracks computer security-related developments, attacks on Indian websites increased from 4 in 1999 to 72 in 2000, whereas Pakistani websites were hacked 7 times in 1999 and 18 times in 2000. During the Kargil war, the first Indian site reported to be hacked was http://www.armyinkashmir.com, established by the Indian government to provide factual information about daily events in the Kashmir Valley. The hackers posted photographs showing Indian military forces allegedly killing Kashmiri militants. The pictures sported captions like 'Massacre', 'Torture', 'Extrajudicial Execution' and 'The Agony of Crackdown', and blamed the Indian government for alleged atrocities in Kashmir.

Two prominent Pakistani hacker groups are the Pakistan Hackers Club (PHC) and the G-Force. The founder of PHC is a Dr. Nuker.[8] The US Department of Justice has identified 'Dr. Nuker' as Misbah Khan of Karachi, who was previously involved in the defacement of the official website of the American Israel Public Affairs Committee (AIPAC). 'Dr. Nuker' struck back in an interview to the magazine *Newsbytes*, where he claimed that the "federal grand jury made a mistake in indicting Misbah Khan of Karachi" and that "he merely uses insecure servers in Pakistan to get online anonymously". The PHC has been in existence for quite some time, and apart from Indian sites, has defaced many Israeli and US websites, including that of the US Department of Energy.

G-Force was founded in May 1998 after the Indian nuclear tests. It is based in Lahore and consists of eight members. Its initial target was Indian sites, but after 9/11, it has been concentrating on US-based sites. According to *zone-h.org,* G-Force has successfully defaced 212 sites. Its 'achievements' include hacking the sites of the National Oceanic and Atmospheric Agency and three military sites associated with the US Defense Test and Evaluation Professional Institute.

Both PHC and G-Force are professional hacking groups with a specific aim: to work for what they believe to be the causes of Kashmir and Palestine. It is still to be seen how their activities will help the causes they claim to support. And while the war rhetoric between nuclear rivals India and Pakistan may have eased, a different battle is raging between the two nations in cyberspace.

Cyber Attacks on Critical Infrastructure

The digital age is creating an information and communications renaissance. Information is as vital to the healthy functioning of communities as clean air, safe streets, good schools and effective public health. Today, IT has a privileged place in the field of infrastructure. Developed countries have become dependent upon computer networks for many essential services including water, electricity, gas, voice and data communications, railways and aviation. In this respect, IT is unlike any other technological development (such as materials or standards) because it acts as an infrastructure in its own right (i.e. the internet) and is central to the governance of infrastructure systems as well. In fact, IT is the brain and nervous system of the overall infrastructure and, thus, is the ‘infrastructure of infrastructure’ or what we can call ‘core infrastructure’.

In general, critical infrastructure is monitored and controlled by computer-based Industrial Control Systems (ICS). While automating industrial processes, the ICS typically collect sensor information and operational data, process them, display the resulting information, and relay control commands to local or remote equipment. Given the prime role of ICS in the functioning of the overall system, they are prime targets for wrongdoers who want to disrupt critical infrastructure. Country-wide infrastructure such as the electricity grid, telecommunications system and transport networks are based on capital-intensive systems, for which standby capacity is frequently difficult and expensive to obtain. These systems increasingly rely on interconnected computer networks, both for operational efficiency and to ensure back-up facilities. Integrating local parts of the infrastructure for greater efficiency implies that a country’s vulnerability to both physical and cyber attacks increases, with every increase in the number of potential access points. By exploiting flaws in the software, vulnerabilities in the architecture or human imperfection, attackers can, in principle, cause large-scale damage with relatively little effort. The potential vulnerability of a single, integrated infrastructure system is further compounded by the interdependence that arises between infrastructures. This is because the provision of service by one system generally depends on services from other infrastructural systems. Not surprisingly, telecommunications and electric power are the most critical processes on which virtually all the others depend.

In addition to greater dependence on technology for operating processes and procedures, increased use of IT has created technical interdependencies between the operators of critical infrastructure and greatly magnified the overall cyber risks.[9] However, there is no turning back. The emergence of e-business has already effected the irreversible reengineering of many corporate structures as well as physical changes to infrastructure systems. Industry must work quickly to adapt its information assurance strategies to protect the IT investments it has made.

Here’s a Vision 2020 no one wants to talk about. Visualise the following scenarios, some of them occurring near simultaneously:

- An unknown hacker attacks the national power grid and manages to black out all of north India and also interfere with the cellular networks. No one knows what is going on.
- An unknown hacker breaks into the Reserve Bank of India's firewalled account of the Consolidated Fund of India and attempts to transfer Rs. 2,000 crore to an international account.
- Reports in the *Srinagar Times* carry articles on the low morale of Indian troops in the Siachin sector. The reports are also corroborated by the radio station *Vadi Ki Awaz*.
- The newly imported AN/TPQ 37 Weapon Locating Radar suddenly develops a critical fault during a period of unusually heavy shelling by an adversary, when the equipment is required the most.
- During the naval manoeuvres off Coco Islands, the Global Positioning System of the Carrier Group shows abnormally large errors, becoming unusable.
- During an air exercise in the Western sector, the pilot of a Mirage 2000 suddenly finds his avionics blanked out, as if by a 'high energy wave'.
- The Naval Integrated Logistic Management System is found to be causing havoc with inventory issues. It is later discovered to be infected by an unknown virus.
- The season's worst fog has affected the working of the Indira Gandhi International Airport and the Air Traffic Control tower reports that its Instrument Landing System is non-functional and its software programme has been fully compromised. It also warns that there's every possibility of the mid-air collision of aircraft cleared for landing.
- The Prime Minister comes live on TV and declares a national emergency. India is under a cyber attack.

Over the past few months, serious security intrusions have been reported in the government networks of Germany, the United States, the United Kingdom, France and New Zealand. India is swallowing the bitter truth: if the future is digital, then the wars of the future will be virtual. Since we lack the means to measure the robustness of our infrastructure systems, it is difficult to know whether our critical infrastructure is becoming more or less robust as a result of government and private initiatives and new technology. The operational environment in 2010-15 is likely to see an increase in the capability and opportunity of known threat sources. Coupled with the broader presence and exposure of control systems to the cyberspace environment, the future operational environment will be both congested and more vulnerable. Should an actor emerge that has the *Intent*, the equation *Threat = Capability + Intent + Opportunity* will be complete.[10]

National Strategy to Secure Indian Cyberspace

An often quoted definition of strategy is that it is "a style of thinking; a conscious and deliberate process; an intensive implementation system; the art of ensuring future success." The starting point of a strategy (or a strategic plan) has to be a threat. Without a threat – real or perceived – there is no need for a strategy. And as the threat evolves, the strategy must evolve in turn. In the national security arena, we are concerned with threats to our national interests – threats which should cause the national security decision-making machinery to go into action. Ideally speaking, the political leadership of a country, in conformity with national policies and objectives, should evolve a Grand Strategy, which is a plan of action for the attainment of these objectives.

A national strategy to secure cyberspace should ideally provide a framework which is essential to our economy, security and way of life. The cornerstone of such a strategy must essentially be a public-private partnership. Only by acting together can we achieve a more secure future in cyberspace. For any strategy to work, there must be a plan in which a broad cross-section of the country is both invested and committed. This strategy, it must be remembered, is not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change and our understanding of cyber security issues improves. We need to continue the national dialogue on cyber security, calling for voluntary partnerships among government, industry, academia and non-governmental groups to secure and defend our cyberspace. Conducting national-level debates and seminars at various IT hubs in the country would help us solicit the views of various stakeholders.

Efforts to span the digital divide are gathering pace. Once the territory of grassroots movements and non-governmental organisations, big businesses are now throwing their weight behind initiatives to connect India. Microsoft, for example, revealed plans to set up a network of 50,000 internet kiosks across India over three years. Called Project Saksham, the plan aims to set up connected PC kiosks in at least 200,000 villages, using existing phone lines or VSAT satellite link-ups. These kiosks are to be run by local entrepreneurs.[11] VSAT is a commercial service typically used to provide internet access to remote locations. It can be expensive but offers speeds up to 2 megabits per second (mbps).

Strategic Objectives for Cyber Defence

In selecting a 'space for solutions' and arriving at a viable national strategy for cyber defence, any nation would be guided by its ability to meet its technical, economic and social needs. The feasibility – political, technical and economic – of adopting various measures to meet the strategic objectives chosen will also be a determining factor. An achievable strategic objective for a developing country like India in the not too distant future (5-10 years) could be:

- Prevent cyber attacks against information systems and IT based/dependent infrastructures.
- Reduce the overall national vulnerability to cyber attacks; and
- Minimise damage and reduce recovery/resuscitation time from cyber attacks that do occur.

Implicit in the above mentioned objectives is the appreciation of how such a strategy might be implemented, what it might cost, whether the leadership is prepared to pay that price and how effective it would be. An assessment would also be needed of whether the leadership believes that through a combination of individual and cooperative terminal defence by owners and operators, damage can be reduced to a manageable level. Finally, the government must also appreciate that damage limitation would entail time, cost and provision of adequate resources. What is required is cyber battle management the ability to detect and assess the goals of an attack and to decide in near real-time which protective counter-measures to take.

Prioritisation of Efforts

There is a need for a synoptic and holistic view of cyberspace. It would be ideal to have a panoramic vantage point from which one can discern attacks coming or spreading. Protecting our cyberspace requires a national effort involving every netizen. Clearly laid out priorities would help in coordinating various agencies involved in this effort. A suggested priority could be:

- Development of a Cyberspace Security Response System: This must include all the stakeholders, governmental and non-governmental entities, and private-sector system owners and operators. Sector-specific Information Sharing and Analysis Centres (ISACs) are recommended. A sector-ISAC is an industry-led mechanism for gathering, analysing, sanitising and disseminating sector-specific cyber and physical security threats, vulnerabilities, incidents, and solutions.
- Implementation of a National Cyber Threat and Vulnerability Mitigation Programme: This would also entail the enhancement of law enforcement capabilities for preventing cyber crimes and prosecuting cyber criminals.
- Promotion of Cyber Security Awareness and Training Programme at the National Level: It is an acknowledged fact that education and outreach play an important role in making users and operators sensitive to security needs.
- Proactive Measures to Secure the Government's Cyberspace: Ministries of the government must be designated as the 'lead agencies' to identify and document enterprise architectures; continuously assess threats and vulnerabilities; and implement security controls and remediation efforts to reduce and manage threats posed to agency operations and assets. They must first identify which part of its infrastructure requires nationally organised protection. This focuses attention on the efficient application of national resources, protecting what is most critical and deferring what is less critical.
- Strengthen counter-intelligence efforts in cyberspace and promote international cooperation to detect and prevent cyber attacks as they emerge.

An attempt must be made to identify priority areas which need immediate attention. Any proposed strategy for cyberspace security would need to identify specific measures to pursue these priorities. Convening and facilitating discussions between government and non-governmental entities is a must before arriving at an action plan. Sharing of information about cyber threats and vulnerabilities with non-governmental entities would go a long way in adjusting risk management strategies and plans as considered appropriate.

Conceptual Structure for Addressing Cyber Security Issues

Faced with the possibility of serious disruption(s) to information systems – a vital national infrastructure – it would be expected that we plan and implement prudent defensive actions. Such plans would obviously form part of the overall defensive Information Operations (IOs) strategy, integrating and coordinating policies, personnel and technology options to protect and defend information and information systems. Policies aimed at protecting critical infrastructure would require a clear logic relating perceived states of vulnerability to the desired aim of those defensive policies. Since defensive actions will imply costs of various sorts – which each country or establishment will seek to minimise – it will be important to note that the defensive systems are not too burdensome. It must also be remembered that absolute defence against attacks has rarely been achieved.

The conceptual structure being suggested involves five related issues. First, it is essential to attempt to deter potential attackers. Second, if attacked, the need is to foil or frustrate the attack and to prevent damage. Third, since success cannot be guaranteed in either preventing or thwarting an attack, the next best tactic would be to limit the damage as far as possible. Fourth, having sustained some level of damage from an attack, the defender must reconstitute the pre-attack state of affairs. Finally, since both offence and defence are influenced by changing technology and incentives to attack, the defender must learn from failure, just as the attacker will. There will be trade-offs between various courses of action from the above conceptual structure or analysis.[12]

Preventing an Attack

There are three possible ways to prevent an attack. One is to deter the attacker by demonstrating the capability to inflict punishment. When the cost of ‘punishment’ is less for the defender than the loss that can be caused by the attacker, there will be an incentive to develop ways of discovering attackers. A second way to prevent an attack is by establishing cyber attacks as unacceptable behaviour in the comity of nations. This can be achieved through formal agreements or through domestic laws and international agreements designed to protect privacy, property rights and other generally accepted areas of mutual interest. A third way to prevent an attack is to preempt the attacker. This would call for national-level surveillance capability in order to provide strategic warning. For the most part, preventing cyber attacks is the responsibility of sovereign states through various law enforcement agencies.

Thwarting an Attack

The detailed knowledge needed to thwart an attack would rest primarily with the owner of the target. There are many ways of defending systems against cyber attacks, and a certain number of measures must be employed for the owner to demonstrate due diligence in protecting property rights. These will include requiring authorisation to enter premises, monitoring and recording the use of the system to detect unauthorised activities, periodic inspection of the integrity of critical software and establishing and enforcing policies governing systems security and responses to unexpected events. There is considerably more potential to protect systems if the owners cooperate for their mutual benefit.

A third approach is to build systems with a degree of intrusion tolerance. These would aim at limiting the effectiveness of single intruders through architectural approaches such as distributed control, multiple redundant systems with voting, incorporation of air gaps and automated and manual monitoring of critical operations. Undertaking cooperative terminal defence would ensure greater overall effectiveness.

Limiting Damage During a Successful Attack

The central theme of this initiative is to limit the damage as a result of an attack. Beyond being able to recognise that an attack is under way, damage limitation implies linking system operation centres for situational awareness and attack assessment. This also implies having established response options at various levels. Damage limitation can also include preplanned redundancy and the establishment of a priority structure to dynamically reconfigure a system and reallocate load in response to system stress. Auditing of the system operations periodically would be essential.

Reconstituting After an Attack

Short-term reconstitution is the first step to meet the most emergent threats to national security, life and property. This may include assessing damage and implementing a recovery plan. Systems are restored from back-ups where possible/feasible and residual resources may have to be curtailed or rationed. Additional capacity may be generated as facilities that are idle or in maintenance are brought online. Long-term reconstitution of facilities and information may also be required, especially where physical damage has occurred. This will involve the identification and stockpiling of long-lead items. Managing such risks will require industry-wide planning to share surviving capacity and insuring against loss.

All these situations will call for a 'worst case scenario' planning. Long-term reconstitution includes the feedback loop, to use actual events to identify failure modes and solutions. Adapting to changing technical capabilities and circumstances has to be a continuous process. Risk management is a must. Effective risk management involves more than just deploying the latest security products and hoping for the best. A more comprehensive approach to information security may involve a process-oriented, standard-based methodology that defines risk management into four discrete components: risk assessment, development of counter-measures, planning and execution of the counter-measures and testing the measures implemented. The response to any threat should be positive and active rather than passive; the paranoid approach may prove counter-productive.

Improving the Defender's Performance

It is an acknowledged management principle that an organisation must learn from experience. Also, events rarely unfold as expected and even if they do, social and technological change will diminish organisational effectiveness. Notwithstanding the same, it is good to plan the defensive approach in a systemic manner. While a system must meet its functional objectives, it is essential that at the outset of the design process, consideration is given to defence against action. Information about the defence of the system should be concealed from potential attackers, and the system should be designed to give unsuccessful attackers as little information as possible on which to develop improved attacks. Finally, during the development process and after, deployment systems should be subject to independent penetration testing.

The Importance of Public–Private Engagement in Cyber Security: Actions and Actors

As a nation decides on the strategy and actions to be taken to protect its cyberspace, it must also understand the implications of their implementation. One question arises, in terms of technical feasibility, with respect to both current technology and future progress through Research and Development (R&D). A second consideration is the cost of implementation, especially weighed against the magnitude and imminence of the threat and the financial burden entailed. Finally, the political implications must be considered, such as who bears responsibility; the extent of coordinated efforts required with other countries; and the balance required between defensive and offensive capabilities. The primary and secondary roles for both the national and private participants in this task of cyberspace protection would need to be properly understood. A suggested delineation of responsibilities in each of the contingencies is enumerated in the following sections.

Deterring an Attacker

The responsibility for deterring an attacker is shared by the system owner/individual and the national government. If the owner has installed effective intrusion-detection software, an intruder is more likely to concede defeat. Secondary roles are played by the national government and NGOs. The national government's law enforcement agencies will offer a more effective deterrent when an attacker has been identified and located. Criminal prosecutions are often lengthy, costly and time consuming, but, if successful, will have some impact on deterring potential attackers by showing that the risks outweigh the gains. If cyberspace could be monitored, it might be possible to spot preparations for an attack and make a preemptive strike. This idea is akin to conventional military thinking, where preparations can be defeated and pre-emptive action taken. The current state of cyber-intelligence and early warning systems are hardly inspiring but such capabilities could, one day, be sufficiently effective. This role obviously falls in the realm of the national government, since the scope for private acts of preemption is limited.

Thwarting Cyber Attacks

The responsibility rests almost entirely with the individual owner(s), for he/she can effectively control what kinds of locks are on the doors, who has the keys and whether the doors remain locked. The owner's responsibility is greater still in the defence of systems against insiders. As their employer, the owner has substantial control over these insiders. Governments can assist in the vetting of employees for sensitive positions by making criminal records available. The choice of building intrusion-tolerant systems is entirely the owners', though systems that incorporate enhanced safety may cost more to build and to operate. Building it 'right' is the goal of every system designer, but success is not always assured.

Limit Damage Sustained During an Attack

This is a highly complex requirement from both the technical and policy points of view, as managing a cyber attack in real-time is difficult. The capabilities for mounting adaptive defence can be found in both the private and public sectors. Globally, sensors and low-level assessments are at the system-owner's level, but higher level assessment is a national function. The collection of forensic information would be distributed, but the processes would need to be specified nationally. Where a number of system owners collaborate to share information on a near-real time basis, the concept of adaptive defence will work well.

Post-attack Reconstitution

This is an area where the system owner has the central role, for only the owner can establish what is operating and what has been shut down, what reconstitution alternatives exist and how remedial measures can be effected operationally. Governments can play an important role in that they can provide back-up personnel and facilities (if available), assist in the coordination of emergency responses or provide leadership in drawing up pre-attack planning for disaster recovery.

Improving Defensive Performance Through Lessons Learnt

This would also help in the design of future systems. Exploitable flaws in systems used would need to be identified so that they can be minimised/ avoided in the future. Since owners have only a limited or restricted view of their systems and their vulnerabilities, third-party assistance such as a security organisation with experience in a wide range of systems may be more effective. It is the responsibility of the owner/operator to employ independent attack teams to review designs and test system penetrations. Third-party mechanisms will also be able to establish models of attack and attackers, and will have a greater incentive to share lessons learnt.

An attempt has been made, therefore, to identify a broad allocation of roles, highlighting that it is the combined effort of all concerned that can make IT systems function well, despite being prone to cyber attacks. The main strength of our cyberspace security strategy is and will remain a public-private partnership. The central government must encourage the creation of, and participation in, public-private partnerships to implement this strategy. Only by acting together can we ensure that adequate investment is made in cyber security measures and enforceable management policies and practices are adopted.

National Cyber Security Awareness and Training Programme

Many cyber vulnerabilities exist because of the lack of cyber security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, Chief Information Officers, Chief Executive Officers and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructure, regardless of whether they exist within the infrastructure itself or outside of it. Lack of trained personnel and the absence of widely-accepted, multi-level certification programmes for cyber security professionals complicate the task of addressing cyber vulnerabilities.[13] Some initiatives which would go a long way in enhancing awareness, education, and training on matters pertaining to cyber security could include:

- A comprehensive national awareness programme to empower all netizens – businesses, workforce, and the general population – to secure their own parts of cyberspace.
- Promote private-sector support for well-coordinated, widely recognised, professional cyber security certifications.

- Seek the help of the National Skills Mission to develop appropriate skills in cyber security measures and as a follow-up of the recommendations of the Knowledge Commission, provide adequate training and education programmes to support the nation's cyber security needs.
- The government could also think of a 'Scholarship for Service' programme which would provide funding to colleges and universities to award scholarships to students in the information assurance and computer security fields, in exchange for their service in the government after they have completed their training.

Regulatory Provisions

Regulation to protect public interest is a universally accepted norm. However, more recently, the regulation of markets and the imposition of technical standards have come to be seen as economically inefficient and inhibiting technical and business innovation. This opinion notwithstanding, there is still significant regulation over matters concerning public safety in transport, food, drugs; in assuring equitable access to telecommunication services; in the protection of financial frauds; and in the protection of the environment. Regulation in cyber security matters will be equally necessary, because when disasters occur, the public reaction is usually to ask why the government did not act sooner and more vigorously. Another possible regulatory role would be to require independent testing or certification of private terminal defence and reconstitution efforts. Government regulation can also play a role in ensuring a minimum quality of service of regulated utilities.

Assistance to Small- and Medium-sized Business (SMB) Enterprises

A survey by Symantec found that 84 percent of the respondents from India were aware of the need to protect information but many had budgets of only Rs 100,000 to work with. The survey found that while there was growing awareness among the SMB enterprises about the various threats to their data, the deployment of relevant solutions to counter this threat had not matched up. Inadequate budgets, coupled with ineffective information security management at the operational level, were the main stumbling blocks. The survey covered verticals such as financial services, healthcare, telecommunications, manufacturing, retail, professional services, education, entertainment and recreation, business support services and real estate. It revealed that small- and medium-sized businesses in India want to protect their information, both internally and externally, but wafer-thin budgets, coupled with inadequate and under-trained manpower are clearly stopping them from doing so.

The government's initiative in pooling security R&D, penetration testing, determining security standards and industry best practices, and contributing to the establishment of educational and training curricula and certification of professional security personnel would be greatly welcomed by such enterprises.

Lessons From Other Countries

The experience of more technically and economically advanced countries that are extensively networked could be very useful in drawing up a national strategy for the protection of cyberspace. The United States' 'National Strategy to Secure Cyberspace' outlines an initial framework for both organising and prioritising efforts. It provides directions to the central government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organisations, and individual Americans can take to improve their collective cyber security. This document also highlights the role of public–private engagement. It is learnt that before drawing up the final document, a draft version of it was released for public comment, and ten Town Hall meetings were held around the nation to gather inputs on the development of a national strategy. Thousands of people and numerous organisations participated in these Town Hall meetings and responded with their comments. Such an exercise/initiative would prove beneficial to our country as well.

Compliance to Best Practices

These relate to the management of security and IT. They include 'best practices' for developing, installing, and operating computers and networks so as to minimise security vulnerabilities and risks. Best practices have been developed in areas such as selecting and managing passwords, deploying firewalls, configuring and upgrading systems, and planning for and responding to security incidents. Information Security Management-Requirement (ISO 27001), IT Service Management System (ISO 20001) and other Service Level Agreements (SLAs) should be complied with and demonstrated. While there are technologies that serve to protect cyberspace, none offer a 'silver bullet' solution for security. Security is possible only through a combination of controls, coupled with good management and operating practices, supporting laws, and effective law enforcement, in short, the security infrastructure. Even then, security is never foolproof.[14]

Central and Nodal Referral Agency for Cyber Security in India

In 2004, the government set up the Indian Computer Emergency Response Team (CERT-In). Such set-ups exist in almost 62 countries of the world covering Asia, North and South America and Europe. CERT-In's main task is to ensure the security of cyberspace in the country by enhancing the security of communications and information infrastructure, through proactive action and effective collaboration, aimed at security incident prevention, prediction and protection and security assurance. It has as a stated mission: Alert, Advice and Assurance. In carrying out its mission, CERT-In has viewed its roles in both reactive and proactive modes, besides identifying its reporting, analysis and response functions.[15] CERT-In's four enabling actions include:

- Enabling the government as a stakeholder to create the appropriate environment/conditions by way of policies and legal/regulatory framework to address important aspects of data security and privacy protection.
- Enabling user agencies in the government and critical sectors to improve the security posture of their IT systems and enhance their ability to resist cyber attacks and recover within a reasonable time, if attacks do occur.
- Enabling CERT-In to enhance its capacity and outreach and to achieve force multiplier effects to serve its constituency in an effective manner as a 'trusted agency'.
- Hold public communication and contact programmes to increase cyber security awareness and to communicate government policies on cyber security.

CERT-In has also circulated security guidelines to all government organisations and made them available on its website as well. The organisation conducts regular security workshops for system and network administrators from the government, defence, public sector and private sector. CERT-In has an important role to play in the overall cyber security efforts. While the Information Technology Act 2008 (ITA 2008) has made some headway in providing legal backing for the conduct of electronic surveillance and to bring cyber terrorists to book, it still needs to be backed up by a comprehensive set of rules focusing on the delivery of security on a national scale in cyberspace. CERT-In should act as a fulcrum for formulating a National Cyber Security Strategy. Besides, it can act as a coordinating agency for national cyber intelligence and integrate the activities of cyber crime policing in different states. It can also enter into cyber crime prevention treaties with other countries to ensure international cooperation against cyber terror. As a counter-intelligence strategy, it can counter-hack, plant its own intelligence gathering mechanisms where required, and defend the country from external aggression through cyberspace. Some similar roles and tasks as assigned to the US Department of Homeland Security could be examined in the Indian context and can be overseen by CERT-In. The organisation should be a single point of contact for the government's interaction with industry and other partners for 24/7 functions, including cyberspace analysis, warning, information sharing and major incident response.

To improve national capabilities for warning, CERT-In should establish an out-of-band private and secure communication network, 'The Cyber Warning and Information Network (CWIN)'. The network must include voice conferencing and data collaboration with the purpose of sharing cyber alert and warning information with the government and industry. The successful functioning of the CWIN will rest on its ability to share sensitive cyber threat information in a secure, protected, and trusted environment.

The National Technical Research Organisation (NTRO) is a premier scientific organisation that was set up in 2003, after India was first exposed to the cyber arsenal maintained by the United States. On the drawing board, the NTRO was conceptualised as an agency that would focus on technical intelligence and surveillance and ensure the security of key government networks. The NTRO's activities include aviation and remote sensing, data gathering and processing, cyber security, crypto systems, strategic hardware and software development and strategic monitoring. The NTRO has, under its umbrella, the National Institute of Cryptology Research, National

Information Infrastructure Protection Centre, Disaster Recovery Centre and Aerospace and Remote Sensing Centre. As much of the work carried out by the NTRO is not available in the public domain, it is difficult to comment on its contribution, especially in matters related to cyber security. Also, it would not be wrong to presume that with so many vital functions to handle, each important in its own right, the attention to cyber security matters may not be as adequate, keeping in mind the urgency and seriousness of the threat. Perhaps due to the enormity of the work involved and the need for more focused attention on cyber-related matters, one of the political parties (the Bharatiya Janata Party) deemed it fit to include in its election manifesto the setting up of an independent organisation, namely the Digital Security Agency (DSA), to holistically address all issues related to cyber security, cyber warfare and cyber counter-terrorism. The NTRO, as the very name suggests, should conduct pioneering R&D and encourage the transfer of results to users everywhere. It may lend its expertise, built over the years, in areas such as encryption technology and penetration testing. Emerging areas of research also can produce unforeseen consequences for security. The emergence of optical computing and intelligent agents, as well as developments in areas such as nanotechnology and quantum computing will, quite likely, reshape cyberspace and its security. NTRO's mission should be to ensure that the nation is at the forefront of understanding these technologies and their implications for security.

The Cyber Security Enhancement Bill has been introduced for the US Senate's final approval. This Bill is the first major cyber security legislation to come up for consideration before the 111th Congress. It is expected to result in substantial investments to create a cyber security workforce as well as cyber security research. The Bill would help the federal government develop a skilled cyber security workforce, coordinate and prioritise federal cyber security research and development, improve the transfer of cyber security technologies to the marketplace and promote cyber security education and awareness of the public.[16] Such a Bill must be introduced in India too, for the vast majority of cyber security breaches occur because current best practices are not followed.

Security Assurance: Actions by Home Users and Small Businesses

Even before tools and counter-forces are deployed, an awareness of the severity of the threat among all users must be a priority. Informed vigilance – a result of education, training and constant reinforcement – is required to ensure protection against current and future exploits. Even with the best tools and systems in place, the greatest danger is that our systems and computers are vulnerable due to complacence or simple ignorance. Home users and small businesses can help the nation to secure our cyberspace by:

- Maintaining a level of awareness necessary for self-protection.
- Using current anti-virus software and updating it with security enhancements at regular intervals.
- Being aware of the security pitfalls while on the internet and adhering to security advisories.
- Maintaining reasonable and trustworthy access control to prevent abuse of computer resources.

Cooperation to Safeguard Shared Information Infrastructure

The US and Indian governments are intensifying their cooperation to address national security issues arising from the increasing interdependency of our critical network information systems involved in outsourced business processing, knowledge management, software development and enhanced inter-government interaction. Enhancing the security of shared information systems was made a priority by India and the US during a November 2001 summit in Washington between President Bush and Prime Minister Vajpayee. Work began in earnest in April 2002 with the establishment of the US-India Cyber Security Forum, a group mandated to cooperate on policy, procedural, and technical issues of cyber security interest to both nations.[17] Both governments are committed to enhancing this cooperation by creating a joint Indo-US Cyber Security Initiative that will focus on capacity building through exchange of experts, training, sharing information, and strengthening public-private partnerships. Since 2002, six working groups have been established within the framework of the Cyber Security Forum to address specific issues:

- Legal Cooperation and Law Enforcement (co-chaired by the US Department of Justice and the Indian Ministry of Home Affairs).
- Research and Development (co-chaired by the Department of State and the Defence Research and Development Organisation within the Ministry of Defence).
- Critical Information Infrastructure, Watch and Warning and Emergency Response (co-chaired by the US Department of Homeland Security and the Indian Computer Emergency Response Team within the Department of Information Technology).
- Defence Cooperation (co-chaired by the US Department of Defense and the Indian Ministry of Defence).
- Standards and Software Assurance (co-chaired by the Department of Commerce and the Indian STQC [Standardisation, Testing, Quality and Certification) within the Department of Information Technology].

To promote international cooperation in this regard, CERT-In is a full member of FIRST (a global leader in incident response and management), APCERT (a trusted contact of computer security experts in the Asia-Pacific region) and a global research partner of APWG (Anti-Phishing Working Group). India must also join the efforts to form an international network capable of receiving, assessing and disseminating this information globally and thereby promoting a global 'culture of security'.

Trends suggest an increase in safe havens for cyber criminals and, hence, the need for international cooperation arrangements. Experience shows that targets and attackers are often not in the same legal jurisdiction and, hence, worldwide cooperation is essential. Efforts must continue to ensure that our laws and procedures to combat cyber crimes are comprehensive. We should, at the same time, improve inter-agency coordination between law enforcement, national security, and defence agencies involved in cyber-based attacks and espionage, ensuring that criminal matters are referred, as appropriate, among these agencies. As of now, cyber criminals seem to have no real threat of prosecution. It is important to create a climate of fear of effective prosecution, as in other types of crimes.

On empirical grounds, one can say that the response to the cyber security challenge is developing along multi-organisational lines, and it appears that this should be the case. It is also clear that while governments are clearly the most important actors in cyber security, other actors, including industry and the private commercial sector, also have a contribution to make. In seeking the security of an organisation, its members, affiliates and their interests, there is a need for a balance to be struck between defensive/passive/protective measures and a more activist or offensive stance. Then, there is a balance to be struck between security measures and civil liberties. And, finally, there is a balance to be struck between securing the specific interests of a given organisation or government, and the more general requirement to create for the benefit of all legitimate users, an international communications and technological environment, which is hostile to the activities and ambitions of cyber terrorists, cyber criminals and hackers.

Promulgation of Best Practices

CERT-In should facilitate a public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during the development process. In the long term, the central issue is the education of the engineers responsible for the design and operation of complex systems. Being a developing country, India will take time to introduce computer technology into older mechanical, electrical and hydraulic systems and this will require new understanding of system complexity. The legacy of complex systems, or dated software, much of it poorly documented and often subject to less than adequate configuration management, further complicates the technical task of the defender.

Corporations must be encouraged to regularly review and exercise IT continuity plans and to consider diversity in IT service providers as a way of mitigating risk. Coordination with other concerned agencies and in partnership with industry to develop best practices and new technology will go a long way in enhancing the security of cyberspace.

Conclusion

Cyberspace provides a platform for innovation and prosperity and the means to improve general welfare around the world. But the broad reach of the loose and lightly regulated digital infrastructure poses great risks to nations, private enterprises and individuals. The Government of India has the responsibility of addressing these strategic vulnerabilities, to ensure that the country and its citizens, together with the larger community of nations, can realise the full potential of the information technology revolution.

India's efforts towards the formulation of a National Cyber Security Strategy are not, so far, distinctly visible. With the enactment of ITA 2008, CERT-In has been provided with some teeth, in that it now has a statutory role to play. While the rules for such roles are being worked out, there is a fair amount of apprehension about some of the operating sections of the revised ITA 2008, especially those related to the protection of civil rights, rights to privacy and protection of propriety data.

Cyber security and personal privacy need not be opposing goals. Cyberspace security programmes must strengthen, not weaken, such protections. CERT-In must continue to meet regularly with privacy advocates to discuss cyber security and the implementation of ITA 2008.

In December 2009, Chinese hackers are believed to have attempted to penetrate India's most sensitive government offices, in the latest sign of rising tensions between the two rival Asian powers. M K Narayanan, India's former National Security Adviser, has stated that his office and other government departments were targeted on 15 December, the same date that several US companies reported cyber attacks from China. This was not the first instance of an attempt to hack into our computers, Narayanan told *The Times*. He said that the attack came in the form of an e-mail with a PDF attachment containing a Trojan, which allowed the hacker to access a computer remotely and download or delete files. The virus was detected and officials were told not to log on until it was eliminated. It is difficult to find the exact source of the virus but China seems to be the main suspect. It seems well founded, Narayanan said, adding that India was cooperating with America and Britain to bolster its cyber defences.[18] But both American and Indian officials believe that China is, at best, an internet mischief maker and, at worst, a potential cyber-adversary. US officials hope that tighter ties with India on internet security issues can help make the networks of both countries stronger.[19]

It must be recognised that cyber security is one of the most serious economic and national security challenges we face today. Cyberspace is real and so are the risks that come with it. Our digital infrastructure must be treated as a strategic national asset and protecting this infrastructure should be a national security priority. Efforts must be taken to deter, prevent, detect and defend against cyber attacks and to recover quickly in the event of an attack. The possibility of cyber warfare should be treated as seriously as the threat of a missile strike, and the prospect of a full-blown internet war is not 'science fiction' any more.

Increased reliance on computers makes any nation vulnerable to cyber attacks and the problem is only growing. The lone answer to this problem is preparedness and vigilance. We can't afford to be surprised by a major cyber attack that leaves us scrambling to create new systems and new defences that are too little and too late. Priorities in the protection of cyberspace must be clearly identified to ensure proper coordination of work assigned to various organisations engaged in this vital aspect of national security. This argues for urgent strategic planning and institutional mechanisms on a national scale before passing a point of no return, if this has not already occurred.

Our reliance on cyberspace will only grow in the years ahead. This national dependency must be managed with continuous efforts to secure cyber systems and the networks that connect to it in order to protect our economy and national security. A well-articulated national strategy is an indication of the nation's resolve to protect its cyberspace. There is an urgent need to prepare a 'Common Operating Vision', which would seek to achieve operational consistency to respond to the ever-widening challenge of cyberspace security. If we act now, we will not only be secure but will also be poised to capitalise on the real promise of the digital revolution. The government needs to conduct a national dialogue on cyber security to develop more public awareness about the threat and risks and to ensure an integrated approach toward the nation's need for security and the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law.

Appendix

Taxonomy of Cyber Threats

Botnets: Botnets are networks of compromised machines under the control of attackers. These days, botnets have become a popular medium for performing malicious activities, ranging from information stealing to using it as a launching pad for distributed attack.

Denial of Service: Intruders launch a DoS attack to overload or halt network services such as web or file servers. Such attacks deny authorised persons access to resources and, thus, delay critical operations.

Elevation of Privilege: This is a process by which a user obtains a higher level of privilege than that for which he/she has been authorised. An intruder may mislead a system into granting him/her unauthorised rights in order to compromise or destroy the system.

Information Disclosure: Information disclosure refers to the act of disclosing information that was previously not known. For example, a user might share certain confidential files over the network, thereby making them accessible to everyone connected to the network.

Phishing: This technique, largely used by hackers, fraudulently acquires sensitive information posted on the internet. The term was coined after intruders began 'fishing' the accounts of unsuspecting Internet Messenger members for information.

Pirated Software: Counterfeit software is illegal and often contains bugs and viruses. Legitimate software provides up-to-date protection against hackers and e-mail viruses as well as providing improved system recovery tools.

Repudiation: Repudiation refers to the denial of having performed an action that other parties cannot disprove. For example, an intruder who has deleted a file can deny it in the absence of mechanisms such as audit records that prove otherwise.

Spam: Unsolicited bulk e-mail messages that can be commercial in nature, such as an advertisement; or non-commercial, such as chain letters or jokes. Spam is usually a vehicle for viruses.

Spoofing: There are two main types of spoofing – IP spoofing and e-mail spoofing. IP spoofing is largely a security exploit. Here the intruder sends data packets that display an IP address different from that of the intruder. Thus, if the packets appear to originate from a computer on the local network, the spoofed IP packet passes through the firewall security without any trouble. This technique is used primarily in one-way attacks such as Denial of Service (DoS). In e-mail spoofing, the e-mail message is forged so that the true address of the sender is not indicated.

Spyware: A programme that covertly gathers information about your online activities without your knowledge. Spyware usually enters the computer while downloading or installing a new programme and allows intruders to monitor and access your computer.

Tampering: Tampering occurs when the contents of data packets are altered incorrectly before they reach their destination. Tampering is done as the data packets travel over the internet or after penetrating a network. The attacker, for example, could alter the information as it leaves your network.

Trojans: As the name suggests, Trojans are malicious programmes that perform tasks contrary to what they indicate they will do. They don't replicate like viruses, but are potentially harmful.

Virus: Viruses are programmes that replicate themselves by infecting other programmes on a computer. Potentially harmful, some viruses lie dormant inside innocuous programmes, while others wreck the operating system as soon as their code is executed.

Worms: Similar to viruses, worms replicate themselves but they do not affect other programmes. On the other hand, they seek other computers connected to the current host.

Notes

1. "Cyberspace," http://www.techterms.com/definition/cyberspace, accessed on 10 February 2010
2. Deepa Kurup, "Web Security Compromised," *The Hindu*, 07 June 2009.
3. Donald D Codling, "Cyber Threats in the 21st Century," FBI Cyber Division, 26 January 2010, www.meeting.afrinic.net/afgwg/presentations/day2/01_02_drccyberthreats.pdf, accessed on 10 February 2010.
4. Bruce Hoffman, "The Use of the Internet by Islamic Extremists," Testimony presented to the House Permanent Select Committee on Intelligence, 04 May 2006, http://www.rand.

org/pubs/testimonies/2006/RAND_CT262-1.pdf, accessed on 20 February 2010.

5. "US Military Flags China Cyber Threat," *Security Focus Brief 696*, 06 March 2008, http://www.securityfocus.com/brief/696, accessed on 15 February 2010.
6. Bryan Krekel, George Bakos, Christopher Barnett, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Prepared for The US-China Economic and Security Review Commission, 09 October 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf, accessed on 15 February 2010. This report presents a comprehensive open-source assessment of China's capability to conduct Computer Network Operations (CNO) during peace-time and periods of conflict.
7. General James E Cartwright, in "China's Military Modernization and Its Impact on the United States and the Asia Pacific," Hearing before the U.S.-China Economic and Security Review Commission, First Session - 110th Congress, 29-30 March 2007, p. 91, http://www.uscc.gov/hearings/2007hearings/transcripts/mar_29_30/mar_29_30_07_trans.pdf, accessed on 10 February 2010.
8. "Cyber Wars Between Pakistan and India," 31 March 2008, http://www.articlesbase.com/internet-articles/cyber-wars-between-pakistan-and-india-373872.html, accessed on 15 February 2010.
9. Lt Gen S R R Aiyengar, "Digital Security Agency," *SP's Land Forces*, September 2009.
10. Peter D Gasper, "Cyber Threat to Critical Infrastructure - 2010-2015," Prepared for presentation at Information & Cyberspace Symposium, Fort Leavenworth, Kansas, 22-24 September 2008, www.usacac.army.mil/cac2/cew/repository/papers/Cyber_Threat_to_CI.PDF, accessed on 10 February 2010.
11. Ravi Venkatesan, "Chairman Speak," Keynote address at a Microsoft seminar on 'India is Innovation,' http://www.microsoft.com/india/keynote.aspx, accessed on 10 February 2010.
12. Lt Gen S R R Aiyengar, "Information Assurance – The Way Ahead," Proceedings of Indian Army-CII seminar, 26-27 May 2005.
13. "A National Cyberspace Security Awareness and Training Program," *The National Strategy to Secure Cyberspace*, February 2003, www.us-cert.gov/reading_room/cyberspace_strategy.pdf, accessed on 15 February 2010.
14. Dorothy E Denning, "Cyber-security as an Emergent Infrastructure," in Robert Latham (ed.), *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (New York: The New Press, 2003), p. 27.
15. "CERT-In," www.cert-in.org.in, accessed on 15 February 2010.
16. Emmanuel Parisse, "US House Passes Bill to Bolster Cybersecurity," *Agence France Presse*, 04 February 2010.
17. "Indo-US Science & Technology Forum," http://www.indousstf.org, accessed on 10 February 2010.
18. "NSA: China Waged Cyber War on India," *Times Now*, 10 January 2010, http://www.timesnow.tv/NSA-China-waged-cyber-war-on-India/articleshow/4336598.cms, accessed on 15 February 2010.
19. Julian E Barnes, "Gates Pushes Ties with India on Cybersecurity," *The Baltimore Sun*, 19 January 2010.