CYBER SPACE VULNERABILITIES AND CHALLENGES: THREATS TO NATIONAL SECURITY DYNAMICS

M.K. SHARMA

Dominating the info spectrum is as critical to conflict as occupying the land or controlling the air has been in past.

— General John P. Jumper
USAF Chief of Staff

Cyber space is shaped by policies; it is not some natural feature or 'thing' that grows wild and free naturally.[1]Today, nations are incessantly trying to shape the realm of the Internet and enforce their authority in cyber space to the best of their ability. The asymmetric threat posed by the information revolution has got cyber security to the centre of national security policy concerns. The importance and relevance of the issue for the security community is based on the fact that the information infrastructure that serves as underlying infrastructure for government organisations, industries and the economy has become a key asset in today's security environment.[2]

All critical infrastructures are becoming increasingly dependent on the information infrastructure for information management, communication

* Wing Commander **M.K. Sharma** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

[1] John Perry Barlaw, "A Declaration of the Independence of Cyber Space" (1996) http://www.eff.org/homes/barlow.html.

[2] National Research Council, *Computer Science and Telecom Board Trust in Cyber Space* (Washington, D.C, 1999).

and control functions. Since the information infrastructure enables both economic vitality and military and civilian government functions, it has become a strong national security component. The dependence of defence and government information infrastructures on commercial (public or private) providers and cross-national inter-connection of infrastructures (post-liberalisation and globalisation) have heightened the security requirement of infrastructures in countries across the globe.

Cyber security means the measures for protecting computer systems, networks and information from disruption or unauthorised access, use, disclosure, modification or destruction.

The sophistication in the hacker tools has come of age from mere password guessing ability and self-replicating codes in the 80s, to password cracking, exploiting known vulnerabilities, back doors and disabling audits in the 90s and gaining all new heights of sophistication with techniques like sweepers, sniffers, hijacking sensors, stealth diagnostics and packet forging or spoofing today. This has resulted in availability of phenomenally powerful hacking tools, with a simultaneous sharp drop in the technical knowledge required to use them.

Cyber security means the measures for protecting computer systems, networks and information from disruption or unauthorised access, use, disclosure, modification or destruction.[3] Connectivity is increasing at a rate beyond the capacity to implement controls. Market pressures on hardware and software vendors reduce the introduction of security features and testing prior to product release. Retrofitting security into existing systems and applications is difficult, expensive, and, in some cases, impossible without serious operational impact. However, a more fundamental problem exists in the implementation of controls in that few organisations invest in proper risk assessment before implementing controls. Even fewer understand and qualify specific threats in order to evaluate risks accurately. The consequences can be profound because not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist

[3] As defined by the National Science and Technology Council (2006), p. ix.

or have minimal impact. Fundamentally, security is the identification and management of risk.

The aim of this paper is:

- To study the factors responsible for rising the vulnerabilities of cyber space.
- To study the nature and type of threats posed to cyber space.
- To review the cyber crime and security assurance level of Indian cyber space.

To find an answer to why cyber security has become an issue today, we must understand that the threats in cyber space remain, by and large, the same as in the physical world, for example, fraud, theft, terrorism, etc. There is an attacker and a victim, and the attacker requires the same three components to be successful: Motive, Opportunity and Means (MOM). However, due to Information and Communication Technology (ICT) induced developments, things have changed today; automation has made attacks more profitable; action at a distance is now possible, with anonymity; and attack technique propagation is now more rapid and easier.

Today, MOM is more powerful than ever. Even a novice can download powerful intrusion tools and find free written guides to penetrate systems. The motive is there because there is no barrier to entry for an attacker: millions of pages of free instruction are available to anyone interested in reading it – massively accessible means. In a few minutes, you can hack a bank account and steal someone's life savings because there are still many financial institutions that do not protect their clients and their systems with any sophistication – for some, this presents an irresistible opportunity. So the stage is set today – powerful motive, perfect opportunity and the best means.

Intruders are building technical knowledge and skills, gaining leverage through automation, exploiting network interconnections and moving easily through the infrastructure, and they are becoming more skilled at masking their behaviour. In addition to this, there are three new trends that make all network dependent organisations transparent and vulnerable: Internet enabled connectivity; wireless networking; and mobile computing. Today, e-commerce, m-commerce supported by well-known brand names and critical sectors certainly make a good recipe for trouble for governments across the globe.

There is an evident reluctance on the part of public and private enterprises to implement cyber security measures, perhaps because the stakeholders, including the customers, have not yet started insisting on an assurance. Many organisations would not want to implement strong security measures thinking that they do not have anything that others would want – probably what they do not realise is that they could become launch pads for attacks on others through bots[4]. Quite possibly, there could be other pressing issues of survival that relegate security to an afterthought, especially in a period of economic recession like the current one. Besides this, there is a very difficult choice between convenience and security measures. The trouble is more serious if you are part of critical information infrastructure[5]—there could be someone who is determined to get you for obvious reasons. The need is to have not only preventive abilities, but also keep a track of the adversary's capabilities with the changing times.

VULNERABILITIES

The argument doing the rounds in various international fora that India is not vulnerable to cyber threats as the network penetration is very low and most government work is still done on paper files, does not stand ground because of the very fact that most of the things (economy, finance, banking, defence Services, academia, R&D centres and other NCII[6]) that matter to the very existence of the nation are networked. Possible vulnerabilities within

[4] A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie—in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from the Russian-based Kaspersky Labs, botnets—not spam, viruses, or worms—currently pose the biggest threat to the Internet. http://en.wikipedia.org/wiki/Zombie_computer

[5] In India, the following sectors are considered critical: telecommunication, energy, defence, banking and finace, railways, space, civil aviation, insurance, ports, petroleum and natural gas, atomic energy and law enforcement agencies. Subimal Bhattacharjee, Argus Integrated Systems and Luthra & Luthra Law Offices, *The Country Survey of India 2006*, CIIP Handbook 2006 edition.

[6] National Critical Information Infrastructures.

various domains are required to be understood as many new sectors get networked each passing day.

Laptops and hand-held systems combined with wireless and cellular technologies add a new dimension to the complexity and control of access to systems and networks.

Are the vulnerabilities to cyber attacks increasing with advancements in ICT? Apart from the increase in the number of techniques and sophistication in the methods of attack enjoying the anonymity of the source, there are increased vulnerabilities due to the sheer size and complexity of networks. Today, hundreds and thousands of small, Personal Computer (PC)-based client systems can be connected into a local area network; each of these systems is then interconnected to thousands to form local and wide area networks. The ability to understand the systems, network topologies, points of access and the myriad applications and users is beyond a single system administrator. This lack of control allows security weaknesses to develop or go unnoticed. As size and complexity grows, so does the speed and frequency of changes in terms of basic technology as well as applications and uses of computers and networks. Often, a system administrator finds it impossible to keep up with the functionality of new hardware and software. Within a large network, systems, applications and databases are added and removed daily. Remote connections are constantly changing. Again, in large networks, it is beyond a single system administrator to keep up with the continuous change. This allows vulnerable or unprotected entry points into the network.

Mobility and portability is yet another factor adding fuel to the fire. Laptops and hand-held systems combined with wireless and cellular technologies add a new dimension to the complexity and control of access to systems and networks Again, authentication of legitimate users becomes difficult, if not impossible; also, tracing suspicious activity is much more difficult. These issues, combined with other techniques such as social engineering and taking advantage of security flaws within software, create environments where weaknesses in security can develop. Security is usually considered an afterthought in network design and implementation, and retrofitting security into an existing network can be costly and time consuming. To gain unauthorised access to systems and data, intruders can exploit all of these weaknesses.

BROAD CATEGORISATION OF INTRUDERS' OBJECTIVES

Any nation's resolve to invest in ICT security stems from the ongoing conflict between attackers and security agencies. This reflects the wide variety of motivations and goals of different players, as well as the technological tools and procedures available. Hackers are only one type of unauthorised users. There are many other types of attackers, including terrorists, criminals, unsatisfied employees, hostile and not so hostile nation-states. When it comes to national cyber security, the distinction between different types of enemies (attackers) on the basis of their source of motivation, and resources available to finance the attack is very important to build and choose the right strategy to handle any contingency.

When we look at the complete ICT infrastructure used by the private and public sectors and individuals worldwide, it mainly consists of three categories of resources: first, computing resources such as Central Processing Units (CPUs) and memory used to run applications; second, storage resources such as disc drives and Storage Area Networks (SANs) used to store data; and third, network resources, including routers, wireless access points and hubs, optical fibre cables and satellite links, which connect multiple storage and computing resources together. Therefore, it is evident that the network components are the most common targets because they provide access and allow the attacker to threaten applications, operating systems or storage or computing resources, once inside.

In the broad perspective of national security, any attack on the ICT infrastructure can be viewed as one or more of the specific goals of a state or non-state actor or individual or group to inflict economic damage on the target. This act has to be driven by some motive, with the specific goal being technical objectives. The motives are human objectives, which include financial gain, inflicting malicious harm or furthering national or ideological interests. To understand the vulnerabilities of our ICT infrastructure, an insight into the specific goals or technical objectives of the attacker serves as a better tool. Broadly, there could be three different objectives of the attacker or a combination of them:

1. **Damaging or Diminishing the Effectiveness of the Vital Cyber Security Infrastructure Components:** These attacks generally cause one or more vital portion of a network infrastructure to either become inoperable or to operate at a diminished capacity. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks or the attacks that could cause a vital server or router to go offline or reboot, fall in this category of attacks. These attacks could be directed at a specific organisation, government or individual, intended to disrupt services for a large number of hosts (i.e. end users) or a network.

   This happened in Estonia when its paperless government was attacked not through it geographical borders but through the Internet, affecting all major commercial banks, telecommunications, media outlets, and name servers. This was the first time and certainly not the last time that a botnet threatened the national security of an entire nation. Like nuclear radiation, cyber war doesn't make you bleed, but it can destroy everything. It's a classic example of a DDoS attack.

   The attacker could also disrupt services for a large number of hosts or networks through worms[7] or viruses[8] that can infect a host and propagate to other connected hosts. In the process, as a byproduct or direct consequence of virus activity, vital data on the infected host could be destroyed. French fighter planes were unable to take off after military computers were infected by a computer virus called "Conficker" transmitted through Windows, in October 2008, as the French military ignored the warnings and failed to install the necessary security measures. [9]

[7] A computer worm is a self-replicating computer programme. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing programme. Worms almost always cause at least some harm to the network, if only by consuming bandwidth http://en.wikipedia.org/wiki/Computer_worm

[8] A computer virus is a computer programme that can copy itself and infect a computer without the permission or knowledge of the owner. http://en.wikipedia.org/w/index.php?title=Special%3ASearch&search=&go=Go

[9] Kim Willsher, "French Fighter Planes Grounded by Computer Virus," *Ouest France*, Published: 11:43 am GMT, February 7, 2009.

Another very popular way this objective can be achieved is through Unsolicited Commercial E-mail (UCE) or spam, as it is commonly known. Analogous to barrage jamming[10] of a radar to saturate its receivers, a large number of spam messages originating from, or sent to, a single e-mail server, can crash it or degrade its performance, in the bargain causing delays in the delivery of important e-mail messages.

2. **Gaining Unauthorised Access to the Target's Sensitive Data and Information:** Most public organisations and particularly the private business organisations are vitally dependent on their proprietary information, including new product information, personnel data and / or from client records. An attacker may derive direct economic benefits from gaining access to and/or selling such information, or may inflict damage on an organisation's reputation. The attack may be preceded by worms and viruses that create back doors in the target's infrastructure (e.g. Blaster worm[11]) for an attacker to enter and collect information. Other ways of gaining confidential information could be: sniffing vital information from the network traffic originating from, or intended for, the target; guessing or cracking passwords on the systems of interest to gain access to the system; or causing a privilege escalation, in which an insider working in the organisation uses security holes to increase attacker's access level.

   Recently, the Chinese firm GE (Geely Excellence) launched a car at the Shanghai motor show with a price tag of £30,000, which is supposed to be the stolen copy of the original Rolls-Royce Phantom design with a £250,000 price-tag, the preserve of a privileged few.[12] Rolls-Royce is considering legal action against the Chinese copycat. This just shows how

[10] Barrage jamming: jamming by transmitting a band of frequencies that is large with respect to the bandwidth of the victim emitter, such that the victim emitter will not be able to avoid this noise signal by retuning. Wing Commander Sanjay Poduval, *Electronic Warfare: War In The Fourth Dimension* (New Delhi: KW Publishers, 2009), p. 31.

[11] The Blaster Worm (also known as Lovsan or Lovesan) is a computer worm that spread on computers running the Microsoft operating systems: Windows XP and Windows 2000, during August 2003. http://en.wikipedia.org/wiki/Blaster_(computer_worm) , http://www.cert.org/advisories/CA-2003-20.html.

[12] "Rolls-Royce-Considers-Legal-Action-Against-30000-Chinese-Copycat," http://www.telegraph.co.uk/motoring/5205369/Rolls-Royce-considers-legal-action-against-30000-Chinese-copycat.html : 9:31AM BST 23 Apr 2009

much of R&D effort can be stolen by unauthorised access to confidential and sensitive data.

A popular way of such attack is phishing[13] in which the attacker attempts to extract private and confidential information from the target by crafting forged e-mails or websites that pretend to originate from, or belong to, an entity the target may trust. Attackers who broke into TD Ameritrade's database (containing all 6.3 million customers' social security numbers, account numbers and e-mail addresses as well as their names, addresses, dates of birth, phone numbers and trading activity) also wanted the account usernames and passwords, so they launched a follow-up spear phishing attack.[14] Almost half of phishing thefts in 2006 were committed by groups operating through the Russian Business Network based in St. Petersburg.[15] Such e-mails generally attempt to solicit bank account numbers, credit card numbers or other private information from their targets for further resale or misuse. They can also modify or delete sensitive information, resulting in damaging consequences for their targets.

3. **Gaining Unauthorised Access to Cyber Resources for Illegal Use:** The technical objective is to attack and utilise the storage and network resources like disc space (for storing illegal images, video games, etc) of the victim's computers. The victim could be anyone from an individual with a computer and a broadband connection to an employee of a large organisation with multiple sites networked together who may possess resources that an attacker could utilise. A more popular form of this type of attack is manifested in breaking into systems to get free services, such as free access to the Internet using a personal or corporate wireless access point or in attacking the billing infrastructure of a cell phone

[13] Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT Administrators are commonly used to lure the unsuspecting public. http://en.wikipedia.org/wiki/Phishing

[14] "Torrent of Spam Likely to Hit 6.3 Million TD Ameritrade hack Victims," http://www.webcitation.org/5gY2R1j1g

[15] Brian Krebs, " Shadowy Russian Firm Seen as Conduit for Cybercrime," *Washington Post*, October 13, 2007.

service provider for getting free access to cell networks. In fact, cellular service providers are more vulnerable to these attacks than fixed line phone service providers. Convergence of digital and voice service on a single network allows attackers to introduce attack packets into the network more easily. Also, the fact that today's cellular networks have a direct connection to the Internet makes them more vulnerable to attacks from the Internet.

Combination of Objectives: Generally, the attacker pursuing one of the goals goes through several steps, which may include one or more of other goals before the final goal is achieved. For example, an attacker may first scan a portion of the network to find any vulnerable hosts, then use an exploit to gain access to a number of personal computers connected to the Internet (objective 3) to perform a DoS attack on part of the target's infrastructure (objective 1), such that the attack disables the protective infrastructure of the target and the attacker may gain access to the target's confidential information (objective 2). The blaster worm that targeted hosts' running server applications took control of vulnerable hosts with the ultimate objective to launch a DoS attack on the Microsoft website that was scheduled to start on a specific day, when all infected hosts would begin generating bogus traffic intended to disrupt Microsoft's infrastructure.

Like all other military targeting, most cyber attacks are preceded by the surveillance and reconnaissance phase in which the attacker gathers maximum possible information about the target.

Like all other military targeting, most cyber attacks are preceded by the surveillance and reconnaissance phase in which the attacker gathers maximum possible information about the target (individual, organisation, network component or nation's critical information infrastructure). This phase helps in identifying weaknesses in the target infrastructure that can later become a target of direct attack. The methods include: network scans to determine the topology of the target network, intercept and look at the content of packets travelling through the data lines using 'sniffer' applications; information about the target from open sources (Internet, print media, other types of media); social engineering, which involves meeting employees of the target organisation under an assumed identity (e.g. a sub-contractor or an employee from a remote unit). The latest tool for gathering information is called wardriving, where vulnerable wireless access points are identified and mapped using wireless laptops equipped with a Global Positioning System (GPS). Information gathering could also be directed to specific network components, hardware or software. An attacker may work to find a hole or bug in an operating system or application that is widely used by the target organisation/nation so that an attack can easily be launched on many individuals/organisations simultaneously (which make the usage of the multi-operating system in an organisation good mitigating strategy against cyber attack).

Broadly, there are two main phases of launching a cyber attack. The first phase is to perform a detailed mapping of the net, collecting data on active network devices to carry out a vulnerability analysis. In this respect, many networks worldwide detect a more or less regular activity of mapping, often performed by unidentified sources. In the second phase, the appropriate software weapon is released; however, release does not mean activation. The activation can be done later, programmed to occur at a certain time, under certain defined, logical conditions or following a specific command. In some cases, the test reaction can also be performed in advance, to evaluate the defence capabilities of the victim system.

Information and Communications Sector: In addition to the natural disasters, the primary threats to this sector are system failures and instabilities arising from the increased volume and complexity of interconnections. In the past, there have been documented deliberate attacks and intrusions through the software-based disruption of network devices and management systems. In recent years, the Public Switching Telephone Network (PSTN) has increasingly become software driven, remotely maintained and managed through computer networks, which has increased the vulnerability to electronic intrusion. The existence of mega-centres for operations support creates a single point of failure and makes the targeting of hostile action easier. As the Internet was basically not designed for high-level security purposes, all infrastructures based on IP (be it Internet-based or Intranet-based) are vulnerable by design.

Energy Sector: The federal government of the United States admits that electric power transmission is susceptible to cyber warfare. The United States Department of Homeland Security works with the industry to identify vulnerabilities and help it enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks is developed. In April 2009, reports surfaced that China and Russia had infiltrated the US electrical grid and left behind software programmes that could be used to disrupt the system. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack. China denies intruding into the US electrical grid. One counter-measure would be to disconnect the power grid from the Internet to decrease the likelihood of attack. Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

The level of vulnerability to this sector has been increased by the recent rapid proliferation of industrywide information systems based on open architecture used in the operating environment. This includes increasing reliance on communication links which sometimes run over public telecommunication networks. The national power grid in India is yet to see the light of day but vulnerabilities on account of using Commercially-Off-the-Shelf (COTS) hardware and software cannot be ruled out. COTS are considered risky because detailed specifications might not be available or may simply not be met by some of the components, causing limitations of functionality or faults due to law quality standards. They may sometimes, have built-in vulnerabilities and may pose problems of security and dependability.

NCW and Defence Intranets: India is rapidly moving towards developing Network-Centric Warfare (NCW[16]) capability. NCW is vital; a nation cannot survive for long against a good adversary without this capability today. It is

[16] NCW, a concept pioneered by the United States Department of Defence, relies on computer processing power and networking communications technology to provide shared information of the battlespace among the armed forces. This shared awareness increases synergy for command and control, resulting in superior decision- making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage, http://en.wikipedia.org/wiki/Network-centric_warfare

estimated that the Indian Air Force (IAF) would possess NCW capability by 2011-12. The backbone of this entire system will be a fibre optic-based network called Air Force Network (AFNET), of which the recently acquired Airborne Warning and Control System (AWACS) will be the sky link to integrate all ground and air-based weapon platforms and communication systems. For the IAF's net-centric operations, the Integrated Air Command and Control Systems (IACCS) riding on AFNET, will provide the connectivity for all the airborne platforms and ground platforms.[17]

If we were to think that all defence networks, are independent networks on dedicated Fibre Optical Cable (FOC) and so are immune to cyber attacks, this could only be wishful thinking.

If we were to think that all defence networks, including the Air Force Network (AFNET), Army Wide Area Network (AWAN)[18], and Navy Enterprise Wide Network (NEWN), etc are independent networks on dedicated Fibre Optical Cable (FOC) and so are immune to cyber attacks, this could only be wishful thinking. While these are amongst the first major initiatives undertaken to prepare the Indian armed forces for fighting in the digital battlespace, these Intranets are also exposed to enormous vulnerabilities. For instance, most of the hardware and software of these projects is of the COTS type, with the fault control and maintenance being undertaken remotely. The risk of not knowing all the details of the hardware, the possibility of hidden bugs in the system, and the controls being remote and at a single point pose threats to secure Command, Control, Communication, Computers, Information, Intelligence (C4I2). The sensitivity of information in defence C4I2 makes these independent Intranets vulnerable to the insiders' threat. Going by Murphy's Law, and given the fact that in all locations/ stations there are a few authorised Internet connections for the field commanders' use and for obtaining meteorological data, etc, the possibility of intermingling/ cross-connections (deliberate or inadvertent) of the Internet and AFNET/AWAN/

[17] Quoted as saying, Vice Chief of Air Staff Air Marshal P. V. Naik at the Nellis Air Force Base, while participating in the prestigious Red Flag exercise, dated 16/8/2008.

[18] Army Wide Area Network (AWAN), which has been designed to connect all Army formations, units, training establishments and logistic installations in the country. President Abdul Kalam congratulated the team of the Corps of Signals and Tata Consultancy Services for undertaking this project and completing it in time across 174 signal centres.

NEWN cannot be totally ruled out in spite of explicit written instructions and Standard Operating Procedures (SOPs) being in place.

There are also the vulnerabilities arising due to non-compatibility of data links of different defence Services Intranets.

There are also the vulnerabilities arising due to non-compatibility of data links of different defence Services Intranets. Sharing of real-time information is vital to execute Effect-Based Operations (EBOs) in a net-centric environment. Integration of old technology weapon platforms to modern Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) networks through interfaces has two distinct vulnerabilities: the limitation on operational capabilities and increased probability of system failure because of system complexity alone, without any external trigger.

The advent of advanced systems like the 'Suter' programme[19] which has been tested with aircraft such as the EC-130, RC-135, and F-16CJ and has been used in Iraq and Afghanistan by the US since 2006 and presumably by the Israeli Air Force to sneak into Syrian air space undetected in Operation Orchard on September 6, 2007[20], has opened up a plethora of new vulnerabilities for systems like the Integrated Air Command and Control Systems (IACCS) of the IAF and computer controlled integrated Air Defence Systems (ADS) around the world.

Banking and Finance Sector: This is, by and large, considered the safest

[19] A military computer programme developed by BAE Systems that attacks computer networks and communications systems belonging to an enemy. Development of the programme has been managed by Big Safari, a secret unit of the United States Air Force. It is specialised to interfere with the computers of integrated air defence systems. Three generations of Suter have been developed. Suter 1 allows its operators to monitor what enemy radar operators can see. Suter 2 lets them take control of the enemy's networks and direct their sensors. Suter 3, tested in summer 2006, enables the invasion of links to time-critical targets such as battlefield ballistic missile launchers or mobile surface-to-air missile launchers. http://en.wikipedia.org/wiki/Suter_(computer_program) and David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week and Space Technology*, October 3, 2007.

[20] US Air Force officials have speculated that a technology similar to Suter was used by the Israeli Air Force to thwart Syrian radars and sneak into their air space undetected in Operation Orchard on September 6, 2007. The evasion of air defence radar was otherwise unlikely because the F-15s and F-16s used by the IAF were not equipped with stealth technology. John Leyden (October 4, 2007). "Israel Suspected of 'Hacking' Syrian Air Defences", *The Register*, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/. Retrieved on 2007-10-05

domain, the main vulnerabilities being of physical nature. India as a nation has put strong measures in place for securing these infrastructures and providing extensive redundancy. However, there remains some level of risk from disruption of telecommunication and electric power services. Besides large-scale infrastructure vulnerabilities, this sector also suffers from lucrative opportunities for theft and fraud in individual branches/institutions.

The most potent and persistent threat to the banking sector comes from the insiders, who might be authorised access to confidential information or operate systems, which could be used for personal profit. Another negative fallout is its intrinsic sensitivity and in order to maintain public confidence, financial institutions will often avoid reporting to the Computer Emergency Response Team (CERT)-In or any external agency. This reduces the transparency of the system, making analyses of intrusions and protection of the overall infrastructure more complicated.

Transportation Sector: As this sector is becoming increasingly reliant on ICT infrastructure, new cyber vulnerabilities are emerging every day, for example, the website of Eastern Railway was hacked on December 24, 2008, by a Pakistani group[21] claiming that the site was hacked in response to the alleged violation of Pakistani air space by the Indian Air Force.[22] These freak incidents may not seem alarming at face value, but certainly show the potential that cyber power holds in future wars in the region. It should serve as a wake up call to military planners to accrue the asymmetric leverage through cyber power in furthering national objectives.

The recent crash of two Washington DC Metro transit trains (June 22, 2009) in which the train ploughed into a stationary train ahead of it, killing

[21] The note posted on the hacked page of the railway website read "Cyber war has been declared on Indian cyberspace by Whackerz- Pakistan," http://www.dnaindia.com/mumbai/report_indo-pak-cyber-war-hots-up_1219482

[22] This hacking incident followed a similar defacement of the website of the Criminal Investigation Department (CID) of the Andhra Pradesh police, which had been compromised by Pakistani hackers soon after the 26/11 strikes. Soon after the attacks, an Indian group -- Guards of Hindustan -- hacked into the website of the Oil and Gas Regularity Authority of Pakistan and posted their logo and the Indian national emblem on it. In retaliation, the Pakistan Cyber Army, hacked the websites of the Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, the Army's Kendriya Vidyalaya of Ratlam and the Oil and Natural Gas Corporation (ONGC). http://www.dnaindia.com/mumbai/report_indo-pak-cyber-war-hots-up_1219482

nine people and injuring more than 70, was the deadliest accident in the 30-year history of the Washington Metro and is being attributed to the failure of the computerised system to halt an oncoming train.[23] This is yet another example of vulnerabilities due to the rapidly expanding use of the intelligent transportation system to optimise and increase overall efficiency.

The most significant vulnerabilities are considered to be those associated with modernisation of the National Air Space System (NAS) for Air Traffic Control (ATC).

The PCCIP[24] report of the US states that the most significant vulnerabilities are considered to be those associated with modernisation of the National Air Space System (NAS) for Air Traffic Control (ATC). This includes plans to adopt the GPS as the sole basis for radio navigation in the country by 2010.

Indian air space management is still evolving. Its infrastructure, mainly shared by the civil aviation sector and Air Force, consists of a confusing mix of obsolescence and modern equipment and infrastructure. The ATC at most Air Force bases is mainly primary radar-based and, at civil airports, it is being done with the Monopulse Secondary Surveillance Radar (MSSR) equipment, with little redundancy in place. Planning of scheduled maintenance also requires ad-hoc change in procedures for controlling, and a breakdown of MSSR is immediately converted into a crisis for ATC. The metro airports have the satellite-based ADS systems, with the Services being provided by the sole provider to the global aviation industry, SITA[25]. The latest of the systems available, like the Controller Pilot Data Link Communication (CPDLC), are data link-based and are, thus, prone to unauthorised intrusions by programmes like 'Suter' which can not only observe or jam but can also manipulate (Suter 3) the data being fed through data links. Even the Modernisation of Airfields Infrastructure (MAFI) project of the IAF is based on the COTS hardware and software

[23] Brian Witte, Brett Zongker, Matthew Barakat, Gillian Gaynair, Alex Dominguez and Sagar Meghani, *Associated Press*, June 23, 2009.

[24] President's Commission on Critical Infrastructure Protection, US.

[25] SITA is a multinational information technology company specialising in providing IT and telecommunication services to the aviation industry. Originally known as the Société Internationale de Télécommunications Aéronautiques, http://www.sita.aero/.

products and shared communication networks. As a consequence, the risk of unauthorised access and the probability of malicious actions would only increase. Before we get our Indian Regional Navigational Satellite System (IRNSS)[26] in place, overreliance on GPS is a matter of concern and to be viewed with caution as access to the Global Navigation Satellite Systems, GPS, is not guaranteed in hostile situations. Besides India does not have ultimate control over GPS services; it is also prone to jamming (transmission of noise interfering with the original signal) and spoofing (broadcast of false GPS information).

THREATS

How do potential cyber disasters compare with disasters in the physical world? In the physical world, there is immediate loss of lives and infrastructure, like in Mumbai 26/11 or US 9/11, or a natural disaster like the Bhuj earthquake on January 26, 2001. On the other hand, the damage from a cyber attack does not necessarily and directly manifest in loss of lives or infrastructure like in the cyber attacks on Georgia and Estonia. However, it can jeopardise/compromise the essential services such as medical information system or transportation system, which, in turn, could affect lives. India, in the very near future is going to get so many of her essential services networked, and a cyber attack disrupting communication and electric power distribution would become a real and quite probable threat. Disruption of transportation (surface and air), shipping, and financial transactions by cyber means would become more frequent and intense. Interaction of the cyber and physical world with terrorist minds would bring out the force multiplier facade of cyber power to the fore. Think of the damage to a railway track being used to carry troops, with simultaneous disruption/altering of trains routing and reservation data by a cyber attack or an aircraft hijacking with a successful

[26] IRNSS is an autonomous regional satellite navigation system being developed by the Indian Space Research Organisation which would be under the total control of the Indian government. The requirement of such a navigation system is driven by the fact that access to the Global Navigation Satellite Systems, GPS, is not guaranteed in hostile situations.:"India to Build a Constellation of 7 Navigation Satellites by 2012", http://www.livemint.com/2007/09/05002237/India-to-build-a-constellation.html

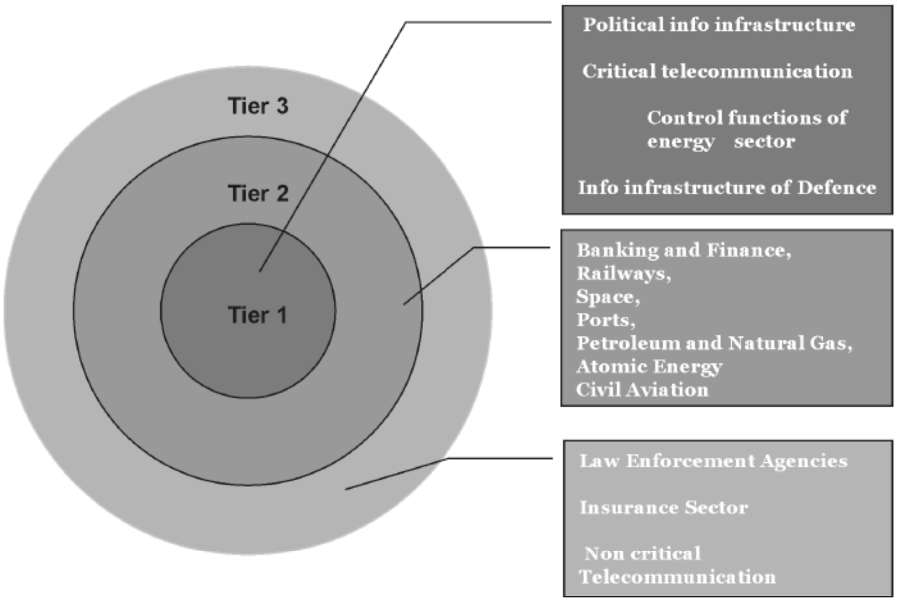
cyber attack on ATC systems. Obviously, the damage would be more catastrophic.

Persistent firepower coupled with persistent ISR cannot be maintained without a truly secure and robust networking of these assets.

Cyber Centres of Gravity: Giulio Douhet in his work *Command of The Air*, has suggested that massed effects against an enemy's centres of gravity can lead swiftly to bloodless victory. For the conduct of such Effect-Based Operations (EBOs), the basic enabler is Network-Centric Operations (NCO). Network-Centric Warfare (NCW) enables Intelligence, Surveillance and Reconnaissance (ISR) results to be applied in near real-time to execute EBO, thus, achieving rapid victory by attacking the coherence of the enemy's ability and will to fight. It is obvious that persistent firepower coupled with persistent ISR cannot be maintained without a truly secure and robust networking of these assets. This is where the cyber threat comes to the centre-stage of security concerns. So, how serious is the threat and how do we assess it? One traditional way (which may not be the best way for this asset, not bound by geographical boundaries and space) of looking at cyber security is that all the national cyber assets be grouped in tiers (say three tiers) on the basis of centres of gravity as shown in Fig 1.

Tier one, the innermost centre of gravity, would consist of those components of the National Critical Infrastructure (NCI) which are critical to national security and sustaining human life such as political information infrastructure, critical telecommunication sector, control functions of the energy sector and info infrastructure of the defence sector, etc. This must be made as robust as possible. The components of Tier two, the next centre of gravity, would consist of those cyber assets which are important to the country's economy even if they are not likely to cause physical harm if disabled, such as banking and finance, railways, space, ports, petroleum and natural gas, atomic energy and civil aviation, etc. The third tier, the outermost centre of gravity, would consist of systems whose disruption would cause considerable personal inconvenience or economic loss but would not present a threat to the existence of the society as a whole, such as law enforcement agencies, insurance sector, non-critical telecommunication sector, etc.

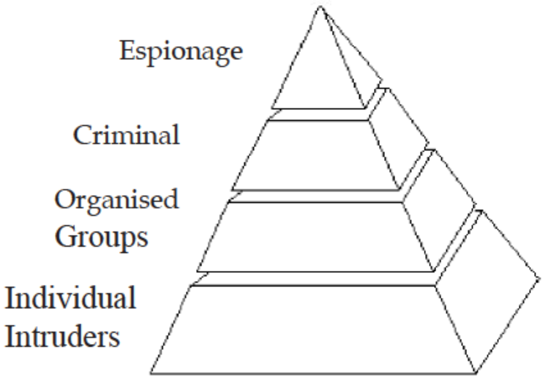
Fig 1: Cyber Centres of Gravity


Tier 3
Tier 2
Tier 1
Political info infrastructure
Critical telecommunication
Control functions of energy sector
Info infrastructure of Defence
Banking and Finance,
Railways,
Space,
Ports,
Petroleum and Natural Gas,
Atomic Energy
Civil Aviation
Law Enforcement Agencies
Insurance Sector
Non critical Telecommunication

CATEGORISATION OF INTRUDERS

Who are the actors? The canvas is very wide: there are professionals or amateurs or hobbyists who would spend nights on the computer to break into electronic systems. Often with no malicious intentions but for a personal challenge or just to grab media headlines. There are also those groups, including insiders, that are involved in industrial, economic or corporate espionage motivated by money or revenge. There are other individuals/corporations who are targeting for financial information resources or actively seeking a competitor's trade secrets, often using insiders. Furthermore, there are politically motivated state and non-state groups, ranging from government agencies like intelligence agencies or military units to terrorist groups; their goals could include information collection, propaganda, electronic surveillance, censorship and sabotage.

Fig 2: Intruder Categorisation Model[27]



To get an insight into both the patterns of activities and the scale and scope of general threats to systems and networks, a general categorisation of the intruders (not exactly hackers[28]) based on the motivations behind intrusions can be done, based upon Kent E. Anderson's model, as shown in Fig 2.

Individual Intruder: Usually acting independently in the pursuit of personal goals, the motive of these individuals is generally the challenge or thrill of gaining access to a computer system. They may cooperate to some extent in loose associations, sharing information and techniques. However, there is usually no strategic planning or organised tactics for penetrating systems or networks. Also, the resources available to this level of intruder are usually limited to popular, off-the-self PCs and peripherals.

Gary McKinnon[29] from north London has been accused of committing the "biggest military computer hack of all times", cracking open the systems

[27] Kent E. Anderson, "International Intrusions: Motives and Patterns" (Proceedings of the 1994 Bellcore/Bell South Security Symposium) May 1994, pp. 3-5.

[28] Due to the academic controversy with the word "hacker" and the common public misconception of a "hacker" as a bad guy, a malafide intentioned youth, the term *intruder* will be used to describe an individual who illegally accesses or makes unauthorised use of a system.

[29] Jon Ronson, in an interview to *The Guardian* on July 9, 2005, revealed that the most exciting thing he saw was a list of officers' names under the heading "Non-Terrestrial Officers" who he thinks are not earth-based. He also found a list of "fleet-to-fleet transfers", and a list of ship names which weren't US Navy ships, but believed to be some kind of spaceship, off-planet. news.bbc.co.uk/1/hi/technology/4715612.stm

of the Pentagon and National Aeronautic Space Agency (NASA). He caused damage and impaired the integrity of information. The US military district of Washington became inoperable and the cost of repairing the shutdown was $700,000 . If extradited to the US, he faces up to 70 years in jail.

Organised Groups: Organised groups vary from loose affiliations with common interests (and often separate, individual goals) to highly cohesive organisations with well-defined goals. The major motivation for this category is entering a computer system to gain access to specific information or system and network resources. Organised groups may have any number of interests in information such as political or environmental vandalism, access to proprietary technical information or personal information such as credit reports.

There are innumerable examples of organised groups, including the German Chaos Computer Club (CCC),[30] the Dutch Hack-Tic group[31], the English group 8lgm, the US Legion of Doom (LOD)[32] and participants of the Japanese Otaku.[33] A classic example of a group loosely organised around to have access to specific information is described in the US Government's Sentencing Memorandum for several Legion of Doom (LOD) members whose motive was to obtain power through information and intimidation.[34]

These groups typically have moderate to high (systems level) knowledge of computer and telecom systems, switches and networks. The resources available may include small networks, bulletin boards/voice mail systems and access to funds via membership dues, newsletter subscriptions and press speaking or book royalties.

Criminals: Currently, this is the highest growth area in terms of both number of intrusions and monetary damage, and the primary motive of the criminal category is to gain access to a system for profit or unfair market share. They have technical abilities ranging from very low to high, or may

[30] K. Brunnstein, "Report: 8th Chaos Computer Congress", *Risks-Forum Digest*, vol. 13, issue 03, January 10, 1992

[31] Ibid.

[32] US Government's Sentencing Memorandum, US v. Grant, Darden and Riggs, Criminal Action Number 1:90-CR-31, December 1990.

[33] K. Greenfield, "The Obsession of the Otaku" *Los Angeles Times*, , September 12, 1993, p. 40.

[34] n. 32.

recruit technical skills (either with or without the individual's knowledge of criminal activity). The crimes involving monetary gain include wire transfer theft, industrial espionage,[35] credit card theft,[36] or pseudo security consultants. It is believed that the development of the Tupolev Tu-144 supersonic aircraft, with its rapid design and similarity to the Concorde, was one of the most prominent examples of industrial espionage in the 20th century.

The 2004 E-Crime Watch Survey published by CERT estimated that companies lost $666 million from e-crimes in 2003. Recently, the Computer Security Institute and the Federal Bureau of Investigation (FBI) reported in their 2005 Computer Crime and Security Survey that 56 per cent of respondents experienced a security breach in 2004 and 13 per cent didn't know if they had a security breach. In the US, a recent annual survey of companies by the Computer Security Institute and the FBI revealed that 90 per cent of all firms have had some type of Information Technology (IT) security breach in the past year. Eighty per cent of respondents reported a financial loss and 74 per cent responded that the Internet was the most frequent source of attack.

Espionage: This category of intrusions has the greatest variety and complexity of methods and resources. Often, the resources available (equipment, manpower and technical knowledge) are only limited by cost versus the potential gain, similar to criminal activity. With the primary motive of access to systems or information for national economic or strategic objectives, this category has direct national security ramifications.

The Internet security company, McAfee, stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities. It is a cyber Cold War, and with many countries

[35] The Government of France has been alleged to have conducted ongoing industrial espionage against American aerodynamics and satellite companies and vice versa. This list, compiled from public sources over the last fifteen years, is of the countries that are known to be customers of stolen US technology: Argentina, Brazil, France, India, Iran, Iraq, Israel, Japan, Lebanon, Libya, North Korea, Pakistan, People's Republic of China, USSR(Russia), South Africa, South Korea, Taiwan.

[36] The cost of credit card fraud reaches into billions of dollars annually. In 2006, fraud in the United Kingdom alone was estimated at £535 million or US$750–830 million at prevailing 2006 exchange rates.

engaged in clandestine activities, intelligence agencies are routinely testing networks, looking for weaknesses. These techniques for probing weaknesses in the Internet and global networks are growing more sophisticated every year.

Several examples of this type of activity have been reported concerning both the former East German intelligence service[37] and the former Soviet Union[38], with the major focus being on obtaining technology. More recently, many countries like China, Germany, Russia, the US, etc are believed to have an interest in obtaining access to proprietary technical information and information that could assist in advancing national economic objectives.

Proper and accurate threat assessments will allow computer security experts, vendors, and government agencies to better predict future vulnerabilities and mitigate damages.

Proper and accurate threat assessments will allow computer security experts, vendors, and government agencies to better predict future vulnerabilities and mitigate damages. Risk is generally defined as "the possibility of loss". As it applies to information technology, risk is "the possibility for loss of availability, integrity, or confidentiality due to a specific threat". Risk assessment is the analysis of the likelihood of loss due to a particular threat against a specific asset in relation to any safeguards to determine vulnerabilities. Assets are those objects, both physical (buildings, computer hardware, laptops) and virtual (e-mail, software, databases) having value to an organisation.

In considering infrastructure vulnerabilities, threats to both individual systems and the infrastructure itself must be evaluated when considering criminal activity. Both share similar enablers as a prerequisite to compromise, however, infrastructure attacks require a more concerted and coordinated effort and provide better data points for indicator and warning analysis. It is important to distinguish between the two types of attacks in threat assessments.

[37] "Economic Espionage", *Capital*, October, 1992.

[38] C. Stoll, *The Cuckoo's Egg*(New York: Doubleday, 1989).

TYPES OF ATTACK

Infrastructure Attack (IA): An attack designed to compromise significantly the function of a whole infrastructure rather than individual components.[39] A successful infrastructure attack could be capable of sustaining compromise beyond a temporary period. This will usually require attacking recovery systems as well. A successful IA may lead to cascading failure in other infrastructures. The longer the compromise is sustained, the further the effects will propagate. A successful infrastructure attack would most likely be viewed as a national security threat by most countries. However, an attack against an infrastructure that causes significant damage and cost, but is recovered without major disruption and does not affect other infrastructure components i.e. the disruption is localised and contained, would be called a limited infrastructure attack. A limited infrastructure attack could be compared with a major natural disaster such as a power outage experienced due to a heavy snowstorm.

Systems Attack: These are the attacks targeted against individual systems or control centres, which are not detrimental to the overall operation of a whole infrastructure or organisation. It is important to assess the potential and actual damage from these attacks. A successful system attack could be an intrusion where the basic integrity of a system is compromised. This compromise may lead to the loss of confidentiality, data integrity, or system resource availability. However, the attack does not target the infrastructure in which the computer operates.

Successful attacks against information infrastructures are possible though very difficult to carry out. One such known attempt was the attack against the French telecommunications infrastructure initiated by the Chaos Computer Club (CCC) in Germany in September 1995.[40] The CCC called for a denial of service attack against French telecommunications systems to protest against nuclear testing in the Pacific. However, at that time, this

[39] Kent Anderson, "Intelligence-based Threat Assessments for Information Networks and Infrastructures," *Network Risk Management, LLC,* pp. 3-5.

[40] M.A. Gasser, *Building a Secure Computer System* (New York: Van Nostrand Reinhold, 1988). Chaos Computer Club, "Stop the Test", http://www.zerberus.de/texte/aktion/atom/, September 1, 1995.

attack had no impact. If a successful attack were simple, a malicious code such as computer viruses or normal component failure would have already caused massive damage. Successful infrastructure attacks will require precise targeting, and successful, coordinated attacks against multiple system and control points, with exact timing to compromise system redundancy. Attacks may also require compromising multiple levels in the infrastructure architecture (i.e. applications, protocols, system software, and hardware) as well as recovery systems such as back-up operations. However, the virtual reality of cyber power is that the ability to cause damage that once required the military of a nation-state is now within the reach of much smaller, less organised groups.

Where do these Threats Come From (Insiders or Outsiders)? Traditional wisdom holds that insiders are the greatest threat to an organisation. This is based on two assumptions: first, insiders have access; and second, they have knowledge of a company's systems, applications and processes. However, the Internet and e-business are creating a new environment. Consider these facts:

- Companies are connecting to the Internet as quickly as possible. These connections occur with little planning and few controls, creating a whole new level of access from the outside.
- With the electronic connection of companies' businesses to their suppliers, customers and partners, the traditional boundaries are becoming blurred. A sub-contractor hired by one of the suppliers (without a background check and little management supervision) may now have access to, and knowledge of, some or all of a company's business applications and systems.
- Most companies no longer build their own proprietary business applications; instead, they purchase standard, off-the-shelf applications for things such as finance, customer relationship management and order management systems. This standardisation allows outsiders to use applications without detailed internal information.

These and other factors have altered the threats that companies now face. The distinction between an outsider and an insider is decreasing rapidly.

Online services are becoming prime targets for cyber criminals.

While statistics and experience show that the insider is still a significant threat, the outsider can no longer be ignored. Current security architectures are based on an organisation's ability to defend a perimeter, while network and application architectures have created information infrastructures without perimeters. In other words, current security architectures are inadequate to protect present information infrastructures.

GLOBAL CYBER TRENDS

Online services are becoming prime targets for cyber criminals. Cyber criminals continue to refine their means of deceit as well as their victims In general, the global threats affecting users today are: new and sophisticated forms of attacks, attacks targeting new technologies, such as VoIP (vishing – phishing via VoIP and phreaking, hacking telephone networks to make free long distance calls) and peer-to-peer services, attacks targeting online social networks, and attacks targeting online services, particularly online banking services. There is a new level of complexity in malware not seen before. These are more resilient, are modified over and over again and contain highly sophisticated functionality such as encryption (e.g. Nuwar[41] also known as 'Zhelatin' and 'Storm' worm' – with a new variant appearing almost daily). There is an increase in threats that hijack PCs with bots. Another challenging trend is the arrival of self-modifying threats. Broadly, there are three major emerging global trends of mischievous activities in cyber space, which have expanded from novice geeks to organised hi-tech criminal gangs:

- Growing threat to national security – web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organised operations aimed at not only financial, but also political or technical gains.
- Increasing threat to online services – affecting individuals and industry

[41] http://threatinfo.trendmicro.com/vinfo/secadvisories/default6.asp?vname=WAR+AGAINST+NUWAR: +FIGHTING+THE+LATEST+PROFIT-DRIVEN,+MULTI-COMPONENT,+FOCUSED+ATTACK

because of growth of sophistication of attack techniques.

- Emergence of a sophisticated market for software flaws – that can be used to carry out espionage and attacks on government and critical information infrastructure.

The North Atlantic Treaty Organisation (NATO) deployed a cyber defence management authority and a cooperative cyber centre of excellence in Estonia in May 2008 and has approached the Network-Centric Operations Industries Consortium (NCOIC) and BAE systems to help NATO in cyber space awareness and cyber defence issues.[42] The recent creation of the US Cyber Command (that will be fully operational in a year under a new post in the White House) is the outcome of the recognition of the cyber threat as one of "the most serious economic and national security challenges."[43] A glimpse of what is likely to follow in the future is given below:

- It is an inevitable reality that some countries will become safe havens for cyber criminals, and international pressure to crack down won't work well (e.g China's ghostnet[44]).
- In the next few years, governments are likely to get aggressive and pursue action against specific individuals/groups/companies, regardless of location.
- It is also likely that governments will start putting pressure on intermediary bodies that have the skills and resources, such as banks, Internet Service Providers (ISPs) and software vendors to protect the public from malware, hacking and social engineering.
- We may see industry sector codes of practice demanding improved security measures, backed probably by assurance and insurance schemes.

[42] Julian Hale "NATO to Shape Rapid Reaction Force", *Defence News*, July 6, 2009, p. 15.

[43] US President Barack Obama's speech on May 29, 2009, *Defence News*, July 6, 2009, p. 11.

[44] GhostNet (simplified Chinese: □□□; pinyin: YōuLíngWang) is the name given to a large-scale cyber spying [1][2[operation discovered in March 2009. It is based mainly in the People's Republic of China and has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to Embassies, Foreign Ministries and other government offices, and the Dalai Lama's Tibetan exile centres in India, London and New York City were compromised. Although the activity is mostly based in China, there is no conclusive evidence that the Chinese government is involved in its operation http://en.wikipedia.org/wiki/GhostNet, http://news.bbc.co.uk/1/hi/world/americas/7970471.stm. BBC News. March 29, 2009.

- Greater connectivity, and more embedded systems would mean less obvious perimeters of security in geographic terms.
- Compliance regulations will drive upgrades and changes and also increase system complexity and legal wrangles – increase in civil suits for security breaches is foreseen.
- Massive data storing patterns that ensure data never goes away (a boon to law enforcement agencies) will be the order of the day.

CHALLENGES TO NATIONAL SECURITY DYNAMICS

There are varieties of intruders such as individual, organised, criminal and espionage armed with different types of attack capabilities in the cyber space. Cyber space in military terms has its own centres of gravity depending upon the vulnerabilities upon which a successful attack would be decisive in a conflict situation. The concern of security policy-makers is to identify the possibilities/probabilities of criminal or espionage type of intruders attacking the innermost cyber centre of gravity.

The Internet has become a tool for political, military and economic espionage today. There has been an appreciable rise in organised cyber attacks in recent times, including the attacks on the US Pentagon in June 2007, Estonia in April 2007, computer systems of the German Chancellery and three Ministries, e-mail accounts at the National Informatics Centre of India, and highly classified government and computer networks in New Zealand and Australia. The software used to carry out these attacks indicates that they were clearly designed and tested with much greater resources than the usual individual hackers. Most government agencies and companies around the world use common computing technologies and systems that are frequently penetrated by criminal hackers and malware. Traditional protective measures are not enough to protect against attacks such as those on Estonia, as the complexity and coordination in using the botnets was totally new. National networks of countries like India with less sophistication in monitoring and defence capabilities could pose serious problems to national security.

Zero-day Threats[45] and Tools for Cyber Crime: With so many PCs now infected (around 5 per cent of all global machines are zombies), competition to supply botnets has become intense. The cost of renting a platform for spamming is now around US$ 3-7 per zombie per week. You can buy a Trojan that is built to steal credit card data and mail it you for as little as US$ 25 to 1,500. Malware is being custom written to target specific companies and agencies. Computer skills are no longer necessary to execute cyber crime. On the flip side, malware writers today need not commit the crimes themselves. People can subscribe to the tools that can keep them updated with the latest vulnerabilities and even test themselves against security solutions. The black market for stolen data (e.g. credit cards, e-mails, skype accounts, etc) is now well established and the cost of obtaining credit cards is upwards of US$ 5. Another black market that is causing alarm to governments is that of Zero-day exploits. In January 2006, a Microsoft WMF (Windows Meta File) exploit was sold for US$ 4,000.

The Internet has become a tool for political, military and economic espionage today.

Bot Networks and Cyber Arms Race: Bot networks are already generating attacks of overwhelming volume, in ways that are nearly impossible to stop or trace back to their origins. Bot networks are growing in number and power, to where they now pose a serious threat to governments, businesses and online consumers. According to Secure Computing, more than 250,000 personal computers are infected with bots each day, putting at least 10 million computers at the disposal of those with bad intentions. Bots are used by illegitimate businesses to generate billions of spam e-mails and to spread malware worldwide. Moreover, criminal organisations use bots for identity theft via phishing scams. Attacks like that in Estonia may be merely practice drills by crime factions to showcase their computing firepower and their ability to disrupt networks.

[45] A computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability, http://en.wikipedia.org/wiki/Zero_day_attack

Law enforcement and Internet infrastructure companies are cooperating to discover who is planting and orchestrating botnet attacks, but with limited success.

Law enforcement and Internet infrastructure companies are cooperating to discover who is planting and orchestrating botnet attacks, but with limited success. The Internet's very nature makes investigations difficult, especially after the fact. In what amounts to an arms race, operators of the Internet infrastructure are investing constantly to add capacity to handle the volumes of transactions generated by bot attacks. They are also adding teams of professionals and new systems to perform real-time network monitoring and rapid response. But there remains one aspect of the bot threat that cannot be addressed by centralised systems or government investigators—the end user. End users are a critical line of defence, in how they recognise and avoid deceptive tricks designed to download bots to their computers. User awareness is becoming even more critical as the Internet rapidly expands beyond the billion people online today, and reaches more than four billion people not yet online.

The Internet Corporation for Assigned Names and Numbers (ICANN), manager of the Internet domain name system, is implementing Internationalised Domain Names (IDNs) that will help the next billion Internet users enter web addresses entirely in their native language and character sets. If these new Internet users are not warned against downloading any patches or new applications unless they are dealing with a trusted website and scanning for viruses and malware, ICANN is inviting the "next billion" users to download the "next billion" bots capable of generating spam, phishing fraud, and the kind of denial-of-service attacks that brought down Estonia's Internet.[46]

Cyber Crime Review—India: Following its yearly assessment, CERT (Computer Emergency Response Team), the apex cyber security division under the Ministry of Information Technology of India, found that cyber crime in the country has accelerated about 50 times since 2004.[47] Highest growth

[46] Steve Del Bianco, Internet Caucus Advisory Committee, October 2007.

[47] Spam News Admin, Friday, April 18, 2008, http://spamnews.com/The-News/Latest-News/Cyber-Crime-Increases-50-Times-in-India-2008041811429/ Posted originally: 04/17/2008.

has occurred in computer related crimes that attack e-commerce businesses and financial service on the net. The agency recorded just 23 cyber crime incidents in 2004 in contrast to a huge 1,237 in 2007. These primarily included phishing attacks, distribution of viruses/malicious code and illegal infiltration to computer networks. Further, according to the CERT's annual report for 2007, there were 392 incidents of phishing, 358 cases of virus proliferation and 223 cases of network infiltration. Compared to this, there were only 3 phishing attacks, 5 cases of virus proliferation and 11 incidents of network infiltration reported in 2004. While spreading viruses comprise a familiar security issue, it is the large number of phishing attacks that India should be concerned about as these usually aim at middle-class consumers who bank or shop online.

CERT, which also tracks website defacement, found 5,863 Indian websites that underwent mutilation by global hackers in 2007.

CERT, which also tracks website defacement, found 5,863 Indian websites that underwent mutilation by global hackers in 2007. In addition, the agency also tracked 1,805 'open proxy' servers that allow anonymous browsing. It also detected more than 25,000 bot-infected computers. These statistics from CERT are, however, only indicative, without giving the actual picture of cyber crime in India, as the agency merely maintains records of cases that are notified to it. Furthermore, data of the government revealed that in January 2008, 87 security related incidents were recorded in contrast to 45 in December 2007. Of these, 47 per cent involved phishing, 25 per cent was related to worm/virus under the malware category, 21 per cent to unauthorised scanning, and 7 per cent to technical help under separate categories.

Implications for Security: Information security experts have traditionally studied threats on the scale of individual computers or organisational networks. While this is a valid practical approach, it does not reflect the reality of actual or potential threats. When computer misuse is evaluated from the view of the intruder, artificial boundaries such as organisational ownership or national borders are meaningless. A critical challenge to security experts, law enforcement and intelligence agencies is the ability to identify emerging new threats. This has been especially difficult in the arena of information security for several reasons:

- Law enforcement and information security experts for the most part do not use an intelligence-driven approach for prevention and control of computer crime. Investigations tend to be reactive and event-driven. While this has limited effectiveness for simple system intrusions, it will not be adequate for sophisticated or infrastructure attacks. Unless a more analysis-based process is employed, prevention will continue to lag behind the threat curve.
- The speed at which new technology is introduced creates a rapidly moving target for threat assessments. Each new technology requires high-level technical expertise to analyse. By the time vulnerabilities are identified, the technology has changed again.
- Key governmental and industry policy-makers lack the understanding of technology or the multi-dimensional aspects of information security. Many security professionals are biased toward a particular product such as intrusion detection systems or firewalls that limit the scope of proposed solutions.

Security Assurance and Role of CERT-In: CERT-In's primary function is to "alert, advice and provide assurance to ensure security of cyber space in the country" by enhancing the security of communications and information infrastructure through proactive action and effective collaboration aimed at security incident prevention, prediction, protection and security assurance.[48] Security assurance must be provided at every level of the security hierarchy, starting from the network level where the vulnerabilities of hardware and software and issues of access control are addressed. At the transmission level, the focus is on access control and data encryption, whereas at the operating system and application level, software loopholes and access issues need attention. The next higher level in the hierarchy of security assurance comprises the data level where privacy of data and its protection

[48] "Securing Indian Cyberspace: Issues and Challenges," http://www.cert-in.org.in

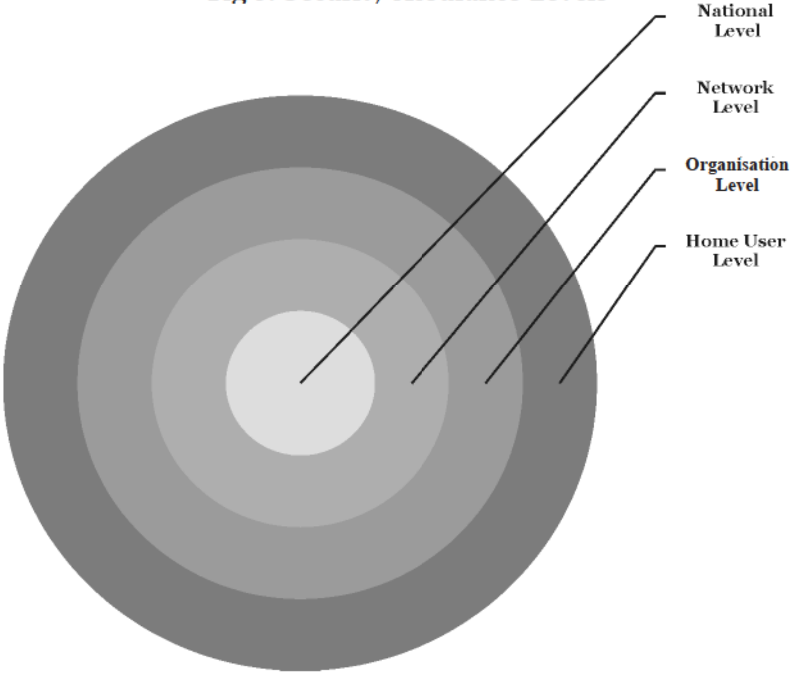
from unauthorised access/manipulation takes precedence, and at the people level, the focus has to be on training, and awareness about cyber security amongst users is crucial. At the organisation level, issues such as cyber security policy implementation and compliance, disaster recovery and legal compliance are important to achieve adequate security assurance.

Cyber Security Assurance Framework: At the national level, we need a strong cyber security assurance framework through which adequate confidence and trust can be built up in cyber power-driven infrastructures and systems. Though it is not possible to make the system 'intruder proof', we can devise a mechanism which can, to a large extent, anticipate potential problems, preempt through proactive measures, protect against considerable damage, and ensure recovery and restoration. This would enable the government, as a key 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 concerns. Specific actions would include National Cyber Security policy, amendments to the Indian IT Act, security and privacy assurance framework, Crisis Management Plan (CMP), etc. This would also enable user agencies in government and critical sectors to improve the security posture of their IT systems and networks, and enhance their ability to resist cyber attacks and recover within a reasonable time if attacks do occur. Specific actions would include security standards/ guidelines, empanelment of IT security auditors, creating a network and database of points-of-contact and Chief Information Security Officers (CISOs) of the government and critical sector organisations for smooth and efficient communication to deal with security incidents and emergencies, CISO training programmes on security related topics and cyber security drills and security conformity assessment infrastructure covering products, processes and people.

At the national level, we need a strong cyber security assurance framework through which adequate confidence and trust can be built up in cyber power-driven infrastructures and systems.

Security Assurance Action Plan: With three clear strategic cyber security objectives i.e. to prevent cyber attacks against the country's critical information infrastructures, to reduce national vulnerability to cyber attacks, and to minimise damage and recovery time from cyber attacks, the security assurance action plan must be implemented at four different levels simultaneously (as depicted in Fig 3).

Fig 3: Security Assurance Levels



At the national level, security assurance can be provided through enactment and implementation of strong cyber laws (e.g. IT Act, 2000) that provide standard guidelines for compliance by all stakeholders in both the private and public sectors. There have to be strict provisions in the law for conformity assessment of IT infrastructure and security incident reporting. Presently, many organisations do not comply with these requirements in spite of existing standard guidelines. Traffic monitoring, routing and gateway controlling is increasingly becoming difficult in a country like India (unlike countries like China where the whole net traffic passes through state-owned information channels) due to multiplicity of service providers. Lawful interception and law enforcement require a proactive approach to avoid a situation where the law is always trying to catch up with the criminals. This would require sufficient and sustained investment of money and talent in the field of R&D on tools and technologies, products and services.

At the lower hierarchical levels (i.e. at the network level, organisation level, small business and home user level), security assurance is gaining more and more importance due to availability of newer malicious tools that target the end user. Compliance with best security practices (e.g ISO 27001) and service quality (e.g. ISO 2001) is essential to plug the gaps in cyber security. Further, illegal use of software is rampant in India and this results in vulnerabilities as most of such software is not updated at regular intervals.

CONCLUSION

If our government and other agencies concerned apply their focus and attention to providing ongoing modern IT security, then can the attackers be easily kept unemployed? The answer is, unfortunately, negative. As attackers are blocked from attacking one way, they will seek another. Attackers previously attacked networks and hosts until it became too difficult, so they switched their focus to attacking applications which were more vulnerable than hosts being blocked at the application level, and now attackers are preying on the end users directly. This can easily bypass most organisations' IT security protocols and processes. In the last few years, new attack patterns have emerged which take advantage of the fact that most individual users know nothing about IT security or their role in keeping things secure.

Our reliance on cyber space is only going to grow in the future. The network of networks spread over the wide spectrum of small and medium business, large enterprises, R&D centres, academia, defence Services, government organisations and national critical infrastructures is intensifying its grip with each passing day. This incremental dependence of the nation on cyber space must be managed with continuous efforts to secure the cyber systems that control our infrastructures. India as a big emerging economy is faced with a complex and evolving challenge more fiercely than the developed nations. Every day, so many new sectors are being networked covering social sectors oblivious of the security aspects of cyber space. This demands awareness and training on a continuous and large-scale basis. To achieve a three-pronged strategic objective of preventing cyber attacks against the country's critical information infrastructure, reducing national vulnerability to cyber attacks and minimising damage and recovery time from cyber attacks, we have to first have a robust system of detecting and assessing the threats and vulnerabilities in cyber space.

The vulnerability in the electronic space can be reduced. There are many products and strategies that can be deployed. There are many robust tools that log attacks and prevent them in real-time. These tools and strategies can provide security for a committed private or public organisation. As long as defence is treated as an ongoing process that is constantly updated and not as an end-state, the battle can be well waged. However, the enormity of the ensuing challenge demands a comprehensive national cyber security policy and strong funding on a continuous basis. Private-public partnership is the key to resolve the issues of talent, infrastructure and R&D facilities. The concept of weekend cyber warriors is worth implementing to outsource the specialised tasks to the large talent pool that exists in the private sector.

The ubiquitous nature of cyber space does not allow anyone to assume something as 'my cyber space' or 'your cyber space' so the need for national cyber security and international cyber security cooperation becomes the priority of our government. With the blurring boundaries between private and public information infrastructures, it requires a long-term effort on the part of both the private sector and the Government of India to use a variety of tools to implement this strategy. Adequate budget allocations are required to provide every department and agency involved in cyber security with resources to execute its responsibilities. In security matters, the past is no guarantee; the present is imperfect; and the future is uncertain. Failure is not when we fall down, but when we fail to get up.