Cyber-Space Security

Shri Ved Prakash Sandlas

Introduction

Computers and internet are invading business, government, national defence and in fact, most aspects of our daily life at break-neck speed. More than one billion people in the world have access to the internet, with a quarter of them with broadband. All these activities now rely on an interdependent network of information technology infrastructures called cyber-space. In the past few years, threats in cyber-space have risen dramatically. Securing cyber-space is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the central government, state and local governments, the private sector, and the people.

A significant amount of our personal information is getting stored either on our own computers or on someone else's system; it may be our income and expenditure details, shopping and credit card records, banking transactions, taxation and other liabilities, and all that information we may not want to make public. Cyber-space security includes protecting personal and classified information by preventing and detecting misuse. For national level defence and security matters, it involves detecting, responding and pre-empting or counteracting cyber attacks.

It is important to recognise and emphasise the related risks and to familiarise with some of the terminologies and international level of concerns and efforts to manage the situation.

Cyber-Space as the New Theatre for War and Conflict

Until 1980s, Space was defined as a new battlefield after Land, Sea and Air, the 'Final Frontier'; when related supremacy was defined in terms of technologies to build and launch missiles and satellite launch vehicles, to defend against 'star-war' type of attacks, and to be able to use and control Space for specific and economic benefits. In fact the relevance of Space activities for India was aptly enunciated by Dr Vikram A Sarabhai: "We are

Shri Ved Prakash Sandlas is a distinguished Scientist and a former Chief Controller R and D, Defence Research and Development Organisation (DRDO), New Delhi.

Journal of the United Service Institution of India, Vol. CXXXVI, No. 565, July-September 2006.

convinced that if we have to play a meaningful role nationally, and in the community of nations, we must be second to none in the application of advanced technologies to the real problems of man and society, which we find in our country."

In the 1990s, information superiority started becoming more important than Space supremacy; concepts of knowledge worker, knowledge industry and knowledge power emerged. Indian computer and software engineers made name for themselves in the international information technology scene, and they contributed to the US and several other countries becoming information giants. India, Indians and Indian web sites, however, are left behind in information generation and supply; there is hardly any Indian on-line-content or information that one may like to download by paying for it. This handicap becomes more pronounced when we want to enter cyber-space for real-life transactions with government agencies, utilities and day to day affairs; notable exceptions being private sector banking and credit card institutions, airlines, and now railways.

It is not just supremacy of cyber-space that is the present issue; the race now is to own cyber-space in such a way that one is assured of all ring-side seats, making all others sit in the back-benches. It is now clear that cyber-space will add a fifth dimension to Land, Sea, Air and Space as a theatre for war and conflict. Only the fastest and the fittest may survive – there is no place for the second best. In the cyber-space, there is no concept of winner and loser; *karo ya maro* has to be the goal.

Definition of Cyber-Space

Cyber-Space is very aptly defined in the February 2003 US Government document entitled *The National Strategy to Secure Cyberspace.* Cyberspace is the nervous system of nation's critical infrastructures and is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables. A nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defence industrial base, energy, information and telecommunications, transportation, banking and finance, chemicals and hazardous materials, postal and shipping. It may be noted that subjects and words such as Strategic, Space, Defence, Nuclear, Police, Security, Paramilitary, etc. are not specifically mentioned.

This document further emphasises that securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from the entire society – the federal government, state and local governments, the private sector, and the people. In fact, it considers private sector as best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where the federal government's response is most appropriate and justified – ensuring the safety of its own cyber infrastructure – or where high transaction costs or legal barriers lead to significant coordination problems.

The US strategy to secure cyberspace articulates five national priorities:-

(a) A National Cyberspace Security Response System.

(b) A National Cyberspace Security Threat and Vulnerability Reduction Programme.

(c) A National Cyberspace Security Awareness and Training Programme.

(d) Securing Government's Cyberspace.

(e) National Security and International Cyberspace Security Cooperation.

The strategy to secure cyberspace is part of an overall effort to protect the US as a nation. It is an implementing component of the 'National Strategy for Homeland Security' and is complemented by 'National Strategy for the Physical Protection of Critical Infrastructures and Key Assets'.

The US has also created the Department of Homeland Security (DHS) on 25 November 2002 to unite 22 federal entities for improving homeland security and to develop a comprehensive national plan for securing key resources and critical infrastructure. DHS is required to be organised as a centre of excellence for cyber-security, to provide technical assistance to the private sector and government entities for emergency recovery plans, and to provide warnings and advice about protective and counter measures. It will also perform and fund research and development, along with other agencies that will lead to new scientific understanding and technologies.

The Law of Cyber-Space

The UN Institute of Training and Research brought out a document titled 'The Law of Cyber-Space' in October 2005 which emphasised concern about absence of globally harmonised legislation turning cyber-space into an area of ever increasing dangers and worries. In many ways, the present situation is similar to the problems faced in dealing with the high seas, when there was no consensus legislation. The international community finally woke up to the challenge, and started negotiations on the Law of the Sea; which took almost a decade to finalise. In the case of cyber-space, the challenge is far greater than high seas; the speed of change is phenomenal, the dangers affect all countries without exception, new shoals and icebergs appear every day, and global responses are sporadic or non-existent. There can be no doubt whatsoever that a globally negotiated and comprehensive Law of Cyber-Space is essential.

The Information Technology Act 2000

The IT Act, 2000 received the assent of the President of India on 09 June 2000. It provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce". It also provides alternatives to paper-based methods of communication and storage of information and will facilitate electronic filing of documents with the government agencies. The act defines the concepts and purpose of Digital Signatures, Certifying Authority, maintenance of Electronic Records, penalties and adjudication for unauthorised access and damage to computer systems, Cyber Appellate Tribunal, liabilities of Network Service Providers, constitution of Cyber Regulations Advisory Committee, and such. For cyber security matters, it empowers a DSP to search and arrest without warrant any one suspected of having committed or about to commit any cyber offence.

UN declares 17 May as the World Information Society Day

On 17 May 2006, UN declared that henceforth the World Telecommunication Day would be known as the World Information Society Day. On this occasion, Kofi Annan stated, thus : "In an increasingly interconnected and networked world, it has become critically important to safeguard our vital systems and infrastructures against attack by cyber criminals, while instilling confidence in online transactions in order to promote trade, commerce, banking, telemedicine, e-government and a host of other e-applications". There is a need to develop a global culture of cyber security, which is especially important for developing countries. In the Institution of Engineers (IE) seminar on 'Promoting Global Cyber Security', the Minister of State for Defence, Shri MM Pallamraju stressed for an India-centric 'national cyber security response system' to deal with threats in cyber-space and from global cyber terrorism.

Information Superiority and Cyber Warfare

Information Technology is a double edged weapon. It provides vast opportunities but simultaneously introduces new vulnerabilities and threats, which may arise through computers, content and connectivity or, to put it differently, hardware, software, information and networks.

Information superiority over our adversaries (including militant and terrorist outfits) is very essential. Non-lethal information weapons can black out communication systems, destroy valuable data and cripple the nation. Therefore, we have to act faster than any adversary. This requires defensive as well as offensive cyber warfare capabilities. Cyber warfare can be a full fledged war and vital infrastructure shall get targeted. To handle cyber wars, highest national level decision making is required, in real time and with full fall-back options. For this purpose, basic building blocks include: excellent monitoring tools for network traffic, web sites and databases; intrusion detection, firewalls, encryption and decryption algorithms, public key infrastructure and remote access facilities.

Offensive cyber warfare spans computer crimes and information terrorism. Everyone is under threat – telephone, power supply, banks, transport, the day to day needs. It is important to create tools, awareness, and structures to assess threats to information resources, including military and economic espionage, computer break-ins, denial-of-service, destruction and modification of data, distortion of information, forgery, control and disruption of information flow, electronic bombs, etc. In essence, the thrust of the initiatives must lead to information assurance like Life Assurance.

Cyber weapons have a range of inter-continental ballistic missiles (ICBMs), speed of high power laser and lethality of both (almost like *Brahmastra).* They are more devastating than nuclear weapons or other weapons of mass destruction (WMDs), are difficult to detect and defend against and are of virtually no cost. It is impossible to limit their battle space, because they are borderless. They do not require any specially trained military organisation, and, hence, any one can master them with minimum effort. Therefore, we should not underestimate the potential of an adversary to build, deploy and use cyber weapons.

Cyber Warfare Ethics

The basic principle of international law relating to military operations and wars prohibits attacking civilians and non-combatant immunity is to be ensured. But in the cyber-space, it is not possible to differentiate between civilians and military personnel. Also, the concept of just war theory states that war should not be initiated by individuals; it must be a collective decision by a known body or a government. But cyber attacks can be easily initiated and managed by motivated individuals. Aggression has to be measured against necessity and proportionality; it cannot be for fun by misguided criminals. It has to be the last resort and should do more good than harm.

'Everything is fair in love and war,' they say. But in the arena of cyber-space, unless otherwise established, nothing is fair in cyber games or cyber wars. Some are even shamelessly fighting for registering .xxx domain!

Cyber Wild West

While justifying creation of global cyber laws, the document 'The Law of Cyber-Space', of the UN Institute of Training and Research has emphasised that Intellectual Property Rights (IPR) damage through internet connected computers has reached $25 to $30 billion per year. Spam now accounts for 45 per cent of all e-mails, or 15 billion messages every day; the world wide cost to business stands at a staggering total of $20 billion a year in lost productivity and technology expenses. At the projected rate of growth, the number of daily spam messages will rise to more than 50 billion by 2007, with costs touching almost $200 billion per year. In a recent survey on e-commerce, it has been noted that

64 per cent decided against purchasing online out of fear. Average losses reported by firms as a result of internet attacks represent about 60 per cent of all other losses. About 40 per cent of firms receive as many as 100 attacks a month, and 80 per cent of these are high magnitude virus and denial of service attacks.

The web site of America's Network reported on 26 March 2006 about an international 'Internet Fraud Crackdown' in the same month. Because of mass-marketing through internet such as bogus lottery, prize and sweepstakes offerings; offers of nonexistent investments; fake offers of 'pre-approved' credit cards or credit-card protection; and tax fraud schemes, more than 2.8 million people, mainly elderly citizens, fell victim to the scams, suffering losses totalling more than $ one billion. A statement from the US Justice Department said that in the US, 139 suspects were arrested, with an additional 426 arrests in Canada, Costa Rica, the Netherlands and Spain as well as Nigeria, Britain and New Zealand.

The web site of Enterprise Innovation, reported on 25 November 2005 the Gartner survey on banking consumers: 40 million Americans think they have received a phishing email during past six months. Cyber criminals using fake emails and web sites to steal account and identity information from consumers is called phishing. Banks are nervous. Of the 1.8 million consumers who recall giving away confidential information such as user ID, password, or credit card number, over half had some form of identity theft related fraud – costing banks and card companies about $1.2 billion in direct losses. It is important for banks to work on stronger methods to authenticate themselves to their customers and their customers to them. They have to resort to shared secrets, trusted third party authentication of users and service providers, and also take help from third-party black lists.

While noting these statistics with concern, we must proceed with caution. Controls and censorship should not sacrifice the benefits of IT as a tool for economic and social progress; respect for privacy, anonymity and freedom of expression are also important.

Terminology of Cyber Attacks

Virus. A piece of code or code fragment – replicates itself when host programme begins to run – erases data, software programme, or memory – to interrupt the action of the computer it infects.

Worm (Turbo Worm). Not just a code but an entire programme – replicates itself even without execution of any other programme – eats up computer resources and/or deletes data – cripples the computer.

Trojan Horse. A programme or code inside a programme – performs a task on the outside, while unleashing a virus or a worm on the inside – can perform information retrieval, without leaving a trace.

Logic Bomb. May release a virus or a worm or perform some other secret task – usually planted by the system developer.

Trap Door. Similar to logic bomb – a secret way back in to the system, left by the designer as a security flaw.

Chipping. For doing the above to the hardware instead of the software – can be a circuitry in a chip.

Enemies of Internet Freedom

America's Network on 3 May 2006, has argued that Asian governments are worst enemies of Internet freedom. They censor web sites and jail people who express odd views online. China, Vietnam and Nepal are feeling more threatened by cyberspace than ever as internet use booms and people seek information. Of the 15 'Enemies of the Internet' named by Paris-based right group, seven are in Asia. These include China, North Korea, Vietnam and Myanmar. Because of this attitude, Asian societies are at risk of seeing more corruption and abuse of government power. Public discontent would also grow, leading to social instability. Politically backward countries are afraid of the Internet; they fear this will spread ideas of freedom and democracy.

The report has emphasised that using sophisticated filtering technology, forcing Internet cafès to register users and service providers to reveal user information, the governments were trying to control modernisation.

Google.com blocked in China was a headline in the *Times of India* of 8 June 2006. Similarly, "authorities shut down Chinese search engines" was a headline in *Telecom Asia* of 21 June 2006. Of course, the censored Chinese-language version, google.cn was still available. Launched in January 2006 amid controversy because Google agreed to censor its service according to the wishes of China's propaganda chief. Chinese blocking was being gradually extended to Google News and Google Mail. Search engines at Sina.com and Sohu.com have been shut down since 19 June 2006.

Cyber Security Measures

Real hard core cyber security work is essential – Firewall is not at all a sufficient measurę. We should not demonstrate any false sense of security. Knowledge of Internet Browser and some surfing does not make one expert in e-governance - nor is a password a real security measure. Most employees are expected to create, use and manage information - but a common mistake is to rely on IT departments instead of building information literacy throughout the organisation. Many organisations are relying on IT departments to manage security and to protect information, particularly sensitive and proprietary data.

It is essential to quickly move away from Newbies (who are beginners and use downloaded tools for capturing passwords sniffed from unsecured channels and cracking a few locks) and Script Kiddies (who are endowed with basic programming skills and use these to customise the downloaded tools) to Coders (who have advanced programming skills and write codes that are used on the Internet) and onward to Professionals and Spooks (who possess advanced skills and are capable of functioning as real Cyber Warriors).

It is true that for most, enterprises security and cyber security are not part of core competencies. Also good security staff are difficult to find and hard to keep. Therefore, it has become essential to outsource protection. Common services that can be outsourced include straightforward offerings such as managed email and virus protection. More complex arrangements include risk management and managed Public Key Infrastructure (PKI).

Recently, the concept of Managed Security Service Provider (MSSP) has emerged. According to the US-based Computer Emergency Response Team (CERT) Coordination Center, MSSP is a recommended option for network boundary protection, including management of firewalls, intrusion detection, security monitoring, risk and vulnerability assessments and penetration testing; incident management, including emergency response and forensic analysis; anti-virus and content filtering and on-site consulting; and data archiving and restoration.

The then Principal Scientific Adviser, Dr APJ Abdul Kalam took initiative to organise the Society for Electronic Transactions and Security (SETS), wh'ch was registered on 22 May 2002. The objective of SETS is to develop technologies and products for protection, surveillance and monitoring and certification in the area of Information Security, to tender advice to the Government on policy formulation and act as a buffer between sensitive user agencies and corporate houses for developing security solutions, to provide consultancy services to governments, banks and other public and private sector institutions to safeguard the information and knowledge generation resources of the country.

Electronic Warfare and Cyber Security

Cyber security, information warfare and electronic warfare are very closely related – all have the three basic constituents: Monitoring, Defensive and Offensive Operations.

ESM (Electronic Support Measures) includes interception, decryption, direction finding, fingerprinting – if the text can not be decoded, even data such as time, regularity, location of source of communication is important.

ECM (Electronic Counter Measures) includes jammers – CW, Impulse, broadband, chirp – to disrupt or deny – create nuisance and force adversaries to use alternative and expensive means.

ECCM (Electronic Counter Counter Measures) takes care of adversary's attempts to jam us – may use frequency hopping, spread spectrum, decoys, etc.

Indian Computer Emergency Response Team (CERT-In)

CERT-In is managed by the Department of Information Technology (DIT) Ministry of Communications and Information Technology. It is likely to become the nation's most trusted referral agency for responding to computer security incidents as and when they occur. It will also assist in implementing proactive measures to reduce the risks of computer security incidents and shall enhance the security of India's communications and information infrastructure through proactive action and effective collaboration. CERT-In has also performed statistical analysis of defaced Indian websites (country code top level domains - ccTLDs.in) and found 667 defacements during 1998-2004 in 6430 registered domains (1998-1, 1999-4, 2000-75, 2001-219, 2002-121, 2003-131, 2004-116).

Army also launched a 'Computer Emergency Response Team' (CERT) website on 14 October 2005 to improve on cyber security and to act as a nodal agency to address Army's cyber security concerns and to protect Army's 'Information Assets'. On 24 February 2006, President Dr APJ Abdul Kalam, while inaugurating and dedicating Army Wide Area Network (AWAN) covering 174 signal centres for messaging services, directory services along with Voice Over Internet Protocol (VoIP), etc. suggested that it may encompass the entire defence services and the inter-linkages with other Departments of the Government of India, particularly those dealing with national security matters and related decision making process. He emphasised the importance of management of internal threats and creation of on-line information content: resources, imageries, previous war experiences, war gaming models, maps, terrain information, support infrastructure, policy documents, decision trees, protocols and databases.

Control of Internet

Like the US control of the GPS, people are worried about Control of Internet. On 10 October 2005, a meeting was held in Geneva in preparation for the World Summit on the Information Society, in Tunis. Many countries of the world have lined up against the US retaining control over the management of internet, which is currently the responsibility of ICANN (Internet Corporation for Assigned Names and Numbers) under the authority of the US Department of Commerce. EU and UN sponsored WGIG (Working Group on Internet Governance) have recommended governance by International Telecommunication Union (ITU).

Concluding Remarks

The telecommunication revolution brought in the concept of 'death of the distance'. Earlier, satellite broadcasting introduced a similar phrase 'global village', now cyber-space has created the 'universal desktop'. The entire world is at our finger tips, we have to just stretch our hand to click and open windows to the entire universe. While the potential and opportunities are endless, risks have increased. We are under continuous attack, from viruses and worms, from cyber criminals and cyber missiles and we may find ourselves in the open, defenceless.

Data traffic will soon exceed voice traffic, so much so that voice and data would merge to such an extent that independent reference to voice as a communication mode may not be relevant. This will make secure communications more difficult to realise. Also, Internet, with ever increasing reach and decreasing cost, may become the only surviving medium of communications in the future. It is no longer a question of whether Voice Over Internet Protocol (VoIP) will wipe out traditional telephony, but a question of how quickly it will do so.

Digital divide and brain drains are creations of negative minds. Our objective should be to build digital bridges or digital highways and create brain gains. ITU's Digital Access Index – measuring the availability of advanced telecommunication and computing technologies – places South Korea, Taiwan and Hong Kong in the top ten ahead of Canada, the US and the UK. Four of the top ten broadband economies are in Asia – in South Korea 79 per cent of households are connected; Hong Kong 74 per cent, Taiwan 60 per cent and Singapore 59 per cent. India lags behind with just one per cent households connected. The silver lining is that the internationalisation of International Telecommunication Union (ICT) has made English less of an advantage, unlike in the past.

Software in local language and mother tongue may soon start giving significant advantage and extra competence, which we should exploit. That is the only way we can involve a large part of our population to solve cyber-space security problems and survive in the race to save ourselves. Unfortunately, there is no 100 per cent guarantee that even with the best precautions some of the bad things won't happen, but there are steps one can take to minimise the chances of harmful intrusions and their damage potentials. For survival, there is no alternative to quick and specific protective and proactive actions, at individual and national levels.

References

1. Ved Prakash Sandlas, "Defence Space Options", *Journal of United Service Institution of India,* Vol. CXXXV, No.561, (July-September 2005).

2. 'The National Strategy to Secure Cyberspace', the White House, Washington, USA, February 2003.

3. Ahmad Kamal, 'The Law of Cyber Space', United Nations Institute of Training and Research, October 2005.

4. 'The Information Technology Act, 2000', *The Gazette of India,* 9 June 2000.

5. "World Broadband Statistics: Q4 2005", *Point Topics* (March 2006).

6. 'Fundamental Principles of Network Security', Christopher Leidigh, American Power Conversion (APC), 2005.

7. 'Analysis of Defaced Indian Websites under in', S Chakrabarty and B Saha, Department of Information Technology, Government of India, 2004.

8. www.presidentofindia.nic.in, address at the inauguration of the AWAN, Vigyan Bhawan, New Delhi, 24 February 2006.

9. www.cert-in.org.in

10. www.us-cert.gov

11. www.telecomasia.net

12. www.americasnetwork.com