Challenges and Prospects of Cyber Security in the Indian Context*

Lieutenant General Nitin Kumar Kohli, AVSM, VSM@

Introduction

The World Telecommunications Day is celebrated on 17 May. India is marching towards Digital India. Approximately 278 million people out of a population of 1.2 billion are connected on the internet.1 Out of six lakh villages, mobile connectivity has been provided to 5.5 lakh villages, only 50,000 villages are left. Government's endeavour is to connect all citizens of the Country through digital means. If this dream has to be realised, we need policies, techniques and procedures which address the issues of 'Cyber Risk and Security' to guarantee success to these concepts.

Indian Cyberspace is under constant threat. Just to highlight the gravity of the situation, according to data from the Computer Emergency Response Team – India (CERT-IN), the cyber espionage incidents have gone up from 23 reported incidents in 2004 to a mammoth figure of 62,189 in 2014.2 Given the number of critical systems reachable via the Internet coupled with the growing technological advancement of other countries and our heavy reliance on imported hardware and software, 'It's a question of when, not if.'

Shifting Trends

From worms and viruses to Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APTs), in the past quarter of a century the sophistication, impact and scale of cyber-attacks have evolved significantly. Technologically advanced nations have been developing ways to use information as a weapon and target financial markets, government computer systems and utilities. Some of the global prominent attacks are Stuxnet, Flame, Dark Seoul and Sony Pictures Entertainment Hack. These attacks were carried out using espionage and a combination of backdoors, Trojans and worms, and were state sponsored.

Although, the bigger attacks are reported, less noticed is growing cottage industry of ordinary people hiring hackers for much smaller acts of espionage. Websites like "Hacker's List" seeks to match hackers with people looking to gain access to competitor's e-mail accounts, databases etc.3

Our Neighbours

China. It has been estimated that 90 per cent APTs are traced to China. China has been accused of cyber attacks not only on the US or India, but also across many nations of the world. China now has both the intent and capability to launch cyber attacks 'anywhere in the world at any time'. China has mounted almost daily attacks on Indian computer networks of both government and private sector, showing its intent and capability4. The Chinese are constantly scanning and mapping India's official networks. This is China's way of gaining 'an asymmetrical advantage' over a potential adversary.

Pakistan. China has found an ally in Pakistan whom it can use as a launch pad to inflict cyber attacks on India. On 26 Jan 2014, Pakistani hackers defaced 2118 Indian websites.5 Pakistan may use mass media and internet to disturb the secularly balanced India by triggering religious sentiments of Indians. The Assam riots that triggered a widespread exodus of north eastern students from cities such as Bangalore and the widespread stone pelting incidents in J&K, confirmed the subversive games Pakistan plays through social networks.

Indian Preparedness

India has issued Cyber Security Policy and legal framework to secure its Cyberspace as elaborated in the succeeding paragraphs.

National Cyber Security Policy 2013

The objective of National Cyber Security Policy (NCSP) 20136 in broad terms is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A National and sectoral 24X7 mechanism has been envisaged to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). CERT-IN has been designated to act as a nodal agency for coordination of crisis management efforts. CERT-IN will also act as umbrella organisation for coordination actions and operationalisation of sectoral CERTs.

The policy calls for effective public and private partnership creating a think tank for cyber security evolution in future. Other important facets of the policy are promotion of research and development in cyber security, development of human resource through education and training programmes and creating a workforce of 500,000 professionals trained in cyber security in the next five years. The policy document aims at encouraging all organisations whether public or private to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cyber security initiatives. The release of the NCSP 2013 is an important step towards securing the cyber space of our Country.

Legal Framework: IT Act 2000 and IT Act (amended) 2008

The highlights are :-7

(a) **Definition of Computer System and Punishment for Cyber Offences.** Provides comprehensive definition of computer systems and ascertains liability on various types of crimes.

(b) **E-Governance and E-Transactions**. Provides legislation for E- governance & E-transactions.

(c) **Authority to Government.** Authorises government for interception, monitoring and blocking of websites.

(d) **Protected Systems.** Under the Act, critical systems can be declared as 'protected systems' and security breaches of such systems attract imprisonment.

(e) **Appellate Tribunals.** Cyber Appellate Tribunal, which is now operational, is expected to expedite legal proceeding of cyber crime cases.

Challenges of Cyber Security in India

Lack of Comprehensive Policy

The NCSP was issued in 2013 but has been proceeding in fits and starts. Some of the shortcomings are as given below:-

(a) **Need for a National Security Policy.** The National Security Council (NSC) has not published any official document outlining the National Security Policy (NSP). Since NCSP was not a subset of any NSP, it was relegated to the status of an isolated departmental document of the Ministry of Communication and Information Technology (MoC&IT) rather than desirable national level policy. The policy does not give any road map, timelines and funding for its implementation.

(b) **Insufficient Private Sector Input,** Including Public-Private Partnerships (PPPs). During the formulation of NCSP minimal effort was made to obtain input and expertise from other sectors. Although it engaged with industry groups such as the Federation of Indian Chambers of Commerce and Industry, the process was half-hearted at best. This excludes an entire pool of talent that is available from India's many start-up firms, as well as individuals.

(c) **Exclusion of Armed Forces.** Unlike the policies of cyber mature nations that recognise cyber security to lie at the broad intersection of both military and commercial networks, the NCSP is largely ambiguous about the role, interplay and interdependence of these two distinct aspects of national cyber security.

(d) **International Cooperation and Advocacy.** The policy fails to mention the leadership role India should be playing in a variety of areas in cyber security, including development of international security standards, testing of ICT products, cyber security norms and conventions, solutions to the issues of Internet governance, among many others.

Organisational Shortcomings

There are around six apex bodies, five ministries and almost thirty agencies that make up the cyber organisation.8

It requires serious introspection to make the entire structure conducive to effective command and control. It is recommended that GoI reconfigures apex bodies to create a single empowered authority to resolve the predicament of multiplicity at the top level.

Lack of Internationally Accepted Policies and Laws

The biggest hurdle before curbing cyber threats at the international level is lack of harmonisation at international level. Till now we have no 'Internationally Acceptable Definition' of cyber warfare. Further, we have no universally acceptable cyber crimes treaty as well.

IT Act 2000 and 2008

The provisions of IT Act are mostly bailable and there has been very low rate of convictions.9 It will not be wrong to say that it is effective in metropolitan cities like Mumbai, Delhi, Hyderabad, Bhopal, Bangalore, etc, but it is feeble in tier-two cities as awareness of the law by enforcement agencies remains a big challenge. This needs to be suitably addressed.

Supply Chain Integrity

Supply chain integrity has become paramount with the needle of suspicion pointing towards the hardware and software that make up the brains and body of cyberspace. While much of the equipment used in global networks is supplied by China, the storage and data storage networks are largely of the US companies. The dominance of Chinese companies like Huawei and ZTE with reportedly close links with the Chinese military is a matter of concern.10 In addition to the widely reported issues with hidden backdoors and kill switches, it is also a fact that network equipment providers get access to sensitive information in the course of providing after sales support.11

International Cooperation

The MoUs signed by India have been lopsided in favour of other nations. The Indo-US Strategic Dialogue held in June 2013 renewed focus on cyber security with the establishment of a Strategic Cyber Policy Dialogue of cyber experts. While the macro issues important to the US are being addressed through these dialogues, they do not seem to provide scope for addressing issues important to India such as evolving the necessary mechanisms for rapid information sharing in the law enforcement process.12

Non Adherence to International Best Practices: ISO 27001

ISO 27001 certification is suitable for any organisation, large or small and in any sector for protection of critical information, such as in the banking, financial, health, public and IT sectors. All critical sector organisations under

Central Government ministries/departments are mandated to implement information security best practices as per ISO 27001. However, there are only 546 organisations in the country which have obtained the certification. What is more intriguing is that the Department of Electronics and Information Technology (DeitY) has not made any effort to ascertain as to why all the Government organisations have failed to obtain ISO 27001 certification.13

Large User Base with Few Experts. With a population of around 1.21 billion, India has so far only 65,000 trained personnel pertaining to cyber security as against the estimated requirement of 5 lakh trained personnel. In addition, there are only 97 Master trainers and 44 empanelled auditors by CERT-IN in the country.14

Pirated Software. According to the Global Software Piracy Study done by an independent firm, Business Software Alliance (BSA), about 60 per cent of Indians used pirated software. Only 33 per cent of companies in India have written policies in place requiring use of properly licensed software. This increases the chance of encountering malware.

Data Traffic Transit through Foreign Countries. Much of the data traffic that traverses through cyberspace touches the US networks at some point, or is carried over these networks. Also, majority of the websites of commercial, NGOs, individuals and private organisations are hosted outside India and thus the data is always vulnerable.15

Lack of Strong Security Culture. India lacks a strong security culture. A country's security culture should permeate all those who are actively engaged in security-related sectors. This is especially important in the cyber security domain, where every individual has the potential to be both a defender and a victim.

Cyber Balance Sheet of Cyber Mature Nations

The USA

Till late nineties, the US suffered from various shortcomings like inadequacy of national policy, multiple organisations, wasteful funding and ineffective regulations to penalise the perpetrators.

Policy Framework. The National Security Strategy (NSS) released in May 2010 called for integration of various agencies.16 As per the guidelines in NSS the Department of Defence (DoD) coined its cyber concerns in the National Defence Strategy (NDS) and the Quadrennial Defense Review (QDR).17 Further, these strategic documents were used by the Joint Staff to formulate the National Military Strategy (NMS). Now, DoD has cyber policies at strategic, operational and tactical levels.

Integration of Organisations. The responsibility of cyber security was spread across the Department of Homeland Security (DHS), DoD and Department of Justice (DoJ), which worked in independent silos and failed to prevent cyber attacks against the US. In 2008 National Cyber Investigative Joint Task Force (NCIJTF) was formed and drove the US towards unity of command.

US CYBERCOM

In the year 2006, Pentagon reported an all time high 360 million attempts, including hacking into the US $300 billion Joint Strike Fighter project.18 The Pentagon spent nearly 14 months in 2008 cleaning the worm 'agent.btz' which originated from a DoD facility in the Middle East. Under these circumstances, the US formed the United States Cyber Command (USCYBERCOM) on 23 June 2009 under the US Strategic Command (USSTRATCOM).19 A four star general wears a dual hat of Director, National Security Agency and Commander, USCYBERCOM. The Command is charged with putting together existing cyberspace resources, creating synergy and synchronising war-fighting effects to defend the information security environment.

Other Cyber Programmes of the USA

Various programmes are run by the NSA with near impunity due to provisions and authorisations under Foreign Intelligence Surveillance Act (FISA). Some of the NSA's programmes are directly aided by national and foreign intelligence agencies as well as by large private telecommunications and internet corporations such as Verizon, Telstra, Google, Microsoft and Facebook.

The cyber security firm Kaspersky Laboratory has disclosed in Feb 2015 that a US cyber espionage group called the 'Equation Group' embedded surveillance tools on the hard drives produced by a number of well known manufacturers like Western Digital, Seagate, Hitachi and Toshiba. It was almost impossible to get rid of the malware, even after disk reformatting and re-installing the computer system.

The US DoD has declared its Cyber Strategy in Apr 2015.20 This new strategy sets prioritised strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focusses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans. The strategic goals listed are as follows:-

(a) Build and maintain ready forces and capabilities to conduct cyberspace operations.

(b) Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions.

(c) Be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence.

(d) Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages.

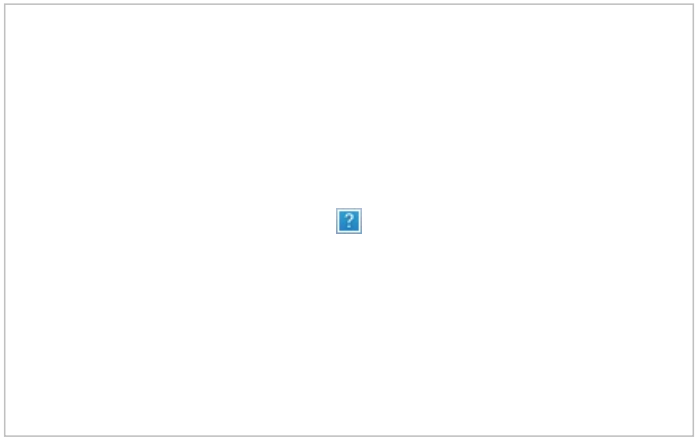
(e) Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

China

The Chinese People's Liberation Army (PLA) is actively developing a capability for computer network operations (CNO) and is creating the strategic guidance, tools and trained personnel necessary to employ it in support of traditional war fighting disciplines. The Chinese have adopted a formal IW strategy called 'Integrated Network Electronic Warfare' (INEW) that consolidates the offensive mission for both computer network attack (CNA) and Electronic Warfare.

Organisations and Capabilities of PLA

Chinese efforts to dominate the information space are driven primarily by three goals – exercise control over their populace, dominate adversaries by dominating the information space and finally overcome the technological gap with the West through strategic intelligence acquisition in the cyber domain. The assessed Cyber structure of China is illustrated in the succeeding paragraphs.21



Cyber Organisation of PLA

Third Department. It is tasked with the foreign signals collection, exploitation and analysis as also communications security for the PLA's voice and data networks. The GSD Third department directly oversees following entities : -

(a) **Operational Bureaus.** There are twelve operational bureaus and every operational bureau has a specific mission such as radio or satellite communications interception, cryptology, translation, information assurance, intelligence analysis, cyber operations which include exploitation, defence and attack. The second, seventh and eighth bureaus are likely to be involved in Cyber operations.

(b) **Technical Reconnaissance Bureaus**. The PLA maintains at least six technical reconnaissance bureaus (TRB) that are responsible for SIGINT collection against tactical and strategic targets and have apparent CNO duties focussed on defence or exploitation of foreign networks.

(c) **Research Institutes.** Science and Technology Intelligence Bureau and, Science and Technology Equipment Bureau oversee three Research Institutes namely 56th Research Institute, 57th Research Institute and 58th Research Institute which focus on codes and passwords, development of communication intercepts and signal processing systems, cryptology and information security technology.

PLA Information Security Base. On 19 July 2010, the PLA is said to have established the "Information Security Base" headquartered under the PLA General Staff Department to serve as the PLA's Cyber Command. The base is likely to consolidate key tasks of China's computer network operations and information warfare.

PLA Information Warfare Militia Units. From about 2002 onwards, the PLA has been creating IW militia units comprising personnel from the commercial IT sector and academia, and represents an operational nexus between PLA CNO operations and Chinese civilian information security professionals.

Hacker-State Collaboration. The Chinese government demonstrates willingness to leverage the power of hacker communities by direct collaboration between state and hackers so that the CNO is coordinated and mission oriented with the ability to deny state involvement. Xfocus is one of the many such hacker groups which has transformed into a commercial information security company. "Red Hackers" or "Hongkes" are Chinese citizens, often motivated by patriotism or financial gains, who act as modern-day privateers attacking foreign targets.

Cyber Security Measures. Chinese authorities have instituted 'The Great Firewall' to regulate the internet in mainland China. Also, China has shifted to indigenous operating system based on Unix called Kylin. It also employs indigenously developed search engines and social networking websites. Some of these are given below: -

	Popular websites	**Chinese Equivalent**	**Type of Application**
(a)	Twitter	SinaWeibo	Mass Messaging

(b)	Facebook	Renren, Pengyou	Social Networking
(c)	Google Talk	QQ	Instant Messaging
(d)	MySpace	Douban, Diandian	Forum/Blog
(e)	Youtube	Youku	Video Sharing
(f)	Whatsapp	Wechat	Mobile Voice and Text App
(g)	Foursquare	Jiepang	Location-based Social Networking App

Recommendations

Formulation of National Security Policy. India should formulate an all-encompassing National Security Policy (NSP) and the National Cyber Security Policy should be a subset of this policy. Thereafter, National Cyber Doctrine and Cyber Security Strategy can be formulated by respective ministries. This would introduce tier-based 'policy-doctrine-strategy' formulation and ensure 'whole-of-nation' approach in cyber security. The policy should give the road map, timelines and funding for its implementation.

Reconfigure Apex Organisation. The apex bodies should be reconfigured to create a single empowered authority to resolve the predicament of multiplicity at the top level. It is proposed that an exclusive 'Cyber Security Center (CSC)' be formed under the NSC, which would be singularly responsible for policy formulation, budget allocation and nationwide implementation

Cyber Crimes and Cyber Terrorism. MHA should be the nodal agency for handling cyber terrorism. To handle cyber terrorism and cyber crime, a slew of measures will be needed, ranging from monitoring and surveillance, investigation, prosecution etc. The National Counter Terrorism Centre being set up should have a strong cyber component.

Cyber Warfare. There is a need to create a Directorate or Special Wing in the NSCS for this. It would oversee and coordinate both defensive and offensive cyber operations. Other aspects of Cyber Warfare to be looked into are:-

(a) **Raising of Cyber Command**. While cyber warfare is an ongoing activity during peace time there is a dire need to develop this capability for a warlike situation. Cyber warfare in a manner is Network Centric Warfare and will form an essential part of preparation of the battlefield in any future conflict. This will comprise not only the three Services but personnel from the DRDO and scientific and technological community.

(b) **Reserve of Young IT Professionals for Cyber Warfare.** There is a need to create and maintain a "surge capacity" for crisis or warlike situation. Young IT professionals constitute a vast resource base and a large number would be willing to loyally serve the nation when required. This resource must be capitalised by raising of cyber warfare reservists which could be embodied, when required.

Capacity Building. Some of the measures are :-

(a) There is need to place special emphasis on building adequate technical capabilities in cryptology, testing for malware in embedded systems, operating systems, fabrication of specialised chips for defence and intelligence functions, search engines, artificial intelligence, routers, etc. In the interim, all software and hardware manufactured by foreign Original Equipment Manufacturers (OEMs) needs to be tested for any security loopholes.

(b) Developing mobile software platforms including operating systems, anti viruses, root kits, malware, viruses, Trojans and other cyber weapons etc.

Public Private Partnership. Close cooperation between the Government and the Private Sector is necessary because much of the infrastructure and networks are in private hands. A joint working group was established in July 2012 with representatives from various ministries of the GoI and the Private Sector but it suffers from many problems like, the lack of a comprehensive road map with timelines and funding.

International Cyber laws. Adopting a proactive approach in the United Nations, including lobbying with like-minded nations in ensuring all encompassing international cyber laws and treaties are promulgated.

Human Resource Development. There is a need to introduce new courses, curriculum and academic institutions in the field of cyber security, ethical hacking, cryptology etc. to boost human resource in the field of cyber warfare.

Synergy and Coordination. There is a need for coordination, planning, understanding and synergy of efforts amongst all civil, military, intelligence, law enforcement and educational organisations responsible for cyber security, information assurance, cyber warfare and perception management.

Research and Development. There is a need to focus on :-22

(a) Functioning and Software design of social networks to ensure 'security and privacy', and emphasis on 'malware detection'.

(b) Develop reliable technology for protection of personal data in third party domain namely; social networks, cloud providers, outsourcing during various phases of its lifecycle; transmission, processing or storage.

(c) Develop mechanisms for ensuring digital rights and protecting privacy with assured empowerment of user to manage their data and avoid anonymous usage.

Conclusion

The exponential growth of cyberspace is possibly the greatest development of the current Century. Cyberspace being the fifth common space, it is imperative that there be coordination, cooperation and uniformity among all agencies to safeguard it. There is no quick fix solution that can secure our cyber space. The solutions are sprinkled in strong policy and law enforcement, real-time information sharing, embracing technology and sensitising our cyber space users on cyber hygiene.

Endnotes

1 'Internet in India 2014', jointly published by the Internet and Mobile Association of India (IAMAI) and IMRB International,

2 Facts revealed in a written reply to the Lok Sabha by Communications and IT Minister Ravishankar Prasad, on 03 Jul 14, 2014,

3 www.hackerslist.com accessed on 18 May 2015

4 www.techcrunch.com/fireeye-apt-30-southeastasia-india-report.html, Accessed on 18 May 2015

5 ''Cyber Warfare: Pakistani Hackers Claim defacing over 2000 Indian Websites", Tribune, 02 Feb 2014.

6 Notification on National Cyber Security Policy 2013 by MoC&IT on 02 Jul 2013.

7 Extraordinary Gazette of India, Part II-section 1, No. 27 New Delhi, Friday, 09Jun 2013

8 Article by Sanjay Chhabra on 'India's National Cyber Security Policy and Organisation- Critical Assessment' in Naval War College journal

9 Op. Cit 7.

10 "Huawei spies for China, claims Ex-CIA Chief", Times of India, 19 Jul 2013.

11 http://www.idsa.in/monograph/Cybersecurity_csamuel.html accessed on 20 May 2015.

12 Ibid.

13 The "Fifty Second Report on Cyber Crime, Cyber Security, and Right to Privacy" issued by the 2013-2014 Parliamentary Standing Committee on Information Technology on 12 Feb 2014.

14 Ibid.

15 Op. Cit. 11.

16 C Henderson, 'The 2010 United States National Security Strategy and the Obama Doctrine of Necessary Force'.

17 United States Department of Defence, 'Quadrennial Defense Review -2014'.

18 Randy James (Time, US, 01 Jun 09) 'A Brief History of Cybercrime'.

19 US Def Sec Robert Gates memorandum (23 Jun 2003) 'Establishment of subordinate unified US Cyber Command under Strategic Command for Military Cyberspace Operations'.

20 US DoD Cyber Doctrine released on April 2015.

21 'The PLA as an Organisation' Volume v1.0 by Rand Publications 2002

22 'Cyber Security: Issues and Challenges", Article published in CSI Communications May 2015 by NJ Rao

*Text of the talk delivered at USI on 20 May 2015 with Lieutenant General Davinder Kumar, PVSM, VSM (Retd) in Chair.

@ Lieutenant General Nitin Kumar Kohli, AVSM, VSM was commissioned into the Corps of Signals on 17 Dec 1977. He commanded a Strike Corps Signal Regiment in the Western theatre, has been the Chief Signal Officer of a Corps and a Command; and was the Director General Manpower Planning at the Army HQ, prior to assuming the appointment of Signal Officer-in-Chief of the Indian Army on 01 Sep 2013.