Vivekananda International Foundation

Cyber Security in India

Present Status

Maj Gen P K Mallick, VSM (Retd)

Issue Brief – October 2017

About the Author

Maj Gen PK Mallick, VSM (Retd) is a graduate of Defence Services Staff College and M. Tech from IIT, Kharagpur. He has wide experience in command, staff and instructional appointments in the Indian Army. He has been the Chief Signal Officers of a Command and a Senior Directing Staff (SDS) at the National Defence College, New Delhi.

Introduction

The Information Technology (IT) Act in India was promulgated as early as 2000. The Indian Computer Emergency Response Team (CERT-In) was established in 2004 and continues to act. India has undertaken several steps at protection, detection and containment of these potentially disruptive attacks against the nation's networks. Government initiatives such as 'Digital India' and 'Smart City', and the increasing involvement of the private sector in nation-building endeavours are progressive steps that are also increasing the scope and complexities of cyber security efforts. It is time to review the Indian Cyber Security scene in the present context.

National Cyber Security Policy

Government of India published The National Cyber Security Policy on 02 July 2013. The salient aspects of the Policy are:-

- Creating a secure cyber ecosystem.
- Creating an assurance framework.
- Encouraging Open Standards.
- Strengthening the Regulatory framework.
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats.
- Securing E-Governance services.
- Protection and resilience of Critical Information Infrastructure.
- Promotion of Research & Development in cyber security.
- Reducing supply chain risks.
- Human Resource Development.
- Creating Cyber Security Awareness.
- Developing effective Public Private Partnerships.
- Information sharing and cooperation.
- Prioritized approach for implementation.

The National Cyber Security Policy, however lacked the following key elements:-

- Milestones and performance measures.
- Cost and resources.
- Roles and responsibilities.
- Linkage with other key strategy documents.

It is time therefore now to review the National Cyber Security Policy.

USA Model

The Government of India has been studying the model of United States of America (USA) on cyber security, and has tried to adopt some of their organisations and policies. It will be worthwhile to see how the USA has organised its cyber security and the models that have been adapted.

The Department of Homeland Security is responsible for protecting nation's critical infrastructure from physical and cyber threats. Cyberspace has united once distinct information structures, including business and government operations, emergency preparedness communications and critical digital, and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of nation's critical infrastructure and key resources to economic and national security.

National Cybersecurity and Communications Integration Center (NCCIC)

The National Cybersecurity and Communications Integration Center (NCCIC), within the Office of Cybersecurity and Communications, serves as a centralised location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local and territorial governments; private sector and international entities. Its activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation and recovery actions.

NCCIC Mission

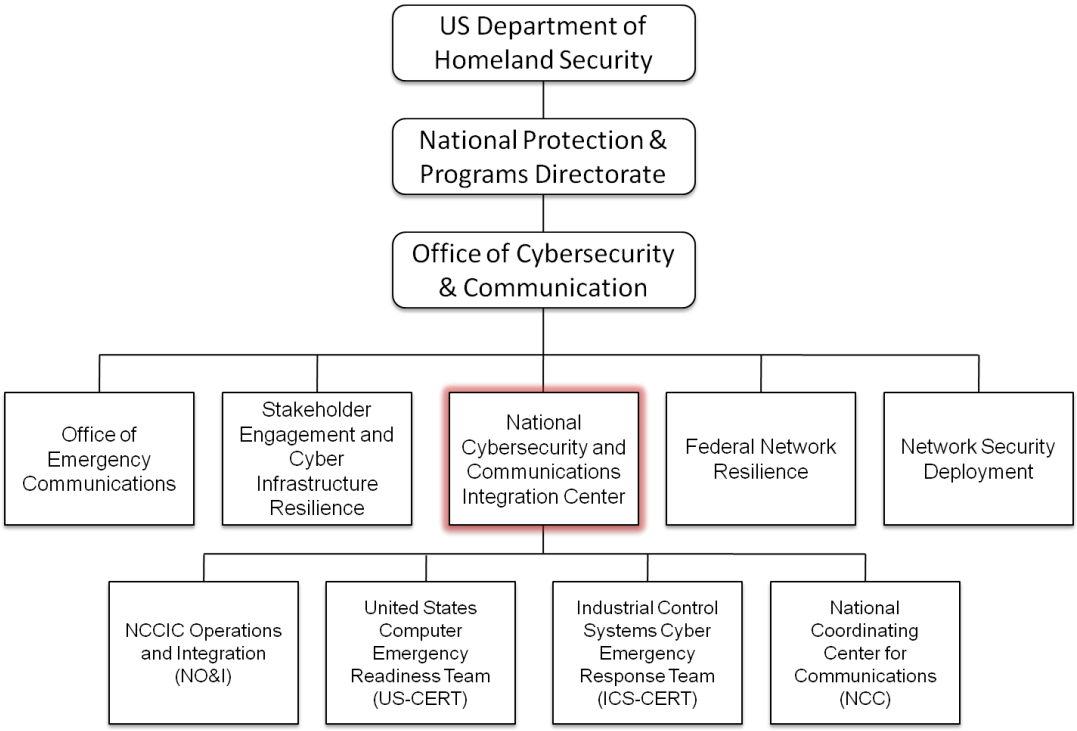
Major tasks before the NCCIC are to operate at the intersection of the private sector, civilian, law enforcement, intelligence and defense communities; to apply unique analytic perspectives; to ensure shared situational awareness; and to orchestrate synchronised response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

The NCCIC's missions include:-

- Leading the protection of federal civilian agencies in cyberspace.
- Working closely together with critical infrastructure owners and operators to reduce risk.
- Collaborating with state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Cooperating with international partners to share information and respond to incidents.
- Coordinating national response to significant cyber incidents in accordance with the National Cyber Incident Response Plan (NCIRP).
- Analysing data to develop and share actionable mitigation recommendations.
- Creating and maintaining shared situational awareness among its partners and constituents.
- Orchestrating national protection, prevention, mitigation and recovery activities associated with significant cyber and communication incidents.
- Disseminating cyber threat and vulnerability analysis information.
- Assisting in the initiation, coordination, restoration and reconstitution of National Security or Emergency Preparedness (NS/EP) telecommunications services and facilities under all conditions, crises, or emergencies, including

executing Emergency Support Function 2- Communications (ESF-2) responsibilities under the National Response Framework (NRF).

Overall cyber security organisation of the USA may be summarised in the following diagram:-



USA Cybersecurity Organisation

Jurisdiction Issues

There is a conflict of interest as to who is overall responsible for cyber security in most countries. In the USA the Department of Defense (DoD) is responsible for cyber attacks originating abroad and for protecting DoD networks, while Department of Homeland Security (DHS) is responsible for coordinating protection of domestic civilian infrastructure. However, many cyber attacks originate from abroad and have the potential to disrupt critical infrastructure. Responding to cyber attacks is a difficult task for DHS because it operates without the requisite authority that would allow it to dismantle a foreign actor's network operations. In addition to these legal complications, DHS lacks the same degree of cyber operations competency as the DoD.

Information sharing between government and the industry has always been a key component of strengthening a country's resilience to hacking campaigns by foreign governments, criminals and hacktivists and non-state actors. However, while the industry is responsible for sharing instances of breaches, there are proprietary, privacy and reputational considerations that can inhibit their willingness to do so freely. There are also major inhibitions to the free flow of information from government to industry – most notably the risk of compromising intelligence sources and methods.

The presence of government bodies, such as DHS, that insulate intelligence agencies from industry is notable. Adding layers of bureaucracy to public private collaboration in cybersecurity decreases the timeliness of the information shared. James Clapper, the

former Director of National Intelligence of USA argues, "The DHS is the appropriate storefront and that's the way it ought to be. I don't think the spy crowd should be directly engaging with the private sector."

Yet this is precisely what the United Kingdom (UK) is seeking to do with its new National Cyber Security Centre (NCSC), which is revamping the way British intelligence agencies collaborate with private industry by leaning toward more open and direct exchanges to help secure the UK against cyber attacks. Chris Inglis, the former Deputy Director of the National Security Agency, argues that the UK has proposed to "radically transform collaboration between intelligence agencies and the private sector." Practically, this has meant bringing in some 650 people from the Government Communications Headquarters (GCHQ), the UK's primary signals intelligence agency and having them work directly alongside industry partners.

The national division of responsibilities for cybersecurity in the USA are as follows:

- The Justice Department would, among other things, "Investigate, attribute, disrupt and prosecute cyber crimes; lead domestic national security operations and conduct domestic collection, analysis and dissemination of cyber threat intelligence;"
- Department of Homeland Security (DHS) would, among other things "coordinate the national protection, prevention, mitigation of and recovery from cyber incidents; disseminate domestic cyber threat and vulnerability analysis and protect critical infrastructure;"
- DoD would "defend the nation from attack; gather foreign threat intelligence and determine attribution and secure national security and military systems."

Critical Infrastructure Protection

Critical Infrastructure is defined by DHS as, "sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof". The 16 sectors designated as critical infrastructure in USA include; Chemical, Communications, Dams, Emergency Services, Financial Services, Government Facilities, Information Technology, Transportation Systems, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Food and Agriculture, Healthcare and Public Health, Nuclear and Water Systems.

As for the identity of the regulator in the cyber field, two options exist. The first is to establish regulation by sector, with the regulator from the relevant sectors. For example, regulation in the field of cyber defense of the health system will be determined by the Ministry of Health; regulation of water corporations will be determined by the Ministry of Infrastructure; and so forth. The other option is regulation through a central regulator. USA has followed sector specific regulator. PPD-21 assigns a federal agency, known as a Sector-Specific Agency (SSA), to lead a collaborative process for critical infrastructure security within each of the 16 critical infrastructure sectors. Each Sector-Specific Agency is responsible for developing and implementing a sector-specific plan

(SSP), which details the application of the National Infrastructure Protection Plan (NIPP) concepts to the unique characteristics and conditions of their sector. Sector-Specific Plans have been updated to align with the NIPP 2013 [https://www.dhs.gov/national-infrastructure-protection-plan].

The Sector Specific Agency for each critical infrastructure in the USA is given below:-

Chemical Sector	The Department of Homeland Security
Commercial Facilities Sector	The Department of Homeland Security
Communications Sector	The Department of Homeland Security
Critical Manufacturing Sector	The Department of Homeland Security
Dams Sector	The Department of Homeland Security
Defense Industrial Base Sector	The U.S. Department of Defense
Emergency Services Sector	The Department of Homeland Security
Energy Sector	The Department of Energy
Financial Services Sector	The Department of the Treasury
Food and Agriculture Sector	The Department of Agriculture and the Department of Health and Human Services
Government Facilities Sector	The Department of Homeland Security and and the General Services Administration
Healthcare and Public Health Sector	The Department of Health and Human Services
Information Technology Sector	The Department of Homeland Security
Nuclear Reactors, Materials, and Waste Sector	The Department of Homeland Security
Transportation Systems Sector	The Department of Homeland Security and the Department of Transportation
Water and Wastewater Systems Sector	The Environmental Protection Agency

National Institute of Standards and Technology (NIST) is responsible for improving the cyber security of critical infrastructure under Executive Order (EO) 13636. It established the voluntary NIST Framework to help critical infrastructure owners and operators reduce cyber risks. NIST Framework for Improving Critical Infrastructure Cybersecurity, version 1.0, 12 February 2014 gives out a fair idea how this organisation helps in cybersecurity efforts. India does not have any such organisation.

In India, Section 70 of the IT Act 2000, Critical Information Infrastructure (CII) is defined as, "The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety." Under Section 70A(1) of the Information Technology (Amendment) Act 2008, the National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical

Research Organisation (NTRO) is the nodal agency that takes all measures including associated Research and Development for the protection of CIIs in India. NCIIPC was deemed to be created by a gazette notification with specific responsibilities for protecting all CII. While the law was amended in 2008, it would take six years before NCIIPC was formally created through a Government of India gazette notification in January 2014.

The NCIIPC started off with several sectors, but has now truncated them into five broad areas that cover the 'critical sectors'. These are:-

- Power and Energy
- Banking, Financial Institutions and Insurance
- Information and Communication Technology
- Transportation
- E-governance and Strategic Public Enterprises

While defence and intelligence agencies have also been included under the CII framework, these have been kept out of the purview of the NCIIPC's charter. Balance of the sectors are now the responsibility of CERT-In. However, CERT-In does not have any executive authority and is known to issue advisories.

Indian Cyber Space

India has taken several steps in the recent past to strengthen its cyber defence capabilities. In a keynote address, delivered in 18th Asian Security Conference on 10 February 2016, the then Deputy National Security Advisor (NSA) of India, stated that:-

- A National Cyber Security Policy has been announced and is being implemented.
- An elaborate National Cyber Security assurance framework is under implementation.
- The National Cyber Security Coordinator was appointed in 2015.
- Coordination amongst various agencies has improved.
- A National Critical Information Infrastructure Protection Centre (NCIIPC) has been set up. There is a regular dialogue with the key sectors of the economy.
- Public-private partnership is being developed. There is an active dialogue between the government and the private sector.
- A National Cyber Coordination Centre (NCCC) is being set up.
- Efforts are being made to develop cybersecurity skills in the country. New cybersecurity curricula are being introduced in the colleges.
- Cybersecurity Research and Development (R&D) policy has also been under active consideration of the government.
- The Indian Computer Emergency Response Team (CERT-In), an organisation that was set up in 2004, has done significant work in dealing with cyber incidents as well as spreading awareness.
- India is pursuing active cyber diplomacy by setting up cybersecurity dialogues with several countries and is participating in several international fora including the UN on cybersecurity.

Critical Issues to be addressed in the Indian Context

Command and Control Set-up

There should be no ambiguity in responsibility of organisations for cyber security. In USA, National Security Agency and The Cyber Command comes under the DoD. In the UK, GCHQ comes under the Foreign Ministry. In Israel, National Cyber Bureau, directly under the Prime Minister, regulates activity in the Cyber Space. In the Indian context, NTRO has been entrusted with this responsibility which doesn't come under any ministry and operates directly under Prime Minister's Office (PMO). The interplay between Ministry of Defence (MoD), Ministry of Home Affairs (MHA), the Armed Forces, and the intelligence agencies, both internal and external, needs to be clearly demarcated. Who will carry out offensive cyber operations in a conflict scenario, can an intelligence agency do it keeping in mind the rules of engagement or the laws of armed conflict?

National Critical Information Infrastructure

National Critical Information Infrastructure Protection Centre (NCIIPC) was formed under National Technical Research Organisation (NTRO). For some selected critical infrastructures, NCIIPC takes the lead role. For other non critical structures, it is the responsibility of the CERT-In. The National Disaster Management Authority (NDMA), under the MHA, has also the responsibility for protection of cyber critical infrastructure. Though NDMA has done very little on this issue. CERT-In is an advisory body and not an implementation agency. Responsibility and authority for all the sub-sectors of critical information infrastructure should be clearly demarcated and made accountable. Lead agency to formulate National Cyber Security Policy is Ministry of Electronics and Information Technology (MeitY). This ministry does not have control over powerful ministries and departments like MoD, MHA and NTRO. The way our ministries work in the stovepipe systems, the interaction, sharing of information, earmarking of specific roles and assignment of responsibility suffer.

We generally follow the USA model. The appointment of National Cyber Security Coordinator directly under the PMO is seen as a positive development, a lot of good works have been done by the National Cyber Security Coordinator. However, he does not have any executive power since it is not under any Ministry. He is not in the loop for cyber operations undertaken by the intelligence agencies. The staff for National Cyber Security Coordinator is meager for a country as huge and diverse as India. Today the post of National Cyber Security Coordinator in the USA has been abolished as it was found that this post has become an extra constitutional authority and was interfering with the routine functioning of the respective Ministries responsible for the cyber security tasks.

Organisations like NTRO or National Cyber Security Coordinator are happy to function under the PMO, as there is no ministerial or legislative control over their functioning. Nevertheless, the PMO as such has not much of the domain expertise on these niche technology areas. As these organisations are protected from routine interferences, they

have virtual independence. In a way it is good that they can get things done at a faster pace. But there is always a danger of getting overboard and taking unnecessary risks with grave consequences when there is no control over them.

Standards and Protocols

We need to have uniform standards, protocols and norms across the country in the cyber domain. The agencies involved are MeitY, Indian Standards Institute (ISI), Bureau of Indian Standards (BIS) and NCCIPC. Is there a need for a central agency like National Institute of Standards and Technology (NIST) of the USA functioning under the Department of Commerce?

Public Private Partnership (PPP)

Indian IT industry is worth 150 billion dollars. They have some well established cyber security procedures. What is the process of exchanging the best practices with this civil sector and the government sector?

There is a serious mismatch of understanding between the civil sector and the government agency of cyber security. The government agencies feel that the private sector is only interested in grabbing the order, but are not serious enough in developing Indian solutions; they don't put adequate effort in research and development (R&D); and are not willing to invest in the country's cyber security infrastructure. On the other hand, the private industry feels that there is very little understanding of cyber security in the top echelons of the government agencies; procedures are too bureaucratic, rigid, long and time consuming; and the vendors are usually treated shabbily. They feel that since they provide cyber security solutions across the globe they have the expertise. If the government wants then they should approach the private industry and not the other way around. They quote the recent example of US, Secretary of Defence, visiting the Silicon Valley and interacting with the behemoths for providing support to Department of Defence cyber activities. Surely there has to be a middle ground where the sharply divergent views can be met.

The private industry is very sensitive to any cyber breach in their respective organisations. They always do the damage control first and would not like to share the information because of commercial reasons. What can NCCIPC and CERT-In do to develop mutual trust and make sure that this information of compromise is shared immediately so that mitigation action across the sectors can be initiated?

In a scenario where a big Indian IT giant has been compromised and data has been stolen and that affected company is reasonably certain from where the attack has come and carries out a hack back against the party, what should be the role of government agencies? Though the private industry is duty bound to report any breach of cyber security to the government agencies, a very large number of such incidents go unreported. What is the mechanism by which punitive action is taken against the defaulters?

A Joint Working Group with Data Security Council of India (DSCI) and National Security Council Secretariat (NSCS) went into various aspects of cyber security in India. The

salient guiding principles and objectives on the Public Private Partnership (PPP) are as under:-

- Given the diverse stakeholders in cyber security, institutional mechanisms should be set up to promote convergence of efforts both in public and private domains.
- Use existing institutions and organizations to the extent possible in both private sector and government and create new institutions where required to enhance cyber security.
- Set up a permanent mechanism for private public partnership.
- Identify bodies that can play a wider role in funding and implementation in the public and private sector.
- Identify areas where both private and public sector can build capacities for cyber security.
- Put in place appropriate policy and legal frameworks to ensure compliance with cyber security efforts.
- Promote active PPP cooperation in international forums and in formulating India's position on global cyber security policies.
- Establish India as a global hub of development of cyber security products, services and manpower.
- Promote indigenization and work on joint R&D projects to meet the cyber security needs of the country.

Four years have passed. There has hardly been any progress on the PPP model.

Critical Information Infrastructure Protection

Regulatory bodies for each subsector of critical infrastructure must be identified and made responsible and accountable for respective sub-sectors. For example, if a serious breach in a nuclear power plant takes place with a potential to great loss to life and property, who should be made accountable. Introduction of private players in nuclear power sectors will make the issue more complicated. Similarly who is responsible for cyber security of the huge defence industrial base of Defence Public Sector Untertakings (DPSUs) and factories under the Ordnance Factory Board (OFB)? With the recent participation of private industries, the cyber security aspects will take more relevance. Who is responsible for the cyber security of the private players of the defence industry?

Code Breaking

India does not have any credible code breaking capability. Introduction of the 128 or the 256 bits keys have made the issue of code breaking extremely difficult. However, this capability exists in NSA of USA, GCHQ of UK and probably in Russia and China. If we do not have this capability, we must make efforts to develop these capabilities. Academia, industry and expertise from countries like Ukraine, Belarus and such other East European countries and South Africa can be explored.

Delay in Implementation of Projects

After the 26/11 attacks on Mumbai, two very important projects were initiated by the Central Government on first track. Both the projects of National Intelligence Grid (NATGRID) and Central Monitoring System (CMS) have cost and time overruns and are still not complete. NATGRID does not have a linkage to the Armed Forces.

The National Cyber Security Centre (NCSC), is an organisation of the UK Government that provides advice and support for the public and private sector in how to avoid computer security threats. It became operational in October 2016, exactly one year after the announcement for its establishment. In India, in principle approval for National Cyber Coordination Centre (NCCC) was accorded in May 2013 with initial budget allotment of Rs. 800 Crores. On 08 August 2017 the parliament was informed that only Phase-I of NCCC has been made operational. When country has adequate fund and expertise this type of bureaucratic delay is not acceptable for such projects of national security.

R&D in the Field of Cyber Security

We have no choice but to have our own software and hardware in niche technology areas as no country shares these. The Wikileaks and Edward Snowden have already revealed the capability of the USA. As an initial effort, Indian researchers should be tasked to develop same kind of capabilities.

We should take a policy decision to use Indian made switching equipment in our selected critical infrastructure. Indian manufacturers like 'Tejas Networks' should be encouraged. The human resource development policies must be suitably modified to attract the right kind of talent to train and nurture them. In spite of the huge budget the NSA has, NSA is most vulnerable from insider's threat. Manning and Edward Snowden are the prime examples. The most secret cyber weapons developed by the NSA have been put on the internet which can be used by anybody in the world for cyber operations. What is the policy to thwart insider threat in our cyber security organisations?

In September 2015, the Indian government released a draft National Encryption Policy that sought to set encryption standards and lay down conditions for decryption of information for lawful investigation. This was hastily withdrawn under pressure from the media. It is time now to catch the bull by the horn. The national security interests must be supreme.

Armed Forces Domain

The cyber security of the three services of the armed forces are not audited by any outside agencies including NCCIPC. The three services don't even audit each other. Respective services certify themselves as cyber secure. This is not acceptable. Cyber security of the IT network of the three services must be audited by some external agency. In USA professional hackers are called in a big bounty programme and challenged to hack DoD classified networks and award huge prize money. This is how

they find out vulnerabilities in their networks. The Indian Armed Forces must also do something like this.

Within the US Department of Defense, there is an organisation called Defense Information Systems Agency (DISA). DISA provides, operates and assures command and control and information sharing capabilities in direct support to joint war fighters, national level leaders and other missions across the full spectrum of military operations. It works under DoD's Chief Information Officer (CIO). In India, the three services as well as the MoD do not have CIOs. Should we have an organisation like DISA in MoD? We must have CIO organisation in MoD as well as in the three services.

There should be clarity as to what is to be constituted as an act of war in the cyber domain. Factors like loss of life and property, economic impact, diplomatic and political effects can be considered which can be termed as attack of significant consequences. Who will give permission for offensive cyber operations? What are the rules of engagement? India procures huge amount of Defence equipment from foreign countries. What is the mechanism to check whether there is any malware in the increasingly sophisticated technology areas? No country shares the codes. What is the mechanism in the procurement of equipment procedure and supply chain management system to ensure that bugs are not present? The human resource development policies for the Armed Forces in the cyber domain will require drastic changes to attract and keep talents in such niche technology areas. Present policies are inadequate.

Armed Forces must initiate R&D efforts on their specific requirements especially in the battlefield. Can they compromise adversary's classified military network, interfere in the command or data link of the Unmanned Aerial Vehicle (UAV)/ drones, task the Special Forces with appropriate wherewithal to compromise adversary's Optical Fibre Communication (OFC) network? Can we de-anonymise the Darknet. It has been done by the three leading universities of three different countries.

Cyber Capabilities at Operational and Tactical Levels (Corps Headquarters and Below)

What is our policy to provide cyber capabilities at operational and tactical level? In USA, for carrying out sophisticated cyber operations in operational and tactical battlefields where proximity to the target is essential, teams from the most elite and niche technology cyber warfare experts of Tailored Access Operations (TAO) of NSA are embedded with appropriate level in the battlefield. Do our armed forces have similar arrangements with NTRO? We may follow the example of the US Marine Corps and its efforts to get SIGINT and Cyber support from NSA.

Cyber Operations in tactical battle area may include the following:-

- Collect intelligence by rapidly exploiting captured digital media.
- Counter and exploit adversaries' unmanned aerial systems by exploiting data feeds.
- Protect friendly unmanned aerial systems operating in the area of operations.

- Gaining access to closed networks in or near the area of operations, including extracting and injecting data.
- Using electronic warfare systems as "delivery platforms for precision cyber effects".
- Exploiting new devices emerging from new trends and opportunities.
- Conducting cyberspace intelligence, surveillance, and reconnaissance (ISR) operations.
- Engaging in offensive social media operations.

Defence Research and Development Organisation (DRDO)

In the recent past, Defence Research and Development Organisation's (DRDO) mandate has been widened to support national cyber security architecture which includes testing capabilities, security solutions, networking systems and cyber defence tools. In this process, it has also established national infrastructure, enhanced defence industrial capability and developed committed quality human resources. We must make all organisations accountable. We should ask Return on Investment from the DRDO to be verified by the stake holders. In USA, DoD is responsible for protecting <.mil> domain and DHS for <.gov> domain. However, for <.com> network which is used by 85 to 90 percent of all internet users, there is no governmental organisation specially responsible. In India, the armed forces refused to run the <.mil> domain, thereby losing the opportunity to gather valuable experience and expertise in the cyber security field. In India, who is responsible for <.com> domain?

Two leading scientific organisations in the country, Bhaba Atomic Research Centre (BARC) and Indian Space Research Organisation (ISRO), have developed world class indigenous security solutions as they had to undergo international restrictions and strict security requirements. BARC has developed an excellent network security solution called
Secure Network Access System (SNAS). Electronic Corporation of India Limited (ECIL) has been made the designated agency for servicing and maintenance. When there is so much of emphasis on Make in India, even in armed forces classified networks this is not being utilized.

It was expected that for armed forces own classified networks switching equipments from manufacturers like Huawei and ZDNet would be excluded and the armed forces would take a lead. This has not happened and because of L1 syndrome the Chinese manufactured IT equipment are now part and parcel of armed forces classified networks. We need to place special emphasis on building adequate technical capabilities in the following are: Cryptology, Digital signatures, Testing for malware in embedded systems, Operating systems, Fabrication of specialized chips for defence and intelligence functions, Search engines, Artificial intelligence, Routers, SCADA systems, etc.

Conclusion

India must enunciate its cyber strategy for both cyber security and offensive cyber operations. A part may be classified but the relevant aspects must be made known to the

people concerned about their tasks and responsibilities. On cyber related issues projects have to be implemented on fast track and no delay is acceptable. Responsibility and accountability of different agencies must be clearly defined. The huge approximately USD 150 billion IT industry should be made a partner in national cyber security efforts as Government alone cannot do this job. There is no alternative to indigenous cyber security solutions. Snowden revelations have shown what the multinational revered companies do for US Government agency like NSA.

Bibliography

- US Army Field Manuals FM 3- 38 and FM 3-12.

- James Van De Velde, The Fifth Domain Won't be the Sole Battleground, August 30, 2017, available at: https://www.thecipherbrief.com/article/exclusive/tech/fifth-domain-wont-sole-battleground

- Lewis, Patricia, Livingstone, David, "What to Know About Space Security", Chatham House, 27 September 2016 available at: https://www.chathamhouse.org/expert/comment/what-know-about-space-security

- Livingstone, David, Lewis, Patricia, "Space, the Final Frontier for Cybersecurity?", Chatham House, September 2016 available at : https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22- space-final-frontier-cybersecurity-livingstone-lewis.pdf

- Suzuki, Kazuto, "Satellites, the floating targets", The World Today, February & March 2016.

- Madeleine MOON (United Kingdom), NATO Parliamentary Assembly, Defence and Security Committee the Space Domain and Allied Defence Draft Report, Sub-Committee on Future Security and Defence Capabilities, 20 March 2017 available at www.nato-pa.int

- Joint Chief of Staffs, "Cyberspace Operations," US Army Joint Publication 3-12, February 5, 2013, available at : http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

- The Department of Defense Cyber Strategy," The Department of Defense, April 2015, available at : https://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

- Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence, February, 2017 available at : http://www.dtic.mil/get-tr-doc/pdf?AD=AD1028516

- From the website of the Prime Minister of Israel, http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx

- Gabi Siboni and Ido Sivan-Sevilla, Israeli Cyberspace Regulation: A Conceptual Framework, Cyber, Intelligence,and Security, Volume1, No.1, January 2017 available at : http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Israeli%20Cyberspace%20Regulation%20A%20Conceptual%20Framework,.pdf

- Puneet Bhalla, Investments in the space and cyber realm for India's national security, CLAWS Journal, Winter 2016 available at : http://www.claws.in/images/journals_doc/273305959_1742641027_PuneetBhalla.pdf

- Cristin Flynn Goodwin J. Paul Nicholas, Developing a National Strategy for Cybersecurity Foundations for Security, Growth, and Innovation, October 2013.

- Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, Drew Herrick, Tactical Cyber ; Building a Strategy for Cyber Support for Corps and Below, Rand Corporation Report available at :

https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf

- Eric Schmidt and Jared Cohen, The New Digital Age, John Murray, 2013.

- USA, Deportment of Defence Strategy for Operating in Cyberspace, July 2011.

- Resilient Military Systems and the Advanced Cyber Threat, US Department of Defense, Defense Science Board (DSB) Task Force Report January 2013, Page 14.

- CYBERSECURITY National Strategy, Roles and Responsibilities Need to Be Better Defined and More Effectively Implemented United States Government Accountability Office Report to Congressional Addressees February 2013.

- Microsoft, Cyber security: More than a good headline, Oct 2011.
http://www.dhs.gov/organization

- United States Government Accountability Office, Report to Congressional Requesters, Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cyberscurity Efforts, April 2013. GAO-13-275.

- Brig Shantanu Dayal et al, Safeguards Required in the Cyber Domain for Security of India's National Interests, Paper submitted to National Defence College for Nationa Defence College Integrated Analysis Group (IAG) Paper, 2013.

- Government releases National Cyber Security Policy 2013, The Economic Times, PTI Jul 2, 2013.
http://www.nic.in/node/41

- 2011-2012 annual report of the Department of Telecommunications.

- Discussion draft on National Cyber Security Policy 2013, Department of IT Ministry of Communications & IT, dated 02 July 2013.

- Ministry of Communication and Information Technology Department of Electronics and Information Technology Notification on National Cyber Security Policy-2013 (NCSP-2013).

- Institute for Defence Studies & Analysis IDSA Task Force Report on India's Cyber Security Challenges, 2012.

- Maj Gen PK Mallick, VSM, Cyber Security – An Appraisal, Perspectives and Reflections of India's Nation Building Ed Dr Rajendra Prasad, Radha Publication, New Delhi, 2014, PP 333-362

(Maj Gen PK Mallick, VSM(Retd) is an expert in Cyber Warfare, Signal Intelligence and Electronic Warfare)

Images:

- http://www.itsecurityguru.org/wp-content/uploads/2016/11/cybersecurity-professionals-top-complaints.jpg
- http://www.thecyberadvocate.com/wp-content/uploads/2015/03/cybersecurity-rules-linkedin.png

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media fields have come together to generate ideas and stimulate action on national security issues. The defining feature of VIF lies in its provision of core institutional support which enables the organization to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelize fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its establishment, VIF has successfully embarked on quality research and scholarship in an effort to highlight issues in governance and strengthen national security. This is being actualized through numerous activities like seminars, round tables, interactive-dialogues, Vimarsh (public discourse), conferences and briefings. The publications of the VIF form the lasting deliverables of the organisation's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org, Website: http://www.vifindia.org
Follow us on twitter@vifindia